Михаил Райтман

ИСКУССТВО ЛЕГАЛЬНОГО, АНОНИМНОГО И БЕЗОПАСНОГО ДОСТУПА К РЕСУРСАМ ИНТЕРНЕТА



bhv®

Михаил Райтман



ИСКУССТВО ЛЕГАЛЬНОГО, АНОНИМНОГО И БЕЗОПАСНОГО ДОСТУПА К РЕСУРСАМ ИНТЕРНЕТА

Санкт-Петербург
«БХВ-Петербург»
2017

УДК 004.738.5
ББК 32.973.26-018.2
Р12

Райтман М. А.

Р12 Искусство легального, анонимного и безопасного доступа к ресурсам Интернета. — СПб.: БХВ-Петербург, 2017. — 624 е.: ил.

ISBN 978-5-9775-3745-2

Описан ряд приемов защиты персональных данных с помощью шифрования, паролей, многофакторной аутентификации, приватного обмена, бесследного удаления информации и других доступных обычному пользователю средств. Приведены способы конспиративного общения по защищенным каналам связи и подключения к анонимным сетям, таким как Tor, I2P RetroShare и др> Описаны способы получения инвайтов в закрытые сообщества, такие как What.cd, и доступа к таким ресурсам, как Pandora и Hulu. Представлено подробное руководство по операционной системе Tails, обеспечивающей максимальный уровень анонимизации и безопасности. В качестве приложения приведен экскурс в Даркнет — теневую сторону Интернета, а также сведения о «варезной» сцене и демосцене, разновидности компьютерного искусства. Краткий глоссарий в конце книги поможет разобраться в специфических терминах.

Для широкого круга читателей

УДК 004.738.5
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	***Екатерина Кондукова***
Зам. главного редактора	***Евгений Рыбаков***
Зав. редакцией	***Екатерина Капалыгина***
Редактор	***Григорий Добин***
Компьютерная верстка	***Ольги Сергиенко***
Корректор	***Зинаида Дмитриева***
Дизайн обложки	***Марины Дамбиевой***

Подписано в печать 30.09.16.
Формат 70x100 1/16. Печать офсетная. Уел печ. л. 50,31.
Тираж 1200 экз. Заказ № 1541.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3745-2

© Райтман'м. А, 2017
© Оформление, издательство "БХВ-Петербург", 2017

Оглавление

ПРЕДИСЛОВИЕ. Добро пожаловать, мистер Андерсон 1

ЧАСТЬ I. ПОДГОТОВКА К АНОНИМНОЙ РАБОТЕ, РЕШЕНИЕ ВОПРОСОВ БЕЗОПАСНОСТИ 5

Глава 1. Защита персональных данных 7
Обеспечение безопасности данных, хранимых на устройстве 8
Шифрование данных в операционной системе Windows 9
Установка DiskCryptor 10
Использование DiskCryptor для шифрования всего компьютера 10
Шифрование данных в операционной системе OS X 11
Шифрование данных в операционной системе iOS 14
Защита портативных носителей данных 16
Безопасность при использовании сетей Wi-Fi 17
Угрозы, возникающие при подключении к открытой сети Wi-Fi 17
Защита собственной сети Wi-Fi 20
Еще о защите персональных данных 24
Безопасный веб-серфинг 26
Приватные режимы браузеров 26
Использование протокола HTTPS 31
Расширение HTTPS Everywhere 31
Удаление истории посещений и cookie-файлов 32
Браузер Internet Explorer 32
Браузер Microsoft Edge 34
Браузер Mozilla Firefox 35
Браузер Opera 37
Браузер Google Chrome 38
Браузер Safari 40
Мобильные браузеры 41

Глава 2. Надежные пароли и двухфакторная авторизация 43
Выбор надежных паролей 44
О «секретных вопросах» 44

Менеджеры паролей 44
Использование мастер-пароля 45
Использование файла-ключа 46
Комбинация мастер-пароля и файла-ключа 46
Синхронизация паролей между несколькими устройствами 46
Менеджер паролей KeePassX 47
Добавление паролей 48
Использование паролей 49
Дополнительные функции 50
Многофакторная аутентификация и одноразовые пароли 51
Создание второстепенных аккаунтов 53

Глава 3. Фишиговые атаки 54
Признаки фишинговой атаки 54
Защита от фишинговых атак 62
Проверка писем через отправителей 62
Использование облачных хранилищ и файловых хостингов 62
Безопасный просмотр подозрительных документов 62
Анализ отправленных по электронной почте сообщений 63
Аутентификация электронной почты 63

Глава 4. Вредоносные программы и защита от них 64
Виды вредоносных программ 64
Вирусы 64
Черви 65
Троянские программы 66
ArcBomb 66
Backdoor 67
Banker 67
Clicker 67
DoS 67
Downloader 68
Dropper 68
Exploit 68
FakeAV 68
GameThief 69
IM 69
Loader 69
Mailfinder 69
Notifier 69
Proxy 69
PSW 69
Ransom 70
Rootkit 70
SMS 70
Spy 70

Прочие вредные программы....70
Adware....71
Pornware....71
Riskware....72
Киберпреступность....73
Поддержка спамеров....73
Организация сетевых атак....74
Ботнеты....74
Платные вызовы и SMS-сообщения....75
Кража электронных денег....75
Кража банковских данных....75
Кибершантаж....75
Целевые атаки....76
Защита от вредоносных программ....77
Антивирусные программы....79
Онлайн-проверка файлов на вирусы....82
Индикатор взлома....83
Действия при обнаружении вредоносной программы....84

Глава 5. Бесследное удаление данных....85
Удаление файлов в программе BleachBit....86
Интерфейс программы BleachBit....86
Безвозвратное удаление файлов и папок....87
Ограничения программ надежного удаления данных....88
Уничтожение данных с жестких дисков....88
Уничтожение оптических дисков....89
Надежное стирание данных на SSD, Flash-накопителях и SD-картах....90

Глава 6. Вкратце о шифровании....91
Шифрование: три важных понятия....91
Закрытые и открытые ключи....91
Сертификаты безопасности....91
Отпечатки ключей....92
Основы PGP-шифрования:....92
Игра с двумя ключами....93
Электронная подпись....93
Принцип работы PGP....94
Сеть доверия....94
Метаданные: что не может PGP....95
Практическое руководство по PGP-шифрованию....96
PGP в Windows....97
Установка GPG4Win....97
Установка Mozilla Thunderbird....97
Установка Enigmail....99
Использование PGP/MIME....101
Оповещение адресатов об использовании PGP....102
Оповещение людей об использовании PGP по электронной почте....102

Оповещение людей об использовании PGP через веб-сайт ... 103
Загрузка ключей на сервер ключей ... 104
Поиск других пользователей PGP ... 105
Получение открытого ключа по электронной почте ... 105
Получение открытого ключа в виде файла ... 106
Получение открытого ключа с сервера ключей ... 106
Отправка зашифрованных сообщений ... 107
Чтение зашифрованных сообщений ... 109
Отзыв PGP-ключа ... 109
Отзыв PGP-ключа с помощью Enigmail ... 109
Отзыв PGP-ключа с помощью сертификата отзыва ... 109
PGP в OSX ... 110
Установка программы GPGTools ... 110
Создание PGP-ключей ... 111
Создание сертификата отзыва ... 114
Создание резервных копий PGP-ключей ... 114
Отправка зашифрованного/подписанного сообщения в Mail ... 114
Настройка почтового клиента Mozilla Thunderbird ... 115
PGP в Linux ... 119
Установка Thunderbird, GnuPG и Enigmail ... 120
Настройка Thunderbird ... 120
Настройка Enigmail ... 122
Использование PGP/MIME ... 123

Глава 7. Приватный обмен информацией ... 124

Основы безопасного общения ... 124
Принцип работы сквозного шифрования ... 124
Голосовые вызовы ... 125
SMS- и MMS-сообщения ... 125
Мгновенные сообщения ... 126
Электронная почта ... 126
Ограничения сквозного шифрования ... 127
Угрозы безопасности сотовой связи ... 127
Определение местонахождения ... 128
Отслеживание сигнала по вышкам сотовой связи ... 128
Отслеживание сигнала с помощью IMSI-ловушки ... 128
Отслеживание сигнала с помощью Wi-Fi и Bluetooth ... 129
Утечка данных о местонахождении при работе приложений и веб-серфинге ... 130
Выключение телефона ... 130
Одноразовые телефоны ... 131
Спутниковые системы навигации ... 132
Прослушивание сотовой связи ... 132
Заражение телефона вредоносной программой ... 133
Анализ содержимого телефона ... 133
Приватная электронная почта ... 134
Приватное получение/отправка SMS-сообщений ... 136

Приватная голосовая связь 140
Программа Signal 140
Установка и первый запуск 140
Делаем зашифрованный звонок 141
Отправляем зашифрованное сообщение 141
Система Stealthphone 142
Blackphone 2 143
Другие устройства 145
Приватный обмен мгновенными сообщениями 146
qTox 146
ChatSecure 148
Установка и настройка 149
Работа в программе 151
Telegram 152
Поддержка русского языка в Telegram 153
Основы Telegram 155
Секретные чаты 157
Создание секретного чата 158
Самоуничтожение сообщений 159
Удаление аккаунта 159
Pidgin 159
Установка и настройка Pidgin с OTR 160
Установка в Windows 160
Установка в Linux 161
Добавление учетной записи 162
Добавление контакта 163
Настройка модуля OTR 164
Безопасное общение 164
Adium 166
Установка программы 167
Настройка учетной записи 167
Защищенный чат 168
Протокол cMix 171
Другие программы 171

ЧАСТЬ П. ЗАЩИЩЕННЫЕ СПОСОБЫ ПЕРЕДАЧИ ДАННЫХ 173

Глава 8. Использование прокси-серверов 175
Использование альтернативных адресов веб-ресурсов 176
Использование анонимайзеров 180
Настройка браузеров для работы через прокси-серверы 185
Браузер Internet Explorer 185
Браузер Mozilla Firefox 186
Браузер Opera 188
Браузер Google Chrome 189
Браузер Safari 191

Настройка мобильных устройств для работы через прокси-серверы 191
Операционная система iOS 192
Операционная система Windows Phone 193
Сети Wi-Fi 193
Сотовые сети для передачи данных 193
Операционная система Android 194
Сети Wi-Fi 194
Сотовые сети для передачи данных 194
Операционная система Blackberry OS 195
Сети Wi-Fi 195
Сотовые сети для передачи данных 196
Использование цепочек прокси 197
Использование файлов автоконфигурации прокси-сервера 199
Браузер Internet Explorer 199
Браузер Mozilla Firefox 200
Браузер Google Chrome 201
Браузер Opera 202
Браузер Safari 203
Использование файлов автоконфигурации прокси-сервера на мобильных устройствах 204
Операционная система iOS 204
Операционная система Android 205

Глава 9. Виртуальные частные сети 207
Программа Hotspot Shield 208
Универсальное решение ZenMate 211
Настройка VPN-туннелей через протокол SSTP 213
SSH-туннель к серверу Amazon 215
Регистрация учетной записи AWS 215
Создание виртуального сервера 218
Настройка подключения к виртуальному серверу 224

Глава 10. Подмена IP-адресов DNS-серверов 226
Подмена IP-адресов DNS-серверов в операционной системе Windows 228
Подмена IP-адресов DNS-серверов в операционной системе OS X 229
Подмена IP-адресов DNS-серверов в операционной системе iOS 230
Подмена IP-адресов DNS-серверов в операционной системе Android 231
Подмена EP-адресов DNS-серверов на маршрутизаторе Zyxel Keenetic 232

Глава 11. Использование протокола IPv6 234
Основы IPv4, IPv6 и NAT 234
Настройка протокола IPv6/Teredo 237
С помощью BAT-файла 238
Настройка вручную 239
Отключение IPv6/Teredo 244
Использование туннельных брокеров 244
IPv6 через *tunnelbroker.net* 244

Глава 12. Дополнительные способы альтернативной передачи данных 248
Turbo-режимы в браузерах 248
Браузер Opera 248
Яндекс.Браузер 249
Использование систем онлайн-переводов 250
Использование специальных расширений браузеров 251
Подключение к Интернету через мобильные устройства 252
Операционная система Android 253
Операционная система Windows Phone 254
Операционная система iOS 255
Операционная система Blackberry OS 256
Внешние устройства и подключения 257

ЧАСТЬ Ш. АНОНИМНЫЕ СЕТИ: ЗАЩИЩЕННАЯ РАБОТА В ИНТЕРНЕТЕ 259

Глава 13. Основные анонимные сети 261
Основы анонимных сетей 261
Децентрализованные анонимные сети 262
ANts P2P 262
Bitoessage 263
Freenet 265
Gnutella 265
I2P 267
RetroShare 267
Гибридные анонимные сети 267
Cjdns 268
Psiphon 269
Tor 270
Java Anonymous Proxy 270

Глава 14. Freenet: концепция свободной сети 275
Принцип работы 275
Установка и настройка клиента 276
Просмотр фрисайтов 277

Глава 15. I2P: проект невидимого Интернета 278
Принцип работы 279
Чесночная маршрутизация 281
Установка программного обеспечения 282
Настройка браузеров для работы с I2P 285
Браузер Internet Explorer 285
Браузер Mozilla Firefox 286
Браузер Opera 287
Браузер Google Chrome 288
Браузер Apple Safari 290
Проверка работоспособности I2P 291

Глава 16. Платформа RetroShare ... 292
Принцип работы ... 292
Общение в RetroShare ... 293
Обмен файлами в RetroShare ... 294
Установка и настройка клиента RetroShare ... 295
Поиск пиров ... 297
Регистрация в чате ... 301

Глава 17. Tor: луковая маршрутизация ... 304
Луковая маршрутизация ... 305
Принцип работы Tor ... 306
Установка приложения Tor Browser ... 309
Получение доступа к *Pandora,com* с помощью PirateBrowser ... 311

ЧАСТЬ IV. ОБЕСПЕЧЕНИЕ МАКСИМАЛЬНОГО УРОВНЯ АНОНИМНОСТИ И БЕЗОПАСНОСТИ С ПОМОЩЬЮ TAILS ... 317

Глава 18. Основы операционной системы Tails ... 319
Введение в Tails ... 319
Программное обеспечение в составе Tails ... 320
Проблемы безопасности при работе в Tails ... 322
Скомпрометированное аппаратное обеспечение ... 322
Установка и подключение к недоверенным системам ... 322
Модификации BIOS и другого встроенного ПО ... 322
Перехват трафика с выходных узлов Tor ... 323
Обнаружение использования Tor и Tails ... 323
Атаки посредника ... 323
Атаки на опознание трафика ... 325
Следы шифрования документов ... 325
Открытые данные зашифрованных сообщений и метаданные документов ... 325
Системы глобальной слежки ... 326
Двойная жизнь ... 326
Слабые пароли ... 326
Эволюция Tails ... 326
Обеспечение защиты пользователя Tails ... 327
Сокрытие факта использования Tails ... 328
Важные замечания касательно посещаемых сайтов ... 328
Важные замечания касательно провайдеров и сетевых администраторов ... 329

Глава 19. Установка и первый запуск Tails ... 330
Загрузка и проверка образа Tails ... 330
Выбор типа носителя ... 331
Запись Tails на носитель ... 332
Запись Tails на DVD ... 332
Windows 7/8/10 ... 332
Windows 2000 и более ранние версии ... 333
OS X El Capitan и более поздние версии ... 334

OS X Yosemite и более ранние версии ... 334
Linux ... 334
Установка Tails на Flash-накопитель или SD-карту ... 335
Windows ... 335
OS X ... 336
Linux ... 338
Установка Tails с помощью Tails Installer ... 339
Обновление Tails ... 340
Автоматическое обновление с помощью Tails Upgrader ... 341
Обновление вручную с помощью Tails Installer ... 342
Обновление через клонирование ... 342
Обновление из ISO-образа ... 342
Запуск операционной системы Tails ... 343
Параметры загрузки ... 346
Меню загрузки ... 346
Окна Tails Greeter ... 347
Пароль администратора ... 348
Спуфинг MAC-адресов ... 348
Необходимость в смене MAC-адреса ... 349
Прекращение смены MAC-адреса ... 349
Дополнительные сведения ... 350
Настройка сети ... 350
Мосты Tor ... 351
Использование сетевых мостов в Tails ... 351
Использование Tor в странах с цензурой ... 352
Отключение от сети (автономный режим) ... 352
Обзор рабочего стола Tails ... 352
Верхняя навигационная панель ... 353
Обзор приложений ... 355
Запуск терминала суперпользователя ... 356
Рабочий стол ... 356
Зашифрованное хранилище ... 357
Меры безопасности ... 357
Создание зашифрованного хранилища ... 358
Запуск мастера создания зашифрованного хранилища ... 358
Настройки хранилища ... 359
Использование зашифрованного хранилища ... 363
Изменение пароля доступа к зашифрованному хранилищу ... 363
Копирование зашифрованного хранилища на новый носитель ... 365
Создание носителя ... 365
Копирование документов с другого зашифрованного хранилища ... 365
Монтирование текущего хранилища ... 365
Копирование файлов в новое хранилище ... 366
Проверка файловой системы зашифрованного хранилища ... 368
Разблокировка хранилища ... 368
Проверка файловой системы ... 368

Удаление зашифрованного хранилища 369
Безопасное стирание зашифрованного хранилища 369
Решение проблем запуска 369
Завершение работы Tails 370
Безопасное стирание Tails 371
Linux 371
Использование дисковой утилиты 371
Сброс носителя с Tails 372
Windows: использование утилиты Diskpart 372
OS X: использование приложения Дисковая утилита 373

Глава 20. Анонимное подключение к Интернету 375
Подключение к сети 375
Общие положения 375
Регистрация на порталах перехвата 376
Управление Tor с помощью Vidalia 377
Карта сети 378
Смена личности в Vidalia 379
Безопасный веб-серфинг в Tor Browser 379
Упреждающая защита с помощью AppArmor 379
Шифрование передачи данных с помощью HTTPS 380
Дополнение HTTPS Everywhere 381
Torbutton 381
Защита от вредоносного кода JavaScript 381
Изменение уровня безопасности 382
Смена личности в Tor 382
Дополнение NoScript для управления сценариями JavaScript 383
Анонимное общение в мессенджере Pidgin 383
Предустановленные учетные записи 384
Протокол шифрования OTR 384
Блокировка Tor IRC-серверами 384
Генерация имени пользователя 384
Поддержка других протоколов 385
Защищенная электронная почта Icedove (Thunderbird) 385
Настройка учетной записи 385
OpenPGP-шифрование с помощью Enigmail 386
Обеспечение дополнительной защиты с помощью TorBirdy 387
Обмен биткоинов в Electrum 387
Использование сети I2P 387
Причины низкой скорости передачи данных в Tor 388
Сложные схемы передачи данных 388
Качество ретрансляторов 389
Злоупотребление сетью Tor 389

Глава 21. Шифрование и конфиденциальность 390
Доступ к жесткому диску компьютера 390
Виртуальная клавиатура 391

Зашифрованные разделы ... 391
Создание зашифрованных разделов ... 392
Определение внешнего носителя ... 392
Форматирование носителя ... 392
Создание зашифрованного раздела ... 392
Использование созданного раздела ... 395
Доступ к ранее созданным зашифрованным разделам ... 395
Шифрование текста с помощью OpenPGP ... 396
Шифрование сообщения с помощью пароля ... 396
Шифрование и подпись сообщения с помощью открытого ключа ... 398
Расшифровка и проверка сообщения ... 400
Надежное удаление данных ... 401
Бесследное удаление файлов ... 403
Затирание свободного места ... 404
Управление паролями с помощью KeePassX ... 405
Создание и сохранение базы паролей ... 405
Разблокировка базы данных в новом сеансе работы ... 406
Использование KeePassX для подстановки паролей ... 407
Вычисление контрольных сумм с помощью GtkHash ... 408
Предотвращение атак методом холодной перезагрузки ... 409

Глава 22. Работа с файлами в Tails ... 410
Работа с документами ... 410
Просмотр и редактирование графических файлов ... 412
Управление мультимедийными данными ... 415
Печать и сканирование ... 418

Глава 23. Дополнительные возможности работы с Tails ... 420
Установка дополнительного программного обеспечения ... 420
Запуск Tails в виртуальной машине ... 422
Обеспечение безопасности ... 422
Приложения виртуализации ... 422
VirtualBox ... 423
Установка VirtualBox ... 423
Запуск Tails из ISO-образа ... 423
VMware Workstation Player ... 425
Установка VMware Workstation Player ... 425
Запуск Tails из ISO-образа ... 426
Боксы ... 429
Установка программы ... 429
Запуск Tails из ISO-образа ... 429
Общий буфер обмена ... 430
Менеджер виртуальных машин ... 431
Установка программы ... 432
Запуск Tails из ISO-образа ... 432
Запуск Tails с USB- или SD-носителя ... 434

Ресурсы в локальной сети 435
Обеспечение безопасности при работе в локальной сети 436
Веб-серфинг в локальной сети 436
Скачивание файлов с локального веб-сайта 436
Скачивание файлов с локального FTP-сервера 436
Подключение беспроводных устройств 436
Некоторые известные проблемы и пути их решения 438
Проблемы с запуском Tails 438
Проблемные Flash-накопители 438
Проблемные компьютеры 438
Компьютеры Mac 439
Компьютеры с переключаемыми графическими картами 439
Архитектура ARM, Raspberry Pi и планшеты 440
Передача Tails другому загрузчику 440
Проблемы с Wi-Fi 440
Интерфейс Broadcom Wi-Fi 440
Интерфейс Broadcom BCM43224 802.1 a/b/g/n 441
Проблемы безопасности 441
Tails не стирает содержимое памяти после завершения работы 441
Tails не стирает содержимое видеопамяти 441
Не работает экстренное завершение работы 441
Ошибка выброса DVD с Tails 441
Не выполняется полная перезагрузка/выключение Tails 441
Прочие проблемы 442
Контент в формате Adobe Flash не отображается 442
Пользовательские настройки системы не сохраняются 443
Утерян пароль для доступа к зашифрованному хранилищу 443
Скачивание файлов по протоколу BitTorrent 443
Скачивание видеофайлов из Интернета 443
Сложности обмена файлами в браузере I2P 443
Проблемы отображения меню загрузки 444
Bluetooth-устройства не работают 444
Сбой применения раскладки клавиатуры 444
Tails не загружается после обновления 444
Сбой предварительного просмотра печати в Tor Browser 444
Замедление графики на некоторых картах NVidia 444

ПРИЛОЖЕНИЯ 445

Приложение 1. Даркнет: подполье Интернета 447
Глубинная Паутина и Даркнет 447
Доступ к Даркнету 448
Анонимная мобильность 448
Аудитория Даркнета 449
Черные рынки Даркнета 451
Криптовалюты 453
Реакция властей на Даркнет 454
Заключение 454

Приложение 2. Варез и Сцена ... 456
Варез: киберпиратство ... 456
История киберпиратства ... 458
Причины, повлиявшие на рост пиратства ... 458
Распространение через скомпрометированные FTP-серверы ... 459
Автоматизированное распространение вареза с помощью IRC-ботов ... 460
Разновидности вареза ... 460
Пиратство в сфере киноиндустрии ... 462
Обозначения варезных файлов ... 463
Формат ... 463
Архивация ... 464
Имена файлов ... 464
Сопроводительные файлы релизов ... 464
Файл *FILE_ID.DIZ* ... 464
NFO-файлы ... 465
SFV-файл ... 467
Прочие файлы ... 467
Последствия нарушения стандартов ... 468
Аудио- и видеорелизы ... 468
Типы видеорелизов ... 468
Типы аудиорелизов ... 474
Релизы программного обеспечения ... 475
Инструменты обхода защиты программ от нелегального копирования ... 476
Преследование по закону ... 479
Опасности, связанные с использованием вареза ... 479
Варезные сайты ... 482
Форумы, где ссылки лежат ... 485
FTP- и HTTP-архивы ... 486
Электронные библиотеки ... 488
Сцена: андеграунд Всемирной паутины ... 490
Развитие Сцены ... 491
Создание релизов ... 492
«Нюки» релизов ... 492
Взлом и обратная разработка ... 494
Топ-сайты ... 494
Система кредитов ... 494
Варезные группы ... 495
Курьеры ... 495
Релизные группы ... 495
aPOCALYPSE PRODUCTION cREW (aPC) ... 496
Challenge Of Reverse Engineering (CORE) ... 496
Centropy ... 497
CLASS (CLS) ... 497
DEViANCE ... 498
DrinkOrDie ... 498
Echelon ... 500
FairLight ... 500

HYBRID 501
International Network of Crackers (INC) 501
Kalisto 501
LineZerO (LzO) 502
Myth 502
PARADOX (PDX) 503
Rabid Neurosis (RNS) 504
Radium 504
Razor 1911 (RZR) 504
RELOADED (RLD) 505
RiSCiSO 506
SKIDROW 506
Superior Art Creations (SAC) 506
The Humble Guys (THG) 508
Tristar and Red Sector Incorporated (TRSI) 509
United Software Association (USA) 510
Несколько слов в заключение раздела 510

Приложение 3. Компьютерное искусство 512
Искусство ASCII-Art 512
Трекерная музыка 514
Интро, демо и крэктро 517

Приложение 4. Получение инвайтов на закрытые сайты (на примере *What.cd*) 520

Приложение 5. Краткий глоссарий терминов пользователя 525

Источники 587

Предметный указатель 589

ПРЕДИСЛОВИЕ

Добро пожаловать, мистер Андерсон

Догадываюсь, сейчас ты чувствуешь себя Алисой, падающей в кроличью нору..

Морфеус, фильм «Матрица»

ВНИМАНИЕ!

Эта книга не является руководством по взлому или доступу к запрещенным ресурсам — все приведенные здесь сведения носят исключительно информативный характер и взяты из открытых и не заблокированных источников!

Автор не несет ответственности за последствия посещения вами упомянутых в книге веб-сайтов, если к моменту выхода книги из типографии некоторые из них окажутся заблокированы согласно законодательству вашей страны.

Необходимо отказаться от посещения заблокированных сайтов и попыток получения доступа к заблокированным сайтам/контенту, если это противоречит законодательству вашей страны.

Эта книга посвящена обеспечению безопасной и анонимной работы во Всемирной паутине. Прочитав ее, вы научитесь защищать свои устройства и данные при посещении веб-узлов, а также обеспечивать конфиденциальность при общении в Интернете. Вы узнаете об анонимных сетях, о существовании которых могли и не догадываться, посещая Всемирную паутину. Привычный для вас мир Всемирной паутины можно представить «матрицей», в которой обитает львиная доля всех пользователей Интернета, но под ней скрывается «Зион», и вы будете поражены, увидев, какие формы жизни в нем существуют. А если по каким-либо причинам вам нужно обеспечить высший уровень приватности при работе на компьютере, причем без привязки к устройству (другими словами, анонимно работать на *любом* компьютере), соответствующий раздел книги посвятит вас в тайны Tails — сверхзащщенной портативной версии операционной системы на основе Linux, которой в 2013 году Эдвард Сноуден пользовался для связи со средствами массовой информации, передавая им секретные данные АНБ. В заключительном разделе книги собраны приложения, содержащие занимательные сведения о Даркнете, варезной Сцене, компьютерном искусстве, а также о терминологии современного интернет-пользователя.

Далее чуть подробнее представлено содержание каждой части книги:

- *часть I* посвящена подготовке к анонимной работе и решению вопросов безопасности. Из *главы 1* вы узнаете об угрозах, исходящих от киберпреступников, а также о том, как обезопасить свой компьютер и соединение Wi-Fi, вы научитесь защищать персональные данные, использовать приватные режимы браузеров и защищенный протокол HTTPS.

В *главе 2* рассказывается о важности использования надежных паролей и о двухфакторной авторизации. *Главы 3 и 4* рассматривают угрозы фишинга и вредоносных программ, а также способы защиты от них. *Глава 5* научит вас бесследно уничтожать файлы. Прочитав *главу 6,* вы познакомитесь с основами шифрования и освоите PGP-шифрование. А *глава 7* раскроет вам сведения о способах приватного обмена электронной почтой, SMS и мгновенными сообщениями, в частности, через приложения Telegram, Pidgin и Tox;

- главы *части II* научат вас получать доступ к американским сайтам, таким как **Hulu.com** и **Pandora.com.** Здесь рассматриваются различные способы получения такого доступа — от простых, наподобие использования онлайн-переводчиков, до продвинутых, основанных, к примеру, на построении SSH-туннеля к виртуальному серверу Amazon;
- материал *части III* позволит вам освоиться в анонимных сетях, незнакомых обывателям. Начав с обзора сетей в *главе 13,* вы изучите такие сети, как Freenet *{глава 14),* I2P *{глава 15),* RetroShare *{глава 16)* и Tor *{глава 17*);
- в *части IV* рассматривается уже упомянутая ранее сверхзащшценная сборка Linux под названием Tails, которую можно установить на любой DVD-, Flash- или SD-накопитель и анонимно использовать на *любом* компьютере. *Главы* с *18-й* по *23-ю* проведут вас через все тонкости работы с этой системой, которой в свое время пользовался Эдвард Сноуден;
- *часть V* включает глоссарий интернет-серфера, а также приложения, содержащие обзор теневой стороны Всемирной паутины — Даркнета, которые помогут вам совершить путешествие в мир вареза и компьютерного искусства.

И это только малая часть того, что вы сможете узнать, прочитав книгу. Кроме нее, вам понадобятся:

- настольный компьютер или ноутбук с установленной операционной системой Windows, Linux или OS X любой версии и доступом в Интернет;
- браузер Mozilla Firefox, Google Chrome или любой другой. Можно пользоваться и браузерами Internet Explorer последних версий или Edge.

> ***АНОНИМНОСТЬ В ИНТЕРНЕТЕ***
>
> **При необходимости сохранять анонимность, безопаснее использовать собственный браузер сети Tor (о ней будет подробно рассказано далее).**

Обязательно следует установить антивирусное программное обеспечение. Скорее всего, вы уже пользуетесь каким-либо антивирусным сканером — например, встроенным в Windows 7/8/10 Защитником Windows (Windows Defender). Функции защиты последнего оставляют желать лучшего, поэтому осмелюсь порекомендовать вам какую-либо из версий антивируса Касперского: Kaspersky Anti-Virus, Kaspersky Internet Security или Kaspersky Total Security, доступных для загрузки по адресу **tinyurl.com/nk67qmy,** — они стоят своих денег. Если же пара тысяч рублей в год вам не по карману, подойдет, к примеру, и программа Kaspersky FREE, загрузить которую можно по адресу **tinyurl.com/gwndx98,** — она бесплатна, имеет русский интерфейс и обеспечивает базовую защиту от вредоносных программ.

> ***СОКРАЩЕННЫЙ ВИД ССЫЛОК***
>
> **Для удобства — чтобы вам не приходилось набирать длинные адреса — все ссылки в книге приведены к сокращенному виду с помощью сайта tlnyurl.com.**

Дополнительно вам могут потребоваться следующие специализированные программы:

- Tor — клиент сети виртуальных туннелей, который позволит вам повысить уровень анонимности и безопасности во Всемирной паутине. По адресу **tinyurl.com/3ty5dkk** доступны для загрузки его версии как для Windows, так и для OS X и Linux. На тот случай, когда Tor может не справиться, я посоветую вам другое аналогичное программное обеспечение;
- **Tails** — дистрибутив этой операционной системы может быть загружен по ссылке **tinyurl.com/7nlfa31;**
- **прочие программные средства** — сюда входят различные клиенты анонимных сетей, а также специализированные утилиты. Обзоры таких программ и ссылки на них будут приводиться по мере необходимости.

На первый взгляд — все. Поехали!

ЧАСТЬ I

Подготовка к анонимной работе, решение вопросов безопасности

Глава 1.	**Защита персональных данных**
Глава 2.	**Надежные пароли и двухфакторная авторизация**
Глава 3.	**Фишинговые атаки**
Глава 4.	**Вредоносные программы и защита от них**
Глава 5.	**Бесследное удаление данных**
Глава 6.	**Вкратце о шифровании**
Глава 7.	**Приватный обмен информацией**

Часть I книги посвящена решению вопросов безопасности, неизбежно возникающих у *каждого* пользователя Интернета. С ростом количества устройств, подключенных к Интернету, растет и число злоумышленников, желающих так или иначе нам навредить. Они преследуют разные цели: одни имеют лишь корыстные намерения (к примеру, похищение персональных данных, особенно часто банковских, или же блокировку компьютера с запросом выкупа), другие — по тем или иным причинам хотят парализовать работу корпоративной сети или испортить файлы документов, третьи вообще балуются, пробуя стабильность систем «на зуб». Объектами их интересов становятся не только настольные компьютеры или ноутбуки, но и мобильные устройства, такие как планшеты и смартфоны. А благодаря развитию концепции Интернета вещей, в недалеком будущем та же участь ждет и смарт-телевизоры, и прочую домашнюю технику, имеющую подключение к Интернету. Так или иначе, прежде чем в полной мере посещать интернет-ресурсы, а тем более гораздо менее безопасные узлы в анонимных сетях, рекомендуется озаботиться решением вопросов защиты персональных данных и самого устройства, с которого вы выходите в Сеть.

ГЛАВА 1

Защита персональных данных

Обеспечение безопасности данных, хранимых на устройстве

Защита портативных носителей данных

Безопасность при использовании сетей Wi-Fi

Еще о защите персональных данных

Безопасный веб-серфинг

Первое, о чем следует задуматься, посещая веб-узлы (не только расположенные в анонимных сетях, но и самые обычные сайты Всемирной паутины), — это обеспечение защиты своих персональных данных. В защите нуждаются как реквизиты банковских карт (которые могут быть похищены и использованы для создания дубликатов карт и съема наличных с вашего счета), так и личные данные (к примеру, ФИО могут быть использованы при составлении фиктивных договоров, а номера телефонов — для отъема денег путем т. н. *преступного «пранка»,* когда звонящий представляется родственником, попавшим в Трудную ситуацию, для решения которой требуются деньги).

Во избежание подобных ситуаций крайне не рекомендуется указывать свои персональные данные на любых сайтах, в том числе и в социальных сетях. В исключительных случаях указание персональных данных может быть допустимо на подтвержденных сайтах, доступ к которым осуществляется через защищенный протокол HTTPS[1] (в таких случаях в начале интернет-адреса сайта вместо префикса **http** используется **https),** хотя и это не обеспечивает должного уровня защиты. А любые банковские транзакции должны подтверждаться с помощью SMS или голосовой связи. Кроме того, вам ничего не мешает сделать заказ в интернет-магазине по телефону, а не заполняя форму на сайте, и оплатить его наличными, а не банковской картой. А если уже и оплачивать товары и услуги через Интернет, то использовать надежные пароли и, по возможности, двухфакторную авторизацию, а в качестве платежного инструмента задействовать надежного посредника, — например, систему PayPal.

Итак, основное правило: **никаких персональных данных в Интернете!** Согласно отчету компании «Лаборатория Касперского» **(tinyurl.com/jlghumo),** свыше 20% россиян несколько раз становились жертвами кражи персональных данных или махинаций с банковскими картами, что почти на треть выше, чем в целом в мире. Это говорит о том, что наши пользователи не слишком задумываются о безопасности персональных данных.

1 *HTTPS* — **HyperText Transfer Protocol Secure, безопасный протокол передачи гипертекста.**

Далее мы рассмотрим основные способы обеспечения безопасности при работе на компьютере или другом устройстве — таком, как смартфон или планшет.

Обеспечение безопасности данных, хранимых на устройстве

Многие из пользователей хранят все данные, включая конфиденциальную информацию, не только собственную, но и других людей (контакты, переписку, документы), на ноутбуках, планшетах и даже смартфонах, забывая, что не так уж сложно украсть смартфон (ноутбук) или быстро скопировать с него данные.

Усложнить доступ к секретной информации злоумышленнику, который способен добраться до нее физически, позволяет *шифрование.* Компьютер, планшет или смартфон нетрудно блокировать паролем, PIN-кодом или защитой с помощью жеста. Увы, эта блокировка не поможет уберечь данные при потере устройства. Да и обойти подобную блокировку легко — ведь данные хранятся на устройстве в открытом виде. И все, что нужно сделать злоумышленнику, — это подключиться к носителю данных (т. е. к жесткому диску компьютера или памяти мобильного устройства) напрямую. Тогда он сумеет просмотреть и скопировать оттуда информацию без знания пароля. Если же вы используете шифрование, злоумышленнику недостаточно получить доступ к устройству, — для расшифровки данных ему понадобится ваш пароль, а обойти хорошую парольную защиту практически невозможно.

Оптимальный способ — зашифровать не отдельные папки, а все данные на устройстве. Большинство компьютеров и мобильных устройств поддерживают полное шифрование. В устройствах под управлением операционной системы Android вы найдете эти настройки в разделе **Безопасность** (Security), а в устройствах компании Apple (например, в iPhone или iPad) в разделе Пароль (Password) — режим шифрования данных автоматически включается при активации блокировки паролем. В домашних версиях Windows для шифрования можно использовать приложения наподобие DiskCryptor (см. далее *разд. «Шифрование данных в операционной системе Windows»).* В операционную систему компьютеров Mac аналогичная функция встроена и называется FileVault (см. далее *разд. «Шифрование данных в операционной системе OS X»).* В дистрибутивах Linux полное шифрование диска, как правило, предлагается при установке операционной системы.

Впрочем, какое бы приложение ни использовалось, шифрование надежно настолько, насколько надежен ваш пароль. Если устройство попадет в руки злоумышленнику, у того будет неограниченное количество времени для подбора пароля. Специальные программы позволяют подбирать пароли со скоростью миллионов операций в секунду, поэтому действительно надежный пароль должен содержать более пятнадцати символов.

Обеспечение безопасности может оказаться непростой задачей. Как минимум, вам надо будет сменить пароли, изменить привычки и, возможно, заменить программы на своем основном компьютере (или мобильном устройстве). В сложном случае вам придется постоянно оценивать вероятность утечки конфиденциальных данных и адекватность защитных мер. Но даже если вы полностью осознаете проблему, некоторые решения могут оказаться вне вашей власти. Например, вы объясняете коллегам потенциальные угрозы, а они по-прежнему используют небезопасные способы общения и навязывают их вам. Такой человек присылает вам письмо с файлом-вложением и уверен, что вы его откроете и прочтете, как это было всегда. Отправитель не принимает при этом во внимание риск, что злоумышленник может выдать себя за него и прислать вам вирус. А если ваш основной компьютер уже заражен?

Большинству пользователей также не понравится идея запоминать и вводить на мобильном устройстве сложные парольные фразы. Поэтому, чтобы обеспечить одновременно и удобство работы, и физическую сохранность, и недосягаемость для злоумышленников действительно конфиденциальной информации, можно ограничить работу с ней одним компьютером, более безопасным, чем все остальные ваши устройства.

Используйте этот компьютер лишь изредка. Работая с ним, уделяйте особое внимание своим действиям. Если нужно открыть вложение или запустить небезопасную программу, сделайте это на другом компьютере.

Для создания безопасного компьютера можно выполнить следующие рекомендации:

- разместите устройство в *физически* более безопасном месте — там, где вы сможете быстро определить вероятность несанкционированного доступа (например, в закрытом кабинете);
- установите на него операционную систему, разработанную специально для обеспечения конфиденциальности и безопасности, — например, Tails (см. *часть IV).* Возможно, эта операционная система не устроит вас в повседневной работе. Но если вам нужен инструмент, чтобы только получать, хранить, создавать и отправлять конфиденциальные сообщения, Tails отлично справится с этими задачами и обеспечит высокий уровень безопасности.

Выделенный безопасный компьютер — не столь уж и дорогая вещь, как может показаться. Устройство, на котором запущено лишь несколько программ, не обязано быть высокопроизводительным или новым, и для использования в этом качестве вы можете задействовать (или приобрести) бывший в употреблении компьютер или ноутбук.

На безопасном компьютере можно хранить основную копию конфиденциальных данных. Но не следует забывать и о недостатках этого решения. Если вы станете записывать на такой компьютер всю самую ценную информацию, он может стать очевидной целью злоумышленников. Поэтому не афишируйте его наличие, не обсуждайте ни с кем его местонахождение и обязательно зашифруйте жесткий диск. И используйте надежный пароль, чтобы в случае кражи устройства нельзя было прочитать записанные на нем данные.

Есть и еще один риск — опасность того, что уничтожение безопасного компьютера приведет к потере единственной копии данных. На этот случай сделайте их копию, зашифруйте и храните в другом месте.

Единственный способ добиться наилучшей защиты устройства с конфиденциальными данными от интернет-угроз, — полностью отключить такой компьютер от Интернета. Убедитесь также, что безопасный компьютер никогда не подключается к локальной сети или сети Wi-Fi, а данные копируются только на физические носители наподобие DVD и Flash-дисков. Если все же ваш безопасный компьютер подключен к Интернету, не рекомендуется использовать на нем привычные аккаунты, — создайте себе новые учетные записи электронной почты и веб-сервисов, используйте сеть Tor, чтобы не раскрывать реальный IP-адрес компьютера. Так вы сможете скрыть связь между вами и этим компьютером на случай, если злоумышленник захочет украсть ваши данные. Аналогичную тактику можно применить и к мобильным телефонам.

Шифрование данных в операционной системе Windows

Целиком зашифровать диск позволяет программа с открытым исходным кодом DiskCryptor. Далее вы узнаете, как установить ее на компьютер под управлением Windows.

ПРОБЛЕМЫ С ШИФРОВАНИЕМ НА КОМПЬЮТЕРАХ С UEFI-ЗАГРУЗКОЙ

Важно учитывать возможные проблемы при шифровании загрузочных/системных разделов на компьютерах с UEFI-загрузкой. Для получения дополнительной информации посетите сайт diskcryptor.net.

Установка DiskCryptor

1. Для загрузки программы DiskCryptor зайдите на страницу по адресу **diskcryptor.net/wiki/Downloads,** щелкните мышью на ссылке **installer** и сохраните файл на компьютер.
2. Установите программу, запустив загруженный файл. В некоторых случаях его понадобится запустить с правами администратора (щелкнув на файле правой кнопкой мыши и выбрав пункт Запуск с правами администратора (Run as administrator) из контекстного меню).
3. Перезагрузите компьютер, чтобы завершить установку. Без перезагрузки вы не сможете начать работу с программой.

Использование DiskCryptor для шифрования всего компьютера

Если зашифровать все содержимое диска компьютера, можно серьезно затруднить жизнь злоумышленнику, который вознамерился получить доступ к вашим файлам (при условии,

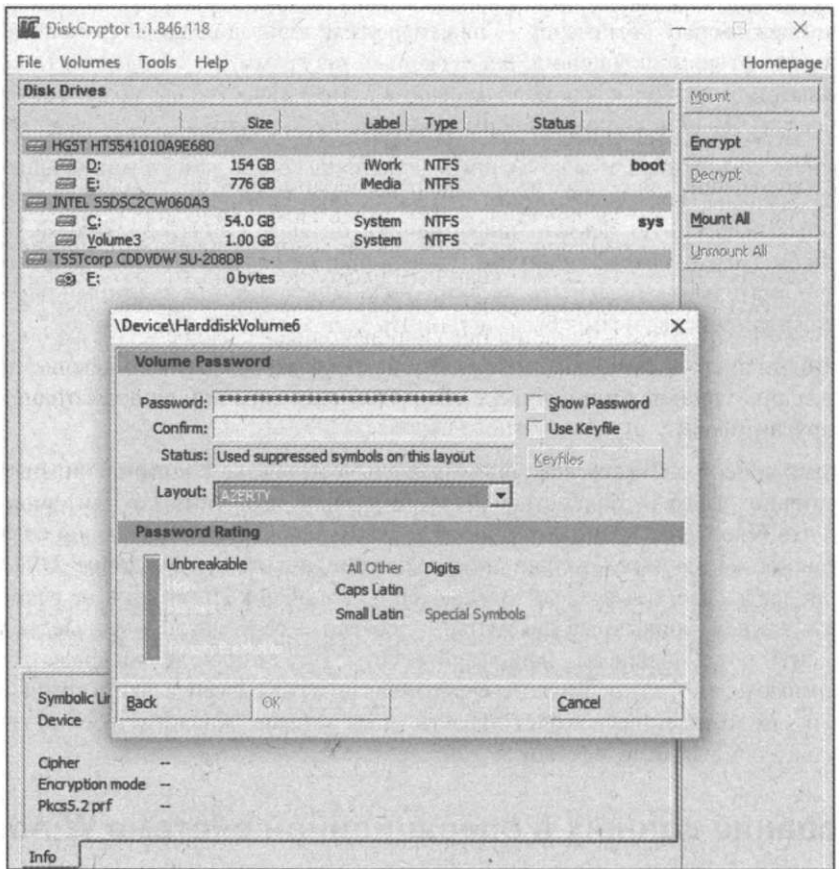


Рис. 1.1. Подготовка диска к шифрованию в программе DiskCryptor

что компьютер похищен в выключенном состоянии), — злоумышленник не сможет даже узнать, какие файлы хранятся на компьютере. Чтобы зашифровать содержимое жесткого диска, выполните следующие действия:

1. Запустите программу DiskCryptor.
2. В списке **Disk Drives** (Диски) выберите нужный диск (например, C:) и нажмите кнопку **Encrypt** (Шифровать) в правой части окна программы.
3. Примите установки по умолчанию — нажмите кнопку **Next** (Далее), затем еще раз нажмите **Next** (Далее).
4. Выбрав надежный пароль, введите его в поля **Password** (Пароль) и **Confirm** (Подтверждение), а затем нажмите кнопку OK (рис. 1.1).
5. Процесс шифрования может занять некоторое время, и когда он завершится (индикатор в нижней части окна исчезнет), перезагрузите компьютер.

Теперь содержимое жесткого диска вашего компьютера зашифровано. Для расшифровки диска следует вновь запустить программу DiskCryptor, выбрать зашифрованный диск в списке **Disk Drives** (Диски) и нажать кнопку **Decrypt** (Расшифровать).

Учитывайте, что злоумышленник или вредоносная программа могут обойти вашу шифровальную защиту, если дождутся, когда вы загрузитесь и введете пароль. Ваши данные защищены, только когда компьютер выключен. Если злоумышленник получит доступ к компьютеру во включенном состоянии, в спящем режиме или даже в режиме гибернации, он сможет добраться до ваших данных.

Шифрование данных в операционной системе OS X

Дополнительную защиту персональных данных в операционной системе OS X обеспечивает функция FileVault. Суть ее заключается в том, что в автоматическом режиме шифруются с использованием надежного алгоритма все объекты, которые вы храните на жестком диске своего компьютера. Это означает, что если вы никому не сообщите свой пароль для входа в систему, прочесть ваши файлы не сможет никто, кроме вас и суперпользователя (главного администратора компьютера). Функция FileVault выполняет свою работу в фоновом режиме и не требует большого количества системных ресурсов. Шифрование особенно пригодится владельцам ноутбуков — в этом случае, если им завладеет кто-либо чужой, то он не сможет просмотреть ваши файлы, не зная нужного пароля.

Действия функции FileVault связаны с некоторыми моментами, о которых вам нужно знать:

- функция активна, пока вы не авторизованы в системе. Как только вы авторизуетесь, ваши файлы станут доступными и уже не будут столь надежно защищены. Поэтому не следует оставлять компьютер без присмотра — блокируйте его, если требуется отойти;
- к вашим защищенным данным имеет доступ root-администратор. В операционной системе OS X у него практически неограниченные права, и с помощью мастер-пароля он легко обойдет защиту функции FileVault;
- существует возможность, что другие пользователи смогут удалить ваши зашифрованные файлы, несмотря на то, что функция FileVault будет включена. В ее обязанности входит только шифрование данных, а не защита их от удаления;
- функция FileVault подчиняется тому, кто введет соответствующий пароль, поэтому, если кто-либо узнает ваш пароль авторизации, он сможет обойти защиту функции;
- если вы единственный пользователь и, следовательно, администратор в системе, то должны помнить свой пароль авторизации и мастер-пароль. Если вы не сможете автори-

зоваться в системе, останется только попрощаться со своими данными, очистить жесткий диск и начать все сначала;

- чтобы использовать функцию File Vault, нужно создать раздел восстановления на загрузочном диске, куда устанавливается система OS X, а не на внешнем накопителе. Если в процессе установки системы OS X вы не создадите раздел восстановления, то не сможете воспользоваться преимуществами функции File Vault.

Чтобы задействовать функцию FileVault, выполните следующие шаги:

1. Авторизуйтесь в системе с учетной записью администратора.
2. Выполните команду меню | **Системные настройки** , | System Preference) и в открывшемся окне щелкните мышью на значке о **Защита и Безопасность** (Security & Privacy).
3. Перейдите на вкладку **FileVault** открывшегося окна.

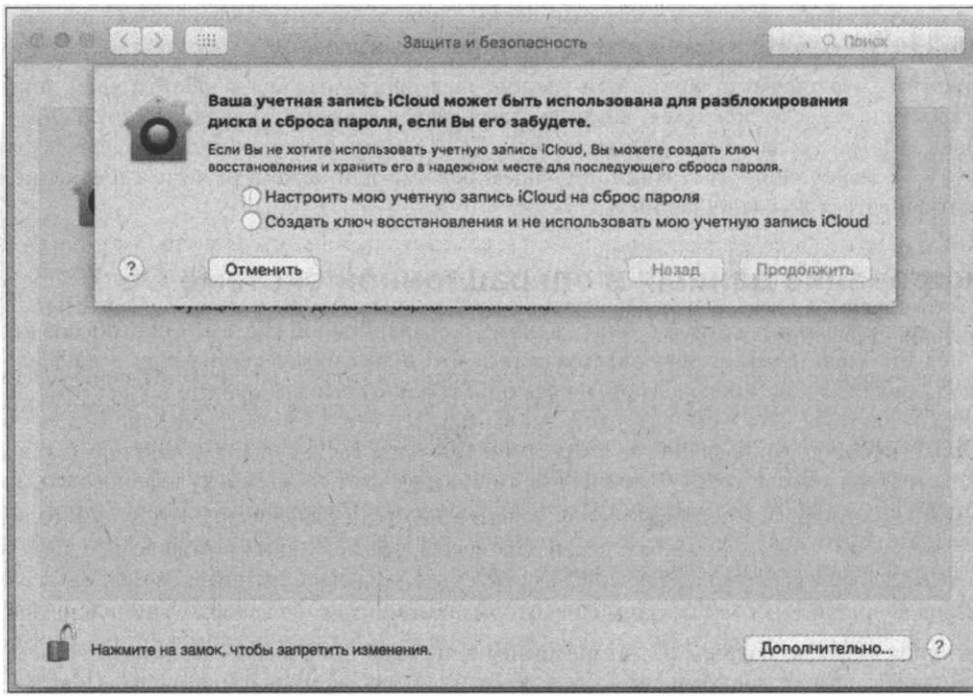


Рис. 1.2. Панель выбора настроек сброса пароля

4. Щелкните мышью на значке и введите имя и пароль администратора, чтобы система разрешила вам настроить необходимые параметры.
5. Нажмите кнопку **Включить FileVault** (Turn On FileVault) — появится панель, на которой вам нужно выбрать, следует ли использовать учетную запись iCloud для восстановления пароля, если вы его забудете (рис. 1.2).

   Для большей безопасности учетную запись iCloud подключать не рекомендуется, т. к. злоумышленник может получить к ней доступ и сбросить пароль без вашего ведома.
6. Выберите вариант создания ключа восстановления и нажмите кнопку **Продолжить** (Continue) — откроется панель с ключом восстановления, который следует использовать

в том случае, если вы (или другой пользователь с правами отключения защиты) забудете пароль к своей учетной записи. Этот ключ позволит отключить защиту, войти в систему и восстановить забытый пароль пользователя (рис. 1.3).

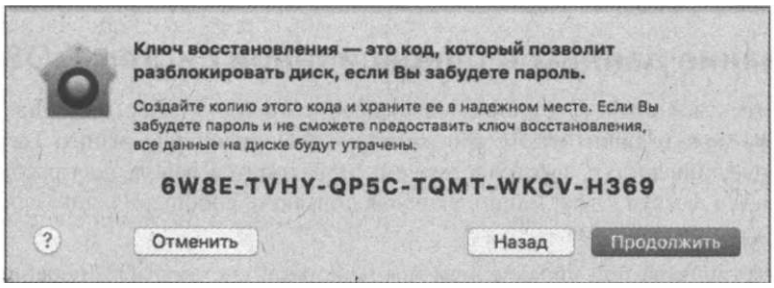


Рис. 1.3. Панель с ключом восстановления

Обязательно сохраните ключ восстановления, т. к. без него вы не сможете войти в систему, если забудете пароль администратора. Ключ восстановления следует сохранить на внешнем носителе, распечатать или записать и убрать в надежное место. Хранить его на диске защищаемого компьютера не имеет смысла, т. к. если вы забудете пароль на вход в систему, то соответственно не сможете добраться и до ключа.

7. Сохранив у себя ключ восстановления, нажмите кнопку **Продолжить** (Continue).
8. Когда система предложит перезагрузить компьютер, нажмите кнопку **Перезагрузить** (Restart). После перезагрузки появится экран входа, введите свой пароль на вход. Система отобразит процесс загрузки, показав вращающиеся шестеренки. Это означает, что функция FileVault включена.
9. Чтобы на компьютере мог работать пользователь, у которого нет прав отключения защиты, войдите в систему под своей учетной записью, а затем выполните команду меню | **Завершить сеанс (***имя пользователя)* (| Log Out *(user name))* и запустите учетную запись пользователя, которому вы собираетесь предоставить свой компьютер.

Учитывайте, что при первом включении функции FileVault шифрование содержимого жесткого диска может занять несколько часов. Процесс будет проходить в фоновом режиме и не потребует много системных ресурсов, поэтому во время первого шифрования вы можете работать в обычном режиме. Несмотря на то, что при первом шифровании допускается переход в спящий режим, выход из системы и даже выключение компьютера, стоит подождать, пока функция закончит свою работу, чтобы гарантированно обезопасить все свои данные.

Если по какой-либо причине вам потребуется выключить функцию FileVault, выполните команду меню | **Системные настройки** | System Preference), щелкните мышью на значке **Защита и Безопасность** (Security & Privacy), перейдите на вкладку **FileVault** и нажмите кнопку **Отключить FileVault** (Turn Off FileVault). После того как вы введете главный пароль и нажмете кнопку OK, система приостановит работу функции FileVault и начнется дешифровка диска.

Чаще всего выключение функции FileVault связано с необходимостью изменить ключ восстановления. Чтобы сделать это, по окончании дешифровки следует нажать кнопку **Включить FileVault** (Turn On FileVault), указать пользователей, которые могут самостоятельно разблокировать жесткий диск, после чего система создаст новый ключ восстановления и

предложит отправить его на сервер компании Apple. Теперь никто не сможет использовать прежний ключ для разблокирования заново зашифрованного диска. А при запросе восстановления компания Apple предоставит только новый ключ на основании серийного номера и номера записи, который вы отправите в запросе.

Шифрование данных в операционной системе iOS

Если пользуетесь мобильным устройством компании Apple — таким, как iPhone, iPod touch или iPad, — вы можете защитить его содержимое с помощью шифрования. Тогда кто бы ни получил физический доступ к устройству, ему понадобится пароль для расшифровки содержащейся в его памяти информации, включая контакты, сообщения, документы, историю звонков и электронные письма.

Для защиты устройства под управлением операционной системы iOS, перейдите на экран **Настройки | Пароль** (Settings | Passcode), коснитесь пункта **Включить пароль** (Enable passcode) и создайте пароль, коснувшись в открывшемся экране пункта **Параметры пароля** (Passcode Options), чтобы использовать пароль из 6 цифр или из совокупности букв и цифр. После установки пароля коснитесь пункта **Запрос пароля** (Require passcode). и выберите вариант **Немедленно** (Immediately), чтобы устройство автоматически блокировалось сразу же после отключения экрана (рис. 1.4).

Вводить пароль, который состоит только из цифр, проще — при разблокировании устройства можно пользоваться цифровым набором. Если же кроме цифр в пароле используются

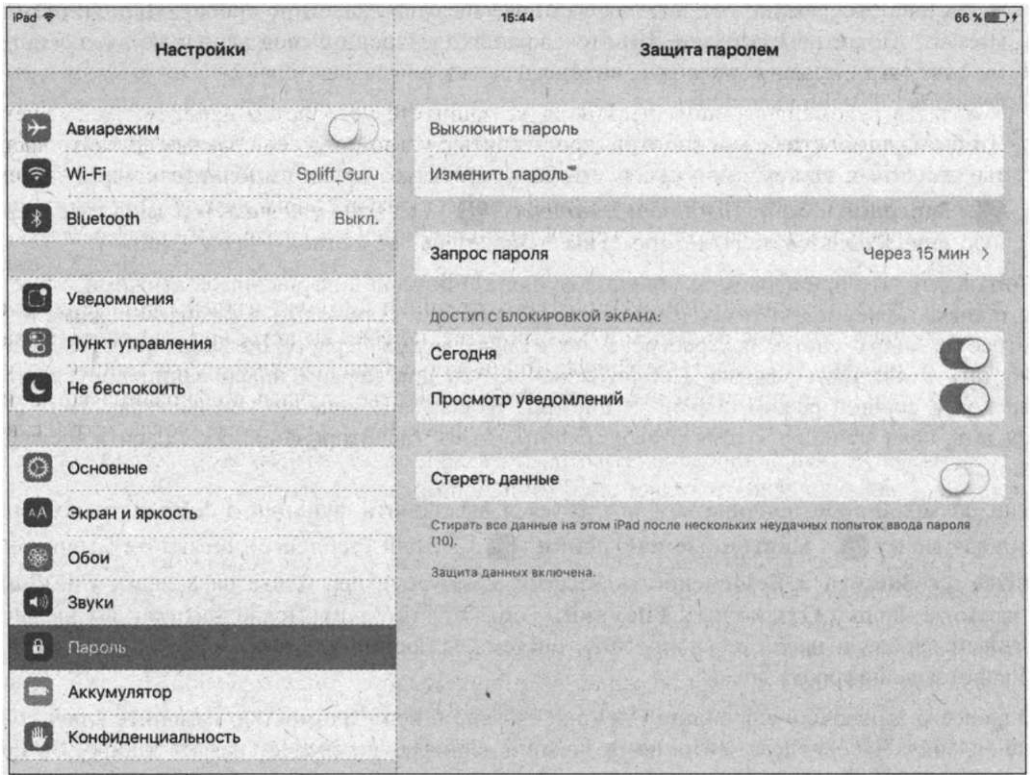


Рис. 1.4. Настройки пароля в операционной системе IOS

буквы и специальные символы, понадобится вызывать виртуальную клавиатуру, что может быть не очень удобно. В любом случае рекомендуется использовать пароль, состоящий из не менее чем 6 цифр.

После установки пароля взгляните на нижнюю часть экрана настроек пароля (см. рис. 1.4) — вы увидите сообщение **Защита данных включена** (Data protection enabled). Теперь устройство зашифровано паролем, который понадобится для разблокирования данных, хранящихся в памяти устройства.

Далее приведены некоторые особенности iOS, о которых следует помнить, имея дело с конфиденциальными данными:

- программа iTunes позволяет сохранять резервные копии содержимого памяти вашего устройства на сопряженный компьютер. Если вы установите флажок **Зашифровать резервную копию** (Encrypt backup) на вкладке **Обзор** (Summary) вашего устройства в окне iTunes, программа станет сохранять резервную копию таких конфиденциальных данных, как пароли к сетям Wi-Fi и электронной почте. При этом сохраняемая резервная копия будет полностью зашифрована. Убедитесь, что используемый вами пароль хранится в надежном месте. Восстановление данных из резервной копии приходится делать нечасто, но возникнет огромная проблема, если пароль для разблокирования резервной копии окажется утерян;
- если вы сохраняете резервные копии в облачном хранилище iCloud, для защиты своих данных нужно использовать длинный пароль и обеспечить его сохранность. Хотя-большинство хранящихся в резервных копиях данных и шифруется, компании-владельцу хранилища, возможно, придется предоставить к ним доступ по требованию соответствующих органов. В особенности это касается электронной почты и заметок, которые сохраняются в незашифрованном виде;
- если вы в рекомендованном здесь порядке защитите устройство паролем, то сможете при необходимости безопасно и быстро удалить с устройства свои данные. В настройках парольной защиты можно указать, чтобы устройство удаляло всю хранящуюся на нем информацию в случае десяти (подряд) неудачных попыток ввода пароля. Для этого следует установить переключатель **Стереть данные** (Erase Data) в активное положение (см. рис. 1.4);
- согласно информации компании Apple, ее сотрудники не могут извлечь данные, хранящиеся непосредственно на вашем iOS-устройстве, но если вы активировали синхронизацию с iCloud или сохраняете резервные копии в облачное хранилище, эти данные могут быть доступны сотрудникам компании. В большинстве случаев шифрование встроенными средствами операционной системы iOS эффективно лишь тогда, когда устройство выключено или заблокировано. Имейте это в виду и, по возможности, старайтесь выключать или блокировать устройство, если подозреваете, что к нему может получить доступ злоумышленник;
- если вы оцениваете риск кражи своего устройства как высокий, то можете активировать функцию **Найти iPhone** (Find My iPhone), чтобы удаленно стереть содержимое памяти устройства, если оно будет похищено. Кроме того, вы сможете определить местонахождение похищенного устройства. Смартфоны и планшеты с поддержкой сотовой связи постоянно /передают эту информацию операторам мобильной связи (при условии включения на устройстве функции передачи данных через сотовую сеть). Однако устройства с поддержкой Wi-Fi — такие, как iPad без поддержки сотовой связи и iPod Touch, этого не делают.

Подробнее о шифровании мы поговорим в *главе 6.*

Защита портативных носителей данных

Обмен объемными данными часто производится с помощью USB-накопителей: внешних Flash-дисков и HDD. Это быстрее и удобнее, а часто и безопаснее, чем передавать гигабайты информации через Интернет.

Но злоумышленник может попытаться похитить внешний накопитель, чтобы заполучить конфиденциальную информацию. А так как в большинстве случаев защиты данных на таких устройствах не предусмотрено, злоумышленнику не потребуется никаких средств для превращения данных в читабельный вид. На этот случай многими производителями разрабатываются защищенные накопители с шифрованием, требующие ввода программного или аппаратного пароля (ПИН-кода) или сканирования отпечатка пальца. На рис. 1.5 показаны Flash-накопители с защитой данных.

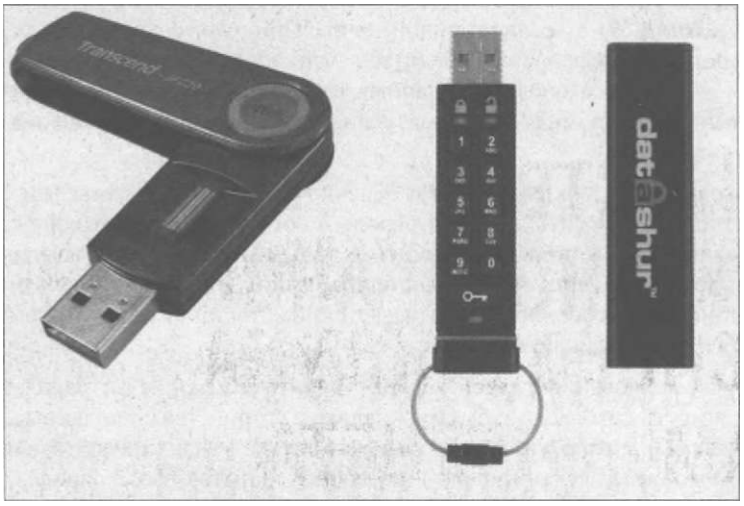


Рис. 1.5. Flash-накопитель с биометрической защитой (слева) и с помощью ПИН-кода (справа)

К таким накопителям относятся, к примеру, устройства Kingston DataTraveler (2000, Vault Privacy или 4000), IStorage datAshur, Samurai Nano Drive, GuardDo Touche и др.

Как правило, доступ к информации на накопителях с алфавитно-цифровой клавиатурой осуществляется с помощью ПИН-кода, представляющего собой число или слово, и для защиты данных используется 256-битное аппаратное AES-шифрование. Кроме того, после нескольких попыток подбора кода включается функция автоматической блокировки и ключ шифрования удаляется, что делает невозможным расшифровку данных.

На Flash-дисках с биометрической защитой (например, Transcend JetFlash 220) используется аналогичный алгоритм шифрования, только доступ к устройству открывается после сканирования отпечатка пальца, совпадающего с ранее сохраненным в памяти носителя. Подобные носители могут также предоставлять дополнительную защиту с помощью программного пароля и самоуничтожения данных.

Несмотря на все достоинства защищенных Flash-накопителей, основным их недостатком является относительно небольшой объем памяти устройства — как правило, не более 64 Гбайт. Решение этой проблемы заключается в использовании внешних портативных дисков, как HDD, так и SSD, емкость которых может достигать 4 Тбайт (рис. 1.6).

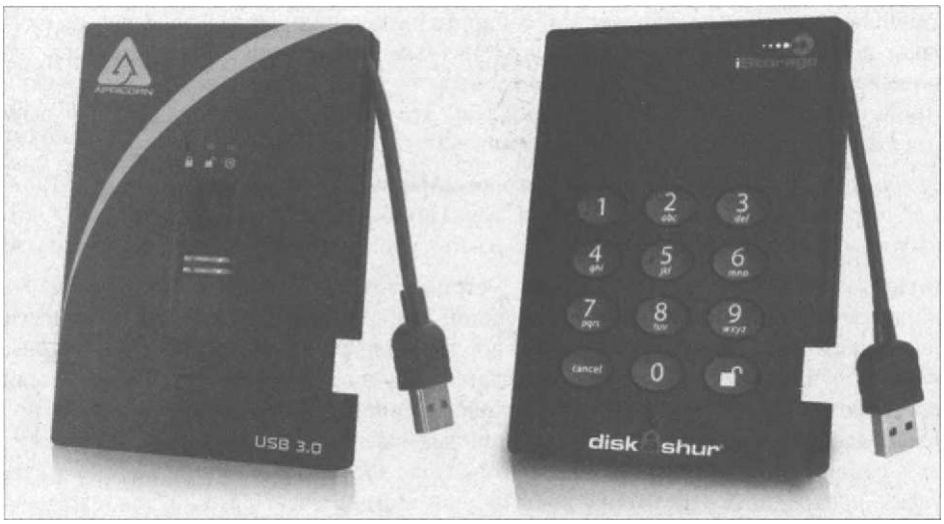


Рис. 1.6. Внешний жесткий диск с биометрической защитой *(слева)* **и с помощью ПИН-кода (***справа)*

Как и в случае с Flash-накопителями, в памяти внешних HDD и SSD-накопителей данные шифруются с помощью 256-битного аппаратного AES-шифрования и защищены функцией уничтожения при попытке подбора пароля методом перебора и взлома методом «грубой силы».

Безопасность при использовании сетей Wi-Fi

Наличие в каждом ноутбуке и нетбуке беспроводной сетевой карты Wi-Fi и довольно демократичные цены на соответствующие точки доступа и маршрутизаторы привели к тому, что многие общественные заведения: кафе, гостиницы, аэропорты и даже торговые центры — стали предоставлять посетителям бесплатный доступ к Интернету в качестве дополнительной услуги или как средство привлечения клиентов. Эта тенденция не могла пройти незамеченной мимо людей, имеющих возможность часто посещать такие заведения.

Разумеется, очень приятно пользоваться услугами, в данном случае, подключения к Интернету, за чужой счет, но, тем не менее, не следует забывать об опасности, которую такой «сыр» таит. А именно — все данные, передаваемые через Интернет с вашего (и на ваш) компьютер или мобильное устройство, легко могут быть перехвачены злоумышленниками, подключившимися к той же сети Wi-Fi. Особенно это касается незашифрованных данных, передаваемых, к примеру, такими программами, как WhatsApp. Сети Wi-Fi по своей природе уязвимы для взлома и «прослушки», однако на них вполне можно полагаться, если применить необходимые меры безопасности.

Угрозы, возникающие при подключении к открытой сети Wi-Fi

Злоумышленники, подключаясь к открытой или даже вашей (слабо защищенной) сети, могут выполнять следующие действия:

- захватывать параметры соединения — с помощью специальных приложений (программных *сетевых сканеров),* установленных на смартфоне, планшете или ноутбуке, по-

сторонние могут без особых усилий собирать разнообразную информацию об активных точках доступа, их названиях, используемых базовых станциях, типе шифрования, подключенных устройствах и просматриваемых на них сайтах, определять, открыт ли на устройствах общий доступ к файлам, и т. п. Эти сведения в комплексе могут использоваться для планирования целенаправленных атак, подобных тем, что описаны далее.

Полностью обезопасить себя от сбора информации сетевыми сканерами невозможно — разве что отказаться от пользования точками беспроводного доступа или, хотя бы, включать адаптер Wi-Fi на своем устройстве только тогда, когда он действительно нужен;

- **считывать трафик** — при установке с устройством соединения Wi-Fi передача пакетов данных осуществляется на соответствующий IP-адрес. Если в точке доступа зарегистрировано несколько устройств, то они игнорируют пакеты данных, предназначенные для других получателей, — так предотвращается хаос в сети Wi-Fi и поддерживается высокая скорость работы. Однако, имея подходящее программное обеспечение, можно «внушить» адаптеру Wi-Fi, что он должен принимать все пакеты вне зависимости от указанных в сетевых пакетах IP-адресов. В этом случае злоумышленник может считывать весь трафик, проходящий через точку доступа, при этом оставаясь в тени, т. к. сам ничего не передает. Затем с помощью фильтров он может найти в записанных сведениях нужную информацию — например, изображения или адреса веб-сайтов.

  Для защиты от такого считывания следует избегать точек доступа без парольной защиты. Хотя это и не панацея, но тогда злоумышленнику надо будет как минимум знать пароль к точке доступа. Кроме того, на всех сайтах, где нужно проходить авторизацию и передавать персональные данные, следует использовать только защищенное соединение через протокол HTTPS (см. далее *разд. «Использование протокола HTTPS»),* а не HTTP, и не заходить на сайты, не поддерживающие шифрование. Осторожность также необходима при работе с мобильными приложениями, т. к. в этом случае пользователь практически не имеет доступа к тонким настройкам. Например, клиент Facebook шифрует только авторизацию, после чего передача данных производится в незащищенном виде. И хотя злоумышленник и не увидит вашего пароля, он сможет читать ваши статусные сообщения и переписку. Поэтому от использования таких приложений при подключении к публичной точке доступа следует полностью отказаться. Альтернативой может служить технология VPN, с помощью которой для вашего интернет-соединения создается защищенный туннель. В этом случае, если злоумышленник перехватит переданный с вашего устройства сетевой пакет, он получит просто беспорядочный набор данных. Для создания VPN-туннелей вы можете использовать утилиты наподобие Hotspot Shield, доступные и для мобильных устройств;

  ОБЯЗАТЕЛЬНА ЛИ ИДЕНТИФИКАЦИЯ В ОБЩЕСТВЕННЫХ СЕТЯХ WI-FI?

  Радость от возможности бесплатного и бесконтрольного подключения к общественным сетям Wi-Fi несколько скрадывает введенное летом 2014 года постановлением правительства РФ № 758 требование обязательной идентификации подключающегося к публичному Интернету пользователя по его удостоверению личности. Согласно документу, оператор связи перед разрешением кому-либо доступа в общественный Интернет обязан потребовать у него ввести номер мобильного телефона, на который отправляется код для подтверждения идентификационных данных.

- **захватывать cookie-файлы для авторизации в аккаунтах** — с помощью соответствующего программного обеспечения злоумышленник может организовать сетевую атаку с использованием протокола ARP (т. н. *ARP-спуфинг)* и легко перехватить сеансовые cookie-файлы, которые идентифицируют участника социальной сети (например, Facebook) после успешной в ней авторизации. Благодаря таким cookie-файлам вам не

требуется вводить пароль каждый раз, когда вы хотите авторизоваться на сайте Facebook. Специальные программы извлекают из трафика все сеансовые cookie-файлы и выводят их на экран в виде списка, после чего одним касанием злоумышленник может войти в ваши текущие сеансы Facebook, Twitter или eBay, после чего весь обмен данными проходит через устройство злоумышленника.

Для защиты от перехвата сеансовых cookie-файлов также можно использовать VPN-туннели;

- **подменять точки доступа** — как вы могли обнаружить, по умолчанию после однократного входа в какую-либо беспроводную сеть устройство автоматически подключается к ней снова, если оказывается в зоне действия сети Wi-Fi с таким же именем. Простейший сценарий атаки выглядит так: из любого смартфона, планшета или ноутбука без особых усилий и дополнительных приложений злоумышленник может сделать точку доступа Wi-Fi с любым именем, после чего сможет считывать в своей поддельной сети все передаваемые данные. Для защиты от таких атак следует удалять сохраненные сети Wi-Fi из списка в настройках устройства, оставляя там только домашние и рабочие;
- **взламывать механизмы шифрования** — злоумышленники, желая получить доступ к важным сведениям (таким как банковские реквизиты, регистрационные данные PayPal или пароли к почте и веб-сервисам), делают ставку на различные уязвимости в реализации механизма шифрования и на промахи пользователей. Например, они могут попытаться перенаправить пакеты информации с помощью ложной точки доступа. А когда пользователь заходит через такую точку на защищенный сайт, злоумышленник может попробовать перенаправить его на незащищенную версию, чтобы узнать пароль или прослушать весь трафик. Распространены и атаки с применением фальшивых сертификатов. В этом случае мошенник использует защищенное соединение как с веб-сервисом, так и, с другой стороны, с пользователем точки доступа. Но вследствие того, что SSL-сертификаты сфальсифицированы, прослушивание трафика не составляет труда.

  Если бы веб-сервисы полностью шифровали весь трафик, то у злоумышленников не было бы возможности использовать прием с перенаправлением пользователей на незащищенные веб-сайты. Однако SSL-соединение пока не получило повсеместного распространения, хотя крупные сервисы и предлагают его по выбору. Поэтому необходимо всегда самим выбирать SSL-соединение, а также проверять, чтобы в адресной строке браузера указывалась информация о защищенном соединении. К сожалению, при работе с мобильными приложениями тип соединения часто не настраивается и не определяется. В этом случае нужно предварительно уточнить наличие таких возможностей в том или ином приложении у его разработчиков. О надежности соединения также свидетельствует соответствующее указание в адресной строке браузера и наличие сертификата. С другой стороны, и это не является стопроцентной гарантией, т. к. можно столкнуться с фальшивыми сертификатами.

Для обеспечения безопасности устройств под управлением операционных систем Android, iOS и Windows Phone необходима регулярная установка системных и программных обновлений. Кроме того, на них обязательно наличие антивирусной программы — к примеру, Kaspersky Internet Security для Android или Kaspersky Safe Browser. Не допускайте также автоматического подключения устройства к сетям Wi-Fi без вашего ведома и, по возможности, используйте VPN-туннели для передачи данных.

На компьютерах под управлением операционной системы Windows и OS X следует отключить общий доступ к файлам и обязательно держать включенным брандмауэр. Проверить соответствующие настройки можно в Windows так: **Панель управления | Брандмауэр**

Windows (Control Panel | Windows Firewall) и в OS X так: **Системные настройки | Безопасность | Брандмауэр** (System Preference | Security & Privacy | Firewall). Здесь также необходимо установить антивирусное программное обеспечение и своевременно обновлять систему и программы. Кроме того, пользуйтесь исключительно сервисами, которые шифруют авторизацию и передачу данных посредством протокола SSL. Обратите внимание, что такие надстройки, как HTTPS Finder или HTTPS Everywhere для Firefox и Chrome, задействуют этот протокол по умолчанию. И, по возможности, также используйте для передачи данных VPN-туннели.

Защита собственной сети Wi-Fi

Разумеется, злоумышленники могут подключаться как к открытым сетям Wi-Fi, так и взламывать закрытые, т. е. защищенные паролем. Существует даже термин для этого явления — *вардрайвинг* — т. е. поиск и взлом беспроводных сетей с различными целями: от простого бесплатного подключения до кражи передаваемых в такой взломанной сети данных. В таких случаях опасность попадания ваших данных к злоумышленникам возникает при подключении вашего устройства не только к публичной, пусть и защищенной паролем сети, но и к вашей собственной!

Проблема состоит в том, что многие пользователи (а, возможно, и вы), устанавливая у себя в квартире (офисе) беспроводную точку доступа, по незнанию или по другим причинам не включают шифрование либо не меняют установленные по умолчанию пароль и имя сети. В первом случае сеть позиционируется как открытая — и к ней без проблем можно подключиться. Такие частные сети попадаются довольно редко, чаще распространены рассмотренные ранее общественные бесплатные сети. Если же владелец роутера не сменил стандартный пароль к своей сети Wi-Fi (а некоторые производители беспроводных маршрутизаторов устанавливают на всех своих устройствах один и тот же ключ безопасности или пароль по умолчанию), то злоумышленник может подобрать его, если известен производитель и/или модель роутера. Такой стандартный пароль, как правило, может быть указан в документации к маршрутизатору или же найден во Всемирной паутине. Получив доступ к сети Wi-Fi пользователя, злоумышленник может получить root-доступ к самому маршрутизатору — это особенно легко, если не изменены дефолтные логин и пароль администратора. Например, обнаружив беспроводную сеть **dlink,** можно с большой вероятностью утверждать, что пользователь использует точку доступа производства компании D-Link, и, скорее всего, для подключения к такому роутеру подойдет один из стандартных паролей этого производителя. Стоит отметить, правда, что современные модели роутеров часто не позволяют использовать стандартный пароль беспроводной сети, как и root-пароль, требуя указать безопасные.

> ***СТАНДАРТНЫЕ ПАРОЛИ БЕСПРОВОДНОЙ СЕТИ WI-FI***
>
> **Списки дефолтных (стандартных по умолчанию) авторизационных данных к разным моделям роутеров доступны, к примеру, по адресам tinyurl.com/mouS8hz и tinyurl.com/pjop84w. Помимо этого, существуют способы использования дефолтных WPS-PIN-кодов — но эта тема выходит за рамки книги и довольно подробно освещается, например, тут: tinyurl.com/oqzu5mc и tinyurl.com/numagu6.**

Часто доступ к чужой сети можно получить, попробовав и один из наиболее распространенных паролей. Согласно исследованиям Лаборатории Касперского[1], 34% пользователей

[1] **См. по ссылкам: tinyurl.com/otin6oq9, tinyurl.com/oqp8x8h и tinyurl.com/nnkczx9.**

применяют простые пароли, среди которых 17% задают в этом качестве дату своего рождения, 10% — номер телефона, 10% — имя и *9%* — кличку домашнего питомца. А вот и другие распространенные пароли: `123`, `12345`, `123456`, `1234567`, `1234567890`, `0987654321`, `7654321`, `654321`, `54321`, `321`, `753951`, `11111`, `55555`, `77777`, `qwerty`, `pass`, `password`, `admin`. В России наиболее популярны пароли из последовательности цифр, о чем говорят неоднократные анализы баз данных разных сайтов[1]. Используются также русские слова, набранные в латинской раскладке. Список наиболее распространенных паролей приведен в табл. 1.1.

Таблица 1.1. *Список наиболее распространенных паролей. Источник:* ***tinyurl.com/nhfok9t***

/	0	000000	1
100827092	10203	1111	11111
111111	1111111	11111111	1111111111
1111114	111222	112233	12
121212	121314	123	123123
123123123	123321	1234	12341234
1234321	12344321	12345	1234554321
123456	1234567	12345678	123456789
1234567890	123654	123789	123abc
123qwe	124578	131313	134679
135790	142536	147258	147258369
147852	159357	159753	159951
19921992	19951995	Iq2w3e	Iq2w3e4r
Iq2w3e4r5t	lqaz2wsx	212121	22222
222222	232323	258456	33333
333333	456	4815162342	54321
55555	555555	654321	66666
666666	666999	7007	753951
7654321	77777	777777	7777777
789456	88888	888888	88888888
9379992	987654	987654321	99999
999999	a	aaaäaa	abcl23
abcdl234	admin	admin123	administrator
andrew	andrey	asdasd	asdf
asdfgh	asdfghjkl	azerty	baseballl
changeme	Charlie	cjkysirj	cjmasterinf
computer	daniel	demo	doudou
dragon	el0adc3949ba59abbe5 6e057f20f883e	easytocrackl	eminem
fktrcfylh	footballl	fuckyou	fyfcnfcbz
fylhtq	genius	george	gewinner
gfhjkm	ghbdtn	guest	hallo

[1] **См. по ссылке: tinyurl.com/oezkux2 и tinyurl.com/q48xv7t.**

Таблица 1.1 *(окончание)*

hallol23	hejsan	hello	holyshlt
iloveyou	internet	jessica	k.,jdm
kikugalanetroot	killer	knopka	letmein
liverpool	lol	101123	lollipop
loulou	lovers	marina	martin
master	matrix	maximius	michael
mirage	monkey	naruto	nastya
natasha	ngockhoa	nikita	nokia
parola	pass	password	passwordl
passwordl2	passwordl23	passwordl234	passwordl2345
passwordl23456	passwordl234567	passwordl2345678	passwordl23456789
pokemon	princess	qlqlql	qlw2e3
qlw2e3r4	qazwsx	qazwsxedc	qql8ww899
qwaszx	qwel23	qweasd	qweasdzxc
qweqwe	qwert	qwerty	qwertyu
qwertyuiop	qwertyuiop[]	root	samsung
sandra	saravn	secret	sergey
shadow	slipknot	soccer	sophie
spartak	stalker	star	sunshine
super	superman	tecktonik	TempPassWord
test	Testl23	thomas	tundra cool2
vfhbyf	vfrcbv	vkontakte	yfnfif
zaqwsx	zxcvbn	zxcvbnm	zzzzzz
йцукен	любовь	пароль	

Этот список приведен- здесь для проверки безопасности вашей собственной сети — если пароль доступа к ней присутствует в списке, или он иной, но тоже примитивный, рекомендуется, не откладывая, сменить его. Для подбора надежного пароля, состоящего, как правило, из букв в разном регистре, цифр и специальных символов, можно обратиться к одной из соответствующих программ, например, к программе KeePassX (см. *главу 2).* Помимо установки надежного пароля, необходимо следовать приведенным ниже рекомендациям для защиты собственной сети Wi-Fi:

- **не пользуйтесь алгоритмом WEP** — этот алгоритм (Wired Equivalent Privacy, конфиденциальность на уровне проводных сетей) безнадежно устарел. Реализуемый им шифр могут легко и быстро взломать большинство даже неопытных хакеров. Вместо него следует перейти на алгоритм WPA2 (Wi-Fi Protected Access, защищенный доступ Wi-Fi), который обеспечивает надежную аутентификацию пользователей с использованием стандарта 802.1x (рис. 1.7). Если какие-либо ваши устройства или точка доступа не поддерживают алгоритм WPA2, вы можете обновить их прошивку или приобрести новое оборудование;
- **обязательно пользуйтесь системой предотвращения/обнаружения вторжений для беспроводных сетей** — обеспечение безопасности Wi-Fi не ограничивается непосредственной борьбой с попытками получить к сети несанкционированный доступ. Хакеры

могут создавать фиктивные точки доступа в сети или проводить атаки на отказ в обслуживании. Чтобы распознавать такие вторжения и бороться с ними, следует внедрить беспроводную систему предотвращения вторжений. Такие системы прослушивают эфир в поисках фиктивных точек доступа и вредоносной активности, по возможности блокируют ее и предупреждают системного администратора. Это скорее решение для корпоративных сетей, но вы можете установить подобное приложение для анализа сети и дома, — например, Snort **(snort.org);**

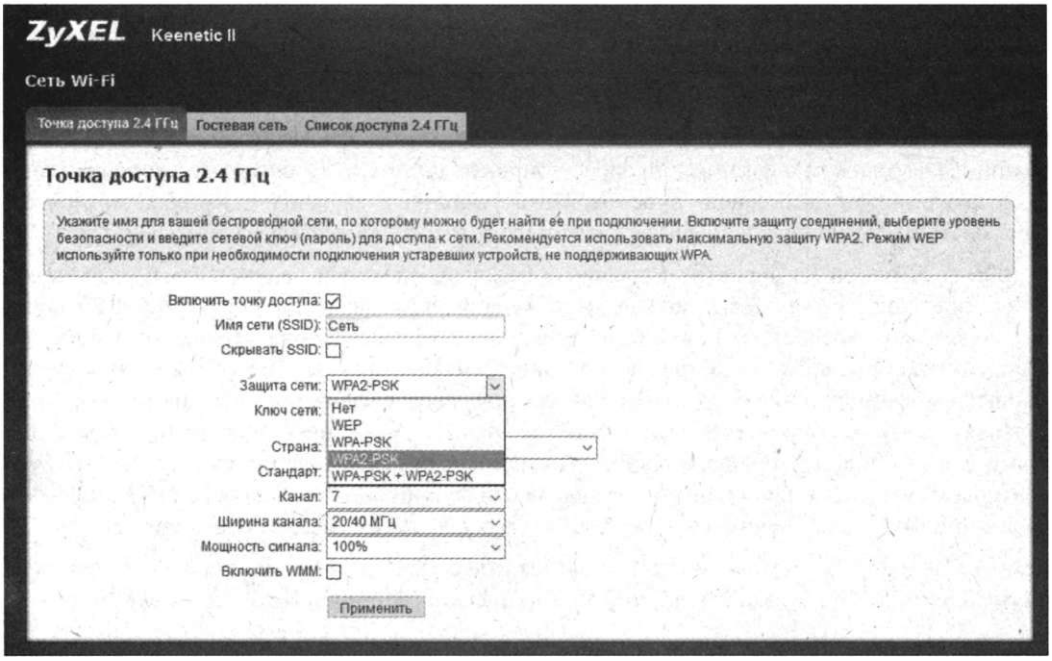


Рис. 1.7. Выбор алгоритма шифрования в настройках маршрутизатора

- **не полагайтесь на сокрытие SSID —** один из мифов Wi-Fi-безопасности состоит в том, что отключение широковещательной рассылки SSID — идентификатора беспроводной сети — «скроет» вашу сеть или, по крайней мере, сам SSID от хакеров. Однако такая опция лишь удаляет SSID из сигнальных кадров точки доступа. Идентификаторы сети по-прежнему содержатся в запросах на ассоциацию 802.11, а также иногда в пакетах проверки и ответах на них. Поэтому перехватчик с помощью анализатора беспроводных сетей может обнаружить «скрытый» SSID довольно быстро, особенно в сети с высокой активностью. Сокрытие SSID также может отрицательно сказаться на быстродействии сети и повысить сложность ее конфигурирования — вам придется вручную вводить название сети на клиентах, что дополнительно усложняет их настройку. Кроме того, увеличится число зондирующих и ответных пакетов в сети, из-за чего снижается ее доступная пропускная способность;
- **не полагайтесь на фильтрацию по MAC-адресам —** еще один миф из области защиты беспроводных сетей гласит, что включение фильтрации по MAC-адресам позволяет создать дополнительный уровень безопасности, предотвращающий допуск в сеть посторонних клиентов. Это до некоторой степени верно, но следует помнить, что при анализе трафика атакующие очень легко могут выяснить разрешенные MAC-адреса и подделать

их на своих устройствах. Поэтому не стоит слишком полагаться на надежность MAC-фильтрации, хотя этой функцией можно пользоваться для ограничения возможности пользователей подключать к сети несанкционированные устройства и компьютеры. Следует также иметь в виду высокую сложность ведения и своевременного обновления списка MAC-адресов.

Еще о защите персональных данных

Ваш провайдер знает о ваших пристрастиях в Интернете все и при необходимости может предоставить сведения об активности IP-адреса вашего компьютера заинтересованным и уполномоченным лицам. При желании они могут получить доступ к любой информации: сведениям о посещенных вами веб-сайтах, содержимом писем электронной почты и сообщений ICQ, узнать ваш физический адрес и личные данные. Администратор корпоративной сети также может выборочно просматривать различные сведения о сетевой активности пользователей — такие как объем загруженного трафика, посещенные веб-узлы и т. п.

В 2006 году одной из директив Евросоюз обязал провайдеров хранить данные о трафике своих клиентов до двух лет и дольше. При желании определенных структур эта информация может быть предоставлена по первому же запросу. В некоторых странах (в том числе и в России) нормативные акты требуют от провайдеров установки оборудования, отслеживающего информационные потоки и контролируемого такими организациями, как Федеральная служба безопасности. Национальные шлюзы также могут контролироваться властями и в том числе запрещать доступ из страны к определенным ресурсам. В США под контролем Агентства национальной безопасности функционирует и проект ECHELON, анализирующий и сохраняющий содержимое сетевых и телефонных сеансов связи.

Кстати, по этой теме вы можете почитать весьма интересные статьи по ссылкам: tinyurl.com/mhh71yf, tinyurl.com/ocqtpd8, tinyurl.com/oj5d5ng и tinyurl.com/ovk5q2x.

ПАРА СЛОВ ОБ ЭЛЕКТРОННОЙ ПОЧТЕ

Сообщения электронной почты, прежде чем, попасть от отправителя к адресату, минуют узлы провайдеров, которыми пользуются оба участника обмена. В том случае, когда сообщение отправляется в другую страну, то, помимо провайдеров, оно минует еще и шлюзы обеих стран. На всех этапах своего пути это сообщение может быть перехвачено кем угодно, начиная от хакеров и заканчивая службами безопасности, — письмо пересылается по открытым каналам связи без какой-либо защиты. Это, как если вы разговариваете по телефону, а некто третий поднял параллельную трубку и подслушивает ваш разговор. При необходимости во время передачи в текст сообщения могут быть внесены изменения, — тем самым вас могут скомпрометировать, испортить вам репутацию и даже подвести под суд. Причем для поиска вашего сообщения не нужно просматривать миллионы посланий — быстро и эффективно все сделает программное обеспечение, фильтрующее поток данных. К примеру, поток электронных писем может фильтроваться на предмет наличия таких слов, как «варез» или «хакер», — в случае обнаружения ключевых слов текст письма будет изучен тщательнее.

Помимо шлюзов и серверов провайдеров, составить ваш портрет может и сам компьютер, которым вы пользуетесь дома, на работе или в интернет-кафе. Все ваши шаги сохраняются в небольших *cookie-файлах,* создаваемых как на локальном компьютере, так и на посещаемом сервере. Cookie-файлы содержат в том числе и сведения о местоположении пользователя — чтобы при запросе пользователя из России открывать страницу microsoft.ru, а не microsoft.com или microsoft.us. Просмотрев cookie-файлы на компьютере, можно сделать

вывод о привычках и пристрастиях его владельца. Поэтому периодически нужно удалять cookie-файлы, накопленные браузером (этот процесс для разных браузеров описан в конце главы).

Помимо прочего, как уже говорилось ранее, трафик с вашего компьютера злоумышленники могут перехватить и использовать в противозаконных целях. Все это к тому, что не стоит руководствоваться мнением, будто передаваемые вами в Интернет данные попадают исключительно на сайт, к примеру, магазина или какой-либо организации. Повторюсь: не рекомендуется указывать свои реальные персональные данные на любых сайтах, которые могут быть скомпрометированы, в том числе и в социальных сетях. Также очень осторожно оплачивайте покупки в Интернете — предпочитайте оплату наличными курьеру или, для покупок в зарубежных магазинах и не принимающих оплату иначе, чем с помощью банковской карты, — пользуйтесь надежными посредниками наподобие PayPal (гарантирующими возврат денежных средств) или надежными паролями (см. *главу 2)* и SMS-подтверждениями. К любым сайтам, на которых производится оплата безналичными способами (так же, как и к сайтам, требующим указания персональных данных), подключение должно производиться через протокол HTTPS (см. далее). Кроме того, важные данные, к примеру — номера банковских карт и их CVV-код — рекомендуется вводить не напрямую нажатиями клавиш, а с помощью виртуальной клавиатуры (рис. 1.8). Вообще, банковские операции лучше выполнять в отдельном защищенном окне браузера, т. н. *песочнице* — это снижает риск, что ваши данные попадут к злоумышленникам. Оба инструмента можно установить как по отдельности, так и в комплекте с антивирусным программным обеспечением, — например, тем же Kaspersky Internet Security (см. рис. 1.8).

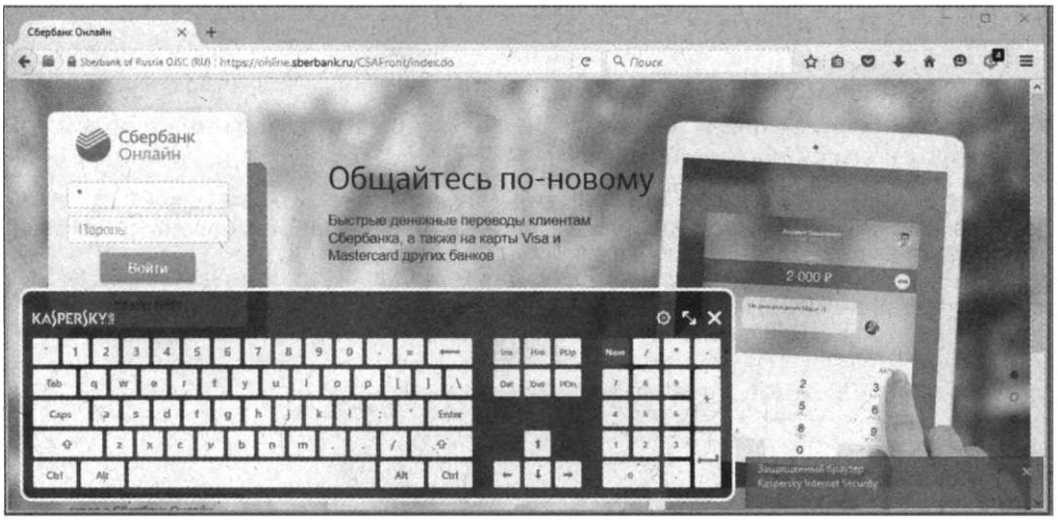


Рис. 1.8. Защищенное окно и виртуальная клавиатура Kaspersky Internet Security

Благодаря защищенному окну и протоколу HTTPS передаваемые данные шифруются и защищаются от утечки, а виртуальная клавиатура при вводе данных позволяет избежать регистрации набираемого текста «кейлогерами» — программами, фиксирующими нажатия клавиш. Имейте, кстати, в виду, что функцией записи нажатия клавиш обладают многие программы, в том числе и небезызвестный Punto Switcher.

Безопасный веб-серфинг

Здесь мы рассмотрим базовые способы обеспечения безопасности при работе в Интернете. Следует упомянуть, что приватные режимы браузеров актуальны только для конкретного устройства, не позволяя другим пользователям того же компьютера (или мобильного устройства) узнать, какие сайты вы посещали. Для более надежной защиты следует использовать методы шифрования (см. *главу 6),* протокол HTTPS (а еще лучше анонимные сети и клиенты для них — например, Tor) или операционную систему Tails (см. *часть IV).*

Приватные режимы браузеров

Приватный режим браузера позволяет сохранить некоторую анонимность исключительно на том компьютере, на котором браузер запускается. Вне вашего компьютера (во Всемирной паутине) данные передаются обычным способом. Смысл приватного режима в том, чтобы скрыть следы пребывания во Всемирной паутине для другого пользователя, подсевшего к вашему компьютеру (или взявшему ваше мобильное устройство) после вас, — чтобы он ничего не узнал о ваших действиях из временных файлов, cookie-файлов, журнала посещений и т. п.

Очевидный недостаток этого метода в том, что после отключения приватного режима вы теряете всю информацию о сеансе и для самого себя, — система забудет введенные логины и пароли, вы не сможете вернуться на ранее посещенный сайт, если не помните его адрес, т. к. журнал посещений будет пуст, и т. п. Тем не менее, метод актуален в некоторых случаях — например, в интернет-кафе (не забывайте, что трафик там не шифруется, и системный администратор, как и провайдер, может проанализировать его), где одним и тем же компьютером пользуется множество людей.

Далее рассмотрены способы использования приватного режима в разных браузерах.

- В браузере Internet Explorer (операционная система Windows) приватный режим можно запустить несколькими способами:
  - щелкнуть правой кнопкой мыши на ярлыке программы, расположенном в панели задач, и выбрать во всплывающем списке команду **Начать просмотр InPrivate** (рис. 1.9);
  - В правом верхнем углу окна программы Internet Explorer нажать кнопку $ и выбрать команду меню **Безопасность | Просмотр InPrivate** (Safety | InPrivate Browsing);

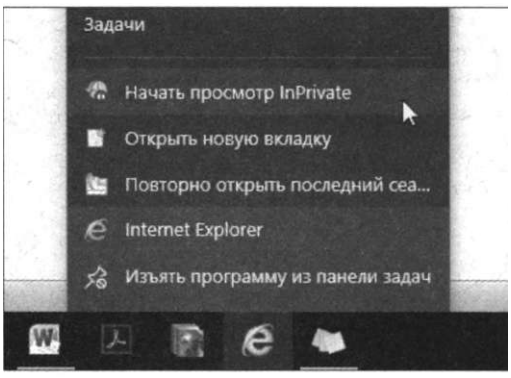


Рис. 1.9. Всплывающий список программы Internet Explorer

- в окне программы Internet Explorer нажать клавишу <Alt>, а затем выбрать команду меню Сервис | Просмотр InPrivate (Tools | InPrivate Browsing);
- в главном окне программы Internet Explorer нажать сочетание клавиш <Ctrl>+ +<Shift>+<P>.

В любом случае откроется новое окно браузера в приватном режиме, о чем сообщит кнопка InPrivate перед строкой ввода адреса (рис. 1.10, *слева),* — нажатие на эту кнопку выводит всплывающие сообщения о предназначении функции.

В окне браузера, запущенном в режиме InPrivate, можно Открывать неограниченное количество вкладок, однако защита распространяется только в пределах этого окна. Режим InPrivate позволяет посещать любые веб-страницы без сохранения временных файлов Интернета, cookie-файлов, журнала посещенных узлов и других сведений. Точнее говоря, журнал посещений веб-страниц, данные форм и паролей, содержимое адресной строки и функции автозаполнения, временные файлы Интернета, cookie-файлы, данные функции автоматического восстановления после сбоя (ACR) и хранилище моделей объектов документов (DOM) сохраняются во время сеанса работы и удаляются после закрытия окна браузера. Данные антифишинга сохраняются в зашифрованном виде. Все элементы, которые вы добавите в Избранное (Favorites) в этом режиме, будут сохранены и после закрытия окна программы.

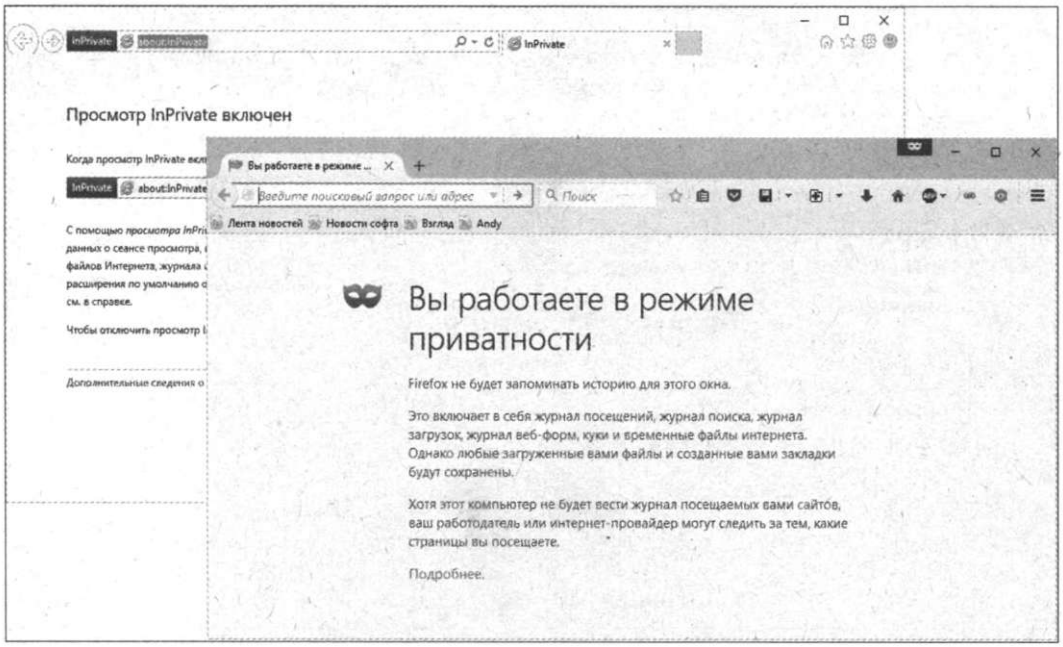


Рис.1.10. Приватный режим в Internet Explorer (слева) и Firefox (*справа)*

АНОНИМНОСТЬ В РЕЖИМЕ INPRIVATE?

Тем не менее, следует учитывать, что сетевой администратор может получить доступ к сведениям о веб-узлах, посещенных даже в режиме InPrivate. Напомню, что с помощью этого режима анонимность во Всемирной паутине не обеспечивается. Режим InPriyate предназначен для ограничения доступа к приведенным данным других (локальных) пользователей компьютера.

- Аналогичным приватным режимом обладает и ближайший конкурент Internet Explorer— браузер Firefox (рис. 1.10, *справа*). Для входа в него достаточно выбрать команду меню **Файл** I **Новое приватное окно** (File | New Private Window) или же нажать сочетание клавиш <Ctrl>+<Shift>+<P>. Выход в «общественный» свет осуществляется закрытием приватного окна. Команда перехода в приватный режим доступна также и во всплывающем списке программы на панели задач. В приватной сессии Firefox не ведет журналы посещений, загрузок, поиска и данных веб-форм, а также не сохраняет временные и cookie-файлы.
- В браузере Google Chrome приватный режим называется «инкогнито» и при работе не закрывает текущее окно браузера, а создает новое — с симпатичным шпионом в левом верхнем углу (рис. 1.11, *слева).* Переход в режим осуществляется выбором команды **Новое окно в- режиме инкогнито** (New incognito window) в меню браузера (открывается щелчком мыши на кнопке) или во всплывающем списке панели задач. С той же целью можно воспользоваться сочетанием клавиш <Ctrl>+<Shift>+<N>. После завершения работы в режиме инкогнито соответствующее окно нужно просто закрыть.

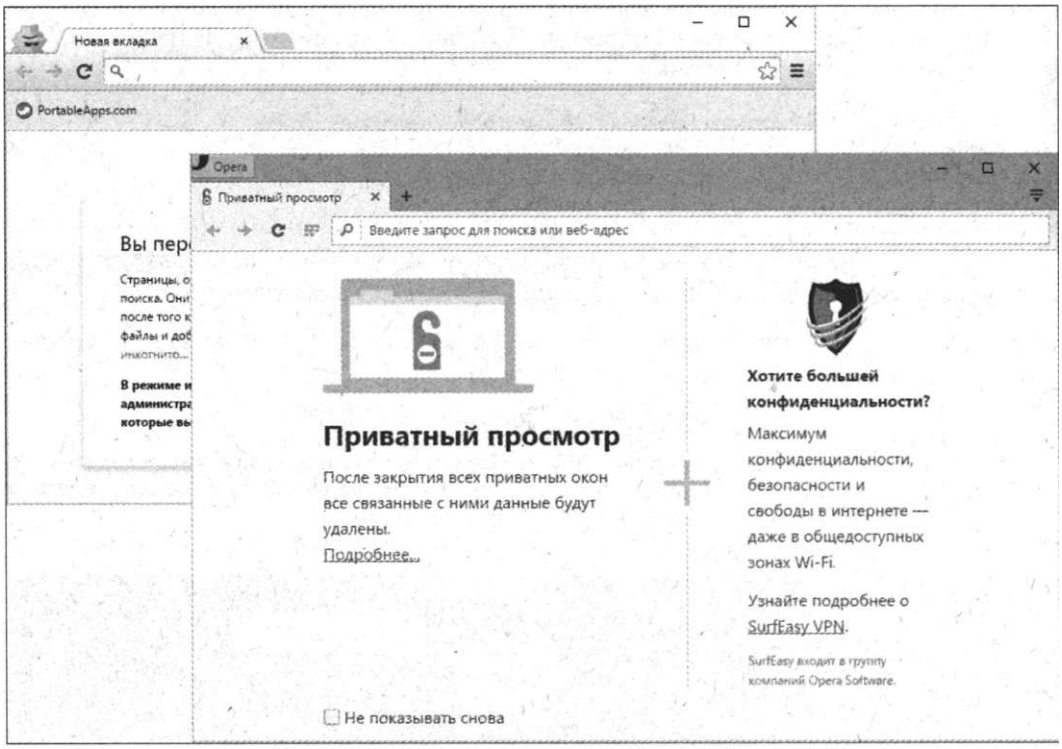


Рис. 1.11. Приватный режим в Google Chrome (слева) и Opera (*справа)*

- В браузере Opera вы можете создавать приватные окна, выбрав команду меню **Файл | Создать приватное окно** (File | New Private Window) или нажав сочетание клавиш <Ctrl>+<Shift>+<N> (рис. 1.11, *справа).* После завершения работы в приватном режиме соответствующее окно надо просто закрыть.
- В браузере Apple Safari приватный режим называется «частным доступом» и при работе не закрывает текущее окно браузера, а переводит его в приватный режим, о чем свиде-

тельствует темный цвет адресной строки (рис. 1.12). Переход в,режим осуществляется выбором команды **Новое частное окно** (New Private Window) в меню **Файл** (File) браузера. Завершив работу в режиме «частный доступ», следует закрыть окно.



На мобильных устройствах также доступен приватный режим:

- На устройствах под управлением операционной системы iOS в браузере Safari следует коснуться кнопки в правом верхнем углу экрана, а затем — появившегося пункта **Частный доступ** (Private). Браузер перейдет в приватный режим (рис. 1.13).

  Чтобы выйти из приватного режима, вновь коснитесь кнопки в правом верхнем углу экрана, а затем пункта **Частный доступ** (Private).

> ***ОСОБЕННОСТИ ПРИВАТНОГО РЕЖИМА НА IOS***
>
> Важно помнить, что если перед выходом из режима **Частный доступ** (Private) вы вручную не закроете открытые вкладки, они автоматически откроются при следующем переходе в режим **Частный доступ** (Private)!

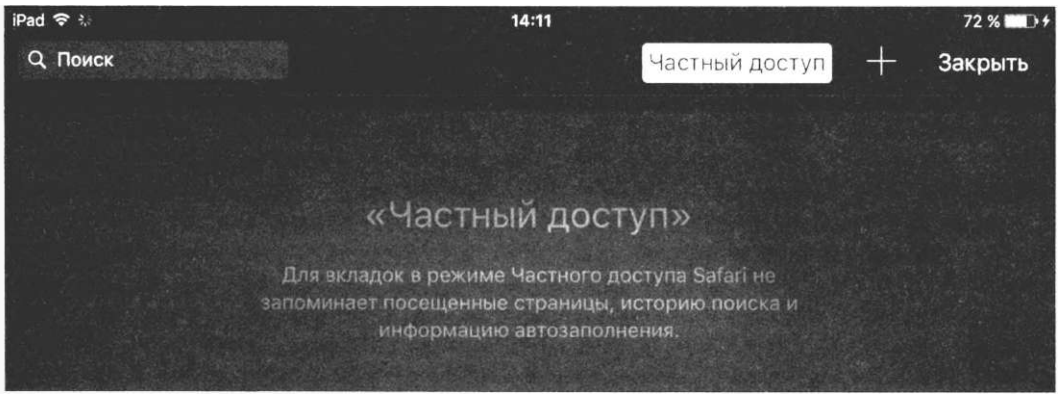


Рис. 1.13. Приватный режим в браузере Safari (iOS)

- На устройствах под управлением операционной системы Android приватный режим можно активировать следующим образом. Запустив браузер Chrome, перейдите в его меню и выберите пункт Новая вкладка инкогнито (New incognito tab) — откроется новая вкладка в режиме инкогнито (рис. 1.14, *слева).*

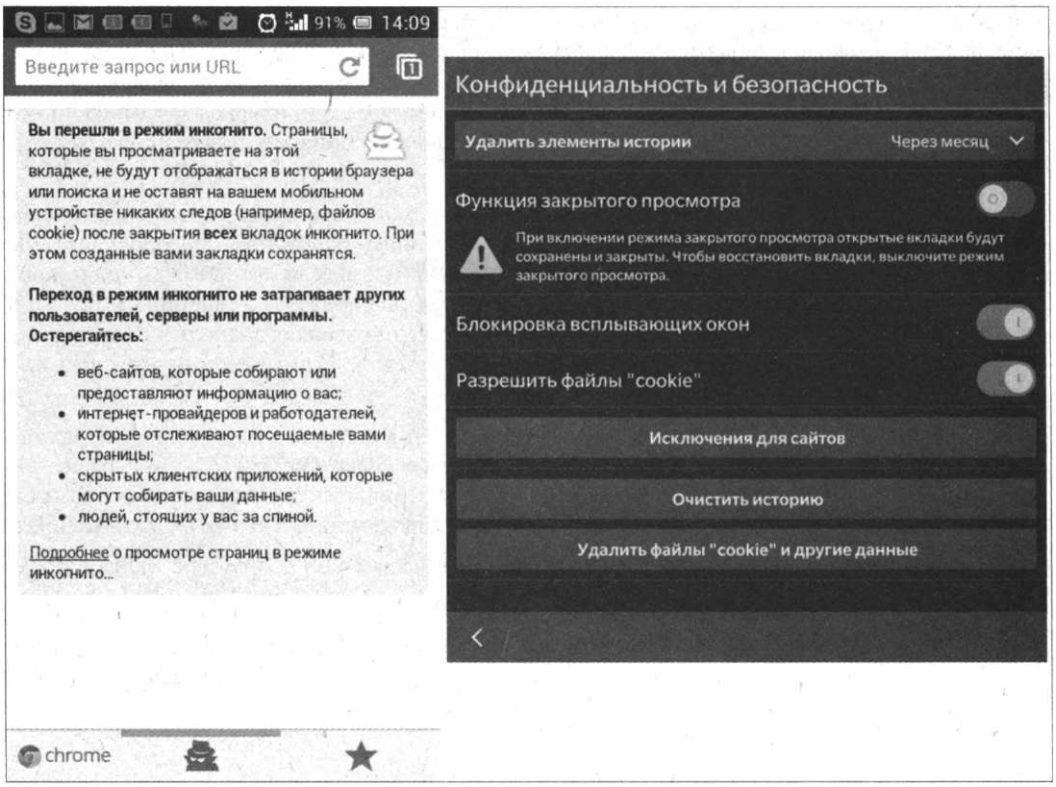


Рис. 1.14. Приватный режим в браузере Chrome на Android *(слева)* **и стандартном браузере Blackberry OS (***справа)*

Чтобы выйти из режима инкогнито:

- в операционной системе версии Android 5.0 и выше — смахните экран сверху вниз и выберите команду Chrome: закрыть все окна в режиме инкогнито (Chrome: Close all incognito windows);
- на устройстве Android более ранней версии коснитесь кнопки **x** в углу каждого окна, открытого в режиме инкогнито.

- На устройствах под управлением операционной системы Blackberry OS откройте меню и выберите пункт Настройки (Settings). Затем, перейдя в раздел Конфиденциальность и безопасность (Privacy and Security), установите переключатель Функция закрытого просмотра (Private Browsing) в активное положение (рис. 1.14, *справа).* Обратите внимание, что при использовании функции закрытого просмотра в операционной системе Blackberry OS все вкладки, которые были открыты, останутся сохранены и повторно восстановлены, когда режим закрытого просмотра будет отключен.

Использование протокола HTTPS

Не так давно организация утечки данных была трудоемким процессом, требовавшим огромных ресурсов и доступа к конкретным объектам. В настоящее же время злоумышленникам стало гораздо проще перехватывать данные отдельных пользователей и даже целых баз данных. Теперь, как только вы начинаете использовать Интернет для хранения, обработки и передачи данных, они становятся уязвимыми для утечки. Весь интернет-трафик, исходящий с вашего компьютера и поступающий на него, может просматриваться теми людьми, кто имеет доступ к компьютерам, через которые проходят ваши данные (начиная с компьютера, обеспечивающего наличие сети в вашем доме или в офисе местного провайдера, вплоть до компьютера в пункте назначения вашего сообщения и всех других находящихся между ними компьютеров).

Единственный способ снизить угрозу перехвата данных и сохранения конфиденциальности передаваемых/получаемых сообщений — использование надежного шифрования. При шифровании сообщения приобретают форму, недоступную для прочтения кем-либо, кроме конечного получателя сообщения. В настоящее время наблюдается тенденция к использованию шифрования все большим числом веб-сайтов, что позволяет защитить передаваемые данные, но, к сожалению, эта возможность используется не всеми интернет-ресурсами по умолчанию.

Чтобы расширить спектр использования алгоритмов шифрования и защитить свои данные, вы можете установить соответствующее приложение, — например, HTTPS Everywhere. Оно представляет собой расширение (плагин) для браузеров, которое активирует функцию шифрования на всех поддерживающих ее сайтах. Расширение призвано решить проблему с сайтами, по умолчанию предоставляющими доступ без шифрования, но, тем не менее, поддерживающими протокол HTTPS, а также с HTTPS-ресурсами, имеющими ссылки на незашифрованные страницы. Для таких сайтов HTTPS Everywhere обеспечивает автоматическое перенаправление запросов на HTTPS-области сайтов. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS.

Расширение HTTPS Everywhere

Расширение HTTPS Everywhere доступно для браузеров Firefox (в т. ч. и в версии браузера для устройств под управлением операционной системы Android), Chrome и Opera и шифрует поток данных, передаваемый между сайтами, поддерживающими протокол HTTPS.

Со страницы **tinyurl.com/38sqvb9** вы можете установить этот плагин, щелкнув мышью на соответствующей ссылке.

> ***HTTPS EVERYWHERE И CHROME***
>
> **Если вы устанавливаете расширение HTTPS Everywhere напрямую из файла, минуя встроенный в Windows-версию браузера магазин Chrome Web Store, программа будет автоматически отключать это расширение после каждого перезапуска. Для решения проблемы следует воспользоваться советами, приведенными на странице tinyurl.com/gqf2udf.**

После установки расширения на панели браузера появится его значок, позволяющий просматривать правила и изменять настройки плагина (рис. 1.15), а подключение к сайтам, поддерживающим протокол HTTPS, будет осуществляться в защищенном режиме, на что указывает название протокола в адресной строке **(https://www.yandex.ru/** в примере на рис. 1.15).

Следует отметить, что с помощью этого расширения зашифрованное соединение будет устанавливаться только с теми сайтами, которые поддерживают протокол HTTPS. Для за-

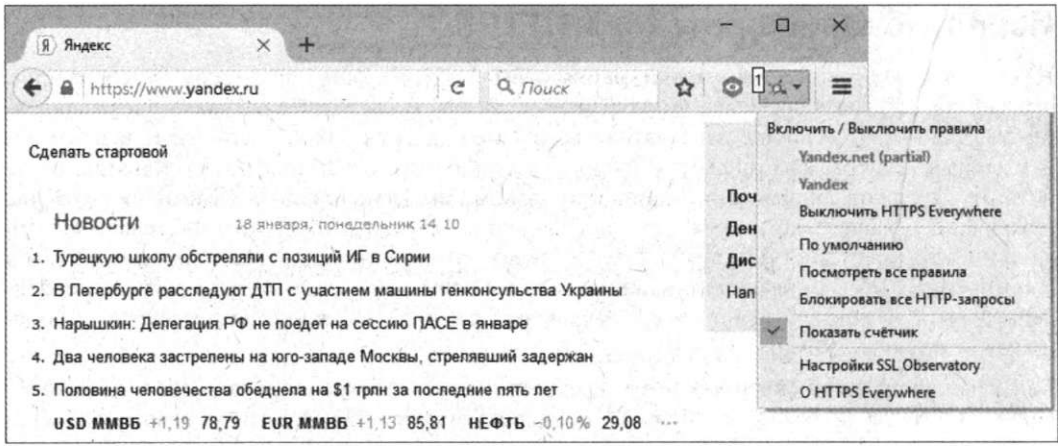


Рис. 1.15. Браузер Firefox с установленным расширением HTTPS Everywhere

шифрованной передачи данных между любыми сайтами следует использовать анонимные сети, такие как **Tor**, или операционную систему **Tails**.

Удаление истории посещений и cookie-файлов

Как известно, если вы работаете не в приватном режиме браузера, вся информация о ваших посещениях различных сервисов прописывается в cookie-файлах, сохраняются также временные файлы и журнал посещенных узлов. В дальнейшем, когда вы попадаете на некий сайт, сервер с помощью cookie-файлов с радостью вас узнает (помимо идентификации по IP-адресу): а, вот и вы, юзер *с*, логином `User12345678` и паролем `qwerty!` Еще одна опасность — этими же cookie-файлами может воспользоваться и злоумышленник, чтобы авторизоваться на сайте, особенно, если вы разрешили браузеру запоминать логины и пароли для тех или иных сайтов.

И вполне закономерно предположить, что, удалив временные файлы, историю посещений и cookie-файлы на своем компьютере, вы озадачите севшего после вас за компьютер другого пользователя (потенциального злоумышленника) вопросом, куда подевалась вся информация о ваших действиях[1]. Это очень простой и наивный способ, совершенно бессильный при серьезном (злоумышленника) подходе к делу, но, тем не менее, следует упомянуть и о нем.

Браузер Internet Explorer

Удалить временные файлы, журнал посещенных узлов и cookie-файлы в браузере Internet Explorer можно так:

1. В окне браузера нажмите сочетание клавиш <Ctrl>+<Shift>+<Delete>. Или же, нажав клавишу <Alt> для отображения строки меню, выберите команду меню Сервис | Удалить журнал обозревателя (Tools | Delete temporary files). В любом случае вы увидите диалоговое окно Удаление истории обзора (Delete temporary files) (рис. 1.16).

[1] **Разумеется, способ бесполезен, если предварительно на компьютер был установлен кейлогер — приложение, фиксирующее нажатия клавиш и записывающее весь текст, который вы набираете с клавиатуры. На этот случай рекомендуется использовать виртуальные клавиатуры, упомянутые ранее.**

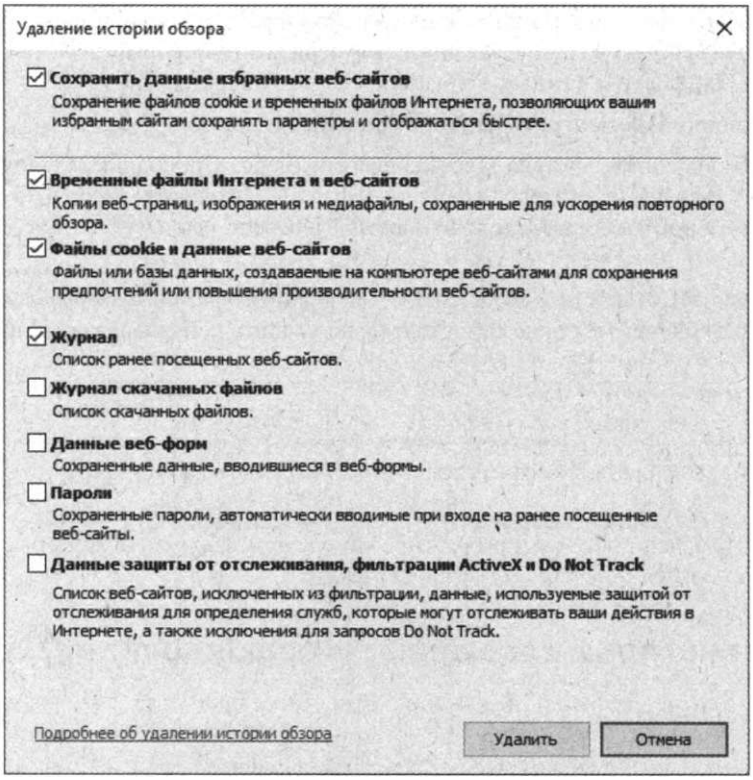


Рис. 1.16. Диалоговое окно **Удаление истории обзора**

Как видно из названий флажков в диалоговом окне, вы можете удалить самые различные данные.

2. Установите нужные флажки — например **Файлы cookie и данные веб-сайтов** (Cookie and website data) для удаления cookie-файлов, и нажмите кнопку **Удалить** (Delete) — все данные выбранных типов будут удалены.

Впрочем, это не самый лучший вариант, т. к. вы потеряете cookie-файлы, созданные для *всех* посещенных вами узлов Всемирной паутины.

> ***РЕЖИМ INPRIVATE***
>
> Процесс удаления cookie-файлов не актуален при работе в браузере в защищенном режиме InPrivate. В этом случае такие файлы, как и все временные объеюы, будут удалены по завершении сеанса работы с браузером и закрытии его окна.

Удалить только определенные cookie-файлы вы можете и вручную. Добраться до их хранилища можно двумя способами: из браузера Internet Explorer и указав путь к каталогу временных файлов Интернета в программе Проводник Windows. Подскажу оба.

Итак, из браузера Internet Explorer:

1. В правом верхнем углу окна Internet Explorer нажмите кнопку и выберите команду меню **Свойства браузера** (Browser settings). Можно также пройти и через основное меню: нажмите клавишу <Alt>, а затем выберите команду меню **Сервис | Свойства браузера** (Tools I Browser Options), — откроется соответствующее диалоговое окно.

2. В открывшемся диалоговом окне **Свойства браузера** (Browser settings) нажмите кнопку **Параметры** (Settings) в группе **Журнал браузера** (Browsing history) — откроется диалоговое окно **Параметры данных веб-сайта** (Settings temporary files).
3. Нажмите кнопку **Просмотреть файлы** (Show files).

Другой способ получения доступа к cookie-файлам (через Проводник Windows) состоит из одного шага — перейдите в каталог временных файлов Интернета, расположенный по адресу **C:\Users\UseAAppData\Local\Microsoft\Windows\INetCache,** где ***User***— имя вашей учетной записи.

В любом случае вы откроете окно с cookie- и прочими временными файлами веб-сайтов (рис. 1.17) — в открывшемся окне самостоятельно удалите ненужные cookie-файлы.

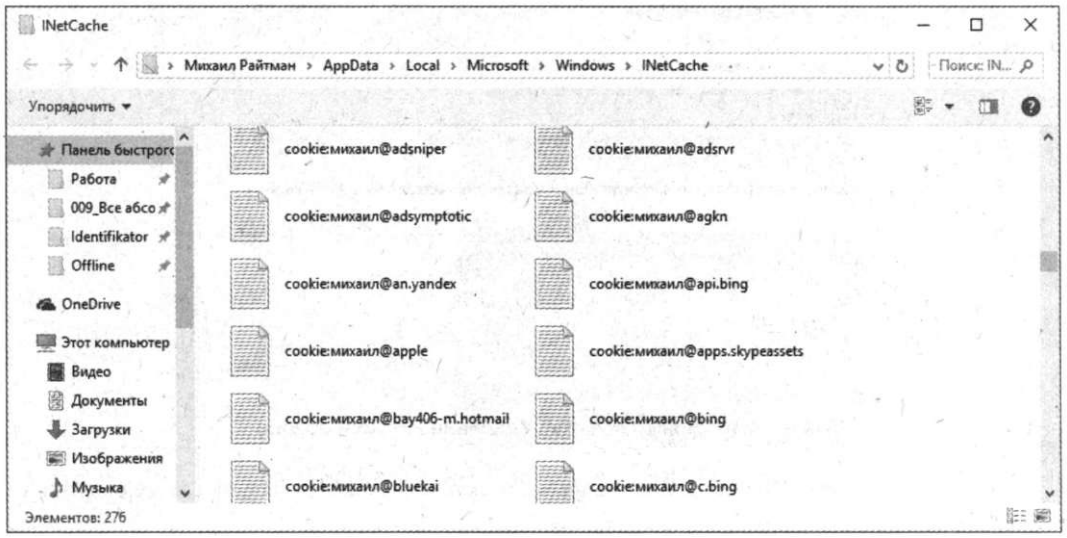


Рис. 1.17. Окно с содержимым каталога cookie-файлов

Вы также можете блокировать создание cookie-файлов на стадии просмотра того или иного веб-сайта, хотя это, возможно, приведет к неправильной работе ресурса. Выполняется такая настройка на вкладке **Конфиденциальность** (Privacy) диалогового окна **Свойства браузера** (Browser settings). Для этих целей предназначены кнопки **Сайты** (Sites) и **Дополнительно** (Advanced):

- кнопка **Дополнительно** открывает диалоговое окно, в котором вы можете задать способ обработки cookie-файлов *всех* веб-узлов, отменив автоматический процессинг;
- заблокировать или же, наоборот, разрешить процесс обработки именно ***выбранных*** узлов в обход политик конфиденциальности вы сможете в диалоговом окне, открывающемся нажатием кнопки **Сайты** (Sites).

Браузер Microsoft Edge

Удалить временные файлы, журнал посещенных узлов и cookie-файлы в браузере Microsoft Edge можно так:

1. В окне браузера нажмите сочетание клавиш <Ctrl>+<Shift>+<Delete>. Или же, нажав кнопку для отображения панели, на вкладке **Журнал** (History) щелкните мышью по

ссылке **Очистка всех журналов** (Clear all history). **В** любом случае вы увидите панель, показанную на рис. 1.18.

Как видно из названий флажков в диалоговом окне, вы можете удалить самые различные данные.

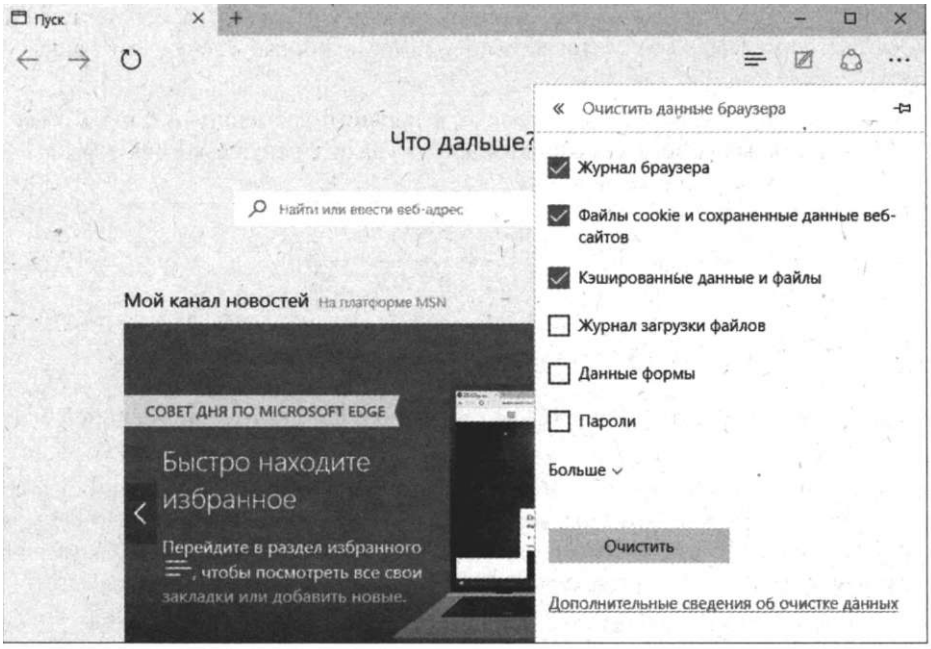


Рис. 1.18. Панель удаления данных в браузере Edge

2. Установите нужные флажки — например, **Файлы cookie и сохраненные данные веб-сайтов** (Cookie and website data) для удаления cookie-файлов, и нажмите кнопку **Очистить** (Clear) — все данные выбранных типов будут удалены.

Браузер Mozilla Firefox

Для браузера Firefox cookie-файлы хранятся в виде базы данных SQL Lite в файле cookie.sqlite, который находится в каталоге C:\Users\имя_вашей_учетной записи\AppData\Roaming\Mozilla\Firefox\Profiles\набор_символов. Журнал посещенных узлов хранится в той же папке, в файле places.sqlite.

В браузере Firefox cookie- и прочие файлы можно удалить следующим образом:

1. Нажав клавишу <Alt>, отобразите строку меню.
2. Выберите команду меню **Журнал | Удалить недавнюю историю** (History | Glear recent history) или же, нажав кнопку , выберите пункт **Журнал** (History), а затем **Удалить историю** (Clear history). Можно использовдть и сочетание клавиш <Ctrl>+<Shift>+ +<Delete>. Откроется диалоговое окно **Удаление недавней истории** (Clear recent history) (рис. 1.19).
3. Установите нужные флажки, например **Куки** (Cookie), и выберите диапазон времени в раскрывающемся списке **Удалить** (Time range to clear).

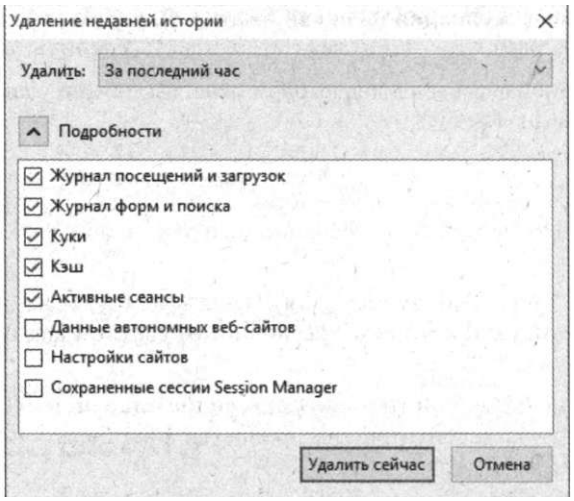


Рис. 1.19. Диалоговое окно **Удаление недавней истории**

4. Нажмите кнопку **Удалить сейчас** (Clear now) — все файлы выбранных типов будут удалены.

Минус этого метода опять же в том, что вы удалите cookie-файлы, созданные для *всех* посещенных узлов Всемирной паутины в выбранный промежуток времени. Но вы можете и вручную удалить cookie-файлы только определенных сайтов — для этого в браузере Firefox предназначено отдельное диалоговое окно. Чтобы попасть в него:

1. Нажав клавишу <Alt>, отобразите строку меню.
2. Выберите команду меню **Инструменты | Настройки** (Tools | Options) — откроется страница настроек браузера.
3. Перейдите на вкладку **Приватность** (Privacy) и щелкните мышью на ссылке **Удалить отдельные cookie** (Remove individual cookie) (рис. 1.20, *слева*) — откроется диалоговое окно **Куки** (Cookie) (рис. 1.20, *справа).*

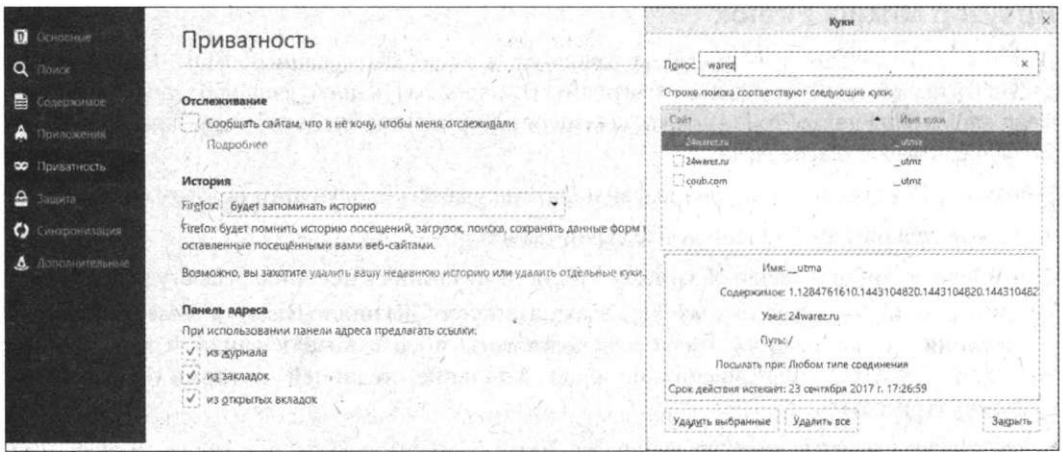


Рис. 1.20. Вкладка **Приватность** страницы настроек браузера и диалоговое окно **Куки**

4. Посредством поиска или прокрутки списка сайтов найдите ресурс, cookie-файлы которого нужно удалить, выделите их и нажмите кнопку **Удалить выбранные** (Remove selected).
5. Нажмите кнопку **Закрыть** (Close).

Браузер Opera

В браузере Opera временные файлы, журнал посещенных узлов и cookie-файлы можно удалить следующим образом:

1. Выберите команду меню **Opera | История** (Opera | History) и на открывшейся вкладке нажмите кнопку **Очистить историю посещений** (Clear browsing data) — откроется одноименная панель (рис. 1.21).
2. В раскрывающемся списке **Уничтожить следующие элементы** (Obliterate the following items from) укажите, за какой период времени должны быть уничтожены временные файлы, включая cookie.
3. Установите нужные флажки — например, **Удалить cookie и прочие данные сайта** (Delete cookie and other site data).

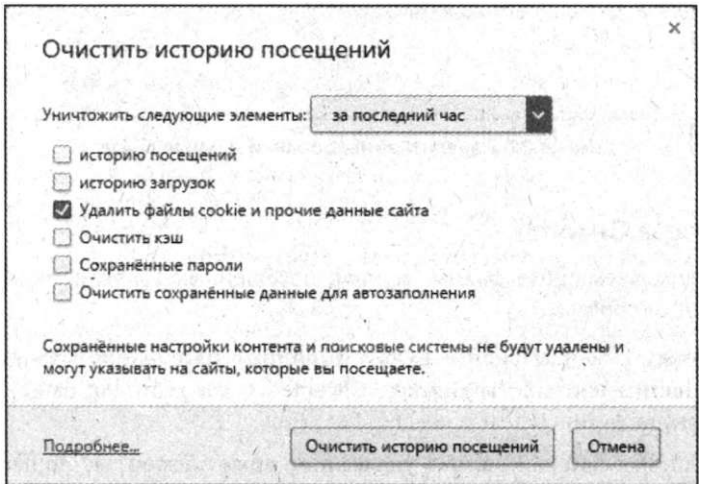
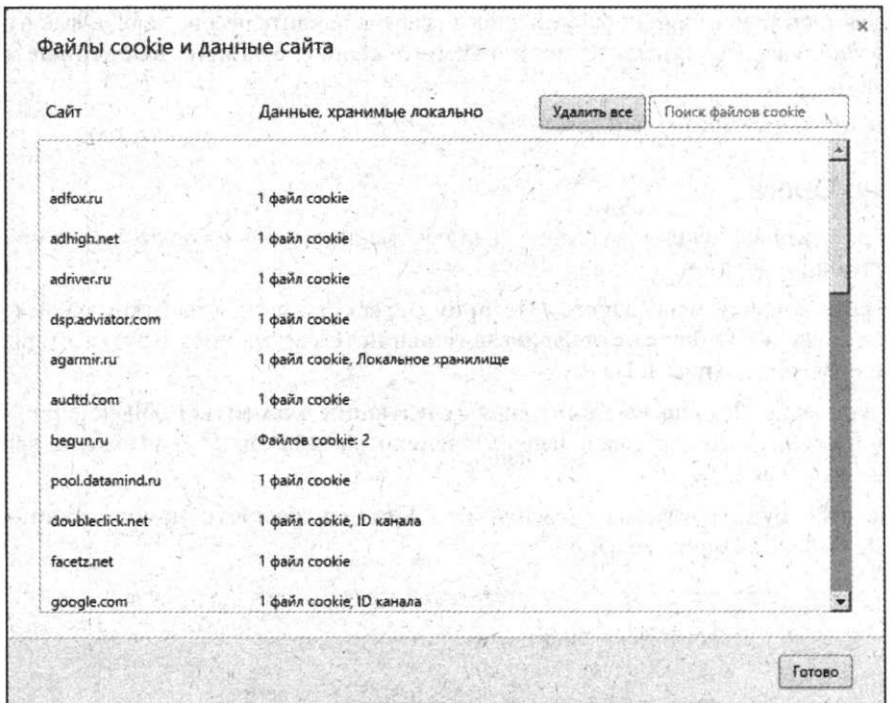


Рис. 1.21. Панель Очистить историю посещений

4. Нажмите кнопку **Очистить историю посещений** (Clear browsing data) — файлы выбранных типов будут удалены.

Для расширенного управления cookie-файлами следует выполнить следующие действия:

1. Выберите команду меню **Opera | Настройки** (Opera | Preferences) — откроется вкладка **Настройки** (Preferences).
2. В разделе **Файлы cookie** (Cookie) нажмите кнопку **Все cookie и данные сайта** (All cookie and site data) — откроется панель **Файлы cookie и данные сайта** (Cookie and site data) (рис. 1.22).
3. Чтобы удалить или изменить конкретную запись cookie, раскройте соответствующую веб-сайту группу и, выделив нужную строку, нажмите кнопку **Удалить** (Delete). Вы также можете удалить все cookie-файлы выделенного сайта, щелкнув мышью по значку x.



1. Нажмите кнопку  и выберите пункт **Дополнительные инструменты | Удаление данных о просмотренных страницах** (Chrome | Clear browsing data) — откроется панель **Очистить историю** (Clear browsing data) (рис. 1.23).
2. В раскрывающемся списке **Удалить указанные ниже элементы** (Obliterate the following items from) укажите, за какой период времени должны быть уничтожены временные файлы, включая cookie.
3. Установите нужные флажки — например, **Файлы cookie, а также другие данные сайтов и плагинов** (Delete cookie and other site and plug-in data).
4. Нажмите кнопку **Очистить историю** (Clear browsing data) — файлы выбранных типов будут удалены.

Для расширенного управления cookie-файлами следует выполнить следующие действия:

1. Перейдя по адресу **chrome://settings/,** нажмите кнопку **Настройки контента** (Content settings) в группе элементов управления **Личные данные** (Privacy) на странице настроек — откроется панель **Настройки контента** (Content settings).
2. В разделе **Файлы cookie** (Cookie) нажмите кнопку **Все файлы cookie и данные сайтов** (All cookie and site data) — откроется панель **Файлы cookie и данные сайта** (Cookie and site data) (рис. 1.24).

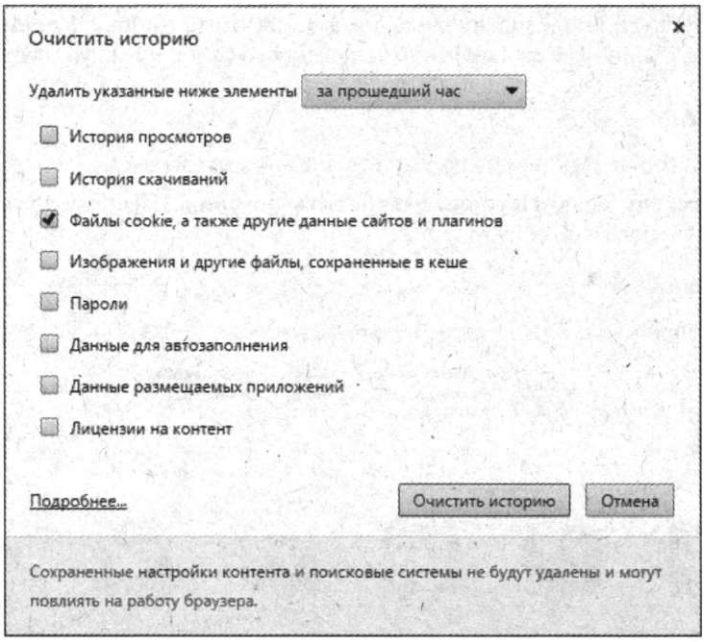


Рис. 1.23. Панель Очистить историю

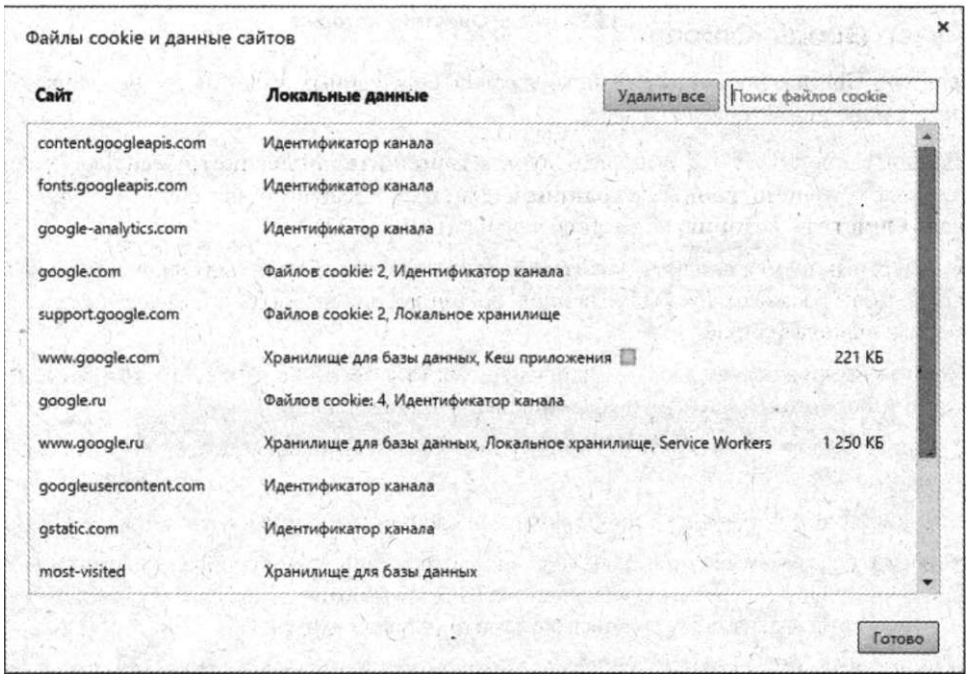


Рис. 1.24. Панель Файлы cookie и данные сайта

3. Чтобы удалить или изменить конкретную запись cookie, раскройте соответствующую веб-сайту группу и, выделив нужную строку, нажмите кнопку **Удалить** (Delete). Вы также можете удалить все cookie-файлы выделенного сайта, щелкнув мышью по значку x.

Браузер Safari

В браузере Safari cookie-файлы можно удалить следующим образом:

1. Выберите команду меню **История | Очистить историю** (History | Clear History)— откроется панель, показанная на рис. 1.25.

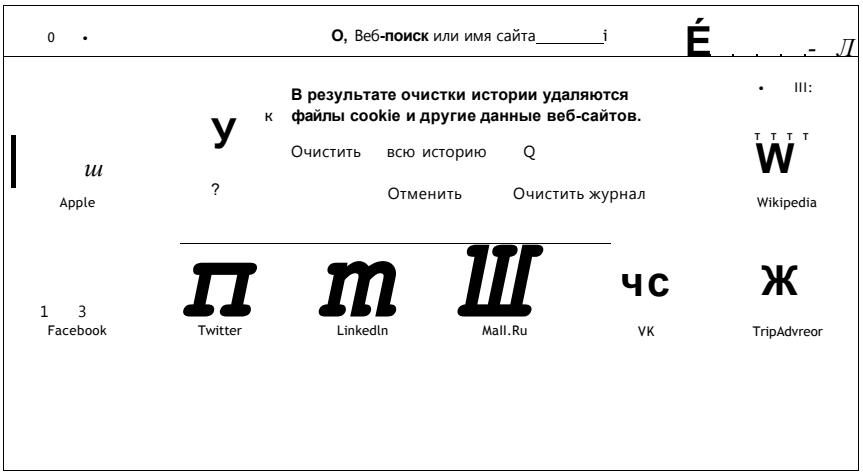


Рис. 1.25. Панель Очистить историю

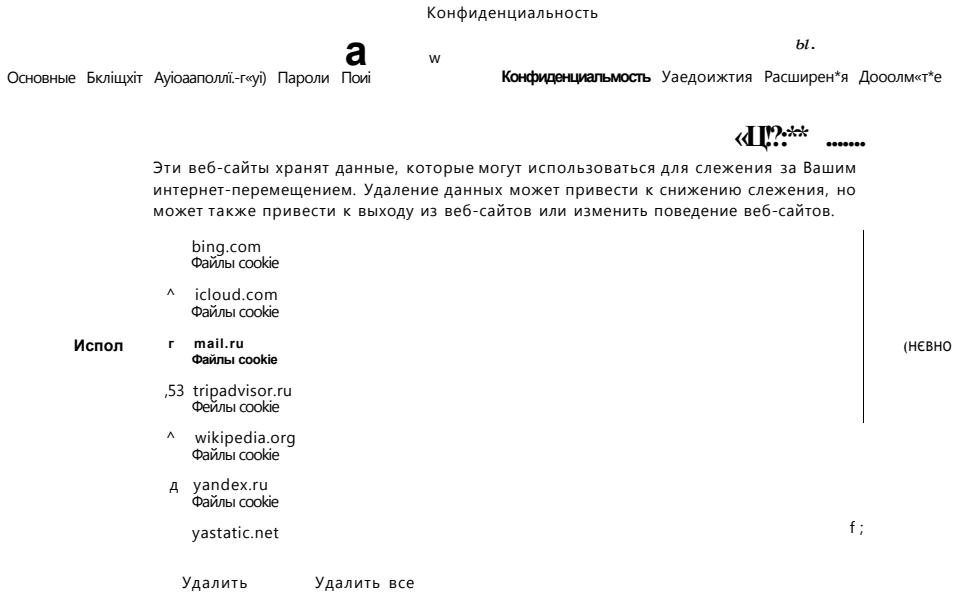


Рис. 1.26. Панель для управления данными сайтов в браузере Safari

2. В раскрывающемся списке Очистить (Clear history from) укажите, за какой период времени должны быть уничтожены временные файлы, включая cookie.
3. Нажмите кнопку Очистить журнал (Clear history) — временные файлы, журнал посещений и cookie-файлы за выбранный период времени будут удалены.

Для расширенного управления cookie-файлами следует выполнить следующие действия:

1. Выберите команду меню Safari | Настройки (Safari | Settings).
2. Перейдите на вкладку Конфиденциальность (Privacy) и нажмите кнопку Подробнее (Details) — откроется панель, показанная на рис. 1.26.
3. Выберите записи (адреса сайтов), которые требуется удалить, и нажмите кнопку Удалить (Remove). Или удалите все cookie-файлы, нажав кнопку Удалить все (Remove all).

Мобильные браузеры

Базовыми возможностями по удалению временных файлов, журнала посещенных узлов и cookie-файлов обладают и браузеры на мобильных устройствах, таких как смартфоны и планшеты. Для мобильных устройств существует множество браузеров, как встроенных, так и сторонних разработчиков, поэтому описывать каждый из них смысла нет, тем более, что принцип удаления временных и cookie-файлов у них схож. Так, на устройствах под управлением операционной системы iOS необходимо перейти на экран Настройки (Settings) и в разделе Safari коснуться пункта Очистить историю и данные сайтов (Clear History and Website Data) (рис. 1.27, *слева).*

В операционной системе Windows Phone удаление временных файлов производится на экране Настройки | Internet Explorer (Settings | Internet Explorer). Для этого служит кнопка Удалить журнал (Delete History) (рис. 1.27, *справа).*



Рис. 1.27. Удаление временных файлов в браузере Safari (iOS) *(слева)* **и в Internet Explorer (Windows Phone)** *(справа)*

На устройствах под управлением операционной системы Blackberry OS откройте меню и выберите пункт **Настройки** (Settings). Затем, перейдя в раздел **Конфиденциальность и безопасность** (Privacy and Security), нажмите кнопку **Функция закрытого просмотра** (Private Browsing) в активное положение (см. рис. 1.14, *справа).*

Браузер, встроенный в операционную систему, содержит кнопку •••, нажав которую и перейдя к настройкам браузера, необходимо открыть раздел персональных данных и нажать кнопку **Очистить историю** (Clear History).

Инструкции для других браузеров вы найдете по адресу **tinyurl.com/zuv31jr.**

ГЛАВА 2

Надежные пароли и двухфакторная авторизация

Выбор надежных паролей

О «секретных вопросах»

Менеджеры паролей

Многофакторная аутентификация и одноразовые пароли

Создание второстепенных аккаунтов

Если вы много времени проводите во Всемирной паутине, то, скорее всего, зарегистрировали на различных веб-сайтах множество аккаунтов. При этом, если вы используете для них один и тот же пароль (или почти такой же, с небольшими вариациями), ваши аккаунты уязвимы к кибератакам. Ведь если хотя бы один из этих веб-сайтов будет взломан, злоумышленники получат доступ к паролям всех его пользователей, а значит, смогут взломать ваши учетные записи и на других сайтах. Такие взломы случаются чаще, чем вы думаете, и зачастую администраторы взломанных веб-сайтов даже не подозревают о произошедшем. Поэтому в целях обеспечения собственной безопасности следует использовать для своих учетных записей надежные и сложные пароли, и, что немаловажно, различные для разных веб-сайтов. Разумеется, такие пароли сложно запомнить, и можно воспользоваться одним из следующих методов:

- **записывать пароли на бумагу** — весьма практично записывать пароли и хранить эти записи в безопасном месте (например, в сейфе или в бумажнике). Вы, как минимум, заметите, если такие записи будут потеряны или украдены, и оперативно смените все пароли;
- **использовать менеджер паролей** — программу для смартфона, планшета или компьютера, которая позволяет создавать, безопасно хранить и даже автоматически подставлять уникальные пароли при авторизации на веб-сайтах и в онлайн-приложениях (см. далее *разд. «Менеджеры паролей»*). Менеджеры паролей также обеспечивают и синхронизацию вашей парольной базы между принадлежащими вам устройствами. Обратите внимание, что менеджеры паролей требуют наличия *мастер-пароля,* после ввода которого вы сможете получить доступ ко всем остальным своим паролям. Мастер-пароль должен быть особенно надежным, но легко запоминаемым, т. к. это единственный пароль, который вы не сможете хранить в менеджере паролей и который понадобится каждый раз при запуске программы (см. далее *разд. «Использование мастер-пароля»*).

Выбор надежных паролей

Существуют несколько паролей, которые все же придется запомнить и которые должны быть действительно надежными. К ним относятся, как минимум, пароли от ваших устройств, пароли для шифрования диска (в том числе и полного) и мастер-пароль от менеджера паролей.

Подобрать пароль из десяти символов — не проблема для мощного современного компьютера. Поэтому короткие пароли, даже составленные из совершенно случайных символов, — например, такие: **a$ct7W.p9!, UTcdp-гE** или **xc,u&Hq1Y {** и им подобные, — недостаточно надежны для использования в шифруемых системах.

Способов создания надежных и легко запоминаемых паролей много. Самым простым и безотказным считается метод Diceware, разработанный Арнольдом Рейнхольдом. В методе Рейнхольда пользователь физически кидает игральные кости, чтобы случайным образом выбрать несколько слов из списка. Выбранные слова образуют парольную фразу. Для шифрования диска (и для менеджера паролей) рекомендуется выбрать как минимум шесть слов. На методе Рейнхольда основан ряд программ выбора паролей, существуют также использующие его онлайн-генераторы паролей — например, здесь: **tinyurl.com/hdub86x.**

При использовании менеджера паролей безопасность всех паролей (включая мастер-пароль) напрямую зависит от безопасности вашего компьютера. Если он заражен вредоносной программой, то может перехватить мастер-пароль во время набора или скопировать содержимое базы паролей. Поэтому очень важно защитить и компьютер, и другие ваши устройства от вредоносных программ (см. *главы 3* и *4).*

О «секретных вопросах»

Важно кое-что знать и о «секретных вопросах» — таких как «Девичья фамилия вашей матери?» или «Кличка вашего первого питомца?». На веб-сайтах подобные вопросы используются для восстановления пароля. Существующий пароль, новый или ссылка для генерации нового пароля (зависит от веб-сайта, на котором восстанавливается пароль) будет отправлен на указанный вами адрес электронной почты.

Однако правильные ответы на многие секретные вопросы злоумышленник может легко найти в открытом доступе (например, в аккаунтах социальных сетей) и с их помощью подменить пароль и получить доступ к вашей учетной записи. Поэтому рекомендуется на «секретные вопросы» указывать выдуманные ответы (которые, как и пароли, не знает никто, кроме вас).

> ***ВНИМАНИЕ!***
>
> **Не используйте один и тот же пароль или секретный вопрос для нескольких учетных записей и для разных веб-сайтов или сервисов.**

Ваши выдуманные ответы на секретные вопросы также рекомендуется хранить в менеджере паролей. Периодически секретные вопросы и ответы на них можно менять.

Менеджеры паролей

Запомнить много разных паролей для авторизации на различных сайтах и в программах сложно. Поэтому люди часто задают всего несколько или даже один пароль для самых разных учетных записей, сайтов и сервисов. В результате один и тот же пароль используется

десятки и даже сотни раз. Повторное использование паролей — прямая угроза для безопасности данных. Если какой-либо ваш пароль попал в руки злоумышленника, тот, скорее всего, попробует его для доступа и к другим вашим учетным записям. Поэтому для обеспечения безопасности *никогда не используйте пароли повторно.*

Но тут возникает проблема — как запоминать многочисленные пароли, если они существенно отличаются друг от друга? Решить эту проблему помогают программы, называемые *менеджерами паролей.* Они позволяют безопасно хранить неограниченное количество паролей и защищают все ваши пароли для разных учетных записей при помощи одного мастер-пароля (в идеале — парольной фразы). Вам будет достаточно запомнить эту единственную фразу (пароль), а остальную работу по созданию и хранению всех прочих паролей возьмет на себя программа.

Менеджеры паролей помогают выбирать надежные пароли. Это крайне важно. Неопытные пользователи часто применяют короткие, простые пароли, которые легко угадать злоумышленнику: password1, qwerty, 12345, дату рождения, имя друга (супруга), кличку животного и тому подобное (см. также табл. 1.1 в *главе 1).* А вот менеджер паролей позволяет создавать и использовать случайные пароли без прослеживаемого стиля или структуры. Такой пароль, например: mdD50*dfjQ32/dfR4$vH0 (s! — невозможно отгадать.

Несмотря на все преимущества, у менеджеров паролей есть один существенный недостаток — все пароли хранятся в одном файле или группе файлов, расположенных в одном месте диска компьютера. Это очевидная цель для злоумышленников.

Рекомендуется также создавать резервные копии файла (файлов), хранящего пароли. Если этот файл будет утерян из-за сбоя или кражи устройства, восстановить пароли может оказаться очень сложно, а в некоторых случаях и невозможно. Менеджеры паролей обычно обеспечивают функционал сохранения резервных копий, но вы можете использовать и собственные средства резервного копирования.

При выборе менеджера паролей учитывайте также, что многие популярные программы этого назначения имеют уязвимости. Поэтому, решая, подходит ли вам тот или иной инструмент, невредно посмотреть имеющиеся о нем в Интернете отзывы и рекомендации специалистов. Со своей же стороны считаю возможным упомянуть в качестве примера менеджера паролей бесплатную программу KeePassX (см. далее *разд. «Менеджер паролей КееРаввХ»).*

Использование мастер-пароля

Мастер-пароль играет роль кода, открывающего сейф (базу данных паролей), — без него невозможно получить доступ к паролям.

- **Мастер-пароль защищает все ваши пароли, поэтому он должен быть надежным!**

  Надежность мастер-пароля обеспечивается его длиной и сложностью. Создавая мастер-пароль, нет надобности озабочиваться присутствием в нем специальных символов, прописных букв или цифр, — парольная фраза из шести случайных слов (в нижнем регистре с пробелами) может быть более устойчивой ко взлому, чем 12-символьный пароль из смеси прописных и строчных букв, цифр и специальных символов.

- **Мастер-пароль необходимо запомнить!**

  Мастер-пароль обеспечивает доступ ко всем остальным вашим паролям, поэтому нужно запомнить его, не записывая. Это еще один аргумент в пользу метода Рейнхольда, использующего ряд простых, легко запоминаемых слов вместо неестественных комбинаций символов, цифр и прописных букв.

Использование файла-ключа

В качестве альтернативы мастер-паролю (парольной фразе) для шифрования базы паролей можно использовать *файл-ключ.* Тогда каждый раз, когда необходимо открыть базу паролей, нужно будет указывать менеджеру паролей путь к файлу-ключу. Этот файл можно хранить на Flash-накопителе или на другом портативном устройстве, подключая его к компьютеру только для доступа к базе паролей. И если злоумышленник получит доступ к жесткому диску вашего компьютера и, соответственно, к базе паролей, он не сможет расшифровать ее, не имея файла-ключа, который хранится у вас на внешнем носителе. Более того, во многих случаях взломщику гораздо сложнее найти файл-ключ, чем подобрать обычный пароль.

Недостаток этого способа в том, что для доступа к паролям всякий раз придется подключать внешний носитель. А в случае утери или повреждения этого носителя вы утратите доступ к своим паролям.

Так что, если вы решите использовать файл-ключ вместо мастер-пароля, убедитесь, что используемый Flash-накопитель физически надежен (невредно иметь и хранящийся отдельно его дубликат) и хранится в безопасном месте, — если злоумышленник его найдет, то сможет получить доступ к вашей базе паролей.

Комбинация мастер-пароля и файла-ключа

Самый безопасный метод шифрования базы паролей — использовать и мастер-пароль, и файл-ключ одновременно. Тогда для вскрытия базы злоумышленнику нужно будет *знать* мастер-пароль и *иметь* файл-ключ. К этому варианту шифрования следует подходить с учетом степени угрозы утечки данных. Большинству обычных пользователей, которые хотят безопасно хранить свои пароли, будет вполне достаточно сложного мастер-пароля. Если же потенциальный злоумышленник обладает огромными вычислительными мощностями, лучше выбирать самое безопасное решение.

Синхронизация паролей между несколькими устройствами

Скорее всего, вы используете для ввода своих логинов и паролей на тех или иных вебсайтах или в сервисах более чем одно устройство — например, и компьютер, и смартфон, и планшет. Учитывая это, многие менеджеры паролей имеют встроенную функцию синхронизации файла хранилища паролей между различными устройствами пользователя. И после выполнения такой синхронизации вы можете пользоваться своими паролями на всех своих устройствах. То есть, добавив новую учетную запись в менеджер паролей на компьютере, вы сможете войти в нее и со смартфона, и с планшета. Некоторые менеджеры паролей позволяют хранить базу паролей «в облаке» — в зашифрованном виде на удаленном сервере. Менеджеры паролей, которые используют собственные серверы для хранения паролей и обеспечивают синхронизацию данных, удобны, но имеют недостаток — они более уязвимы к атакам, т. к. злоумышленник может взломать их сервер. Если же вы храните пароли только на своем компьютере, то злоумышленник должен сначала получить доступ к компьютеру и лишь затем к паролям.

Менеджер паролей KeePassX

KeePassX — замечательный инструмент. Эта программа позволяет организовать хранение всех паролей в одном месте, а также использовать устойчивые ко взлому пароли без необходимости их запоминать. Вам нужно будет помнить лишь один мастер-пароль, который служит для доступа к базе остальных паролей.

Загрузите дистрибутив программы KeePassX с сайта **keepassx.org/downloads** — там доступны версии программы как для операционной системы Windows, так и для OS X. Программа не требует установки — достаточно распаковать в какую-либо папку архив с файлами приложения.

Напомню, что программа KeePassX хранит добавленные пароли в зашифрованном виде в базе данных. Доступ к зашифрованной базе паролей может быть защищен тремя способами: мастер-паролем, файлом-ключом и с применением обоих способов одновременно.

1. После завершения установки запустите программу KeePassX. В меню **Хранилище** (Database) выберите пункт **Новое хранилище** (New Database) — откроется диалоговое окно с запросом ввода мастер-пароля и/или использования файла-ключа (рис. 2.1).

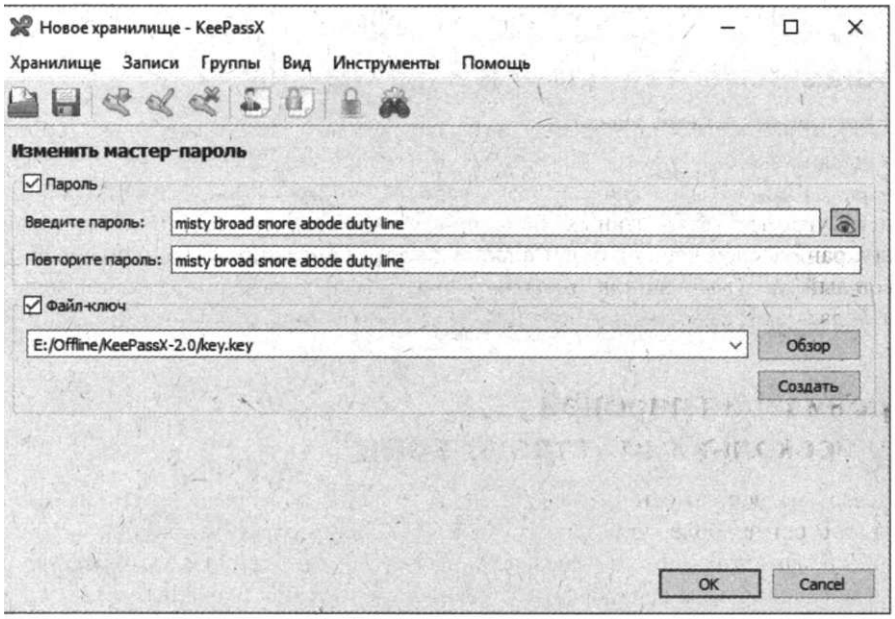


Рис. 2.1. Первичная настройка программы KeePassX

2. Установите один или оба флажка на выбор. Если вы хотите видеть пароль во время его ввода, нажмите кнопку в правой части окна программы.

   В качестве файла-ключа можно использовать любой существующий файл — например, фотографию вашей кошки (можно также создать новый файл-ключ нажав кнопку **Создать).** Обратите внимание, что выбранный файл не должен изменяться! Если содержимое файла изменится, он станет непригодным для расшифровки вашей базы паролей (перемещение файла и смена его имени роли не играют).

3. Создав базу паролей, нужно ее сохранить. Для этого нажмите кнопку OK, а затем выберите команду меню Хранилище | Сохранить хранилище (Database | Save Database).

   Впоследствии вы можете переместить файл хранилища в любую другую папку на жестком диске и даже использовать ее на другом компьютере. В любом случае программа KeePassX сможет открыть этот файл, если, конечно, у вас есть мастер-пароль и/или файл-ключ.

Добавление паролей

Для создания нового или добавления имеющегося пароля выберите команду Записи | Добавить новую запись (Entries | Add New Entry). В открывшемся окне (рис.2.2) заполняют, как правило, следующие поля:

- в поле Заголовок (Title) введите описательное название, по которому легко узнать, к какому веб-сайту или программе относится добавляемый пароль;
- в поле Имя пользователя (Username) укажите имя пользователя (логин), соответствующее паролю (поле можно оставить пустым, если имя пользователя не используется);

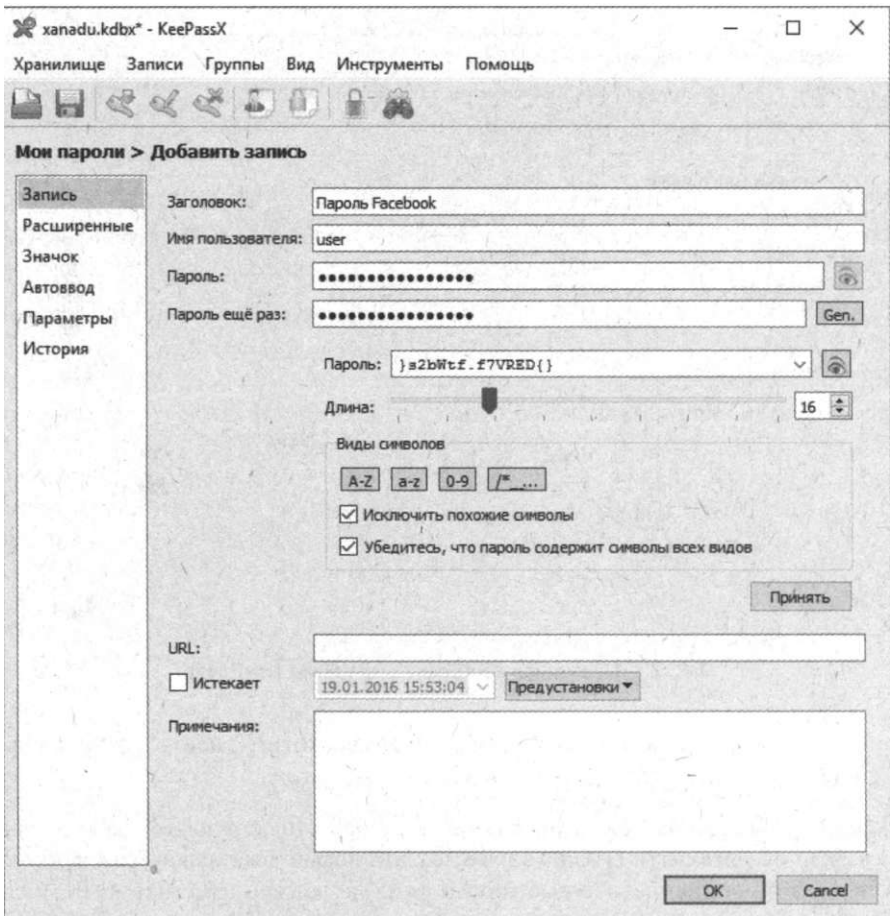


Рис. 2.2. Добавление пароля в программе KeePassX

- в поле **Пароль** (Password) указывается пароль. Если вы создаете новый пароль (например, регистрируетесь на новом сайте и хотите создать новый, уникальный, сгенерированный случайным образом пароль), нажмите кнопку **Gen.** справа от поля ввода, — отобразятся элементы управления генератора паролей (см. рис. 2.2). Здесь доступно несколько настроек, включая ползунковый регулятор длины пароля и кнопки видов символов, которые программа должна использовать для его создания.

  ОРГАНИЗАЦИЯ ПАРОЛЕЙ

  Программа KeePassX позволяет «разложить» пароли по группам по аналогии с папками. Для этого служат команды меню Группы (Groups), а также панель в левой части окна программы. Группирование паролей не влияет на функциональность программы KeePassX.

  При создании случайного пароля запоминать его нужды нет — программа KeePassX сохранит его и каждый раз, когда вам понадобится его ввести, позволит скопировать и вставить в соответствующее поле на сайте или в приложении. В этом и заключается основное преимущество менеджера паролей: вы можете использовать разные, длинные, сгенерированные случайным образом пароли для *каждого* веб-сайта/сервиса, без необходимости запоминать их или записывать на бумагу.

  Если сгенерированный пароль вас устраивает, нажмите кнопку **Принять** (Apply) — пароль будет автоматически вставлен в йоля **Пароль** (Password) и **Пароль ещё раз** (Repeat). Если же вы добавляете уже существующий пароль, его нужно будет повторно ввести в поле **Пароль ещё раз** (Repeat) вручную.

- После нажатия кнопки OK новый пароль будет добавлен в базу данных (хранилище). Не забудьте сохранить ее, выбрав команду меню **Хранилище | Сохранить хранилище** (Database | Save Database). Если вы не сделаете этого, после перезапуска программы все изменения будут утеряны.

Чтобы изменить сохраненный пароль, следует двойным щелчком щелкнуть мышью на его названии в правой части окна.

СОХРАНЕНИЕ ИЗМЕНЕНИЙ В KEEPASSX

Программа KeePassX не сохраняет изменения автоматически. Если вы создали в программе KeePassX пароли, не успели сохранить изменения, а работа программы прервалась из-за сбоя, добавленные пароли будут утрачены. Вы можете изменить это поведение в настройках программы KeePassX.

Использование паролей

Чтобы воспользоваться паролем из базы программы KeePassX:

1. Щелкните правой кнопкой мыши на записи и выберите в контекстном меню (рис. 2.3) команду **Скопировать имя пользователя** (Copy Username to Clipboard) или **Скопировать пароль** (Copy Password to Clipboard).

   Также можно использовать сочетания клавиш: <Ctrl>+<B> — для копирования имени пользователя (логина) или <Ctrl>+<C> — для. копирования пароля.

2. Перейдите к окну программы или веб-сайту, где следует ввести имя пользователя и/или пароль. Вставьте скопированный текст в соответствующее поле, нажав сочетание клавиш <Ctrl>+<V>.

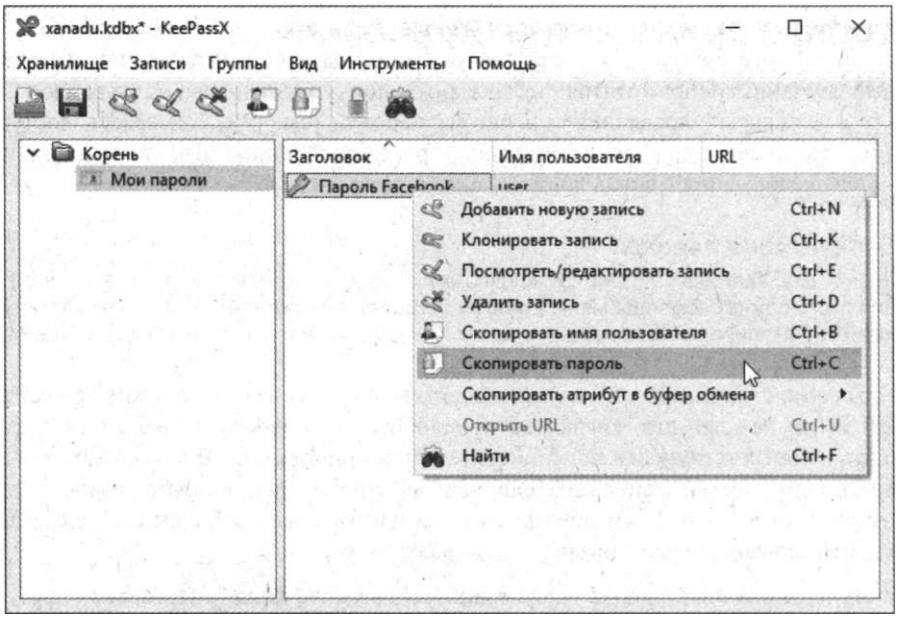


Рис. 2.3. Контекстное меню записи пароля в программе KeePassX

Дополнительные функции

В базе паролей программы KeePassX можно искать данные. Для этого нажмите кнопку Найти (Find), введите текст запроса в появившееся поле окна программы и нажмите клавишу <Enter>. Кроме того, записи можно сортировать, нажимая на заголовки столбцов в главном окне.

Можно «заблокировать» хранилище, выбрав команду меню Хранилище | Закрыть хранилище (Database | Close Database). Чтобы снова получить доступ к паролям, нужно будет ввести мастер-пароль (и/или указать путь к файлу-ключу).

Можно также настроить программу на автоматическую блокировку хранилища через определенное время простоя. Это пригодится, чтобы злоумышленники не имели доступа к паролям во время вашего отсутствия. Чтобы активировать функцию автоматической блокировки, выберите команду меню Инструменты | Настройки (Extras | Settings), перейдите на вкладку Безопасность (Security), установите флажок Заблокировать хранилище после неактивности длительностью (Lock databases after inactivity of) и укажите значение в секундах в поле ввода со счетчиком.

Программа KeePassX позволяет сохранять в защищенном виде не только имена пользователей, но и пароли. Вы можете создавать в ней записи и для хранения другой важной информации — например, номеров и PIN/CVV-кодов банковских карт, серийных номеров программных продуктов и т. п. Информация, которую вы вводите в поле Пароль (Password), необязательно должна быть паролем, — записывайте туда любые важные данные, а поле Имя пользователя (Username) можно оставить пустым или записать туда какую-либо уточняющую информацию.

Многофакторная аутентификация и одноразовые пароли

В качестве дополнительных параметров защиты многие онлайн-сервисы и приложения применяют системы безопасности, основанные на многофакторной аутентификации и одноразовых паролях.

Принцип действия *двухфакторной (двухэтапной) аутентификации* заключается в том, что для успешной авторизации на сайте нужно иметь в руках определенный физический объект — как правило, мобильный телефон или токен безопасности (специальное USB- или автономное устройство) (рис. 2.4).



Рис. 2.4. Токены безопасности

Двухфакторная аутентификация защищает вашу информацию даже в том случае, если пароль был взломан или украден (если только злоумышленник не завладел физическим устройством или специальными кодами, которые оно генерирует). Это означает, что для получения полного доступа к вашей учетной записи злоумышленнику нужно завладеть как вашим компьютером, так и вашим смартфоном или токеном.

Чтобы включить двухфакторную аутентификацию на большинстве платформ, вам понадобится лишь мобильный телефон, способный получать SMS-сообщения.

Сам процесс включения зависит от используемой платформы, различается и терминология. В Facebook этот процесс называется «подтверждением входа» (tinyurl.com/lbjy62w), в Twitter — «проверкой входа» (tinyurl.com/pcf8mzx), а в Google — «двухэтапной аутентификацией» (tinyurl.com/obcr9ye). Указанные здесь ссылки действительны после авторизации на соответствующих сервисах.

Полный список сайтов, поддерживающих двухфакторную аутентификацию, доступен по адресу twofactorauth.org. Чтобы обезопасить свои персональные данные, рекомендуется согласно этому списку включить двухфакторную аутентификацию на всех важных веб-аккаунтах.

Настроить двухфакторную аутентификацию можно, только если ее поддерживает онлайн-сервис или приложение. Двухфакторная аутентификация может быть реализована несколькими способами:

- каждый раз, когда вы пытаетесь авторизоваться на новом устройстве, сервис отправляет на ваш телефон SMS-сообщение с дополнительным защитным кодом, который нужно ввести на сайте (рис. 2.5). Как вариант, на телефон может быть совершен голосовой вызов и код продиктован автоматизированной системой;

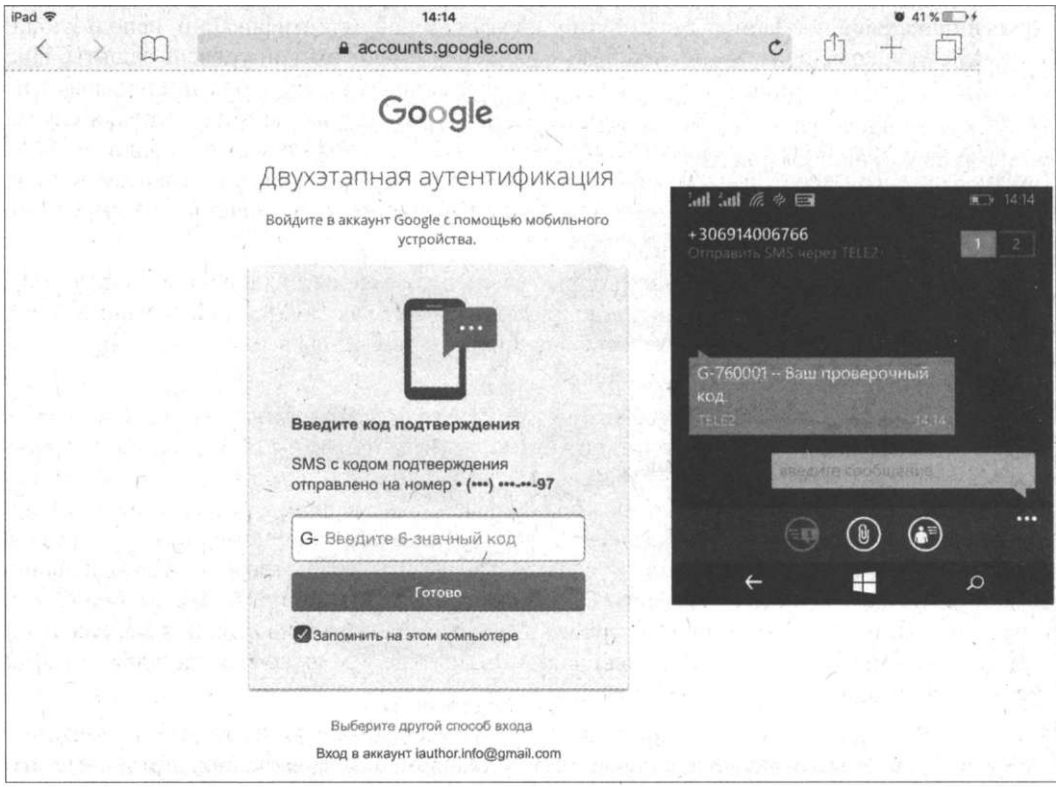


Рис. **2.5. Двухэтапная аутентификация на сайте Google — форма ввода кода** *(слева)* **и SMS-сообщение с кодом (***справа)*

- при каждой авторизации на новом устройстве вы запускаете на телефоне приложение аутентификации, которое генерирует защитный код;
- вы подключаете через USB-интерфейс (или используете автономный) брелок-токен, генерирующий защитный код, который требуется ввести, либо с которого нужно считать данные. На сайте Google, к примеру, используются токены стандарта FIDO U2F.

Некоторые сервисы (например, тот же Google) позволяют генерировать список *одноразовых паролей.* Даже если при вводе одноразового пароля шпионская программа его перехватит, злоумышленник не сможет использовать этот пароль в будущем. Пользователю же, после прохождения двухфакторной аутентификации, для входа в учетную запись понадобится ввести свой пароль и одноразовый пароль.

Хотя двухфакторная аутентификация и предлагает более безопасный способ входа в учетные записи, с ее использованием повышается риск того, что пользователи не смогут войти в свои аккаунты, например, в случае утери телефона, смены SIM-карты или выезда в другую страну, не включив роуминг. Во избежание этого многие поддерживающие двухфакторную аутентификацию сервисы позволяют создавать «резервные» списки кодов или коды «вос-

становления», при помощи которых вы всегда сможете разблокировать свою учетную запись. И если вы обеспокоены возможностью потери доступа к своему телефону или другому устройству аутентификации, вам необходимо распечатать список таких кодов и всегда носить его с собой. Помните, что хранить коды безопасности необходимо особенно бережно, не допуская доступа к ним третьих лиц.

Другой проблемой, связанной с системами двухфакторной аутентификации, использующими SMS-сообщения, является то, что SMS-сообщения имеют низкий уровень защиты. Продвинутый злоумышленник, имеющий доступ к телефонным сетям, теоретически может перехватить и использовать в своих интересах коды, отправляемые по SMS. Нередки случаи, когда злоумышленникам удавалось перенаправлять на свой телефон звонки и SMS-сообщения, предназначенные другим абонентам, или получать доступ к сервисам мобильного оператора, которые отображают текстовые сообщения, отправляемые на определенный номер телефона.

Если вы обеспокоены атаками такого уровня, отключите аутентификацию с помощью SMS-сообщений и используйте специальные приложения, такие как Google Authenticator и Authy. К сожалению, отключение SMS-аутентификации доступно не для всех сервисов, поддерживающих двухфакторную аутентификацию.

Более того, двухфакторная аутентификация требует от вас предоставления используемому сервису больше информации, чем вы, возможно, хотите. Допустим, для доступа к сервису Twitter вы используете псевдоним. И даже если вы тщательно скрываете от этого сервиса идентифицирующую вас информацию, подключаясь к нему через Tor или VPN, то при включении двухфакторной аутентификации через SMS-сообщения номер вашего телефона станет сервису известен. И если этот сервис будет когда-либо взломан, злоумышленник может узнать номер вашего телефона. Возможно, для вас это не проблема, особенно если вы уже используете в том или ином сервисе свое настоящее имя, но если для вас важно сохранять анонимность, вам надо дважды подумать, прежде чем включать где-либо двухфакторную аутентификацию через SMS-сообщения.

Также стоит отметить, что по данным проводимых исследований, некоторые пользователи упрощают свои пароли после включения двухфакторной аутентификации, считая, что второй фактор обеспечивает их безопасность. Не поддавайтесь такому соблазну и *обязательно выбирайте надежные пароли даже после включения двухфакторной аутентификации.*

Создание второстепенных аккаунтов

В конечном счете, у злоумышленников всегда есть как минимум один способ получения вашего пароля — они могут напрямую угрожать вам физической расправой. Если вы оцениваете эту угрозу как реальную, подумайте о том, как скрыть само существование данных или, защищенного паролем устройства. Например, можно зарегистрировать еще одну учётную запись и хранить там маловажную информацию, чтобы при необходимости, не задумываясь, выдать к ней пароль. При этом настройки ваших устройств не должны позволить злоумышленнику определить, что учетная запись, пароль от которой вы раскрыли, является «неосновной».

Отображается ли ваша основная учетная запись при входе в операционную систему компьютера? Может быть, автоматически открывается при запуске веб-браузера? Если это так, нужно изменить настройки, чтобы замаскировать вашу основную учетную запись.

ГЛАВА 3

Фишинговые атаки

Признаки фишинговой атаки

Защита от фишинговых атак

Фишинг — это вид интернет-мошенничества, целью которого является получение различной конфиденциальной информации. Наибольший интерес для мошенников представляют данные банковских карт и счетов, а также пароли и логины к различным платежным системам. Не брезгуют мошенники и данными, позволяющими получить доступ к учетным записям электронной почты, социальных сетей и систем обмена мгновенными сообщениями, а также и любыми прочими (номерами телефонов, данными регистрации и т. п.).

Признаки фишинговой атаки

Под понятием *фишинга* скрывается атака, при которой злоумышленник отправляет на первый взгляд безобидное электронное письмо или публикует ссылку (где угодно — например, в социальной сети или в чате), являющиеся на самом деле вредоносными. Фишинговые атаки являются распространенной формой заражения компьютеров вредоносными программами, которые скрывают свое присутствие на компьютере и могут быть использованы удаленно для управления зараженным компьютером, кражи информации или слежки за пользователем.

Злоумышленник, как правило, составляет фишинговое сообщение так, чтобы мотивировать пользователя открыть ссылку или вложенный файл, который может содержать вредоносный код. Для фишинга может также использоваться интернет-чат. Поэтому важно проверять ссылки, получаемые по электронной почте или в чате, — веб-адреса, указанные в электронных письмах, могут быть обманными. Так, представленный в письме веб-адрес может содержать ссылку на совершенно другой веб-сайт. И для того, чтобы увидеть настоящий прописанный в ссылке адрес, на нее необходимо навести указатель мыши.

Некоторые злоумышленники, чтобы нас одурачить, используют доменные имена, похожие на веб-адреса популярных сервисов: http://wwwmicrosoft.com/ и http://www.microsoft.com/ — это не одно и то же! Используются также и сокращенные URL-адреса. Поэтому, если вы получили сокращенный URL, — например, tinyurl.com/twitter, попробуйте проверить его реальный адрес при помощи сервиса checkshorturl.com.

Существует еще один способ обмана, при котором вы получаете ссылку на файл, якобы расположенный на сервисе типа Google Docs или Dropbox. Перейдя по этой ссылке, вы на

экране увидите аналог страницы входа на соответствующий сервис, предлагающий вам ввести свое имя пользователя и пароль. Но вполне возможно, что ссылка увела вас на поддельный сайт, содержащий похожую на настоящую копию страницы входа. Так что, если вы и перешли по ссылке, то, прежде чем вводить пароль, проверьте адресную строку своего веб-браузера — она отображает реальный адрес страницы. И если доменное имя не соответствует сайту, на который вы планировали войти, не продолжайте! Подставная веб-страница, как правило, выглядит очень похожей на настоящую (рис. 3.1), но не является ею на самом деле, а введенные на ней логин и пароль передаются мошенникам.

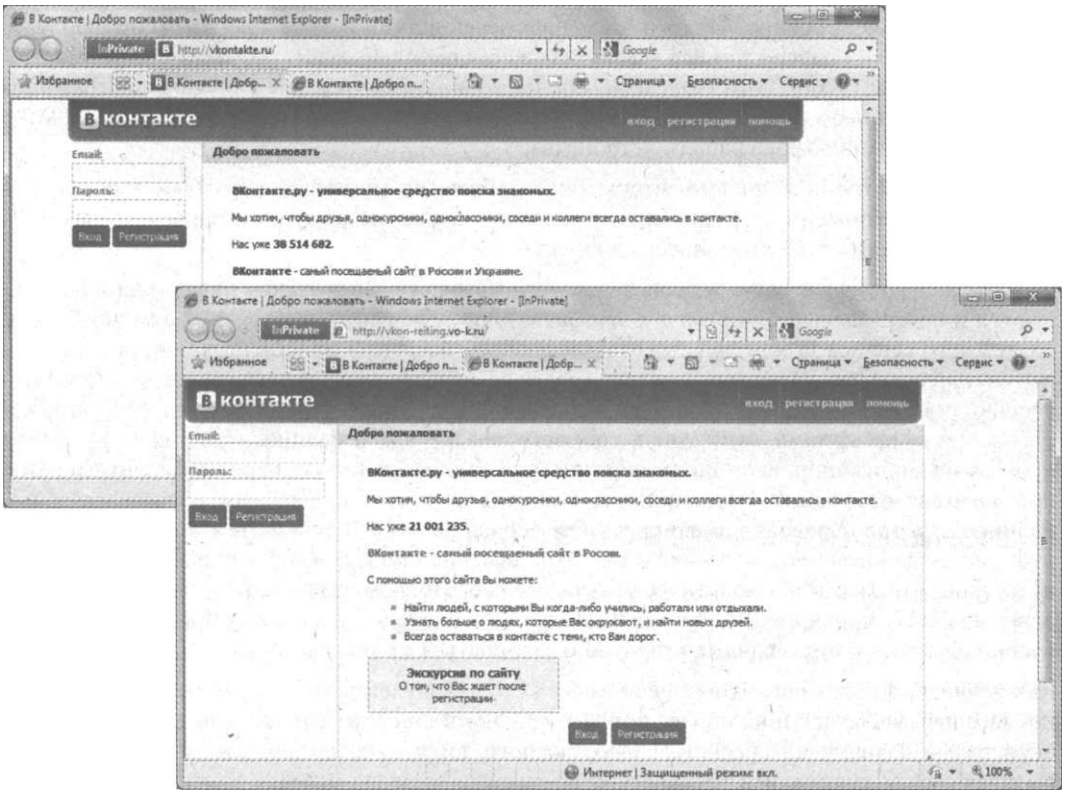


Рис. 3.1. Оригинальный сайт (*вверху*) и фишинг-сайт *(внизу)*

Помните, что наличие логотипа компании не гарантирует подлинность страницы — любой желающий может создать свою страницу и скопировать на нее подлинный логотип или дизайн, чтобы попробовать вас обмануть.

Используются в фишинговых схемах и психологические методы — например, пользователь получает письмо якобы от администрации почтового сервиса, в котором сообщается, что в связи с техническими проблемами была повреждена основная база данных сервиса, и теперь для восстановления доступа к почтовому ящику пользователю необходимо подтвердить пароль и логин на веб-странице, ссылка на которую приведена в письме (разумеется, она ведет на подставную страницу, созданную мошенником). Естественно, боясь потерять доступ к почтовому ящику, многие попадаются на такой, в общем-то, нехитрый трюк. Через некоторое время оказывается, что на самом деле никаких сбоев не было, а учетная запись пользователя используется мошенниками для рассылки спама.

С теми же целями рассылаются сообщения, что ваш якобы одноклассник оставил вам сообщение. Например, представьте, что вы получили электронное письмо от дяди Бори, в котором он пишет, что во вложении — фотографии его детей. Так как у дяди есть дети, и письмо, похоже, пришло с его адреса, вы открываете сообщение и видите, что в письмо вложен файл Word. Открыв его, вы видите странное окно, которое отображается всего несколько секунд и затем исчезает. После этого на экране появляется нечитаемый документ Word, а может даже отображаются фотографии дядиных детей!

Дядя Боря не отправлял этого письма — его отправил тот, кто знает, что у вас есть дядя Боря (и что у него есть дети). Документ Word, который вы открыли, запустил программу MS Word и одновременно, воспользовавшись имеющимся в этом программном продукте изъяном, запустил содержащийся в документе собственный код. В результате, помимо отображения файла Word, этот код загрузил на ваш компьютер вредоносное программное обеспечение, способное получать доступ к вашим контактам, а также записывать данные с веб-камеры и микрофона вашего устройства.

Подделать электронное письмо, чтобы оно отображало неверный обратный адрес, очень просто. А это означает, что проверки указанного в письме обратного адреса отправителя недостаточно для подтверждения его личности.

В последнее время наряду с психологическими методами выуживания информации используются и программные. Например, пользователь получает письмо якобы от администрации платежного сервиса WebMoney, в котором сообщается, что в их клиентской программе обнаружена серьезная уязвимость, и пользователю необходимо скачать и установить новую версию, ссылка на которую приведена в письме. Естественно, страница, с которой загружается «новая» программа, выглядит в точности так же, как и официальная, но загружаемая программа модифицирована таким образом, что ключевые файлы, пароль и идентификатор пользователя отсылаются мошенникам. Получив контроль над счетом пользователя, мошенники быстро переводят имеющиеся там деньги на другой счет, затем в другую платежную систему, после чего — в наличные. Эти действия проделываются очень быстро, и вернуть деньги оказывается практически невозможно. Причем, даже если у пользователя нет денег на счету, мошенники могут взять кредит от его имени, и тогда ему придется не только восстанавливать контроль над счетом, но и разбираться с банком.

Как правило, фишинговые атаки не являются столь нацеленными — злоумышленник обычно массово рассылает письма (их принято называть *спамом)* сотням или тысячам людей, оповещая о наличии интересного видео, важного документа или претензий по оплате, или выдавая себя за сотрудника технической поддержки вашей компании. В некоторых случаях атакующие и не пытаются установить программное обеспечение на ваш компьютер, а вместо этого просто запрашивают у вас личную информацию, — такую как финансовые данные или пароли. Расчет здесь на то, что некоторые из получателей «клюнут» на уловку и предоставят запрашиваемую конфиденциальную информацию.

> ***СПАМ***
>
> **Спам — это электронный эквивалент бумажной рекламы, которую бросают в почтовый ящик. Однако спам не только раздражает, он может быть опасен, если является частью фишинговой атаки, цель которой — выудить деньги, обманным путем получить пароли, номера кредитных карт, банковские учетные данные или распространить вредоносный код На компьютерах получателей.**

Помимо фишинга, во Всемирной паутине существует большое количество и других видов мошенничества. Вот некоторые из них.

- **Использование взломанных аккаунтов в различных социальных сетях и системах мгновенного обмена сообщениями для выманивания денег.** Этот вид мошенничества

является одним из самых распространенных. Со взломанного аккаунта социальной сети — например, «Одноклассники», всем пользователям из контакт-листа рассылаются сообщения, в которых «по большому секрету» указывается короткий номер, на который можно отправить бесплатное SMS-сообщение, чтобы получить на счет мобильного телефона небольшую, в пределах 100-200 рублей, сумму от компании, проводящей рекламную акцию (рис. 3.2). SMS-ка оказывается далеко не бесплатной, и счет мобильного телефона не пополняется, а заметно уменьшается, причем сумма, в зависимости от варианта аппетита мошенников, начинается от 100 и заканчивается несколькими тысячами рублей. В качестве вариаций схемы используются ссылки на веб-страницы, открыв которые в браузере мобильного телефона, пользователь активирует платную услугу и звонки на платные номера.

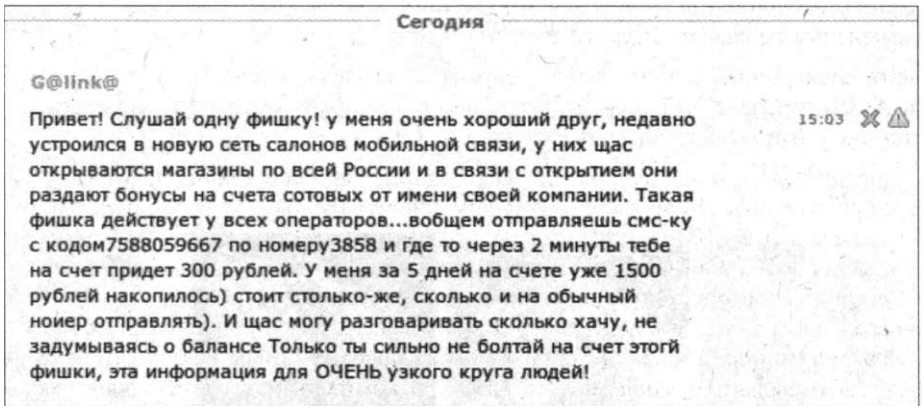


Рис. 3.2. Фишинговое сообщение со взломанного аккаунта социальной сети

- Ресурсы, предлагающие услуги по взлому аккаунтов электронной почты, социальных сетей и систем мгновенного обмена сообщениями. Естественно, эти услуги не бесплатны, и в большинстве случаев в качестве доказательства приводится письмо, написанное якобы со взломанного почтового ящика, или скриншот домашней страницы. К сожалению, не все такие предложения обманны, — в некоторых случаях заказанные аккаунты действительно взламываются. В роли заказчиков выступают обычные пользователи. Сначала те, кому по различным причинам — от проверки супруга на верность до наказания хама — надо получить контроль над чужим аккаунтом, а затем те, кого взломали, — чтобы вернуть себе контроль над аккаунтом и наказать заказчиков взлома. В результате такого «круговорота» и реальные исполнители, и мошенники не остаются без работы.

- Сайты, предлагающие программное обеспечение, обладающее фантастическим функционалом, — от программ для мобильных телефонов, якобы позволяющих с помощью камеры телефона видеть человека сквозь одежду чуть ли не в рентгеновском спектре или читать SMS-сообщения на чужих телефонах, до чудо-антивирусов, сканирующих жесткий диск компьютера через браузер за пять минут и находящих вирусные и троянские программы в системных папках Windows даже на компьютерах под управлением операционных систем Linux и на мобильных телефонах. Купить такие программы можно очень недорого, отправив SMS-сообщение стоимостью «не более десяти рублей». На самом деле отправка сообщения обойдется далеко не в десятку (вспомните про сноску-звездочку и мелкий шрифт), а установленная программа может оказаться вирусом,

блокирующим работу компьютера и требующим отправки платного сообщения за его разблокировку.

- Интернет-магазины, предлагающие различные товары по бросовым ценам. Вы запросто можете у них обнаружить новейший ноутбук стоимостью в 50 000 рублей по цене в пять раз дешевле. Обычно такие магазины требуют предоплату, и через некоторое время исчезают, а доверчивые покупатели так и не получают заказанных товаров. Сюда же относятся магазины т. н. «таможенного конфиската» (рис. 3.3).

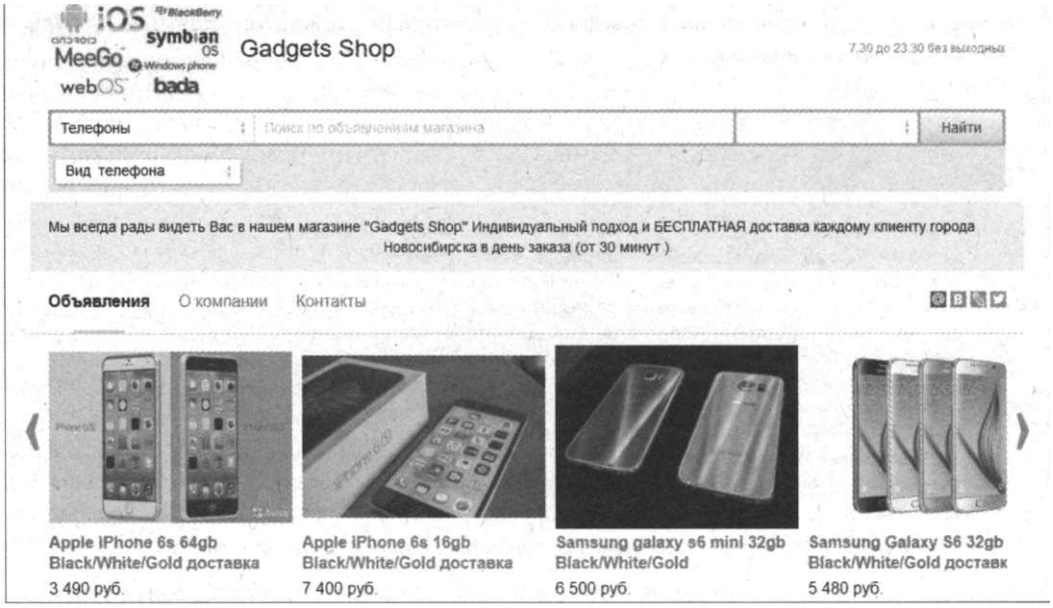


Рис. 3.3. Пример сайта-лохотрона

- Уведомления об огромных выигрышах в лотереях, о своем участии в которых пользователь ничего не знал, — например, лотереи по адресам электронной почты или по номеру ICQ. Для получения такого выигрыша следует уплатить какой-нибудь сервисный сбор. Естественно, после его уплаты никакого выигрыша пользователь не получит, и сервисный сбор ему тоже никто не вернет.
- Запросы ввода номера мобильного телефона — могут выдаваться на страницах для скачивания каких-либо файлов, для получения пароля для распаковки архивов и установки программ, на фишинговых версиях сайтов банков и социальных сетей. Как правило, после указания номера телефона вы без уведомления подписываетесь на некую услугу, за которую ежемесячно (еженедельно или ежедневно) некая сумма будет сниматься с баланса сотового телефона. Проверить подключенные услуги, в том числе и подобные платные, можно в личном кабинете на сайте вашего сотового оператора (что тоже является отнюдь не тривиальной процедурой, поскольку операторы всячески открещиваются от участия в подобных схемах, утверждая, что они лишь посредники, и перенаправляя вас непосредственно к организатору платной услуги, который тоже не спешит ее заблокировать).

Такого рода схем довольно много, периодически появляются новые их варианты, и универсального способа защиты от мошенничества нет. Тем не менее, почти все эти способы ос-

нованы на доверчивости и незнании правил безопасности во Всемирной паутине. Приведу несколько несложных советов, следуя которым можно не попасться на удочку мошенникам.

- Заведите себе несколько адресов электронной почты — рекомендуется иметь, по крайней мере, два таких адреса:
  - *личный адрес электронной почты* — этот адрес должен использоваться только для личной корреспонденции. Поскольку спамеры создают списки возможных адресов электронной почты (используя комбинации очевидных имен, слов и номеров), необходимо придумать такой адрес, который спамерам будет трудно угадать. Личный адрес не должен состоять из вашего имени и фамилии, а чтобы защитить его, следуйте указанным далее рекомендациям. Никогда не публикуйте личный адрес электронной почты на общедоступных интернет-ресурсах, в том числе и в социальных сетях. Если требуется опубликовать личный адрес в электронном виде, замаскируйте его, чтобы спам-боты не смогли его «распознать». Например, ivanov.ivan@mail.ru — это простой адрес, который без труда «вычислят» спамеры. Вместо этого попробуйте представить его в таком виде: ivanov точка ivan собака mail.ru. Можно также опубликовать личный адрес в виде графического файла, а не в виде ссылки. Если же личный адрес обнаружен спамерами, его следует сменить. Несмотря на очевидные неудобства в общении со своими привычными адресатами, изменение адреса электронной почты поможет избежать получения спама;
  - *публичный электронный адрес* — используйте этот электронный адрес для регистрации на общедоступных форумах и в чатах, а также для подписки на почтовую рассылку и прочие интернет-услуги. Попробуйте завести несколько публичных адресов — в этом случае будет больше шансов отследить, какие службы отправляют адреса спамерам. Ну, а слишком популярный у спамеров свой публичный адрес можно просто бросить, перестав проверять.
- Никогда не отвечайте на спам — большинство спамеров фиксируют получение ответов. Обычно, чем больше вы отвечаете на спам, тем больше его приходит.
- Не переходите необдуманно по ссылке «Отказаться от подписки» в электронных письмах, полученных из неизвестных источников. Спамеры отправляют поддельные письма с предложением отказаться от подписки. Таким образом они собирают активные адреса электронной почты.
- Не отвечайте на письма и сообщения от незнакомых людей и ни в коем случае не переходите по ссылкам, содержащимся в таких посланиях. Если вы получили сообщение о необходимости обновления какой-либо используемой вами программы, не переходите для этого по ссылке, приведенной в письме, даже если вы ожидали такого письма, и оно выглядит настоящим. Лучше самостоятельно загрузите программу из раздела загрузок официального сайта.
- Используйте регулярно обновляемый спам-фильтр — во многих браузерах имеются дополнительные компоненты, блокирующие переход на фишинговые веб-страницы или предупреждающие о том, что страница является мошеннической. В роли таких фильтров могут выступать специальные модули, входящие в состав некоторых антивирусных пакетов.
- Своевременно обновляйте браузер — убедитесь, что на компьютере используется самая последняя версия веб-браузера и загружены все последние исправления, связанные с безопасностью.

- **Проверяйте письма от знакомых отправителей** — получив письмо или сообщение с предложением открыть веб-страницу или загрузить файл по указанной ссылке от знакомого вам человека, следует убедиться, что сообщение было отправлено именно им. К слову, злоумышленникам доступна возможность подделывать адреса отправителя — поэтому единственным верным способом подтвердить письмо будет голосовой или SMS-контакт с отправителем.
- **Не загружайте программы с сомнительных сайтов** — особенно это касается программ, отвечающих за безопасность компьютера и клиентских программ систем электронных платежей. Лучше потратить лишних пятнадцать минут на поиск официального сайта программы, чем загрузить модифицированную или зараженную вирусом программу. По этой же причине платные программы лучше покупать легально, поскольку большинство «генераторов ключей» и «кряков», помимо взлома программ, могут иметь и другие функции: от кражи паролей до установки на ваш компьютер программ удаленного администрирования, или просто являться вирусами.
- **Не храните пароли к учетным записям различных сервисов в памяти клиентских программ или браузера —** большинство различных сервисов разрешают сохранять регистрационные данные пользователя в cookie-файлах, что позволяет не вводить при каждом их посещении логин и пароль. Обычно для этого следует установить специальный флажок при авторизации. Старайтесь не использовать такую функцию, поскольку некоторые вредоносные программы могут извлекать из cookie-фашюв регистрационные данные и отсылать их своему создателю.
- **Следуйте указаниям по обеспечению безопасности,** рекомендуемым производителем программы, особенно это касается программ-клиентов различных платежных систем. К примеру, при использовании системы WebMoney не ленитесь защищать свой кошелек с помощью ограничения диапазона IP-адресов, с которых разрешен доступ, разрешите двухфакторную авторизацию посредством мобильного телефона (см. *разд. «Многофакторная аутентификация и одноразовые пароли» главы 2).*
- **Не отсылайте никуда логины и пароли к учетным записям** и не вводите их на вебстраницах, кроме тех, которые отвечают за авторизацию. Помните: ни администрация, ни службы технической поддержки различных сервисов никогда не требуют сообщить им пароль к учетной записи или конфиденциальные реквизиты платежной системы или банковской карты. Никакие банковские службы не требуют передать им такие данные, как CW- и ПИН-код вашей пластиковой карты. Эти коды известны только собственнику карты.
- **Периодически меняйте пароли к учетным записям** электронной почты, системам мгновенного обмена сообщениями, платежным системам и различным веб-сервисам. Не используйте короткие, легко угадываемые пароли. Если выбор пароля составляет трудность, можно использовать специальные программы, генерирующие пароли по различным правилам, в том числе и удобопроизносимые, но в то же время практически не поддающиеся подбору (см. *главу 2).*
- **Внимательно следите за адресами в строке браузера,** особенно при переходе по ссылкам из присланных писем. Кстати, вполне реальна ситуация, когда электронное письмо или ICQ-сообщение со ссылкой на вредоносный сайт приходит от вашего зарегистрированного в системе друга (об отсылке сообщения он, естественно, понятия не имеет). Обратите внимание, что личные и финансовые данные на крупных сайтах для обеспечения защиты их от перехвата передаются по протоколу HTTPS. Об этом вам сообщит адрес в строке браузера (например: https**://gmail.com).**

- Не ведитесь на низкие цены, миллионные выигрыши, прочие призы и подарки — *никто* и *ничего* вам просто так или с ущербом для собственных финансов не отдаст! Прежде чем совершать сомнительную покупку, проверьте в официальных интернет-магазинах, сколько реально стоит предлагаемый продукт. Если вам предлагают его слишком дешево — велик шанс, что с вас возьмут деньги, а покупку вы не получите.

  Покупка может оказаться и слишком дорогой — вы останетесь с покупкой, но переплатите за нее в несколько раз. В этом ключе в нашей стране реализуется множество товаров через «магазины на диване», рекламу по радио и во Всемирной паутине с информацией о якобы большой скидке, — если позвонить и заказать прямо сейчас или в течение часа после передачи. Разумеется, себестоимость, реальная цена проданного вам товара в таких случаях в разы, а то и в десятки раз ниже.

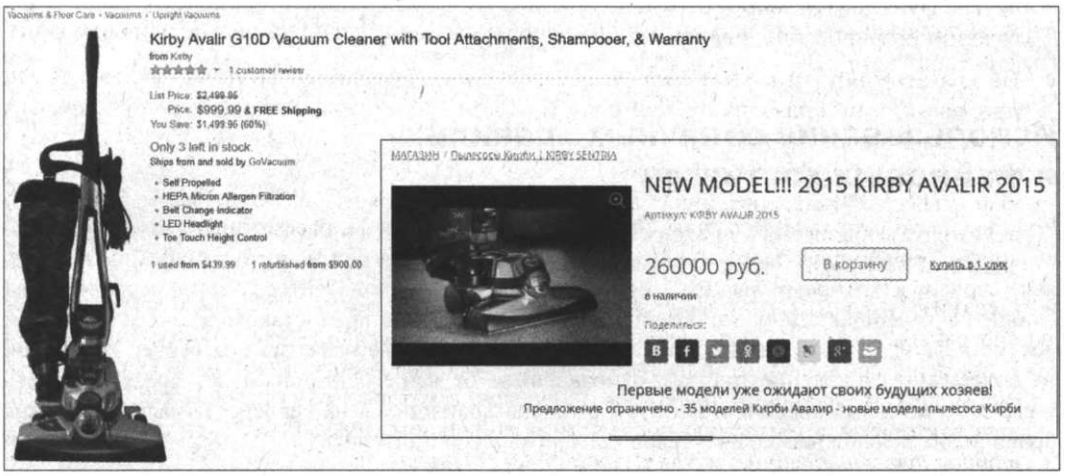


Рис. 3.4. Больная российская тема: чудо-пылесос Kirby в продаже в России (*справа*) и в США *(слева)*

Как можно видеть, пылесос Kirby в магазине Amazon.com стоил по курсу на момент написания книги около 80 тыс. рублей (рис. 3.4, *слева).* Согласитесь, что оформив доставку в любой город России через посредника типа «Бандеролька» за несколько тысяч рублей, приобрести пылесос на сайте Amazon выгоднее, чем в нашей стране (рис. 3.4, *справа).*

- Проверяйте сайты по базам черных списков (например: tinyurl.com/43mp4tc и др.) и вносите туда те, которые обнаружили сами.

Приведенные советы, а также здравый смысл и некоторая доля осторожности снижают до минимума риск попасться на удочку мошенникам.

[1] **Сколько же лохов ведется на призрачные миллионные выигрыши по телевидению, SMS и звонкам по телефону, приобретают дорогущие китайские подделки по почте, пускают на порог дистрибьюторов пылесосов и отвечают на электронные письма с соблазнительными предложениями! Видимо, денег у населения излишне много ©.**

Защита от фишинговых атак

Главное правило защиты от фишинговых атак: *никогда не открывать ссылки и вложения, отправляемые на вашу электронную почту.* Однако это решение не подходит для большинства пользователей. Но как же отличить вредоносные вложения и ссылки от безопасных?

Проверка писем через отправителей

Один из способов проверки подлинности отправителя письма — связаться с человеком, отправившим письмо, через другой канал связи. Если электронное письмо предположительно было отправлено вашим банком, вы можете позвонить в банк или открыть браузер и ввести вручную адрес веб-сайта вашего банка, вместо того чтобы открывать содержащиеся в письме ссылки. Аналогично, вместо того чтобы открывать вложение вашего дяди Бори, вы можете позвонить ему по телефону и спросить, действительно ли он отправил вам фотографии своих детей.

Использование облачных хранилищ и файловых хостингов

Если вы часто отправляете файлы, например, своим коллегам, рассмотрите вариант отправки другим, более проверяемым способом, чтм электронная почта. Загрузите файлы на частный сервер, к которому вы оба имеете доступ, или воспользуйтесь таким сервисом, как Google Drive, Яндекс.Диск или Dropbox. И если вы обычно предоставляете своим адресатам доступ к файлам, загружая их в облачное хранилище, на веб-сайт или на сервер компании, то содержащее вложение письмо, отправленное от вашего имени, будет сразу вызывать у его получателя подозрение. Взлом и подмена хранящихся на сервере данных — это, как правило, более сложная задача, чем подделка электронного письма.

Безопасный просмотр подозрительных документов

Некоторые пользователи постоянно получают содержащие вложения письма от незнакомцев. Это в особенности касается, например, журналистов, получающих документы от источников, или специалистов, работающих с общественностью. В таких случаях сложно определить, является ли документ или ссылка, которую вы собираетесь открыть, вредоносной. Полученные от незнакомцев документы лучше открывать с помощью таких сервисов, как Google Docs (tinyurl.com/ncpdrsa) и Etherpad (etherpad.org). Во многих случаях это позволит защититься от наиболее распространенных эксплойтов, встроенных во вредоносные документы.

> ***ЭКСПЛОЙТ***
>
> **Эксплойт — это программа, сценарий, фрагмент программного кода или последовательность команд, использующие уязвимости в коде сайта или программном обеспечении сервера и служащие для проведения атак на сайт или сервер.**

Обратите также внимание на специальные операционные системы, разработанные с целью минимизации угроз со стороны вредоносных программ, — например, на Tails (см. *часть IV)* или Qubes. Qubes — это другая операционная система на базе Linux, которая тщательно разделяет приложения, не позволяя им влиять на работу друг друга, тем самым ограничивая воздействие любых вредоносных программ. Обе системы разработаны для использования на ноутбуках и стационарных компьютерах.

Вы можете также загрузить подозрительные ссылки и файлы на сайт онлайн-проверки на вирусы — например, на VirusTotal (см. *разд. «Онлайн-проверка файлов на вирусы» главы 4).* Это онлайновый сервис, позволяющий проверить файлы и ссылки в нескольких разных антивирусных базах и немедленно сообщающий результат. Такое решение не является абсолютно надежным, поскольку антивирусы зачастую не могут обнаружить новые вредоносные программы или нацеленные атаки. Однако, если вы еще не используете антивирусную программу, — это лучше, чем ничего.

Важно отметить, что любой файл (или ссылка), который вы загружаете на публичный веб-сайт, такой как VirusTotal или Google Docs, может быть просмотрен сотрудником этой компании или, возможно, всеми, кто имеет доступ к этому веб-сайту. Если содержащаяся в файле информация является конфиденциальной, вам стрит задуматься над альтернативным способом проверки документа.

Анализ отправленных по электронной почте сообщений

В некоторых фишинговых электронных письмах злоумышленники представляются сотрудниками службы технической поддержки или технологической службы компании, запрашивая у вас пароли, удаленный доступ специалиста к вашему компьютеру, отключение некоторых функций обеспечения безопасности на вашем устройстве или установку нового приложения. В письме может быть предоставлено основательное объяснение необходимости этого действия — например, с уведомлением, что ваш почтовый ящик переполнен, что ваш компьютер сломан или взломан хакером.

К сожалению, последствия выполнения таких мошеннических инструкций могут оказаться крайне негативными для безопасности ваших персональных данных и компьютера (устройства). Особенно остерегайтесь разглашения технических сведений или следования техническим инструкциям, пока не будете абсолютно убеждены в подлинности источника таких запросов.

Аутентификация электронной почты

Более сложный, но эффективный способ предотвращения фишинга, — использование программного обеспечения, которое позволяет убедиться в том, что электронное письмо было действительно отправлено тем, кто в нем указан в качестве отправителя, и его содержимое не было модифицировано в процессе передачи. Сделать это позволяет использование для шифрования и подписи ваших электронных писем инструмента PGP (см. *главу* 6). Подписывая электронное письмо при помощи PGP, вы гарантируете получателю, что содержимое этого письма может быть отправлено только тем, кто имеет доступ к вашему закрытому ключу PGP и, таким образом, оно вряд ли является вредоносным. Недостатком этого метода является то, что обе стороны должны установить программное обеспечение для работы с PGP и уметь им пользоваться.

Если содержание присланного вам электронного письма (или ссылки) кажется подозрительным, не открывайте его до тех пор, пока не разберетесь в ситуации с помощью представленных здесь советов и не убедитесь, что оно не является вредоносным.

ГЛАВА 4

Вредоносные программы и защита от них

Виды вредоносных программ

Киберпреступность

Защита от вредоносных программ

Действия при обнаружении вредоносной программы

Разного рода злоумышленники стараются получить контроль над вашим устройством (ноутбуком, стационарным компьютером, смартфоном или планшетом) и применять его для того, чтобы собирать о вас информацию, следить за вами или использовать ваше устройство в своих неблаговидных целях. Далее вы узнаете о нескольких способах получения контроля над компьютерами и о том, как защититься от таких атак.

Виды вредоносных программ

Видов вредоносных программ много, и чтобы разобраться «кто есть кто» в этом мире компьютерных опасностей, мы рассмотрим здесь их стандартную классификацию.

Вирусы

Вирусы появились во времена мэйнфреймов[1], когда персональных компьютеров еще не было, и представляют они собой одну из первых форм вредоносного программного кода. Компьютерные вирусы обычно не являются самостоятельными программами — чтобы вирус заработал, он должен быть внедрен в код любой другой программы. Основная особенность вирусов — способность к самовоспроизведению кода, внедренного в установленные на компьютере программы без согласия его пользователя.

Распространяются вирусы вместе с зараженными программами. При запуске зараженной вирусом программы запускается и сам вирус, выполняющий заданные его создателем функции, в число которых входит в первую очередь нанесение вреда операционной системе, а также дальнейшее заражение других программ. Получить вирус можно разными способами: от перехода по вредоносной ссылке или запуска файла-вложения в неизвестном письме до заражения при заходе на вредоносный сайт.

[1] Мэйнфреймы — большие, размером часто со шкаф, универсальные высокопроизводительные серверы, имевшие широкое распространение в 1960-1990-х годах. Позавчерашний день вычислительной техники.

Вирусы обычно подразделяются по типу объектов, которые они заражают, по методам заражения и выбора жертв. По способу, которым вирусы заражают компьютер, их можно классифицировать так:

- *файловые вирусы* — чаще всего они внедряются в исполнительные модули программ (файлы, с помощью которых производится запуск той или иной программы), что позволяет им активироваться в момент запуска программы, влияя на ее функциональность. Внедрение может проводиться либо изменением кода атакуемого файла, либо созданием его модифицированной копии. Таким образом, вирус, присутствуя в файле, активируется при доступе к этому файлу, инициируемому пользователем или самой операционной системой;
- *вирусы загрузочного сектора* — такие вирусы проникают в загрузочные секторы устройств хранения данных (жесткие диски, Flash-накопители, внешние HDD). Активация вируса происходит при загрузке операционной системы с зараженного носителя. При этом вирус либо нарушает работу загрузчика операционной системы, что приводит к невозможности ее загрузки, либо изменяет файловую таблицу носителя с тем, чтобы прекратить доступ системы к файлам определенного типа;
- *макровирусы* — это вирусы, заражающие файлы документов, используемые офисными приложениями наподобие Microsoft Office, допускающими включение в эти файлы так называемых *макросов* (небольших программ, написанных, как правило, на языке Visual Basic);
- *вирусные скрипты* — такие вирусы, написанные на языках Visual Basic, JavaScript и т. п., на компьютер пользователя, чаще всего, проникают в виде почтовых сообщений, содержащих во вложениях файлы-сценарии. Могут они также встраиваться в HTML-документы, и в таком случае они запускаются браузером, причем не только с удаленного сервера, но и с локального диска.

Любой вирус может обладать функциями и троянской программы (см. далее).

Черви

Черви, в отличие от вирусов, это настоящие компьютерные программы. Они способны к самостоятельному распространению по локальным сетям и через Интернет различными методами: от рассылки своих копий по электронной почте до прямой передачи на другие компьютеры с использованием имеющихся в программах и операционных Системах так называемых *уязвимостей.* Часто для активации червя со стороны пользователя даже не требуется никаких действий.

Помимо функций самовоспроизведения и самораспространения вирусы и черви, как правило, наделяются различными деструктивными функциями, но даже если никаких деструктивных действий в них не предусмотрено, массовая рассылка червей может вызвать перегрузку сети и снижение ее работоспособности.

Черви в некотором смысле представляют собой вирусы, т. к. созданы на основе саморазмножающегося кода. Однако черви не могут заражать существующие файлы. Вместо этого червь поселяется в компьютер отдельным файлом и ищет уязвимости в Сети или в системе для дальнейшего самораспространения. При этом некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые поселяются лишь в оперативной памяти компьютера.

Компьютерные черви могут использовать ошибки конфигурации сети (например, чтобы скопировать себя на полностью доступный диск) или бреши в защите операционной системы и приложений.

Черви также могут подразделяться по способу заражения (электронная почта, мессенджеры, обмен файлами и пр.). Большинство компьютерных червей распространяется следующими способами:

- в виде файла, отправленного во вложении в электронном письме;
- в виде ссылки на веб- или FTP-ресурс;
- в виде ссылки, переданной через IM-сообщение;
- через пиринговые сети обмена данными;
- как сетевые пакеты.

Попав на компьютер, черви проникают прямо в компьютерную память, откуда затем их код активируется.

Троянские программы

Троянские программы, или, попросту, *трояны,* в отличие от вирусов и червей не способны к самораспространению, и для их активации требуется запуск их пользователем или другой вредоносной программой. Получили они свое название от одноименного печально известного мифологического коня — вредоносный компонент проникает в систему под видом какой-либо полезной программы или утилиты.

Как правило, троянскую программу предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности она делает то, что нужно злоумышленникам. И основная задача троянских программ состоит именно в различной деструктивной деятельности: от блокирования различных программ или установки рекламных баннеров до шифрования файлов и перехвата паролей к платежным системам.

Современные троянские программы эволюционировали до таких сложных форм, как, например, *бэкдор* (перехватывает на компьютере административные функции операционной системы) и *загрузчик* (устанавливает на компьютер жертвы вредоносный код). Эти весьма опасные приложения могут выполнять следующие несанкционированные пользователем действия:

- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сетей.

Далее мы рассмотрим классификацию троянских программ по типу действий, выполняемых ими на компьютере, подробнее.

ArcBomb

ЭТИ троянские программы представляют собой архивы, специально сформированные таким образом, чтобы вызывать при попытке распаковать данные нештатное поведение архиваторов, — зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных. Встречаются три вида подобных троянских архивов:

- содержащие *некорректный заголовок* архива или *испорченные данные* внутри архива — все это может привести к сбою в работе конкретного архиватора или алгоритма распаковки при разборе содержимого архива;
- содержащие значительных размеров объект, состоящий из *повторяющихся данных,* — это позволяет запаковать его в архив небольшого размера (например, 5 Гбайт данных упаковываются в RAR-архив размером 200 Кбайт);
- содержащие *одинаковые объекты* — огромное количество одинаковых объектов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10 тыс. одинаковых объектов в RAR-архив размером 30 Кбайт).

Backdoor

Троянская программа типа Backdoor предоставляет злоумышленникам возможность удаленного управления зараженными компьютерами. Заразив компьютер, злоумышленники могут удаленно выполнять на нем любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку. В зависимости от функциональных особенностей конкретного бэкдора, взломщик может устанавливать и запускать на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру. Бэкдоры часто используются для объединения группы компьютеров-жертв в *ботнет* (зомби-сеть) для использования в криминальных целях.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде разработчика.

Banker

Банковские трояны предназначены для кражи учетных данных систем интернет-банкинга, электронных платежей и банковских (как кредитных, так и дебетовых) карт.

Clicker

Такие троянские программы разрабатываются для неинициированного пользователем обращения с зараженного компьютера к тем или иным к интернет-ресурсам (обычно, к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных объектов, в которых указаны «стандартные» адреса интернет-ресурсов (например, файла hosts в операционной системе Windows). Злоумышленники могут преследовать при этом следующие цели:

- рост посещаемости каких-либо сайтов с целью увеличения показов рекламы;
- организация DoS-атаки (см. далее) на какой-либо сервер;
- привлечение потенциальных жертв для заражения вирусами или троянскими программами.

DoS

Троянские программы типа DoS предназначены для проведения атак типа «отказ в обслуживании» (Denial of Service) на целевые веб-адреса. При такой атаке с зараженных компью-

теров системе с определенным адресом отправляется большое количество запросов, что может вызвать ее перегрузку и привести к отказу в обслуживании запросов реальных посетителей. Часто для проведения успешной DoS-атаки злоумышленники предварительно заражают «троянами» этого вида множество компьютеров (например, путем массированной спам-рассылки), после чего каждый из зараженных компьютеров атакует заданную жертву. Такая атака носит название DDoS (Distributed Déniai of Service, распределенный отказ в обслуживании).

Downloader

Троянские программы типа Downloader способны загружать и устанавливать на компьютер жертвы новые версии вредоносных программ, включая троянские и рекламные. Загруженные из Интернета программы потом либо запускаются, либо регистрируются трояном на автозагрузку.

Такой вид деструктивных программ в последнее время стал часто использоваться для первоначального заражения компьютеров посетителей инфицированных веб-страниц, содержащих эксплойты (см. далее).

Dropper

Эти программы используются взломщиками для скрытой установки троянских программ и/или внедрения вирусов, находящихся в теле троянов такого типа, а также для предотвращения обнаружения вредоносных программ, поскольку не каждая антивирусная программа способна выявить все компоненты подобных троянских программ.

После сохранения вредоносной программы типа Dropper на диске (часто в системном каталоге Windows) происходит ее выполнение, причем обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве, неверной версии операционной системы и др.). В результате злоумышленники достигают двух целей:

- скрытной инсталляции троянских программ и вирусов;
- защиты от обнаружения деструктивных программ антивирусами, поскольку, как уже отмечалось, не все они в состоянии проверить все компоненты внутри таких троянов.

Exploit

Эксплойты — это программы с данными или кодом, эксплуатирующие с заведомо деструктивной целью уязвимость (или несколько уязвимостей) в работающих на компьютере приложениях.

Злоумышленники обычно используют эксплойты для проникновения на компьютер жертвы с целью последующего внедрения вредоносного кода (например, заражения всех посетителей взломанного веб-сайта вредоносной программой). Эксплойты интенсивно используются и червями для проникновения на компьютер без ведома администратора.

Широко известны и так называемые программы Nuker, которые отправляют на локальный или удаленный компьютер специальным образом сформированные запросы, в результате чего система прекращает свою работу.

FakeAV

Программы типа FakeAV имитируют работу антивирусного программного обеспечения. С их помощью злоумышленники пытаются вымогать у пользователя деньги в обмен на обещание обнаружения и удаления несуществующих угроз, о которых они ему сообщают.

GameThief

Игровые трояны крадут информацию об учетных записях участников сетевых игр и передают ее злоумышленнику.

IM

Троянские программы типа IM крадут логины и пароли к программам мгновенного обмена сообщениями, таким как ICQ, MSN Messenger, Skype и др., и передают эту информацию злоумышленнику. Для передачи данных могут быть использованы электронная почта, протокол FTP, веб-запросы и другие методы.

Loader

Троянская программа типа Loader (загрузчик) представляет собой небольшой код, используемый для дальнейшей загрузки и установки полной версии вредоносной программы. После того как такой загрузчик попадает в систему (например, при сохранении вложения электронного письма или просмотре зараженного изображения), он соединяется с удаленным сервером и загружает весь код своей программы.

Mailfinder

Такие троянские программы способны собирать на компьютере адреса электронной почты с последующей передачей их злоумышленнику через электронную почту, HTTP, FTP или другими методами. Украденные адреса используются злоумышленниками при проведении последующих рассылок вредоносных программ и спама.

Notifier

Эта вредоносная программа скрыто передает своему разработчику сообщения о том, что зараженный компьютер в настоящий момент активен (подключен к Интернету). При этом на адрес злоумышленника отправляется информация об этом компьютере — например, его IP-адрес, номер открытого порта; адрес электронной почты и т. п.

Такие троянские программы используются в многокомпонентных троянских пакетах для извещения злоумышленника об успешной установке вредоносных программ в атакуемой системе.

Proxy

Эта вредоносная программа позволяет злоумышленнику получить неинициированный администратором анонимный доступ к различным интернет-ресурсам через компьютер жертвы. С помощью троянских программ такого типа через зараженные компьютеры, используемые в качестве почтового прокси-сервера, обычно организуется рассылка спама.

PSW

Вредоносные программы типа PSW (Password Stealing Ware, приложение для кражи паролей) служат для кражи с зараженных компьютеров административных аккаунтов (логинов и паролей). При запуске эти трояны ищут необходимую им информацию в системных файлах или реестре. В случае успешного завершения поиска программа отсылает найденные данные своему разработчику. Некоторые трояны этого вида крадут и регистрационную информацию к различному программному обеспечению.

Троянские программы типа PSW, занимающиеся кражей банковских аккаунтов, аккаунтов к программам мгновенных сообщений, а также аккаунтов к компьютерным играм, относятся к типам Banker, IM и GameThief соответственно. В отдельный вид троянские программы типа PSW выделены в силу их многочисленности.

Ransom

Троянские программы этого типа могут изменить данные на компьютере таким образом, что компьютер перестает нормально работать, а пользователь лишается возможности использовать определенные данные. Злоумышленник обещает восстановить нормальную работу компьютера или разблокировать данные после уплаты запрашиваемой суммы.

Rootkit

Руткиты — это программы, предназначенные для сокрытия в системе определенных объектов или действий. Часто основная их цель — предотвратить обнаружение вредоносных программ, зтобы увеличить время их работы на зараженном компьютере. Сам по себе руткит ничего вредоносного не делает, но в подавляющем большинстве случаев используется вредоносными программами для увеличения собственного времени жизни в пораженных системах из-за затрудненности своего обнаружения. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), объекты и процессы в памяти зараженного компьютера, деструктивная сетевая активность. Это становится возможным благодаря тесной интеграции руткита с операционной системой. А некоторые руткиты (так называемые буткиты) могут начать свою работу даже прежде, чем загрузится операционная система. Однако, как бы ни развивался этот тип троянских программ, сложные современные антивирусные программы способны обнаружить и обезвредить практически все существующие разновидности руткитов.

SMS

Такие деструктивные программы отправляют с зараженного мобильного устройства текстовые сообщения на платные телефонные номера с повышенным тарифом, записанные в теле самой программы.

Spy

Шпионские программы типа Spy способны скрыто наблюдать за использованием компьютера, например, отслеживая вводимые с клавиатуры данные, делая снимки экрана и получая список работающих приложений. Цель таких программ — кража паролей и прочей конфиденциальной информации, которая передается злоумышленнику, зачастую в открытом виде.

Прочие вредные программы

Некоторые вредные программы характеризуются тем, что не предназначены для нанесения ущерба компьютеру, на котором выполняются. К таким программам относят утилиты для отображения рекламы, рассылки спама, создания и модификации вредоносных программ, взлома паролей сайтов и т. п. Эти программы устанавливаются на компьютер самим пользователем или загружаются другими вредоносными программами.

Рассмотрим три основные категории таких программ: Adware, Pornware и Riskware. Они разрабатываются легально, но в определенных случаях могут представлять опасность для пользователей компьютеров (действуя так же, как шпионское программное обеспечение).

Adware

Adware — это программы, которые предназначены для демонстрации рекламы на компьютере, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о пользователе (например, какого рода сайты он посещает), чтобы реклама соответствовала его интересам. Adware-программы собирают данные с вашего согласия, поэтому не следует путать их с троянскими программами-шпионами, которые собирают информацию без вашего разрешения и ведома. Однако если Adware-программа не уведомляет о сборе информации, то она считается вредоносной.

За исключением показа рекламы и сбора данных такие программы, как правило, не проявляют своего присутствия в системе. Обычно они не размещают свой значок на панели задач, и в меню запуска программ они тоже отсутствуют.

Adware-программы могут попасть на ваш компьютер двумя основными путями:

- *с бесплатным или условно-бесплатным программным обеспечением* — Adware-программы могут входить на вполне законных основаниях в состав некоторых бесплатных или условно-бесплатных программ (например, mTorrent) в качестве рекламной составляющей. Доходы от такой рекламы помогают финансировать их разработку;
- *через зараженные веб-сайты* — к несанкционированной установке Adware-программы на ваш компьютер может привести посещение зараженного веб-сайта. При этом часто задействуются хакерские технологии — например, для проникновения на компьютер может использоваться уязвимость браузера и троянская программа, предназначенная для скрытой установки Adware. Действующие таким образом Adware-программы часто называют Browser Hijackers (от англ. *Hijack* — захватить).

Adware-программы зачастую не имеют процедуры удаления и, как отмечено ранее, иногда для проникновения на компьютер и незаметного запуска используют сомнительные технологии. Однако поскольку Adware-программы могут присутствовать на вашем компьютере на законных основаниях, антивирусные решения не всегда способны определить степень опасности конкретной Adware-программы.

Многие бесплатные или условно-бесплатные программы после их регистрации или приобретения перестают отображать рекламу. Однако в некоторых программах используются сторонние Adware-утилиты, которые иногда остаются на компьютере пользователя и после регистрации или приобретения программы. При этом в ряде случаев удаление Adware-компонента может привести к нарушению функционирования основной программы.

Pornware

Pornware— это программы, отображающие на устройстве порнографический контент. Кроме программ, осознанно устанавливаемых некоторыми пользователями на свои компьютеры и мобильные устройства для поиска и отображения порнографического контента, категория Pornware также включает программы, установленные на устройство без уведомления пользователя со злонамеренной целью. Обычно такой целью является рекламирование платных порнографических веб-сайтов и сервисов.

Злоумышленники для установки Pornware-**программ** на ваш компьютер, планшет или смартфон часто используют неисправленные уязвимости, имеющиеся в популярных приложениях и операционных системах. Кроме того, заражение устройств Pornware-программами возможно с помощью троянских программ, таких как Downloader и Dropper. Далее представлены некоторые примеры Pornware-**программ:**

- **Porn-Dialer** — программы, дозванивающиеся до телефонных служб «для взрослых», телефонные номера и/или специальный код которых сохранены в теле таких программ;
- **Porn-Downloader** — такие программы загружают из Всемирной паутины на компьютер пользователя порнографические мультимедийные файлы;
- **Porn-Tool** — программы этого типа осуществляют поиск и отображение порнографического контента на компьютере пользователя. Например, это могут быть специальные панели инструментов для веб-браузеров и проигрыватели видеороликов.

В отличие от вредоносных программ, Pornware уведомляют пользователя о совершаемых ими действиях.

Поскольку Pornware-программы могут сознательно загружаться пользователями, антивирусные решения не всегда могут определить, опасна ли для устройства конкретная Pornware-**программа.**

Riskware

К категории Riskware относят легальные программы, которые могут причинить вред компьютеру, если используются злоумышленниками для удаления, блокирования, изменения или копирования данных, а также для нарушения работы компьютеров и сетей. В категорию Riskware входят следующие виды программ, нашедшие широкое применение в легальных целях:

- утилиты удаленного администрирования;
- программы-клиенты IRC;
- программы дозвона;
- программы для загрузки файлов;
- программное обеспечение для мониторинга активности компьютеров;
- менеджеры паролей;
- серверные веб-службы, такие как FTP, Web, Proxy и Telnet.

При таком большом количестве легальных программ, некоторые из функций которых могут быть использованы злоумышленниками в незаконных целях, нелегко решить, какие из программ представляют угрозу. Например, программы удаленного администрирования часто используются системными администраторами и службами поддержки клиентов для диагностики и устранения неполадок, возникающих на компьютерах пользователей. Однако если такая программа установлена на вашем компьютере злоумышленником (без вашего ведома), он получит к нему удаленный доступ. И тогда, полностью контролируя ваш компьютер, злоумышленник сможет использовать его практически в любых нужных ему целях.

Кроме того, учитывая, что Riskware-программы могут присутствовать на компьютере на законных основаниях, степень опасности той или иной Riskware-программы не всегда могут определить и антивирусы.

* * *

Сейчас провести четкую грань между различными видами вредоносных программ становится все труднее. Уже никого не удивить троянскими программами, способными заражать другие программы, и вирусами, шифрующими документы и требующими деньги за ключ для их расшифровки.

Более подробную информацию о вирусах и прочих вредоносных программах можно найти на различных ресурсах, посвященных безопасности компьютеров и компьютерных сетей. В табл. 4.1 приведен небольшой список таких ресурсов.

Таблица 4.1. *Ресурсы, посвященные компьютерной безопасности*

Название ресурса	Адрес веб-сайта	Краткое описание
SecureList.com	securelist.ru	Веб-узел по безопасности Лаборатории Касперского
Центр безопасности	tinyurl.com/nk3cr7d	Веб-узел по безопасности компании Microsoft
SecurityLab.ru	securitylab.ru	Информационный портал. Новости о различных событиях в сфере безопасности
Anti-Malware	anti-malware.ru	Информационно-аналитический центр по безопасности
Информационная безопасность	habrahabr.ru/hub/virus/	Публикации на Хабре

Киберпреступность

Наиболее опасную категорию злоумышленников составляют хакеры, создающие для использования в криминальных целях компьютерные вирусы и троянские программы, которые способны:

- красть коды доступа к банковским счетам;
- рекламировать продукты или услуги на компьютере жертвы;
- нелегально использовать ресурсы зараженного компьютера, чтобы осуществлять DDos-атаки;
- осуществлять шантаж.

Далее подробнее рассказывается о том, как действуют киберпреступники, и о риске, которому подвергаются их жертвы.

Поддержка спамеров

Многоцелевые троянские программы, функционирующие как прокси-серверы, способны атаковать и заразить множество компьютеров, создав из них так называемую *зомби-сеть*. Преступники получают контроль над каждым компьютером такой зомби-сети и могут использовать их вычислительные ресурсы для массового распространения электронных сообщений со спамом. При организации зомби-сети из нескольких тысяч — или даже десятков тысяч — зараженных компьютеров спамеры получают следующие преимущества:

- спам распространяется анонимно — служебная информация о доставке сообщения не позволяет узнать реальный адрес спамера;
- массовая рассылка спама проводится очень быстро — сообщения отправляются одновременно с большого количества зомби-компьютеров;
- технологии черных списков, которые не пропускают почту, отправленную с адресов из черного списка, часто неэффективны для борьбы с сообщениями такого рода. Причина

в том, что слишком большое количество компьютеров, отправляющих спам, входит в состав зомби-сети, и многие из них ранее не были задействованы при рассылке.

Организация сетевых атак

Пропускная способность любого сетевого ресурса — например, инфраструктуры, поддерживающей веб-сайт компании, является одной из важнейших его характеристик. Успех распределенных сетевых атак типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) как раз и основан на ограничении пропускной способности атакуемого ресурса. Во время DDoS-атаки веб-ресурсу отправляется огромное количество запросов с целью исчерпать его возможности обработки данных и нарушить его нормальное функционирование. Типичными целями DDoS-атак являются интернет-магазины, интернет-казино, социальные сети, предприятия или организации, чья работа связана с предоставлением услуг во Всемирной паутине. В настоящее время такой вид криминальной деятельности весьма распространен.

Сетевые ресурсы (например, веб-серверы) всегда имеют ограничения по количеству одновременно обрабатываемых запросов. Кроме ограничения мощности сервера, канал, по которому сервер связывается с Интернетом, также обладает конечной пропускной способностью. Если число запросов превышает предельные возможности какого-либо компонента инфраструктуры, могут возникнуть следующие проблемы с уровнем обслуживания:

- формирование ответа на запросы происходит значительно медленнее обычного;
- некоторые или даже все запросы пользователей могут быть оставлены без ответа.

Для отправки на ресурс сверхбольшого количества запросов киберпреступники часто создают из зараженных компьютеров зомби-сеть. Поскольку преступники могут полностью контролировать действия каждого зараженного компьютера зомби-сети, совокупный масштаб такой атаки может быть для атакованных веб-ресурсов чрезмерным.

Обычно конечная цель злоумышленника — полное прекращение нормальной работы веб-ресурса, полный «отказ в обслуживании». Злоумышленник может также требовать денег за прекращение атаки. В некоторых случаях DDoS-атака может использоваться для дискредитации бизнеса конкурента или нанесения ему ущерба.

Ботнеты

Слово Botnet (ботнет) образовано от слов *robot* (робот) и *network* (сеть) — так называют управляемую удаленно единую сеть, в которую киберпреступники, используя специальные троянские программы для обхода систем защиты компьютеров и получения контроля над ними, объединяют компьютеры ничего не подозревающих пользователей.

Иногда киберпреступникам удается заразить вредоносными программами и взять под контроль тысячи, десятки тысяч и даже миллионы компьютеров и таким образом получить в свое распоряжение громадную зомби-сеть. Такие сети можно использовать для осуществления DDoS-атак, крупномасштабных кампаний по рассылке спама и других типов киберпреступлений.

В некоторых случаях киберпреступники создают сети зомби-компьютеров, а затем продают доступ к ним другим преступникам или сдают их в аренду. В частности, спамеры арендуют или приобретают такие сети для проведения крупномасштабных кампаний по распространению спама.

Платные вызовы и SMS-сообщения

Киберпреступники создают и распространяют троянские программы, заражающие мобцльные телефоны, после чего телефон начинает осуществлять звонки и отправлять SMS-сообщения без ведома пользователя. Такие вредоносные программы инициируют несанкционированные звонки и SMS-сообщения на дорогостоящие платные номера или оплачиваемые SMS-сервисы, управляемые преступниками.

Кража электронных денег

Кроме использования троянов для кражи денег с личных и корпоративных банковских счетов, киберпреступники также создают и используют программы-шпионы, которые воруют электронные деньги из электронных кошельков пользователей, — например, со счетов WebMoney или Яндекс.Деньги. Эти троянские программы собирают информацию о кодах/паролях доступа к учетным записям пользователей, а затем отправляют ее преступнику. Обычно такая информация собирается путем поиска и расшифровки файлов, в которых хранятся персональные данные о владельце счета.

Кража банковских данных

С ростом популярности услуг интернет-банкинга, кража данных, используемых в таких системах, стала одним из наиболее распространенных видов преступной деятельности в Интернете. Кроме логина и пароля для доступа к личным и корпоративным банковским счетам, киберпреступники также крадут номера банковских карт.

Для получения доступа к банковским реквизитам и следующей за этим кражи денег преступники используют несколько способов:

- *поддельные страницы* — троянские программы могут атаковать компьютеры и выводить на их экран поддельное диалоговое окно или изображение. Такое окно может имитировать вид веб-страницы банка пользователя, на которой пользователю предлагается ввести имя пользователя и пароль;
- *спам и фишинг* — фишинговые сообщения электронной почты могут имитировать сообщения от банка пользователя, запрашивающие подтверждение имени пользователя и пароля. Чтобы убедить пользователя ввести свои персональные данные, в таких сообщениях часто говорится, что если пользователь не введет требуемые данные, его доступ к счету будет приостановлен. В других случаях сообщается, что пользователь выиграл денежный приз, и ему предлагается указать свои банковские реквизиты для его перечисления;
- *клавиатурные шпионы* — клавиатурные шпионы отслеживают активность на компьютере жертвы, ожидая, когда пользователь подключится к настоящему веб-сайту банка. И как только пользователь переходит на веб-сайт банка, троян начинает записывать последовательность нажатий пользователем клавиш на клавиатуре. Это позволяет злоумышленнику украсть данные (включая логин, имя пользователя и пароль), с помощью которых преступник может получить доступ к счету пользователя и снять оттуда деньги.

Кибершантаж

Программы-вымогатели — это троянские программы, предназначенные для вымогания денег у жертвы. Часто такие программы требуют у жертвы плату за отмену изменений, которые были произведены троянской программой в его компьютере. После установки троян

либо шифрует информацию, которая хранится на компьютере жертвы, либо блокирует нормальную работу компьютера, выводя на экран сообщение с требованием выплаты некоторой суммы за расшифровку файлов и восстановление работы системы. В большинстве случаев сообщение с требованием перевода денег появляется, когда пользователь перезапускает компьютер после того, как произойдет заражение.

ДЛЯ РАЗБЛОКИРОВКИ WINDOWS ОТПРАВЬТЕ SMS

Может возникнуть ситуация, когда доступ к интерфейсу операционной системы окажется перекрыт, а на экране вы увидите сообщение с предложением отправки платного SMS, чтобы получить код для разблокировки компьютера. Не попадайтесь на эту удочку! В ответ вы получите сообщение типа: «Вы — полный идиот! Отправьте еще сообщение!». Это не что иное, как программы-вымогатели (Trojan-Ransom), существующие уже давно. Справиться с ними можно совершенно бесплатно, посетив веб-сайт sms.kaspersky.ru и загрузив специальную антивирусную утилиту. В некоторых случаях может понадобиться подобрать с ее помощью несколько кодов разблокировки. Если выход в Интернет с заблокированного компьютера невозможен, вы можете воспользоваться другим компьютером или мобильным телефоном/смартфоном с доступом в Интернет. Подробно процесс разблокировки описан на странице по ссылке tinyurl.com/6jw66af.

Программы-вымогатели все чаще используются киберпреступниками по всему миру. Однако сообщения с требованием выкупа и способы вымогания денег в разных регионах могут быть разными. Например:

- *поддельные сообщения о наличии нелицензионных приложений* — такие трояны отображают сообщение о том, что на компьютере жертвы установлено нелицензионное программное обеспечение и требуется его оплата;
- *поддельные сообщения о нелегальном контенте* — в странах, где использование пиратского ПО менее распространено, всплывающее сообщение троянов-вымогателей может имитировать сообщение правоохранительных органов об обнаружении на компьютере контента, содержащего детскую порнографию или другого нелегального контента. Сообщение сопровождается требованием уплаты штрафа.

Целевые атаки

В отличие от массовых атак (цель которых — заражение максимального количества компьютеров), в целевых атаках используется совершенно иной подход. Целевые атаки, как правило, направлены на заражение сети определенной компании или организации или даже одного сервера в сетевой инфраструктуре организации, для чего может быть написана специальная троянская программа.

Киберпреступники регулярно проводят целевые атаки на предприятия, обрабатывающие или хранящие информацию, которая может быть использована ими для получения незаконного дохода. Наиболее часто целевым атакам подвергаются банки и биллинговые компании (например, телефонные операторы). Серверы банков или банковские сети преступники атакуют, чтобы получить доступ к их данным и осуществить незаконный перевод средств с банковских счетов пользователей. Если для атаки выбирается биллинговая компания, преступники пытаются получить доступ к учетным записям пользователей или украсть ценную информацию, такую как клиентские базы данных, финансовые сведения или технические данные.

Зачастую невольно преступнику помогают сотрудники компаний, ответив на фишинговое электронное письмо, выглядящее как сообщение из ИТ-отдела компании, в котором в целях тестирования сотруднику предлагается ввести свой пароль доступа к корпоративной систе-

ме. В иных случаях преступники могут использовать личную информацию, собранную на веб-сайтах социальных сетей, чтобы выдать себя за одного из коллег сотрудника. В таком случае фишинговый запрос имени пользователя и пароля выглядит так, как если бы он действительно был отправлен коллегой. Это помогает запрашивать у сотрудников их пароли, не вызывая подозрения.

Защита от вредоносных программ

Лучшая защита от атаки вредоносными программами — профилактика против заражения. Эта задача может оказаться непростой, если злоумышленник использует так называемые *уязвимости нулевого дня* (Oday), т. е. уязвимости в программном обеспечении компьютера, неизвестные его разработчикам. Злоумышленники могут получить доступ к уязвимостям нулевого дня и через них установить на ваш компьютер вредоносные программы.

> ***ЧТО ТАКОЕ УЯЗВИМОСТЬ?***
>
> *Уязвимость* **(или *баг*) — это ошибка в коде или логике работы операционной системы или программы. Так как современное программное обеспечение очень сложное и включает много функций, разработчикам очень непросто создать программное обеспечение, в котором совсем нет уязвимостей.**

Впрочем, поиск уязвимостей нулевого дня — дело недешевое, а повторно использовать их еще труднее (когда уязвимости обнаружены, их обычно оперативно исправляют). Поэтому злоумышленник может обманом подталкивать вас собственноручно установить вредоносную программу. Существует множество способов такого обмана. Вредоносный код может скрываться за ссылкой на веб-сайт, документ, PDF-файл или даже программу для обеспечения безопасности компьютера. Для атаки могут использовать электронную почту (письмо будет выглядеть как отправленное от известного вам человека), сообщение в Skype или Twitter, ссылку, опубликованную на вашей странице в Facebook. Чем точнее направлена атака, тем упорнее будут злоумышленники в своих попытках заставить вас скачать и установить вредоносный код. В частности, это может быть:

- *вложение в электронное письмо, содержащее вредоносную программу,* — вас могут обманом убедить запустить программу, после того, как вы откроете безобидное на вид, но на самом деле зараженное вредоносной программой вложение в электронное письмо.

  Вредоносные программы позволяют активировать на вашем компьютере микрофон и передавать ваши разговоры, записывать видео с экрана, захватывать вводимую с клавиатуры информацию, копировать файлы и даже подменять данные. Будьте очень внимательны, открывая вложения в электронные письма, и если сомневаетесь — перепроверяйте факт отправки вложения у отправителя;

- *вредоносная ссылка* — компьютер можно заразить вредоносной программой и удаленно, инициировав посещение веб-страницы. Если при переходе по ссылке отображается окно, предлагающее установить программное обеспечение, — не соглашайтесь. А если веб-браузер, антивирусная программа или поисковая система предупреждают вас о том, что сайт, возможно, заражен, прекратите загрузку страницы и закройте ее.

  Обращайте также внимание на *расширения* скачиваемых файлов. Если вы, к примеру, нашли ссылку на RAR-архив, torrent-файл, PDF-файл или изображение в формате IPG, а после щелчка на ней предлагается загрузить исполняемый файл (с расширением exe), — будьте уверены, перед вами вредоносное приложение. Зачастую вредоносные приложения способны устанавливать программы, загружаемые не с официальных сайтов, а с ре-

сурсов-коллекторов типа **Softpedia.com,** а также всевозможные панели и надстройки со страниц файловых хостингов;

- *подключение через USB или Thunderbolt* — злоумышленники могут скопировать вам вредоносную программу или другим образом получить контроль над вашим компьютером, подключившись через порт USB или Thunderbolt. Весьма опасны и диски CD/DVD — иногда они содержат программу (например, зараженный файл autorun.exe), которая запускается автоматически, и ваш компьютер, таким образом, подвергается заражению сразу после подключения носителя. Поэтому будьте внимательны, подключая устройства к вашему компьютеру, отключите автозапуск устройств в настройках операционной системы, а также не допускайте к вашему устройству незнакомцев.

В настоящее время наиболее уязвимы следующие программы, операционные системы и платформы:

- Java — поскольку Java установлена более чем на трех миллиардах устройств, работающих под управлением различных операционных систем, для атак с использованием уязвимостей Java на разных платформах и ОС создаются специальные эксплойты;
- **Adobe Reader —** программа Adobe Reader является мишенью для многих атак, в связи с чем в нее внедряются все более совершенные инструменты для защиты программы от действия эксплойтов, поэтому киберпреступникам все сложнее и сложнее создавать эффективные эксплойты для этого приложения. Однако на протяжении последних 18 месяцев Adobe Reader все еще был популярной мишенью веб-угроз;
- **Windows и Internet Explorer —** действующие эксплойты по-прежнему используют уязвимости, которые были обнаружены еще в 2010 году, в том числе связанные с центром поддержки Windows и неправильной обработкой файлов **JPEG;**
- **Android —** киберпреступники могут использовать эксплойты для получения прав root-доступа на вашем устройстве. После этого они получат практически полный контроль над устройством под управлением этой операционной системы.

В последнее время одной из самых популярных у злоумышленников стала технология распространения вредоносного кода через веб-страницы. Осуществляется это так. На веб-сайте размещается зараженный файл и программа-скрипт, эксплуатирующая уязвимость браузера. При посещении пользователями такой страницы программа-скрипт, используя эту уязвимость, загружает зараженный файл на компьютер пользователя, а затем запускает файл на выполнение.

Чтобы заразить максимальное количество компьютеров, создатель вредоносной программы применяет ряд методов привлечения внимания пользователя к такой веб-странице, — например, рассылает спам-сообщения со ссылками на зараженную страницу через электронную почту и IM-мессенджеры или через поисковые системы. При этом после сканирования поисковыми системами текста на зараженной странице ссылка на эту страницу включается в списки результатов поиска.

Первый шаг для защиты от подобного заражения — не открывать документы и ссылки. У продвинутых пользователей со временем развивается «инстинкт»: они чувствуют, что может оказаться вирусом, а что нет. Но хорошо спланированная направленная атака бывает весьма эффективной. Если вы используете почтовую службу Gmail, попробуйте открывать подозрительные вложения при помощи сервиса Google Drive, а не скачивать их на компьютер, — это поможет защититься от заражения. В менее распространенных операционных системах, таких как Ubuntu или Chrome OS, риск заражения существенно ниже, но для искушенного злоумышленника и это не проблема.

Другой способ обезопасить компьютер от вредоносных программ — *всегда использовать актуальные версии программ (особенно Java и Adobe Reader) и последние обновления в области безопасности, в том числе и антивирусного приложения.* Компании-разработчики регулярно исправляют ошибки и предоставляют исправления в качестве обновлений. Без обновлений вы рискуете остаться с уязвимостями.

Антивирусные программы

На любом компьютере, а также и на мобильных устройствах (особенно, работающих под управлением операционной системы Android) рекомендуется установить и регулярно обновлять антивирусную программу. Будет неправильно рекомендовать какой-либо конкретный продукт как самый качественный. Большинство современных антивирусных программ представляют собой весьма эффективные комплексы по защите устройств от вредоносных программ.

Антивирусный комплекс, по сути, не является единой программой и состоит из отдельных модулей, каждый из которых выполняет свою защитную функцию. Обычно антивирусный пакет содержит как минимум три модуля: антивирусный сканер, отвечающий за проверку файлов и папок по требованию; резидентный сканер, проверяющий открываемые файлы в режиме реального времени; и почтовый сканер, проверяющий письма, приходящие по электронной почте. В зависимости от производителя и версии, количество модулей и их функциональность могут изменяться. Например, антивирусные пакеты класса Internet Security содержат в своем составе также брандмауэр, контролирующий все сетевые соединения, спам- и фишинг-фильтры (рис. 4.1).

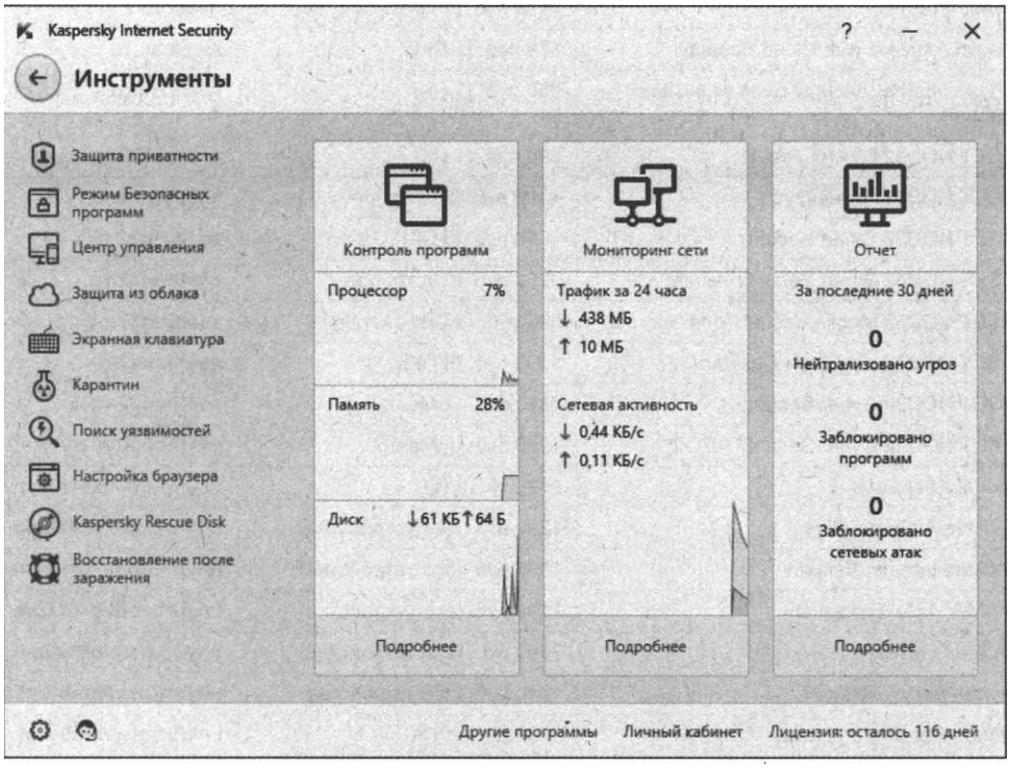


Рис. 4.1. Интерфейс программы Kaspersky Internet Security

В большинстве своем антивирусные программы — платные, хотя некоторые производители параллельно выпускают и бесплатные версии с урезанной функциональностью. Тем не менее, даже такие урезанные версии часто способны обеспечить хотя бы базовую защиту компьютера. Перечень самых популярных платных антивирусных программ приведен в табл. 4.2.

Таблица 4.2. *Сравнение цен на популярные платные антивирусные программы*

Название	Стоимость лицензии на 1 год	Веб-сайт
Антивирус Касперского	1320 руб. (2 ПК)	kaspersky.ru
Kaspersky Internet Security	1800 руб. (2 устройства)	kaspersky.ru
Kaspersky Internet Security для Android	399 руб. (1 устройство)	kaspersky.ru
Kaspersky Internet Security для Mac	1200 руб. (1 Mae)	kaspersky.ru
Kaspersky Total Security	1990 руб. (2 устройства)	kaspersky.ru
Антивирус Dr.Web	1090 руб. (1 устройство)	drweb.com
Dr.Web Mobile Security	299 руб. (1 устройство)	drweb.com
Dr.Web Security Space	1290 руб. (1 устройство)	drweb.com
avast! Pro Antivirus	650 руб. (1 ПК)	avast.ru
avast! Internet Security	850 руб. (1 ПК)	avast.ru
avast! Premier	1150 руб. (1 ПК)	avastru
eScan Antivirus with Cloud Security	550 руб. (1 ПК)	avescari.ru
eScan Internet Security Suite with Cloud Security	850 руб. (1 ПК)	avescari.ru
ESET NOD32 START PACK	990 руб. (1 ПК)	esetnod32.ru
ESET NOD32 Антивирус	1390 руб. (3 ПК)	esetnod32.ru
ESET NOD32 Smart Security	1950 руб. (3 ПК)	esetnod32.ru
ESET NOD32 Smart Security Family	2250 руб. (5 устройств)	esetnod32.ru
ESET NOD32 Mobile Security для Android	590 руб. (3 устройства)	esetnod32.ru
ESET NOD32 для Linux Desktop	1390 руб. (3ПК)	esetnod32.ru
ESET NOD32 Cyber Security	1390 руб. (1 Mae)	esetnod32.ru
ESET NOD32 Cyber Security PRO	1950 руб. (1 Mae)	esetnod32.ru
McAfee Antivirus	999 руб. (1 ПК)	tinyurl.com/864kkqm
McAfee Antivirus Plus	1299 руб. (все устройства)	tinyurl.com/864kkqm
McAfee Internet Security	1899 руб. (все устройства)	tinyurl.com/864kkqm
McAfee Total Protection	2499 руб. (все устройства)	tinyurl.com/864kkqm
McAfee LiveSafe	2699 руб. (все устройства)	tinyurl.com/864kkqm
Norton Family Premier	1240 руб. (все устройства)	tinyurl.com/pm8yzgf
Norton Security Standard	1299 руб. (1 ПК)	tinyurl.com/pm8yzgf
Norton Security Deluxe	1799 руб. (5 устройств)	tinyurl.com/pm8yzgf

Таблица 4.2 (окончание)

Название	Стоимость лицензии на 1 год	Веб-сайт
Norton Security Premium	2599 руб. (10 устройств)	tinyurl.com/pm8yzgf
Norton Mobile Security	930 руб. (все устройства)	tinyurl.com/pm8yzgf
Panda Antivirus Pro	770 руб. (1 ПК)	tinyurl.com/hvbf5t9
Panda Internet Security	962 руб. (1 ПК)	tinyurl.com/hvbf5t9
Panda Global Protection	1347 руб. (1 ПК)	tinyurl.com/hvbf5t9
Panda Gold Protection	1890 руб. (1 ПК)	tinyuri.com/hvbf5t9
Titanium AntiVirus + Security	325 руб. (1 устройство)	trendmicro.com.ru
Titanium Internet Security	797 руб. (1 устройство)	trendmicro.com.ru
Titanium Maximum Security	1147 руб. (3 устройства)	trendmicro.com.ru
Titanium AntiVirus для Mac	647 руб. (1 устройство)	trendmicro.com.ru
Titanium Mobile Security	1832 руб. (все устройства)	trendmicro.com.ru

Большинство производителей выпускают три модели антивирусного продукта: собственно, сам антивирус (сканирует на вирусы и обеспечивает мониторинг), решение типа Internet Security — для активных посетителей Всемирной паутины, а также комплексное или максимальное решение, дополненное различными функциями. Кроме того, распространение получают антивирусные решения для мобильных устройств. Как правило, в домашних условиях с лихвой хватает одной из первых двух моделей — тут решать вам. Самая простая модель — Antivirus — отлично справляется со всеми задачами обеспечения защиты от вирусов, в том числе и во Всемирной паутине.

Если вам жаль средств на покупку (и ежегодную оплату подписки, хотя продление, обычно, дешевле, чем покупка новой программы), то вы можете воспользоваться одним из бесплатных антивирусов, список которых приведен в табл. 4.3.

***Таблица 4.3.** Популярные бесплатные антивирусные программы*

Название	Веб-сайт
Avast! Free Antivirus	avast.ru/index
AVG Anti-Virus	freeavg.com
Avira AntiVir Personal	avira.com
ClamAV	clamav.net
ClamWin Free Antivirus	ru.clamwin.com
Comodo Antivirus	antivirus.comodo.com
Dr.Web CureIt!	freedrweb.com/cureit/
Kaspersky Free	kaspersky.ru/free-antivirus
Microsoft Security Essentials (до версии Windows 7)	tinyurl.com/negz2vp
NANO Антивирус	nanoav.ru

Таблица 4.3 (окончание)

Название	Веб-сайт
Outpost Security Suite FREE	free.agnitum.com/index.php
Panda Free Antivirus	cloudantivirus.com/ru/

Онлайн-проверка файлов на вирусы

Кроме установки специализированных программ вы можете также проверять единичные файлы на своих компьютерах в режиме онлайн, — через Интернет. Дело в том, что несмотря на все старания производителей антивирусов, создатели вредоносных программ обычно опережают их как минимум на один шаг. И как бы вы ни доверяли производителю своего антивирусного пакета, всегда может случиться так, что какую-то угрозу ваша антивирусная программа заметит позже, чем нужно. Если вы подозреваете, что попавший на ваш компьютер файл заражен вирусом или является вредоносной программой, для проверки отдельных файлов на вирусы можно воспользоваться интернет-сервисами, имеющимися почти у каждого производителя антивирусных средств.

Работа с такими сервисами очень проста: на специальной странице вы указываете путь к файлу, который хотите проверить, он загружается на сервер сервиса, проверяется антивирусной программой, а затем на странице отображается результат сканирования. Существуют также сервисы, проводящие проверку файлов сразу несколькими антивирусными программами, — для большей достоверности результатов (табл. 4.4).

***Таблица 4.4.** Онлайн-ресурсы, позволяющие проверить файлы на вирусы*

Название ресурса	Адрес веб-сайта	Краткое описание
Jotti.org	virusscan.jotti.org/ru	Проверка производится 20-ю различными антивирусами. За один раз можно проверить до 5 файлов объемом не более 50 Мбайт (рис. 4.2)
VirusTotal	virustotal.com/ru	Для проверки используется 54 антивирусные программы. За один раз можно проверить один файл или архив. Допустимый объем загружаемого файла — не более 128 Мбайт
VirSCAN.org	virscan.org	Проверка производится 39-ю различными антивирусами. За один раз можно проверить один файл или архив в формате ZIP или RAR, содержащий не более 20 файлов. Допустимый объем загружаемого файла — до 20 Мбайт

Помимо проверки отдельных файлов, по схожему принципу может быть организована и проверка всего жесткого диска компьютера. Такой онлайн-сканер есть, например, на сайте Panda Security. Скорость проверки онлайн-сканером напрямую зависит от скорости подключения вашего компьютера к Интернету.

Проверять веб-страницы и даже файлы до того, как они будут открыты в браузере или загружены на компьютер, помогут и различные плагины к браузерам.

Ну и наконец, можно воспользоваться различными бесплатными антивирусными утилитами и сканерами, не требующими установки на компьютер и не конфликтующими с уже установленными антивирусными программами, но, тем не менее, позволяющими просканиро-

вать компьютер на наличие вирусов. Как правило, это урезанные версии обычных антивирусных сканеров — например, утилита Curelt! от компании Dr.Web **(freedrweb.com/cureit/),** или изначально бесплатные сканеры — такие, как AVZ, или портативная версия бесплатного антивирусного сканера Clam Win.



Рис. 4.2. Онлайн-проверка на вирусы на сайте virusscan.jotti.org

ПЕЧАЛЬНЫЙ ОПЫТ...

В качестве наглядного примера могу привести печальный опыт одной организации. Локальная сеть в этой организации не была подключена к Интернету. За состоянием антивирусной защиты никто из системных администраторов особо не следил, полагая, что «подцепить заразу» неоткуда. Соответственно, антивирусные базы были, мягко говоря, не актуальными. Но однажды кто-то из клиентов принес Flash-диск с документами, зараженный одной из модификаций вируса Autorun. Вирус заразил рабочие станции и серверы в локальной сети, уничтожив все электронные таблицы и заменив- содержимое документов и изображений, среди которых были сканированные копии довольно важных бумаг, нецензурной бранью. Заодно были «почищены» от перечисленных данных и архивы, хранящиеся на серверах.

Халатность системных администраторов обернулась для них суровым наказанием в виде выговора от явившегося с утра руководителя, потрясающего распечаткой какого-то договора, собственноручно подготовленного им накануне, и рассказавшего им всю правду о том, какие они работники, а также «горячей благодарности» остальных сотрудников организации за сверхурочную работу по восстановлению утерянных документов.

Индикатор взлома

Если не получается определить наличие вируса с помощью антивируса, можно попробовать обнаружить признаки взлома. Например, компания Google иногда уведомляет пользователей Gmail о своих подозрениях касательно атаки на учетные записи со стороны поддерживаемых государством взломщиков. Если вы замечаете произвольное включение индикатора активности веб-камеры, это также может быть признаком взлома (впрочем, более продвинутая вредоносная программа способна отключить такой индикатор). Встречаются и менее очевидные признаки. Так, вы можете заметить, что в вашу учетную запись заходили с незнакомого IP-адреса. При этом бывает, что настройки оказываются изменены, и копии пи-

сем перенаправляются на неизвестный пользователю адрес электронной почты. Если вы знакомы с мониторингом сетевого трафика, временные показатели и объемы трафика тоже могут служить индикаторами взлома. Однозначным признаком может стать подключение вашего компьютера к серверу управления и контроля — компьютеру, который отправляет команды зараженным машинам или получает от них данные.

Действия при обнаружении вредоносной программы

1. *Немедленно отключите компьютер от Интернета и прекратите работу* — то, что вы вводите с клавиатуры, возможно, отправляется злоумышленнику! Порой лучше обратиться за помощью к эксперту по цифровой безопасности — он выяснит подробную информацию о вредоносной программе. Однако ее удаление еще не гарантирует безопасность компьютера. Некоторые вирусы позволяют злоумышленникам устанавливать на зараженный компьютер и дополнительные программы. Это могло произойти и с вами.
2. Зайдите в свои учетные записи с другого компьютера (свободного от вредоносного кода) и *смените пароли.* Каждый пароль, который вводился с зараженного компьютера, по умолчанию считается скомпрометированным.
3. Возможно, для удаления вредоносных программ есть смысл *переустановить операционную систему* — это позволит избавиться от большинства вирусов, но некоторые (самые изощренные) разновидности могут сохраниться. Если вы имеете представление о дате заражения вашего компьютера, то можете восстановить файлы по состоянию до этой даты. Учтите, что *файлы, созданные после даты инфицирования, могут стать причиной повторного заражения компьютера.*

ГЛАВА 5

Бесследное удаление данных

Удаление файлов в программе BleachBit

Ограничения программ надежного удаления данных

Уничтожение данных с жестких дисков

Уничтожение оптических дисков

Надежное стирание данных на SSD, Flash-накопителях и SD-картах

Большинство пользователей считают, что достаточно отправить файл в «корзину», очистить ее, — и файл удален. Это не совсем так. При удалении файла операционная система просто скрывает его от пользователя, а пространство, занятое на диске этим файлом, помечает как «свободное», чтобы в дальнейшем использовать его для записи информации. Могут пройти недели, месяцы, а то и годы, пока «удаленный» файл будет перезаписан другими данными, а до тех пор он остается на диске. Немного усилий, инструменты для восстановления данных, — и файл восстановлен. Итак, данные не удаляются сразу и бесповоротно — они остаются на компьютере, пока не понадобится место для других данных.

Если вы хотите удалить файл наверняка, нужно сразу перезаписать его другой информацией, — тогда восстановить данные будет нельзя. Возможно, ваша операционная система уже содержит какой-либо инструмент, позволяющий записывать поверх удаляемого файла набор «случайных» данных и таким образом защищать конфиденциальность стираемой информации.

> ***БЕЗОПАСНОЕ УДАЛЕНИЕ ДАННЫХ В OS X***
>
> **В операционной системе OS X можно надежно стирать файлы, перемещая их в корзину, а затем выбирая команду меню Finder | Очистить Корзину необратимо (Finder | Secure Empty Trash).**

Для операционной системы Windows и Linux в качестве инструмента для необратимого удаления файлов можно использовать бесплатную программу BleachBit (см. далее).

Обратите также внимание: надежное удаление данных с твердотельных накопителей (SSD, Flash-дисков и карт памяти SD) — трудная задача. Причина в том, что в подобных типах носителей применяется технология нивелирования износа, что создает проблему для надежного удаления данных, т. к. эта технология подразумевает поочередное использование всех сегментов памяти вместо постоянной работы с одними и теми же ячейками (о стирании данных с SSD, Flash-дисков и карт памяти SD рассказано в соответствующем разделе в самом конце главы).

Удаление файлов в программе BleachBit

Для быстрого удаления отдельных файлов и периодического выполнения заданных действий по удалению данных можно использовать программу BleachBit. Программа позволяет также создавать свои собственные условия удаления данных. Дистрибутивы программы BleachBit для операционных систем Windows и Linux можно найти на странице: tinyurl.com/y9746nw.

Для установки BleachBit:

- в операционной системе Windows двойным щелчком щелкните по скачанному файлу ***дистрибутива, подтвердите установку программы и следуйте далее указаниям*** мастера установки;
- в операционной системе Linux воспользуйтесь возможностями «Центра приложений» или выполните эту процедуру в терминальном режиме. В последнем случае используется команда:

```
sudo apt-get install bleachbit
```

Интерфейс программы BleachBit

Запустив программу BleachBit, вы увидите ее главное окно (рис. 5.1).

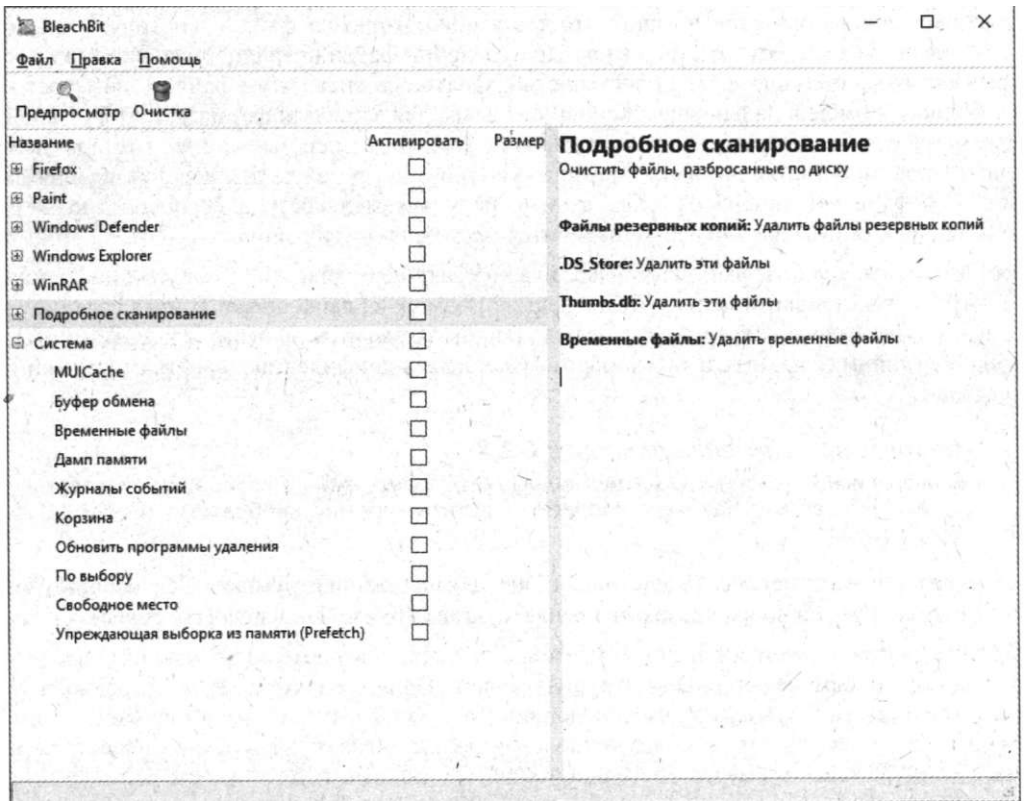


Рис. 5.1. Главное окно программы BleachBit

Помимо доступных для очистки системных компонентов, программа определит несколько установленных на компьютере популярных программ и покажет настройки для каждой из них. Так, BleachBit поможет избавиться от следов, которые оставляет установленный браузер (в нашем примере — Firefox). Установив флажок Firefox, вы увидите, что автоматически окажутся отмечены настройки Cookies, Временные файлы (Temporary files) и другие. Вы можете сбросить ненужные флажки, если это необходимо. Нажмите кнопку Предпросмотр (Preview), чтобы просмотреть, какие файлы будут удалены (рис. 5.2).

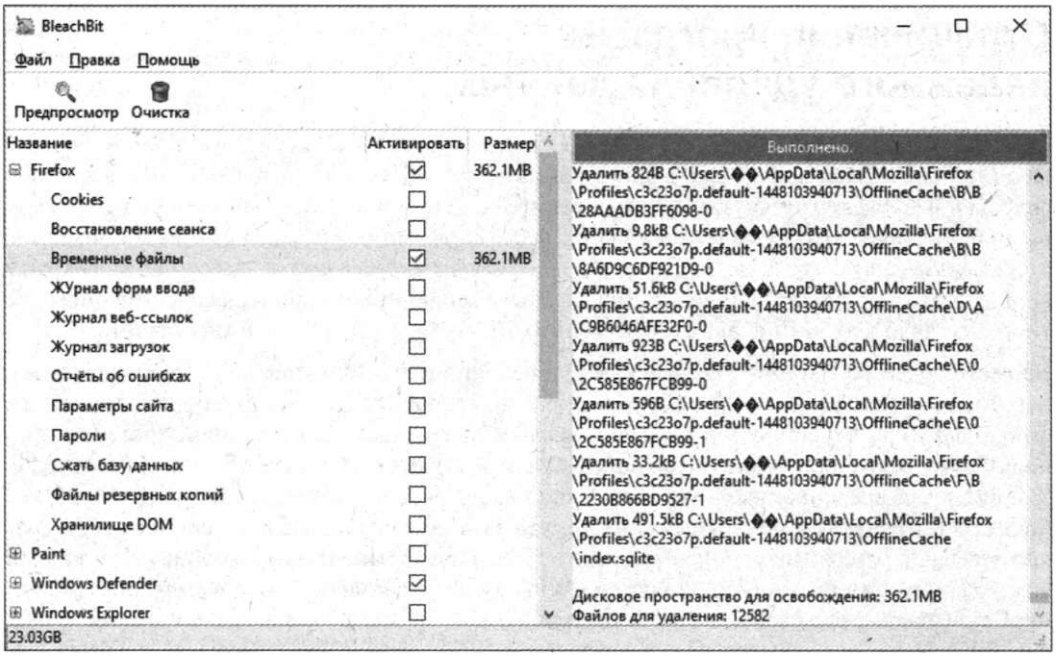


Рис. 5.2. Просмотр удаляемых файлов

Если еще нужных вам файлов среди подготовленных к очистке не окажется, нажмите кнопку Очистка (Clean) — программа выполнит удаление выбранных файлов, продемонстрировав вам индикатор процесса.

Безвозвратное удаление файлов и папок

Для безвозвратного удаления файлов и папок (каталогов):

1. Выберите команду меню Файл | Удаление файлов (безвозвратно) (File | Shred Folders) или Файл | Удаление каталогов (безвозвратно) (File | Shred Files) — откроется окно выбора файлов или папок соответственно.
2. Выберите файлы или папки для удаления — появится запрос, хотите ли вы навсегда удалить выбранные объекты.
3. Нажмите кнопку Удалить (Delete) — программа отобразит имена и размеры удаленных объектов. Обратите внимание, что при удалении каталогов программа BleachBit надежно стирает каждый файл в папке, а затем и саму папку.

* * *

В программе BleachBit доступны и другие функции. Самая полезная из них — очистка свободного пространства. С ее помощью можно избавиться от всех следов ранее удаленных файлов. Дело в том, что операционная система Windows часто оставляет фрагменты удаленных файлов, так вот процедура очистки свободного пространства перезапишет его случайными данными. Обратите внимание, что на это может понадобиться немало времени, — в зависимости от объема жесткого диска и количества свободного пространства.

Ограничения программ надежного удаления данных

Описанная только что процедура позволяет надежно удалить файлы, расположенные исключительно на жестком диске вашего компьютера. Но она не затронет резервные копии, сохраненные на других дисках, Flash-накопителях, серверах электронной почты и в облачных хранилищах. Чтобы надежно удалить файл со всеми его резервными копиями, нужно стереть *сам файл и каждую из его копий, где бы они ни находились.* А если файл сохранен в облачном хранилище (наподобие Яндекс.Диска или Dropbox) или на файлообменном хостинге, как правило, нет никаких гарантий, что его вообще удастся надежно удалить.

Кроме того, даже если вы удалили с диска все копии файла, существует вероятность, что некоторые следы файла на нем все же остались. Это происходит не из-за ошибки удаления файла, а в силу особенностей работы с файлами как самой операционной системы, так и пользовательских программ, хранящих записи о документах, которые они обрабатывали. К примеру, в операционных системах Windows и OS X пакет Microsoft Office может хранить ссылку на файл в меню Недавние документы (Recent Documents), даже если сам файл уже удален, а резервные копии актуального файла могут находиться в специальном временном хранилище (в операционной системе Windows — в каталоге **C:\изегз\имя_пользователя** AppData\Roaming\Microsoft\Word\). В операционной системе Linux (и в других UNIX-подобных системах) программы пакетов OpenOffice.org и LibreOffice могут хранить не меньше записей о файлах, чем Microsoft Office, а в соответствующих журналах останутся зафиксированными команды, из которых можно узнать имя файла, даже если сам файл был надежно удален. Программ, которые ведут себя подобным образом, великое множество. А если вы вдобавок пользовались встроенным в операционную систему поиском, то имя файла может сохраниться и в его истории.

Таким образом, приходится признать, что даже после надежного удаления файла его имя может на какое-то время сохраниться в системе. И только полная перезапись всего диска и новая установка операционной системы могут дать гарантии, что файл или его фрагменты нигде не сохранились.

Уничтожение данных с жестких дисков

Если вы собрались подарить/продать или отправить жесткий диск на свалку, важно убедиться, что никто не сможет извлечь с него оставшуюся там информацию. К сожалению, многие владельцы компьютеров забывают это делать, и жесткие диски зачастую переходят к новым владельцам, полные конфиденциальных данных.

Перед тем как расстаться с диском, надежно удалите с него все данные. Для этой цели существует специальная программа — Darik's Boot and Nuke (рис. 5.3). Загрузить ее можно

с адреса: dban.org, а руководства по ее использованию широко доступны во Всемирной паутине, например, отсюда: tinyurl.com/zhqqr3w.

В некоторые программы для шифрования дисков встроена возможность уничтожения мастер-юпоча. Поскольку ключ — это крошечный объем данных, его можно уничтожить практически мгновенно, и после этого все зашифрованные данные становятся недоступными навсегда. Такой подход позволяет сэкономить массу времени по сравнению с программами наподобие Darik's Boot and Nuke (они на емких дисках могут работать очень долго). Но если вы не используете шифрование всего диска, придется надежно стереть на нем все данные описанными ранее способами.

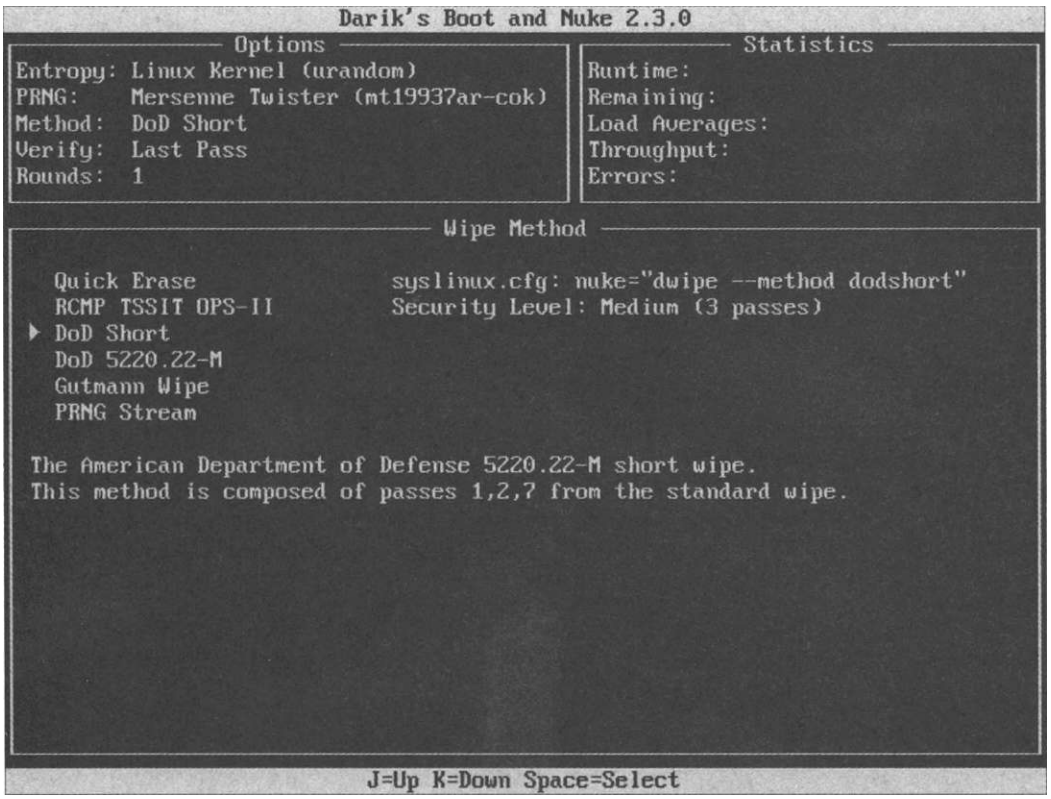


Рис. 5.3. Выбор метода уничтожения данных в программе Darik's Boot and Nuke

Уничтожение оптических дисков

Для дисков CD\DVD\Bluray лучше использовать тот же подход, что и для бумажных носителей, — шредер. Существуют недорогие устройства, которые способны «перемолоть» ваши диски. Никогда не выбрасывайте диски в мусор, если вы не уверены на 100%, что на них нет никакой важной информации.

Приобрести шредеры можно, к примеру, на сайте tinyurl.com/zlevdd7. Покупка устройства для уничтожения дисков более актуальна, скорее, для офиса, а в домашних условиях диски можно уничтожать любыми другими физическими методами.

Надежное стирание данных на SSD, Flash-накопителях и SD-картах

К сожалению, технологии производства твердотельных накопителей (SSD, Flash-дисков и SD-карт) делают трудным (если вообще возможным) надежное стирание данных— как удаление отдельных файлов, так и зачистку всего свободного пространства. Попросту говоря, на сегодняшний день не существует работающего способа надежного удаления данных с твердотельных накопителей. Лучше всего выстраивать защиту данных на таких носителях на основе шифрования — тогда информация хоть и останется, но для любого попытавшегося извлечь данные будет выглядеть как абракадабра.

Как было сказано ранее, твердотельные диски (SSD) и Flash-накопители используют технологию под названием *нивелирование износа.* Ее суть в том, что дисковое пространство на таком носителе разбивается на блоки, подобные страницам книги, и когда происходит запись файла, ему сопоставляется конкретный блок или блоки. Если же требуется перезаписать данные, сначала определяется, в каких блоках это можно сделать, поскольку на носителях SSD и Flash блоки «изнашиваются» — каждый блок может быть использован для записи и перезаписи ограниченное число раз, а потом он теряет работоспособность (представьте, что вы пишете карандашом и стираете написанное ластиком — рано или поздно бумага протрется до дыр).

Для решения этой проблемы контроллеры SSD и Flash-накопителей заботятся о том, чтобы число актов записи в каждый блок было примерно одинаковым по всему носителю, и это позволяет продлить ему жизнь. Бывает, что вместо перезаписи конкретного блока, где изначально находился файл, диск не затрагивает этот блок, а помечает его как неработающий и записывает данные в другой блок (вы пропускаете страницу своей записной книжки, записываете нужное на соседнюю и делаете исправление в оглавлении книжки). Такие действия происходят на низком уровне в электронике диска, и операционная система даже не подозревает об этом. Соответственно, если вы хотите удалить или перезаписать какой-либо файл, нет гарантий, что так и произойдет. Это и есть главная причина, по которой так трудно надежно удалить данные с твердотельного накопителя.

ГЛАВА 6

Вкратце о шифровании

Шифрование: три важных понятия

Основы PGP-шифрования

Практическое руководство по PGP-шифрованию

Шифрование — математическая наука о кодах, шифрах и засекреченных сообщениях. На протяжении всей истории люди использовали шифрование для обмена посланиями, содержание которых, как они надеялись, не сможет прочитать никто, кроме адресатов. Сегодня есть компьютеры, способные выполнять шифрование, а цифровые технологии шифрования вышли за рамки простых сюжетов. Шифрование теперь применяется для более сложных задач — таких как подтверждение личности отправителя сообщения или анонимный просмотр веб-сайтов с помощью сети Tor. При определенных условиях шифрование может быть полностью автоматическим и легким в применении. Но если что-то пойдет не так, полезно понимать суть происходящего, — тогда вы будете лучше защищены от проблем.

Шифрование: три важных понятия

Закрытые и открытые ключи

Одно из самых важных понятий в шифровании — *ключ.* В распространенных схемах шифрования используется *закрытый ключ,* который хранится в секрете на вашем компьютере и позволяет читать адресованные вам сообщения. С помощью закрытого ключа также можно ставить на отправляемых сообщениях защищенную от подделки цифровую подпись. *Открытый ключ* — файл, которым вы можете делиться с другими людьми. Он позволяет им обмениваться с вами шифрованными сообщениями и проверять ваши подписи. Закрытый и открытый ключи — парные, зависимые друг от друга.

Сертификаты безопасности

Второе очень важное понятие — сертификат безопасности. Это своего рода открытый ключ для предотвращения атак посредника. Сайт, имеющий доступ к сертификату, может продемонстрировать удаленным системам, что сертификат существует, и что никакая другая система (без сертификата) не пытается изменить передаваемые данные. Веб-браузер на вашем компьютере может устанавливать зашифрованные соединения с сайтами посредством про-

токола HTTPS. В таких случаях браузер верифицирует сертификаты, проверяя открытые ключи доменных имен (например, **www.google.com** или **www.amazon.com).** Использование сертификатов — один из способов подтвердить подлинность имеющегося у вас открытого ключа пользователя или веб-сайта, чтобы вы могли безопасно обмениваться с ним информацией.

Время от времени появляются сообщения об ошибке сертификата безопасности. Как правило, причиной является попытка общественной точки доступа, где вы находитесь, «вскрыть» ваш обмен зашифрованными данными с веб-сайтом. Кроме того, такая ошибка часто появляется из-за бюрократических проблем в системе сертификатов. А также возникает при попытке злоумышленника взломать ваше зашифрованное соединение.

К сожалению, крайне сложно установить истинную причину возникновения ошибки сертификата безопасности. Поэтому при возникновении такой ошибки нельзя принимать исключения для сайтов, на которых у вас зарегистрирована учетная запись или откуда вы получаете особо важную информацию.

Отпечатки ключей

Ключи в шифровальных системах с открытым ключом — очень большие числа, иногда из более чем тысячи цифр. *Отпечаток ключа* гораздо короче. Это число (набор чисел и букв), которое уникально для того или иного ключа и позволяет не анализировать все символы при проверке подлинности ключа. Предположим, вы с собеседником обменялись копиями ключей, а потом решили убедиться, что копии соответствуют оригиналам. Вам пришлось бы потратить уйму времени, сверяя все символы каждого ключа. Вместо этого можно сверить отпечатки ключей. В современных средствах шифрования отпечатки, как правило, состоят из 40 букв и цифр, например: 5d44 4rt8 9167 7401 40dl 5ws4 200z q561 23sd yl91. И если вы аккуратно сверите отпечаток импортируемого ключа с отпечатком, который вам сообщит настоящий владелец, то можете быть уверены в подлинности ключа (некоторые программы предлагают более удобные способы проверки ключей).

Если проверка отпечатка пройдена, больше шансов, что ваш собеседник действительно тот, за кого себя выдает. Но этот метод несовершенен — злоумышленник может использовать тот же отпечаток, если скопирует или украдет ключ.

Основы PGP-шифрования

PGP-шифрование (от англ. Pretty Good Privacy, вполне хорошая приватность) — это одна из первых популярных реализаций шифрования с открытым ключом, созданная программистом Филом Зиммерманном в 1991 году, чтобы помочь пользователям защитить свои коммуникации. При правильном использовании PGP может защитить содержимое ваших сообщений и даже файлов от самых серьезных средств злоумышленников. Когда Эдвард Сноуден говорил о шифровании, он подразумевал именно PGP и связанные с ней программы.

ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

В традиционных шифровальных средствах для шифрования и расшифровки сообщения используют один и тот же ключ. В асимметричном шифровании (шифровании с открытым ключом) используют два парных ключа: один для шифрования (открытый), другой для расшифровки (закрытый). В этом масса преимуществ. В частности, вы можете делиться открытым ключом со всеми. Пока вы имеете доступ к своему закрытому ключу, любой пользователь, у которого есть ваш открытый ключ, может безопасно общаться с вами. Подобные системы используются для шифрования электронных писем и файлов по стандартам PGP, OTR (при обмене мгновенными сообщениями) и SSL/TLS (для просмотра веб-страниц).

К сожалению, PGP — не самый легкий для освоения и использования инструмент. Стойкое шифрование, реализованное в PGP (шифрование с открытым ключом), — мощное, но довольно мудреное средство защиты. Сама программа PGP существует четверть века и является ровесником самых первых версий Microsoft Windows. С тех давних пор внешний вид PGP не очень изменился. Впрочем, разработано много программ, которые скрывают «древний» дизайн PGP и заметно упрощают ее использование, особенно в части шифрования и аутентификации электронной почты (основные функции PGP). Далее вы научитесь работе с этими программами. Но предварительно посвятим несколько минут основам шифрования с открытым ключом.

Игра с двумя ключами

Возьмем обычный текст — например, «Привет, друг!». Зашифруем его — превратим в код, который непонятен для чужих глаз (скажем, ad&dsDE76vx+fdgQl). Отправим этот код через Интернет. Наше сообщение может увидеть множество людей, но кто из них поймет содержание? В таком виде письмо дойдет до получателя. Он и только он может расшифровать и прочитать исходный текст.

Откуда получатель знает, как расшифровать сообщение, если это не может сделать никто другой? У получателя есть дополнительная информация, недоступная для остальных. Назовем ее *ключом для расшифровки.* Этот ключ *раскодирует* содержащийся в зашифрованном сообщении текст. Но отправитель должен предварительно сообщить ключ получателю. В этом и заключен недостаток такой стратегии — если вы думаете, что вашу почту могут перехватывать, как вы перешлете ключ? Ведь злоумышленник перехватит и его. Тогда нет смысла отправлять зашифрованные сообщения. С другой стороны, если у вас есть секретный способ передать ключ, почему бы не использовать этот же способ для отправки *всех* секретных сообщений?

Шифрование с открытым ключом — замечательное решение проблемы. Каждый человек, участвующий в переписке, может создать два ключа. Один ключ (*закрытый*) нужно держать в тайне и никогда не передавать другим людям. Другой ключ (*открытый*) можно передать всем, кто желает переписываться. Неважно, кто получит доступ к открытому ключу. Вы можете опубликовать его во Всемирной паутине, откуда его будут скачивать все желающие.

Сами «ключи», по сути, представляют собой очень большие числа с определенными математическими свойствами. При этом открытый и закрытый ключи связаны между собой — если вы шифруете что-либо открытым ключом, расшифровать это можно только парным закрытым ключом.

Допустим, вы хотите отправить своему другу секретное сообщение. У него есть закрытый ключ, а парный ему открытый ключ Он загрузил на свою веб-страницу. Вы скачиваете его открытый ключ, с его помощью шифруете сообщение и отправляете адресату. И только он сможет расшифровать сообщение, потому что лишь у него есть парный закрытый ключ.

Электронная подпись

Шифрование с открытым ключом избавляет вас от проблемы передачи адресату ключа для расшифровки (у адресата уже *есть* ключ). Нужно лишь получить соответствующий открытый ключ для шифрования — он доступен всем желающим, даже злоумышленникам. Но открытым ключом можно только шифровать, но *не* расшифровывать.

Итак, то, что зашифровано определенным открытым ключом, может быть расшифровано только парным ему закрытым ключом. Но это еще не все. Если, наоборот, применить к сообщению закрытый ключ, результат можно обработать только с помощью парного открытого ключа.

Зачем? Кажется, нет никакой пользы в защите секретного сообщения при помощи закрытого ключа. Всякий, у кого есть ваш открытый ключ (а он доступен любому в этом мире), может снять такую защиту. Предположим, вы написали сообщение «Привет Андрею!» и применили к этому тексту свой закрытый ключ. Кто угодно может потом прочитать это сообщение, использовав парный открытый ключ, но лишь один человек (и это главное!) мог написать сообщение, — владелец упомянутого закрытого ключа. Конечно, если он аккуратно хранит свой закрытый ключ. Так вы можете подтвердить свое авторство. То же самое мы делаем, когда *подписываем* бумаги в реальном мире.

Подпись также защищает сообщение от редактирования. Если кто-то попытается изменить текст «Привет Андрею!» на «Привет Владу!», заново подписать сообщение у злоумышленника не получится (у него нет вашего закрытого ключа). Таким образом, цифровая подпись гарантирует, что сообщение было действительно написано его автором и не изменилось при передаче.

Итак, шифрование с открытым ключом позволяет шифровать и безопасно пересылать сообщения всем, чьи открытые ключи вам известны. Если, в свою очередь, ваш открытый ключ известен другим людям, они могут отправлять вам сообщения, которые будете способны расшифровать только вы. Вы также можете подписывать сообщения. Тогда всякий, у кого есть ваш открытый ключ, сможет удостовериться в подлинности ваших писем. Если вы получили сообщение с чьей-то цифровой подписью, то можете использовать открытый ключ отправителя и убедиться, что сообщение написал именно он.

Вы, вероятно, уже догадались, что пользы от шифрования с открытым ключом тем больше, чем больше людей знает этот ваш ключ. Очевидно также, что надо обеспечить безопасное хранение своего закрытого ключа, — ведь если кто-либо получит копию вашего закрытого ключа, он сможет выдавать себя за вас и подписывать сообщения от вашего имени. В программе PGP имеется функция отзыва закрытого ключа — она позволяет предупредить людей о том, что ключу больше нельзя доверять, но это не лучшее решение. Главное правило для шифрования с открытым ключом: *храните закрытый ключ в надежном месте.*

Принцип работы PGP

Использование PGP — это, главным образом, работа по созданию и применению открытых и закрытых ключей. С помощью PGP вы можете создать пару ключей (открытый/закрытый), защитить закрытый ключ паролем и использовать ключи для подписания и шифрования сообщений. Программы на основе PGP также позволяют скачивать открытые ключи других пользователей и загружать свой открытый ключ на серверы — хранилища, где другие пользователи могут его найти.

Итак, свой закрытый ключ вы храните в безопасном месте и защищаете его длинным паролем. Открытый ключ можно предоставлять всем, с кем вы хотите переписываться, и тем, кто хочет быть уверенным в подлинности ваших писем.

Сеть доверия

В шифровании с открытым ключом существует потенциальная проблема. Допустим, вы распространяете открытый ключ Эдварда Сноудена (по крайней мере, вы так утверждаете).

Если люди вам поверят, они начнут отправлять Сноудену письма, зашифрованные этим ключом. Они также будут считать, что все сообщения, подписанные этим ключом, созданы Сноуденом. Такое случается редко, но в реальной жизни были прецеденты.

Возможен также сценарий атаки, когда злоумышленник находится между двумя сетевыми собеседниками, читает их письма и периодически вставляет в переписку свои (сбивающие с толку) сообщения. Интернет устроен так, что информация проходит через множество разных компьютеров. Поэтому такая атака («атака посредника») вполне возможна. Из-за нее обмен ключами без предварительных договоренностей — дело рискованное. «Вот мой ключ», — говорит Эдвард Сноуден и отправляет вам открытый ключ. Что, если посредник прервал передачу ключа Сноудена и подменил его ключ на собственный? Как убедиться, что ключ действительно принадлежит конкретному человеку?

Можно, конечно, получить ключ от человека напрямую, но это не намного проще, чем передавать друг другу единственный ключ и защищать его от перехвата. Впрочем, как бы там ни было, но наиболее надежным способом защиты от перехвата представляется обмен открытыми ключами при личных встречах.

АТАКА ПОСРЕДНИКА

Представьте, что вы общаетесь с вашим другом (допустим, Дмитрием) с помощью зашифрованных мгновенных сообщений. Чтобы убедиться, что это действительно Дмитрий, вы просите собеседника назвать город, где вы впервые встретились. «Магадан», — отвечает он. Правильно! Увы, втайне от вас и Дмитрия кто-то третий перехватывает ваши сообщения. Ваши послания для Дмитрия попадают к злоумышленнику, а тот, в свою очередь, связывается с Дмитрием, и наоборот. Вы думаете, что наладили безопасный канал связи, а на самом деле общаетесь через шпиона! Такая атака называется *атакой посредника.* **Злоумышленник может перехватывать информацию, изменять и подделывать сообщения. Поэтому программы для коммуникаций в Интернете должны защищать от этого типа атак, от злоумышленников, которые могут контролировать какую-либо часть сетевой инфраструктуры между собеседниками.**

Тем не менее, PGP предлагает решение получше — *сеть доверия.* Если вы считаете, что ключ принадлежит определенному человеку, вы можете подписать этот ключ и загрузить его (вместе с подписью) на сервер открытых ключей. Оттуда подписанный ключ могут скачивать заинтересованные люди. В целом, чем больше людей, которым вы доверяете, подпишет ключ, тем выше доверие к такому ключу. PGP позволяет подписывать чужие ключи и доверять другим пользователям — если они подпишут ключ, ваша программа автоматически будет считать его достоверным. Разумеется, сеть доверия не лишена недостатков. Но на сегодняшний день, если вы не готовы передавать ключи исключительно при личной встрече, использование сети доверия и серверов открытых ключей — самая подходящая альтернатива.

Метаданные: что не может PGP

PGP обеспечивает секретность, подлинность и целостность содержимого сообщений. Но это не единственные аспекты приватности. Как уже упоминалось, информация о вашем сообщении (*метаданные*) может быть такой же разоблачающей, как и его содержимое. Если вы используете PGP для переписки с каким-нибудь известным в вашей стране диссидентом, то можете оказаться в опасности из-за самого факта шифрованного обмена сообщениями. Даже расшифровывать их необязательно. В некоторых странах вам может грозить наказание только за отказ расшифровать ваши сообщения.

МЕТАДАННЫЕ

Метаданные — это данные о некоторой информации, но не сама информация. Например, сведения о том, кто, когда, откуда, куда отправил электронное письмо — метаданные {а содержание письма — нет). Метаданные часто раскрывают больше информации и нуждаются в более серьезной защите, чем сами данные.

PGP не скрывает информацию об адресате и сам факт использования шифрования. Если вы загружаете свой открытый ключ на серверы ключей или подписываете ключи других пользователей, то фактически демонстрируете всему миру, какой именно ключ принадлежит вам, и кого вы знаете. Но вы не обязаны это делать — вы можете хранить свой открытый ключ в секрете, давать его только тем, кому доверяете, и просить их не загружать его на серверы открытых ключей. То есть, вам не обязательно связывать ключ со своим именем.

СЕРВЕРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Чтобы отправить сообщение человеку, использующему шифрование с открытым ключом (например, PGP), нужно знать, какой ключ применить для шифрования. *Сервер открытых ключей* **выполняет функцию «телефонной книге». Он позволяет программам найти открытый ключ по адресу электронной почты, имени владельца или отпечатку ключа, а потом скачать этот ключ на свой компьютер. Как правило, такие серверы синхронизируют базы данных между собой и не могут сами проверять публикуемые ключи на подлинность. Кто угодно от любого имени может загрузить открытый ключ на сервер. Поэтому есть шанс, что ключ на сервере, связанный с именем человека или его адресом электронной почты, окажется подделкой. Для подтверждения аутентичности ключа надо проверить его подписи или сверить его отпечаток с тем, который получен от владельца иным надежным путем.**

Скрыть переписку с определенным человеком сложнее. Один из вариантов — использование обоими собеседниками анонимных учетных записей электронной почты через сеть Tor (см. *главу 17). А* PGP по-прежнему будет обеспечивать приватность вашей переписки, подлинность и целостность сообщений.

Практическое руководство по PGP-шифрованию

PGP — способ уберечь от злоумышленников сообщения вашей электронной почты в случае их перехвата, а также (хоть и в меньшей степени) от прочтения, если компьютер, на котором находится почта, оказался в чужих руках. PGP также пригодится для подтверждения, что письмо действительно отправлено тем, кто его подписал, а не злоумышленником (обычное электронное письмо очень легко подделать). Эта функция особенно важна, если вы — в группе риска, т. е. можете стать жертвой утечки данных.

Для работы с PGP нужно в дополнение к вашей привычной программе электронной почты установить некоторые утилиты. Понадобится также создать закрытый (секретный) ключ, который предстоит надежно оберегать. С помощью этого закрытого ключа вы будете расшифровывать поступающие сообщения и ставить собственную цифровую подпись при отправке исходящих сообщений, чтобы подтвердить свою личность. Наконец, вы создадите и научитесь распространять свой открытый ключ — небольшой фрагмент данных, который нужен, чтобы другие люди могли отправлять вам шифрованные письма, а также проверять вашу цифровую подпись.

ВНИМАНИЕ!

Для ведения шифрованной переписки требуется, чтобы PGP-совместимые программы были установлены у каждого ее участника.

PGP в Windows

Чтобы использовать PGP для обмена защищенными электронными письмами в операционной системе Windows, нам понадобятся три программы: GnuPG, Mozilla Thunderbird и Enigmail. Шифрование и расшифровку электронной почты осуществляет программа GnuPG. Mozilla Thunderbird — клиент электронной почты, позволяющий читать и отправлять электронные письма без привлечения веб-браузера. Enigmail — плагин к Mozilla Thunderbird, который связывает две упомянутые программы.

> ***PGP И ДРУГИЕ ПОЧТОВЫЕ СЕРВИСЫ***
>
> **Обратите внимание — здесь мы говорим об использовании PGP с почтовым клиентом Mozilla Thunderbird. Скорее всего, вы уже используете некий почтовый клиент (или пользуетесь веб-сервисом — например, Gmaii). Мы не будем останавливаться на том, как интегрировать PGP в те или иные программы. Вы можете установить Thunderbird и попробовать PGP или поискать прочие технические решения, которые позволят использовать PGP с вашей любимой программой. Вы также можете обратиться к справочной системе используемого почтового клиента, чтобы узнать о возможностях совместного использования PGP-шифрования.**

Стоит обратить внимание, что при использовании PGP электронное письмо шифруется не полностью — информация об отправителе и адресате, а также тема сообщения остаются *незашифрованными*! В существующих программах электронной почты нет возможности шифровать данные об отправителе и адресате. Mozilla Thunderbird с плагином Enigmail позволяют шифровать содержимое почты, но если кто-то шпионит за вами, он по-прежнему может видеть, с кем и когда вы обмениваетесь сообщениями.

Установка GPG4Win

Приложение GnuPG (также известное как GPG) для операционной системы Windows можно получить по адресу **gpg4win.org.** Для загрузки выбирайте наиболее свежую версию GPG4Win и только с компонентом GnuPG (Vanilla или Light). После загрузки запустите скачанный файл и установите приложение GPG4Win, следуя указаниям мастера инсталляции.

Установка Mozilla Thunderbird

Откройте веб-сайт Mozilla Thunderbird по адресу **mozilla.org/ru/thunderbird/** и нажмите зеленую кнопку **Загрузить бесплатно.** После загрузки запустите (с правами администратора) скачанный файл и установите приложение Mozilla Thunderbird, следуя указаниям мастера инсталляции. Затем выполните следующие действия:

1. Запустите приложение Mozilla Thunderbird. При первом запуске Mozilla Thunderbird появится небольшое окно с просьбой подтвердить некоторые настройки по умолчанию (рис. 6.1).
2. Нажмите кнопку **Установить по умолчанию** (Set as Default) — в следующем диалоговом окне отобразится предложение получить новый адрес электронной почты.
3. Нажмите кнопку **Пропустить это и использовать мою существующую почту** (Skip this and use my existing email) — откроется новое окно.
4. Укажите в нем имя, адрес электронной почты и пароль, а затем нажмите кнопку **Продолжить** (Continue).

   Во многих случаях программа Mozilla Thunderbird может автоматически определять нужные настройки (рис. 6.2).

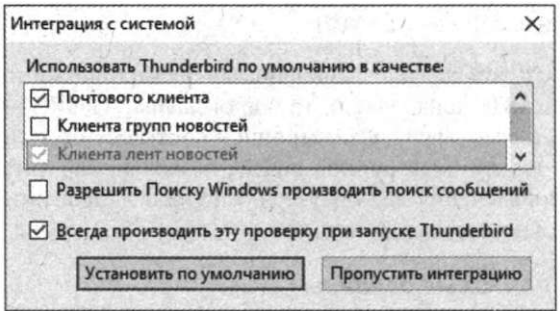


Рис. 6.1. Настройки интеграции Mozilla Thunderbird с системой

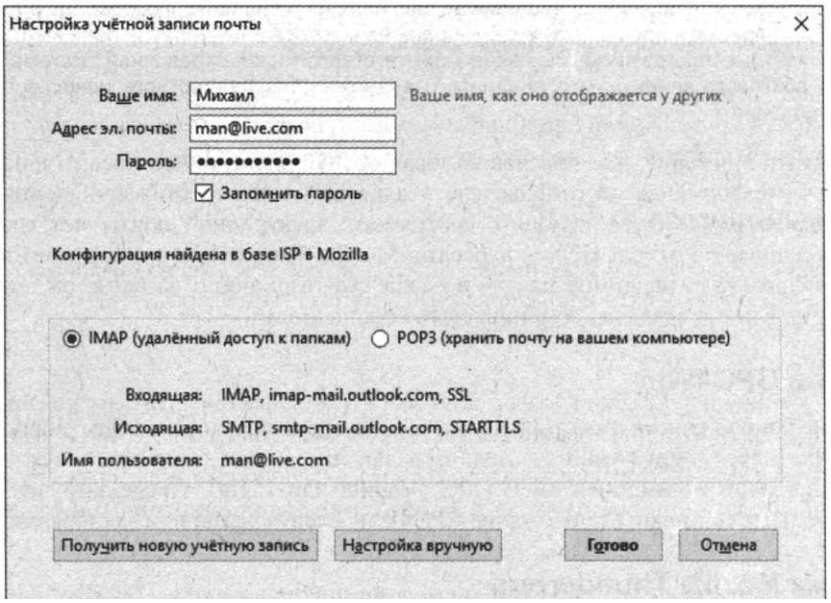


Рис. 6.2. Настройки учетной записи в Программе Mozilla **Thunderbird**

Но иногда Mozilla Thunderbird недостаточно информации, тогда настраивать почту придется вручную. Далее показано, как это делается для учетной записи Gmail:

- Ваше имя (Your Name) — введите ваше имя или псевдоним;
- Адрес эл. почты (Email address) — укажите ваш полный адрес Gmail (в формате username@gmail.com);
- Пароль (Password) — ваш пароль Gmail;
- для сервера входящей почты IMAP:
  - в раскрывающемся списке выберите пункт IMAP;
  - имя сервера: imap.gmail.com;
  - порт: 993;
  - SSL: SSL/TLS;
  - аутентификация: Обычный пароль (Normal password);

- для сервера исходящей почты SMTP:
  - имя сервера: smtp.gmail.com;
  - порт: 465 или 587;
  - SSL: SSL/TLS;
  - аутентификация: Обычный пароль (Normal password).
- Имя пользователя (Username): введите в оба поля ваш полный адрес Gmail (в формате username@gmail.com).

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Если для Google-аккаунта у вас включена двухфакторная аутентификация, то вы не сможете в Thunderbird использовать свой обычный пароль Gmail. Чтобы получить доступ к Gmail, вам придется создать новый пароль Gmail специально для Thunderbird. Более подробная информация содержится в справочной системе Google.

5. Когда все данные будут аккуратно введены, нажмите кнопку Готово (Done) — Thunderbird загрузит копии электронных писем с почтового сервера на ваш компьютер. Попробуйте отправить друзьям тестовое сообщение.

Установка Enigmail

Использование Thunderbird с дополнением Enigmail позволяет легко шифровать и расшифровывать содержимое электронной почты. Но, как уже отмечалось, при этом информация об отправителе и получателе не шифруется, а если ее зашифровать, письмо не сможет быть отправлено.

Загрузить дополнение Enigmail в формате XPI можно с веб-сайта tinyurl.com/jyqxdwq. Дополнение Enigmail устанавливается не так, как Mozilla Thunderbird и GPG4Win:

1. Нажмите кнопку j в правом верхнем углу окна Thunderbird и выберите пункт Дополнения (Add-ons) — откроется вкладка Управление дополнениями (Add-ons Manage).
2. Нажмите кнопку чтобы отобразить меню.
3. Выберите в этом меню пункт Установить дополнение из файла (Install add-on from file) (рис. 6.3) — откроется диалоговое окно выбора файла.

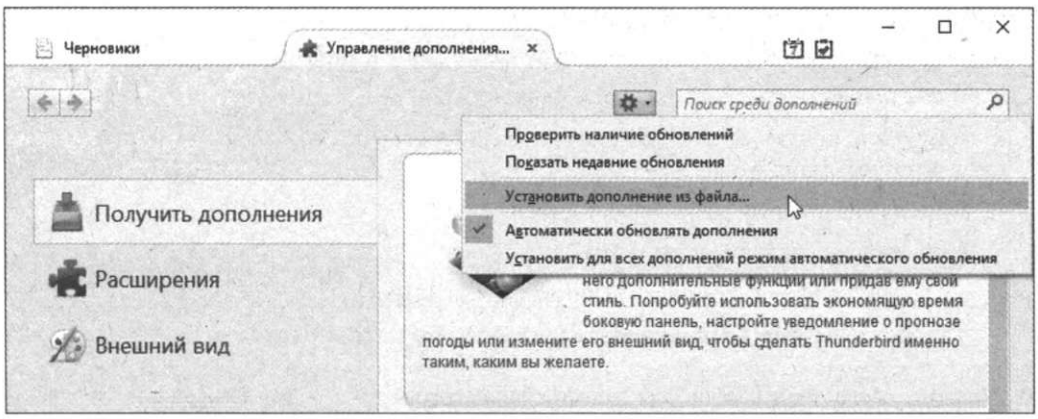


Рис. 6.3. **Установка дополнения в программе Mozilla Thunderbird**

4. Перейдите в папку, в которую был сохранен загруженный файл Enigmail, и выберите его (файл с именем вида enigmail-1.8.2-tb+sm.xpi). Нажмите кнопку Открыть (Open).
5. В диалоговом окне с запросом подтверждения на установку Enigmail нажмите кнопку Установить сейчас (Install Now).
6. После установки Enigmail браузер Mozilla Thunderbird предложит перезагрузиться, чтобы активировать Enigmail.
7. Щелкните мышью на ссылке Перезагрузить сейчас (Restart Now) — после перезагрузки программы Mozilla Thunderbird откроется дополнительное диалоговое окно с предложением настроить дополнение Enigmail.
8. Установите переключатель в положение Start setup now (Начать установку сейчас) и нажмите кнопку Далее (Next) — вы увидите диалоговое окно с предложением выбрать режим настройки программы: для начинающих пользователей, для опытных и для экспертов (вручную). Нам предпочтителен первый вариант.
9. Установите переключатель в положение I prefer a standard configuration (recommended for beginners) (Я предпочитаю стандартную конфигурацию (для начинающих)) и нажмите кнопку Далее (Next) — откроется диалоговое окно, в котором нужно указать пароль для защиты закрытого ключа (рис. 6.4).

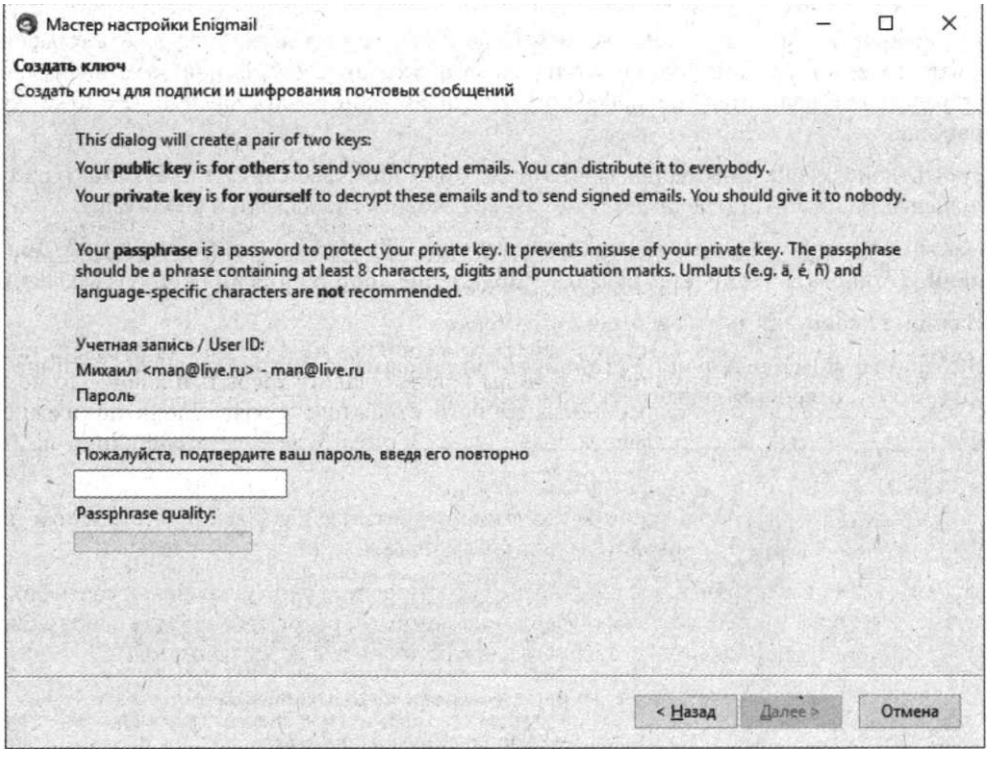


Рис. 6.4. Создание пароля для защиты закрытого ключа

10. Укажите желаемый пароль для защиты закрытого ключа — он должен состоять из не менее чем 8 символов и содержать латинские буквы, цифры и знаки пунктуации. Введите пароль в оба поля и нажмите кнопку Далее (Next).

11. Теперь помогите программе сгенерировать ключи, перемещая мышь и щелкая ее кнопками, нажимая клавиши клавиатуры и выполняя на компьютере другие активные действия, — плагин Enigmail создаст пару ключей. Когда этот процесс завершится, появится окно с сообщением и запросом о создании сертификата отзыва (рис. 6.5).

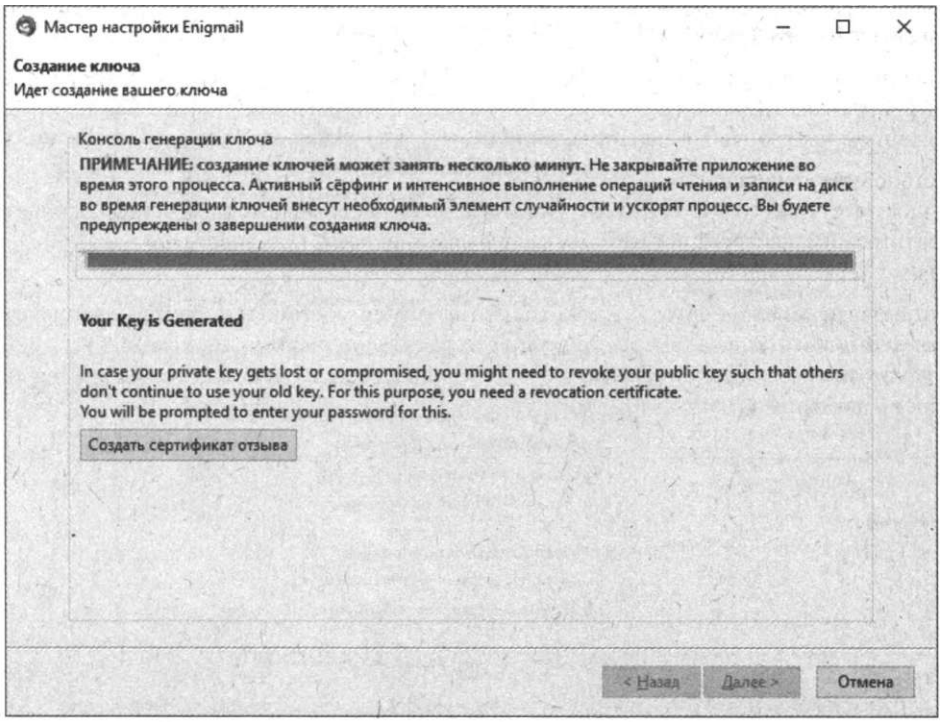


Рис. 6.5. Создание ключей завершено

Такой сертификат может быть полезен, если возникнет необходимость отозвать прежние ключи. Обратите внимание — если вы просто удалите закрытый ключ, это не повлечет за собой неработоспособность парного открытого ключа. Люди по-прежнему смогут отправлять вам зашифрованные письма, но вы будете не в состоянии их расшифровать.

12. Нажмите кнопку Создать сертификат отзыва (Generate Certificate) — откроется диалоговое окно с запросом пароля, созданного на шаге 9.
13. Введите пароль к закрытому ключу, после чего откроется окно сохранения сертификата отзыва. Хотя вы можете сохранить файл и на компьютере, рекомендуется использовать для этого Flash-накопитель, который вы должны хранить в безопасном месте.
14. Вот и все, что касается создания открытого и закрытого ключей.
15. Нажмите кнопку Далее (Next), а затем кнопку Готово (Finish).

Использование PGP/MIME

Последний шаг настройки программы Thunderbird — включение использования PGP/MIME. Этот способ позволяет упростить отправку зашифрованных писем с вложениями.

Вы можете найти эти настройки, нажав кнопку Щ в правом верхнем углу окна Thunderbird и выбрав пункт Настройки | Параметры учетной записи (Options I Account Settings). Откроется одноименное диалоговое окно.

Выбрав в этом окне вкладку Защита OpenPGP (OpenPGP Security), установите флажок Использовать PGP/MIME по умолчанию (Use PGP/MIME by default) (рис. 6.6). После нажатия кнопки OK использование PGP/MIME по умолчанию будет включено.

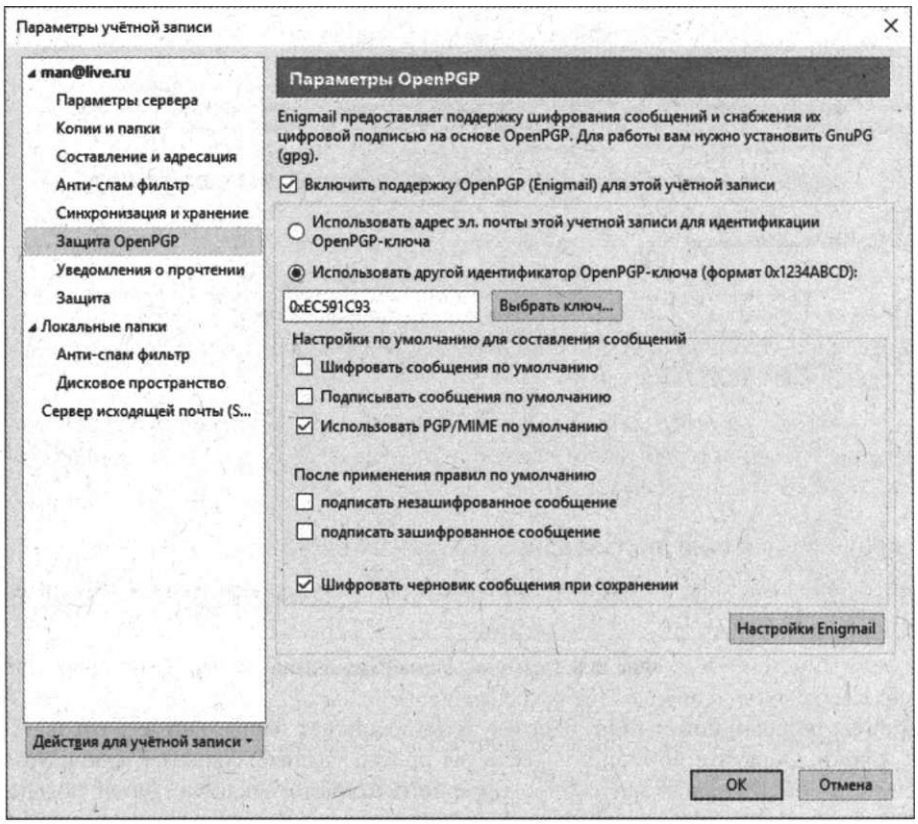


Рис. 6.6. Настройки OpenPGP в программе Thunderbird

Оповещение адресатов об использовании PGP

Итак, у вас есть возможность использовать шифрование PGP. Хорошо бы сообщить об этом участникам вашей переписки — тогда вы сможете обмениваться с ними шифрованными письмами. Существует три способа это сделать:

Оповещение людей об использовании PGP по электронной почте

Вы можете отправить другому человеку ваш открытый ключ по электронной почте как вложение.

1. Нажмите кнопку Создать (Write) в окне программы Mozilla Thunderbird.
2. Укажите адрес и тему письма, например: мой открытый ключ. Выберите в меню Enigmail пункт Присоединить мой открытый ключ (Attach My Public Key) (рис. 6.7).

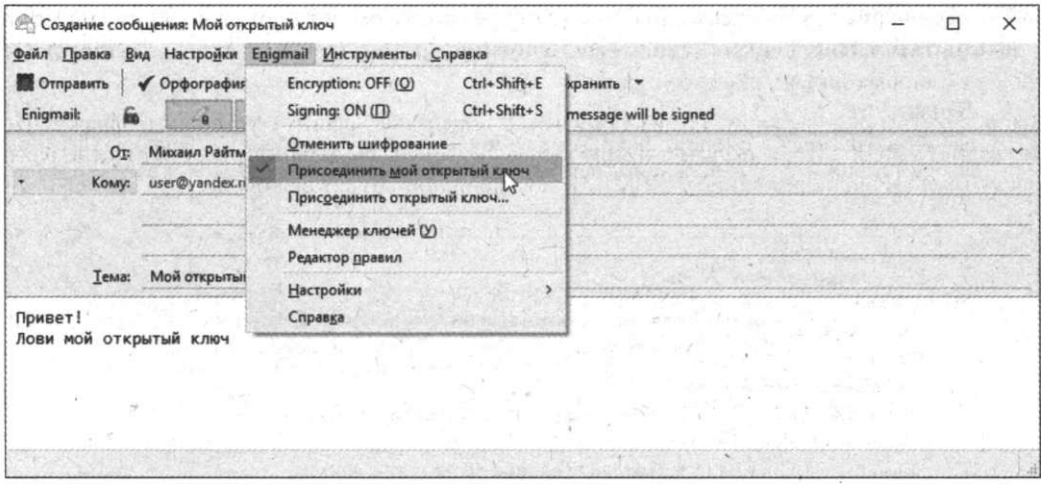


Рис. 6.7. Вложение открытого ключа **в** письмо

3. Отправьте электронное письмо — получатель сможет загрузить и использовать открытый ключ, посланный вами.

   При использовании этого метода рекомендуем получателю письма проверить отпечаток вашего ключа по альтернативному каналу связи (на случай, если электронная почта уже перехватывается и подделывается).

Оповещение людей об использовании PGP через веб-сайт

Вы можете дополнительно разместить свой открытый ключ на каком-либо веб-сайте, загрузив туда файл и указав ссылку на него.

1. Нажмите кнопку ____ в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Менеджер ключей** (Enigmail | Key Management).
2. В открывшемся диалоговом окне выделите ключ и щелкните по нему правой кнопкой мыши для вызова контекстного меню.
3. Выберите **в** контекстном меню пункт **Экспортировать ключи в файл** (Export keys to file) (рис. 6.8).

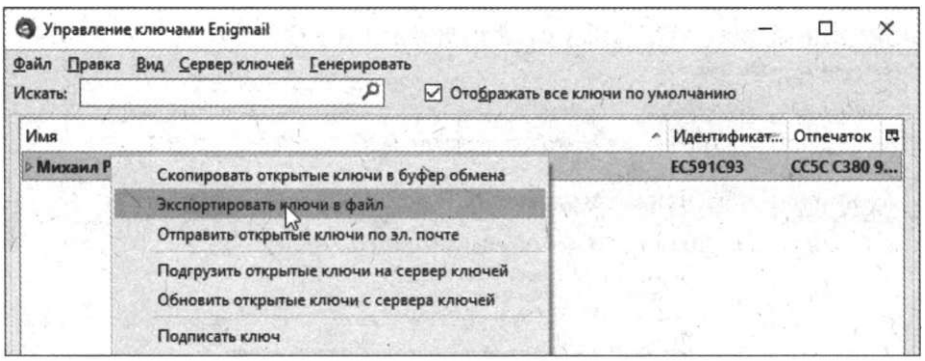


Рис. 6.8. Экспорт ключей **в** файл

4. **В** открывшемся диалоговом окне с предупреждением нажмите кнопку **Экспорт только открытых ключей** (Export Public Keys Only) (рис. 6.9).

> ***ВНИМАНИЕ!***
>
> Не нажмите кнопку **Экспорт закрытых ключей** (Export Secret Keys)! Экспорт закрытого ключа позволит злоумышленнику притвориться вами (если ему удастся угадать/взломать ваш пароль).

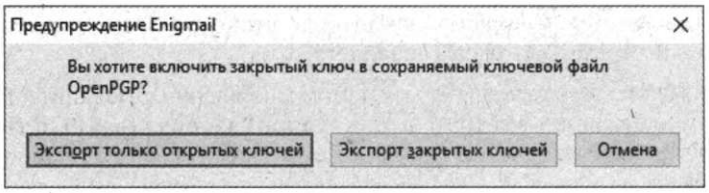


Рис. 6.9. Предупреждение об экспорте ключей

5. Откроется окно сохранения файла — сохраните открытые ключи в желаемую папку, например, в **Документы** (Documents).

   Теперь вы можете использовать этот файл по своему усмотрению — например, выложить его на файловый хостинг Яндекс.Диск и предоставить собеседникам ссылку.

Загрузка ключей на сервер ключей

Серверы ключей облегчают поиск и скачивание открытых ключей. Большинство современных серверов ключей синхронизируются друг с другом. Таким образом, если чей-либо открытый ключ загружен на один сервер, он, в конечном счете, становится доступен на всех серверах. Но следует помнить о специфике работы серверов ключей — ключ, который загружен на сервер, не может быть впоследствии оттуда удален, вы сможете только ***отозвать*** его. То есть, после загрузки вашего открытого ключа на сервер все будут знать, что вы используете PGP. Решите, насколько это для вас приемлемо.

1. Нажмите кнопку в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Менеджер ключей** (Enigmail | Key Management).
2. В открывшемся диалоговом окне выберите команду меню **Сервер ключей | Подгрузить открытые ключи** (Keyserver | Upload Public Keys) (рис. 6.10).

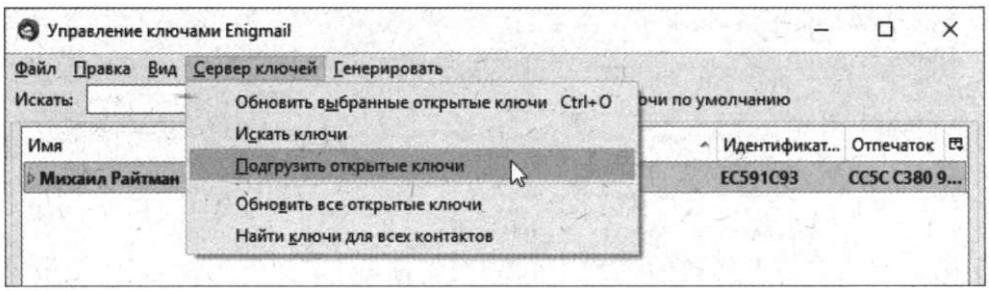


Рис. 6.10. Выгрузка открытых ключей на сервер

Поиск других пользователей PGP

О том, что у вас есть возможность использовать шифрование PGP, вы нужным людям сообщили. Теперь вам нужно обзавестись открытыми ключами участников вашей переписки, чтобы иметь возможность читать их шифрованные сообщения.

Получение открытого ключа по электронной почте

Вы можете получить открытый ключ как вложение электронной почты.

1. Щелкните мышью по полученному сообщению, чтобы отобразить текст письма в нижней части окна программы Mozilla Thunderbird.
2. Обратите внимание на вложение под текстом сообщения. Щелкните правой кнопкой мыши на этом вложении и выберите пункт **Импорт ключа OpenPGP** (Import OpenPGP Key) в контекстном меню (рис. 6.11) — откроется диалоговое окно импорта ключа.

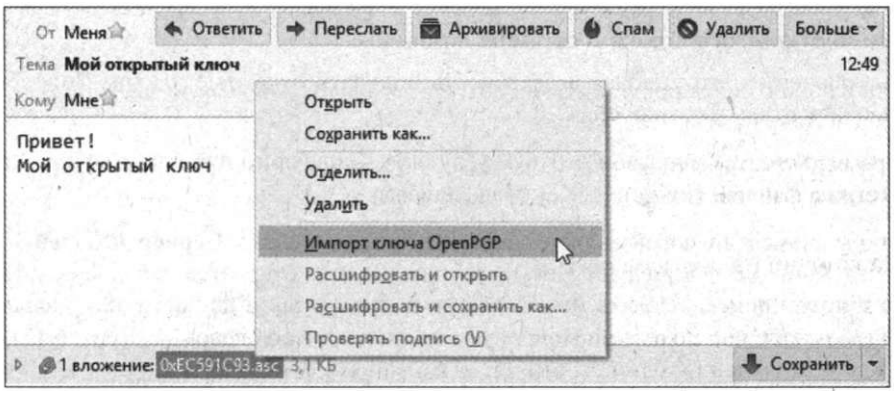


Рис. 6.11. Импорт ключа OpenPGP

3. Нажмите в нем кнопку **ОК.**

Нажав кнопку в правом верхнем углу окна Thunderbird и выбрав пункт **Enigmail** | **Менеджер ключей** (Enigmail | Key Management), вы сможете проверить результат. Обратите внимание — ваш ключ PGP выделен жирным шрифтом (потому что у вас есть и закрытый, и открытый ключи), А вот открытый ключ, который вы только что импортировали, не выделен жирным шрифтом, потому что соответствующего закрытого ключа у вас нет (рис. 6.12).

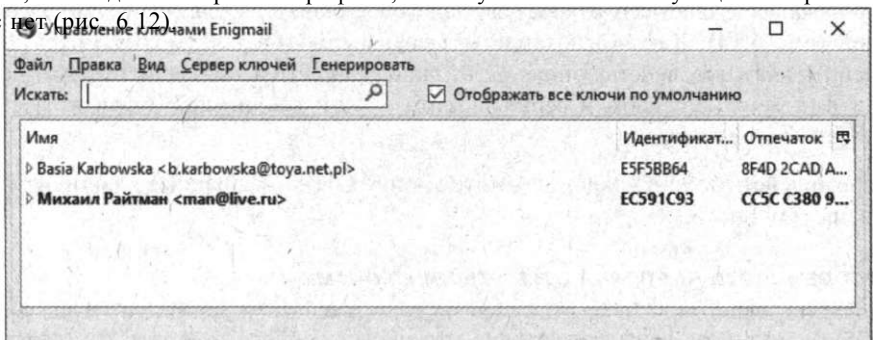


Рис. 6.12. Результат импорта открытого ключа

Получение открытого ключа в виде файла

Открытый ключ часто можно получить, загрузив его с веб-сайта, куда его выложил владелец. В этом случае выполните следующие действия:

1. Нажмите кнопку в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Менеджер ключей** (Enigmail | Key Management).
2. Выберите команду меню **Файл | Импортировать ключи из файла** (File | Import Keys from File).
3. Файлы открытых ключей могут иметь различные имена и даже разные расширения — например: asc, рдр или дрд.
4. Выберите файл и нажмите кнопку **Открыть** (Open).
5. В открывшемся диалоговом окне нажмите кнопку OK.

Получение открытого ключа с сервера ключей

Серверы ключей — это удобная возможность получать открытые ключи. Попробуем выполнить поиск открытых ключей.

1. Нажмите кнопку ___ в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Менеджер ключей** (Enigmail | Key Management).
2. В открывшемся диалоговом окне выберите команду меню **Сервер ключей | Искать ключи** (Keyserver | Search for Keys) (см. рис. 6.10) — откроется небольшое диалоговое окно с полем поиска. Искать можно как по полному, так и по частичному адресу электронной почты, или по имени. Попробуем найти ключи со словом rus (рис. 6.13).

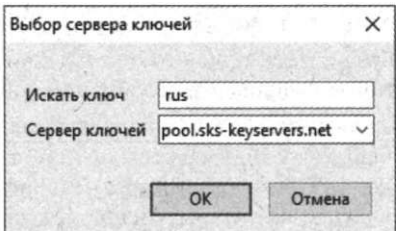


Рис. 6.13. Настройки поиска открытых ключей

После нажатия кнопки **OK** откроется диалоговое окно с результатами поиска открытых ключей (рис. 6.14). Как можно видеть, каждый пользователь может иметь несколько ключей, причем все действующие. Если окно прокрутить, вы заметите, что некоторые ключи выделены курсивом и серым цветом, — эти ключи либо были отозваны, либо сроки действия их истекли.

3. Выберите действующий ключ и нажмите кнопку **OK** - выбранные ключи будут импортированы (см. рис. 6.12).

ОСОБЕННОСТИ ВЛАДЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ

Обратите внимание — открытый ключ на сервер может загрузить кто угодно. Нельзя исключить, что один из найденных вами ключей загружен вовсе не тем, кто представляется его владельцем. В этом случае очень важно сверить отпечатки ключей.

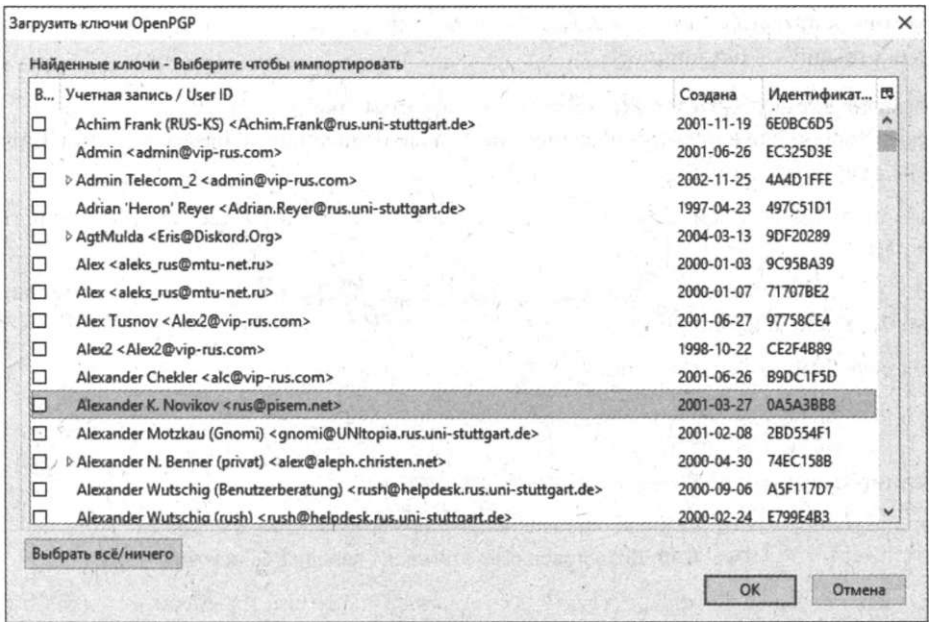


Рис. 6.14. Результаты поиска открытых ключей

Отправка зашифрованных сообщений

Отправим первое зашифрованное письмо.

1. **В** главном окне Mozilla Thunderbird нажмите кнопку **Создать** (Write) — откроется окно нового сообщения.
2. Напишите сообщение, выбрав адресата, чей открытый ключ у вас уже есть, — Enigmail обнаружит ключ и автоматически зашифрует сообщение (рис. 6.15).

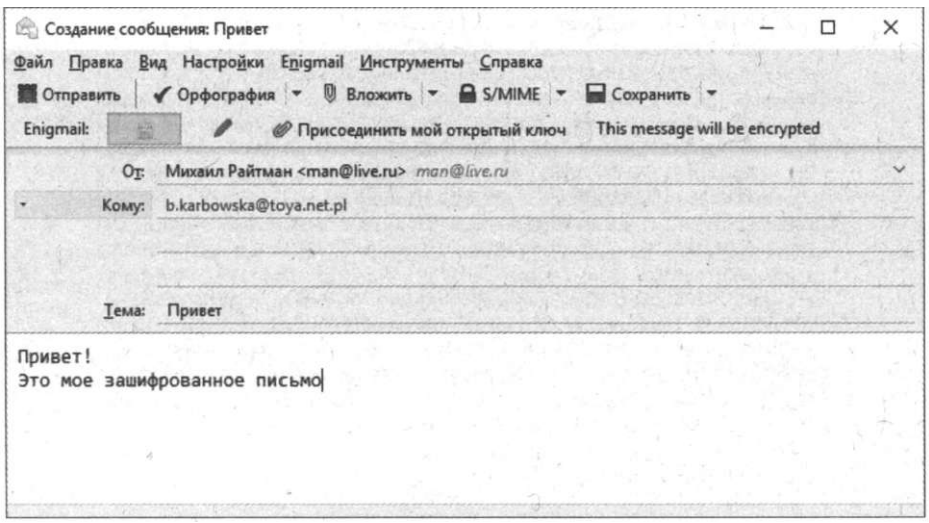


Рис. 6.15. Создание зашифрованного сообщения

Обратите внимание — тема письма не будет зашифрована, поэтому для нее лучше выбрать что-нибудь безобидное.

3. Нажмите кнопку Отправить (Send) — откроется диалоговое окно, в котором нужно ввести пароль для вашего PGP-ключа (не пароль от почтового ящика!) (рис. 6.16).

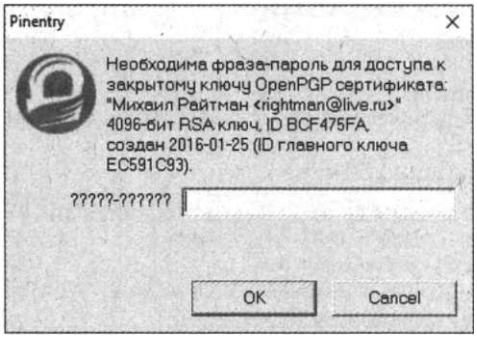


Рис. 6.16. Диалоговое окно для ввода пароля PGP-ключа

4. Введите пароль и нажмите кнопку ОК — ваше электронное письмо будет зашифровано и отправлено.

После шифрования содержимое письма будет выглядеть иначе — например, текст письма, показанного на рис. 6.15, преобразуется так, как показано на рис. 6.17.

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIMA4XhuUO89HX6ARAAoHAUBG7JaiGDNiMNxT2+kkhTzJGeHfBYPWxPVV5bkodI
3XcjrISP8ZpjQ1gqOgOH6Ol7ovOf6bBvr7LNP0BbFbrSw7cUiEk8dv1+7BaNSE5x
YEtKDY7MsW3x0MQbLjAw8qaGyXHOHxS4dlCdYB6GW1PN3XJ/9JRJw4QwGt5PTp0Q
eGEwgfnJig+lJqu3B1Go4BK4ME3zvkSX9vQUCeJwfBP2P84XeCei7Jrgs1MGp5Lt
Q/0lKQPpNCuCa8sKNwI1Sh0qQ4q4wBDdq5F1TGzEqL4bTeIVZkTwl1kqIgw/61dG
iTIBVic+RN45q7z4akxFB8HucOx39dxD2JvCEofwk/zZRaAoxscSW8q5RQY/G4uN
6SB+rgRg4NSZUbcyclhsCCP7dLGt6nHwMaEM4AWvwNMfpxmhX6dKdsUP1yjLTIWU
VSlmBzhIfgF5t3ayFDwRCXBFM42l9tXYgaulL1K5WUAAzlYhDvdjVaYTO8pL2bpX
td+Kkrfgaf/eJ/zjeQkvEXgi3oYQ3FRTrTT3LmBR2ss54qlaBSdeCDpTE+6uqzcr
8sX+lxF78phXaioEuhey6P6+lCyGzDN8djnEU/bgkSY/Gi54iOv8/pKsKtCQoZQy
UtZnG4WwiaQcS+I0WoNmJAYB1lveUcIWQV8t594ieIu8Vu8ngZnW4r+rueEhULPS
wQoBdOMJ6tWRTwSbUAQWlBUo66d74NpSGw/dizc6WTdNutmafjUbAfBCqhjx2eRI
i8Po8rG5dujJNIzIszabwFVYg1rxPRQ04IO71aXZZwiZp+MQ9cMDKRte9wSoycLH
iWamT+sjUQ3W7xLBcmyDBqs0rtYaiKAvxDjoy4LuuKB2vQCZ2H23O3/wj5+oYcDC
ajo9++arPznj8lyjwRk5m/2dAmgxALKHxtjRTHTOb2RZjcoQmT35Ug73+oUFzAPs
aTpUe1HO7PzZlbo06LDk1Bw9eu8Mu+0SHnfX7VP+7ObAHHGtp/n5n8MYNpvK91Fr
O6YuVETG+HXx18pBcxW2aKAzUC1xIFc/+XWm9yeBuBKOBMfvULn8kYu6W4fZWLcP
B2CX+W1jRBykt+Kat2HbAPEP1dk1YkBccOfvJ7QkzzFa3gPjMNa28yA4j9tybmeq
qXlY3SSZPMDKRsmJkD3ViE1R4U4xiRa+1MmaLm8JbmAuAtExHxru5EyDyMjwY+Jz
4R/Bg5ULCsoL8O7J7k5hHgnnQcnu3bZp/bzQOWmCrqKaaVrU+TQFIyZlZn180UR8
9BULv+9qbJ060aYC2KkUNV9Q/euvX5MGXcvrlA==
=ZrD9
-----END PGP MESSAGE-----
```

Рис. 6.17. Зашифрованное письмо

Чтение зашифрованных сообщений

1. Если вы получили зашифрованное письмо, щелкните по нему мышью — откроется диалоговое окно с запросом пароля к PGP-ключу (это не пароль электронной почты!)
2. Введите пароль и нажмите кнопку OK — сообщение будет расшифровано.

Отзыв PGP-ключа

Срок действия PGP-ключей, созданных в программе Enigmail, — пять лет. Возможно, вам понадобится прекратить действие своего ключа ранее этого срока. Например, если вы захотите создать новый, более защищенный, PGP-ключ или если потеряете файлы с ключами.

Отзыв PGP-ключа с помощью Enigmail

Самый простой способ отозвать свой PGP-ключ в Enigmail — использовать встроенный диспетчер ключей.

1. Нажмите кнопку в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Менеджер ключей** (Enigmail | Key Management).
2. Щелкните правой кнопкой мыши по вашему PGP-ключу (выделен жирным шрифтом) и выберите команду **Отозвать ключ** (Revoke Key) — откроется окно с запросом подтверждения.
3. Нажмите в этом окне кнопку **Отозвать ключ** (Revoke Key) — откроется окно для ввода пароля.
4. Введите пароль от PGP-ключа и нажмите кнопку **ОК.**
5. Нажмите кнопку OK в следующем открывшемся диалоговом окне.

В окне **Управление ключами Enigmail** (Enigmail Key Management) вы заметите изменения — ваш PGP-ключ стал серым и выделенным курсивом (рис. 6.18).

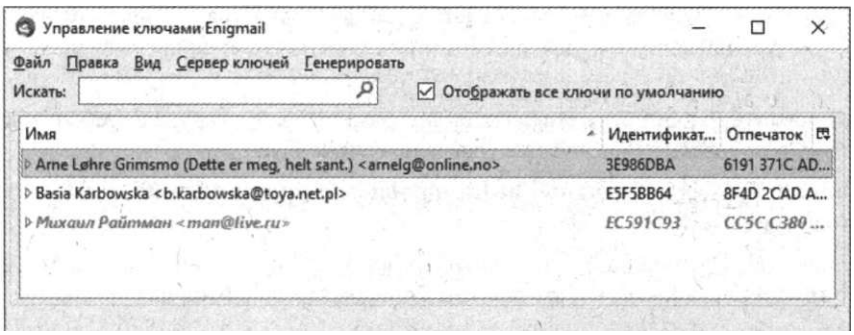


Рис. 6.18. Ключ отозван

Отзыв PGP-ключа с помощью сертификата отзыва

Ранее мы говорили о том, что Enigmail генерирует и импортирует сертификаты для отзыва ключей. Поскольку у вас уже есть сертификат отзыва, вы можете использовать его для отзыва своего ключа.

1. Нажмите кнопку; в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Менеджер ключей** (Enigmail | Key Management).

2. Выберите команду меню **Файл | Импортировать ключи из файла** (File | Import Keys from File) — откроется диалоговое окно, в котором можно выбрать сертификат отзыва.
3. Выберите файл сертификата и нажмите кнопку **Открыть** (Open) — появится сообщение о том, что сертификат был успешно импортирован, а ключ — отозван.
4. Нажмите кнопку OK и вернитесь к окну **Управление ключами Enigmail** (Enigmail Key Management) — вы увидите, что отозванный ключ стал серым и выделен курсивом (см. рис. 6.18).

Если отозванный вами ключ принадлежит вам, и вы ранее загрузили свой открытый ключ на сервер ключей, рекомендуется обновить информацию и на сервере. Это поможет другим людям сориентироваться и не использовать отозванный ключ.

PGP в OS X

Здесь мы рассмотрим, как работать с PGP на компьютере Mac. Вы можете воспользоваться в качестве клиента электронной почты как встроенной в OS X программой Apple Mail, так и популярным почтовым приложением Mozilla Thunderbird. На данный момент нет возможности использовать PGP непосредственно с веб-сервисом электронной почты — таким как Gmail или Mail.ru. Но вы можете настроить PGP-шифрование для отправки писем со своего привычного почтового адреса в программе Mail или Thunderbird.

> ***ВНИМАНИЕ!***
>
> **Для ведения шифрованной переписки требуется, чтобы PGP-совместимые программы были установлены у каждого ее участника.**

Установка программы GPGTools

PGP — открытый стандарт, поддерживаемый во множестве различных программ. В этом разделе рассматривается программа GPG Suite, входящая в пакет GPG Tools. Программа работает в среде OS X, является бесплатной и распространяется с открытым исходным кодом (код программы доступен для разработчиков, желающих проверить ее на ошибки и бэкдоры).

После установки GPG Suite вам нужно будет создать свою пару ключей, после чего вы сможете начать работать с PGP в Apple Mail или Thunderbird.

1. Откройте в браузере страницу **https://gpgtools.org/gpgsuite.html** и нажмите кнопку **Download GPG Suite.**
2. После загрузки DMG-образа программы откройте его и щелкните двойным щелчком на кнопке **Install** (Установить) — отобразится список компонентов для установки.

   В основном, перечисленные в нем утилиты работают в фоновом режиме. Их задача — обеспечить использование PGP другими программами на вашем компьютере:

   - GPGMail позволяет программе Apple Mail отправлять и читать шифрованные сообщения;
   - GPG Services добавляет в OS X функционал, с помощью которого можно использовать PGP не только для электронной почты, но и в других приложениях (например, в текстовом редакторе);
   - GPG Keychain позволяет управлять открытыми и закрытыми ключами примерно так, как паролями;

- GPGPreferences служит для изменения настроек PGP;
- наконец, MacGPG2 является основным инструментом, который другие программы используют для шифрования и подписи сообщений.

3. Нажмите кнопку **Продолжить** (Continue), а затем кнопку **Установить** (Установить Install), чтобы установить GPG Suite. При необходимости, введите пароль администратора.

Когда установка завершится, автоматически откроется утилита GPG Keychain, и вам будет предложено создать ключи (рис. 6.19).

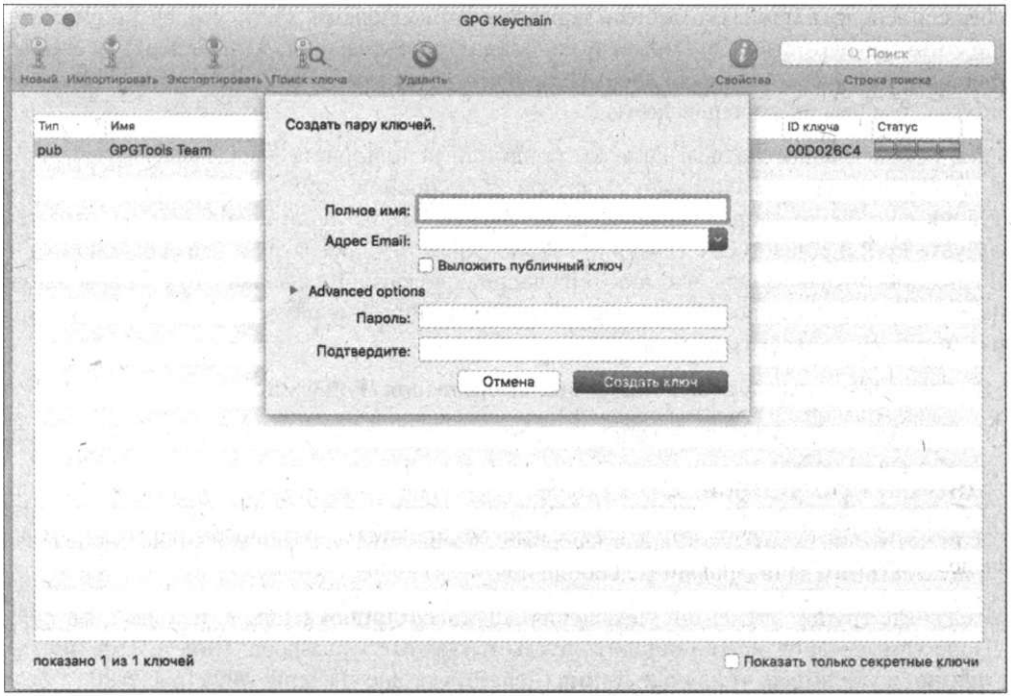


Рис. 6.19. Панель для создания ключей на фоне окна в PGP Keychain

Если Keychain не откроется автоматически, запустите ее вручную (программа находится среди ваших приложений).

Создание PGP-ключей

Следует потратить немного времени и определиться с настройками PGP-ключей, поскольку позже будет трудно изменить их свойства. Если вы опубликуете ключ, то не сможете отменить эту публикацию (до сих пор часто попадаются тысячи открытых еще в 1990-х годах ключей со старыми именами и недействующими адресами электронной почты).

PGP-ключ содержит имя и адрес электронной почты, которые идентифицируют его владельца. Эти данные — один из способов для отправителя понять, кому принадлежит тот или иной ключ. В большинстве случаев правильный путь — указать при создании ключа PGP реальный адрес электронной почты, а затем загрузить ключ на публичный сервер ключей. Тогда пользователи, которые захотят отправить вам зашифрованное письмо, смогут использовать верный ключ. Они станут отправлять вам сообщения, шифруя их именно ва-

пшм открытым ключом. А получатель вашего сообщения с цифровой подписью сможет проверить эту подпись.

Этот подход годится не для всех. Модель угроз может быть такой, что лучше не связывать ключ PGP с реальным именем его владельца. Прежде чем раскрыть свою личность, Эдвард Сноуден общался с журналистами, используя PGP и анонимный адрес электронной почты. Его ключ, разумеется, не был ассоциирован с его настоящим именем.

Загружать открытые ключи на сервер — обычная практика. Но это действие свидетельствует о том, что вы шифруете информацию (даже если не используете свое реальное имя). Кроме того, как будет понятно далее, другие пользователи тоже могут загружать ваш ключ на сервер и подписывать его своими собственными ключами, подтверждая таким образом ваше с ними знакомство. Это может быть нежелательно, если вы хотите держать свои коммуникации в секрете (или если злоумышленник хочет представить дело так, будто вы общаетесь с тем или иным человеком).

Общие рекомендации таковы. Если вы привыкли использовать псевдоним, сделайте это и для ключа (и укажите какой-нибудь другой, не основной адрес электронной почты). Если ситуация еще более напряженная, и вы не хотите, чтобы люди вообще знали, что вы используете PGP и общаетесь с теми или иными адресатами, не загружайте свой ключ на публичный сервер и убедитесь, что никто из ваших адресатов не сделает это с вашим ключом. Существуют и другие способы проверки ключей, которые не размещены на публичных серверах (о них было рассказано ранее).

1. Введите свое имя или псевдоним в поле Полное **имя** (Full N?ime).
2. В поле Адрес Email (Email Address) укажите свой основной или дополнительный адрес электронной почты.
3. Установите флажок **Выложить публичный ключ** (Upload public key after generation), если хотите загрузить свой ключ на сервер, чтобы другие люди могли быстро его найти и посылать вам зашифрованные сообщения.
4. Раскройте группу элементов управления **Advanced options** (Дополнительные настройки). Поле комментария можно оставить пустым, укажите тип ключа: **RSA и RSA (по умолчанию)** и убедитесь, что в поле **Длина** (Length) указано значение **4096** (рис. 6.20).

   Обратите внимание, что для открытого ключа установлен определенный срок действия. Когда он истечет, ваши собеседники больше не смогут использовать этот ключ, чтобы шифровать для вас сообщения. Специального предупреждения или подсказки об этом вы не получите. Так что сделайте в своем календаре пометку, чтобы обратить внимание на истекающий срок ключа, к примеру, за месяц до указанной даты.

   Кстати, срок службы действующего ключа можно продлить, определив для него новую, более позднюю дату. Можно создать и новый ключ. В обоих случаях понадобится связаться с вашими собеседниками по электронной почте и убедиться, что они получили ваш новый ключ.

   Если же управление ключом является для вас проблемой, можно снять ограничение по дате, хотя в этом случае другие люди могут попытаться использовать ваш «вечный» ключ, даже если у вас не будет больше парного закрытого ключа, или вы вообще перестанете использовать PGP.
5. Укажите пароль для защиты PGP-ключа в поля ввода **Пароль** (Password) и **Подтвердите** (Confirm), а затем нажмите кнопку **Создать ключ** (Generate key).

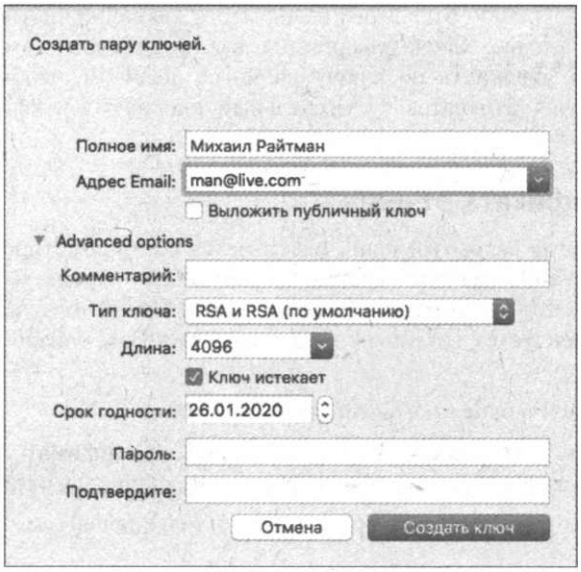


Рис. 6.20. Настройки ключа

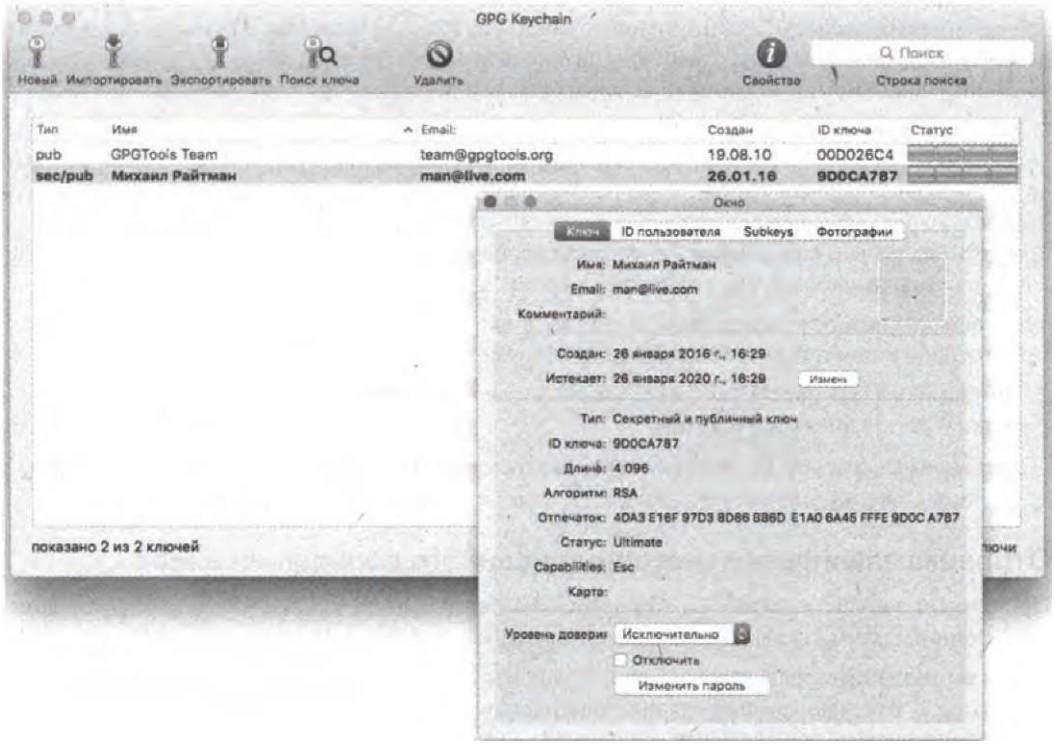


Рис. 6.21. КЛЮЧ **создан!**

Компьютер начнет генерацию открытого и закрытого ключей. Обычно это занимает не более минуты. Когда создание ключа завершится, вы увидите ключ в окне программы GPG Keychain. Вы можете щелкнуть по ключу двойным щелчком, чтобы посмотреть информацию о нем, включая отпечаток — уникальный способ идентифицировать ключ PGP (рис. 6.21).

Создание сертификата отзыва

Бывают ситуации, когда закрытый ключ оказывается скомпрометирован — кем-либо скопирован. Или вы случайно удалили его, или забыли к нему пароль. В таких случаях вы можете сообщить всем, что отзываете (отменяете) ключ. Для этого существует специальный сертификат, и рекомендуется создать его прямо сейчас. Вам понадобится закрытый ключ (и пароль к нему).

1. Выделите свой ключ в окне программы GPG Keychain.
2. Выберите команду меню **Ключ | Сгенерировать сертификат отзыва** (Key | Create Revocation Certificate), а затем сохраните файл, нажав кнопку **Сохранить** (Save).

Вы можете хранить этот файл вместе с резервной копией ключей (см. далее).

Создание резервных копий PGP-ключей

Если вы потеряете доступ к закрытому ключу, то не сможете расшифровать поступающую почту (или ранее полученную зашифрованную почту). Закрытый ключ, как уже неоднократно подчеркивалось, нужно хранить самым надежным образом. Вы можете сохранить резервную копию ключа на Flash-накопителе и хранить его в каком-нибудь надежном месте. Копия понадобится, если вы потеряете свой ключ.

В том случае, если у вас украли компьютер или резервную копию ключа, злоумышленник вовсе необязательно сможет прочесть ваши зашифрованные сообщения, — если, разумеется, вы использовали надежный пароль. Впрочем, ради большей безопасности в таком случае, возможно, есть смысл отозвать ключ PGP и создать новый. С помощью прежнего закрытого ключа все еще можно будет расшифровывать старые сообщения, но нельзя будет воспользоваться парным ему открытым ключом для шифрования новых писем.

1. Чтобы создать резервную копию ключа, в окне программы GPG Keychain Access выберите свой ключ и нажмите на панели инструментов кнопку **Экспортировать** (Export).
2. Вставьте в USB-порт Flash-накопитель, а затем выберите его в раскрывающемся списке **Где** (Where) панели сохранения.
3. Установите флажок **Включить секретный ключ в экспорт** (Allow secret key export) и нажмите кнопку **Сохранить** (Save).

Отправка зашифрованного/подписанного сообщения в Mail

При первом запуске программы Apple Mail мастер поможет вам настроить учетную запись электронной почты (здесь не описывается способ настройки почтового аккаунта).

Когда вы создадите новое сообщение, то увидите две кнопки справа от поля **Тема** (Theme): кнопка_____отвечает за шифрование сообщения, а кнопка — за цифровую подпись.

Если замок закрыт, письмо будет зашифровано (рис. 6.22).

Подписать можно любое сообщение, даже если получатель не использует PGP. При создании цифровой подписи требуется закрытый ключ, поэтому при подписании первого сообщения в программе Mail появится окно с запросом пароля.



Рис. 6.22. Окно нового сообщения в программе Apple Mail

Зашифровать сообщение можно только в том случае, если адресат пользуется PGP-шифрованием и у вас есть его открытый ключ. Если кнопка, отвечающая за шифрование, затенена и выглядит как , ее нажатие не приведет к результату, т. к. сначала нужно импортировать открытый ключ адресата. Попросите его прислать вам ключ или используйте приложение GPG Keychain, чтобы найти ключ на сервере ключей.

Для обеспечения дополнительной безопасности вы можете проверить ключ, полученный от адресата.

Настройка почтового клиента Mozilla Thunderbird

В этом разделе вы узнаете, как шифровать почту в почтовом клиенте Mozilla Thunderbird, используя плагин Enigmail.

1. Откройте веб-сайт Mozilla Thunderbird по адресу **tinyurl.com/pgee2u5** и нажмите зеленую кнопку **Загрузить бесплатно.**
2. После загрузки запустите скачанный файл и в открывшемся окне перетащите значок приложения Mozilla Thunderbird на папку **Приложения** (Applications) (рис. 6.23).
3. Запустите приложение Mozilla Thunderbird из папки **Приложения** (Applications) или с экрана **Launchpad** и подтвердите запуск, нажав кнопку **Открыть** (Open), а затем кнопку OK.
4. Нажмите кнопку **Установить по умолчанию** (Set as Default), чтобы использовать программу в качестве клиента электронной почты по умолчанию. В следующем диалоговом окне отобразится предложение получить новый адрес электронной почты.
5. Нажмите кнопку **Пропустить это и использовать мою существующую почту** (Skip this and use my existing email) — откроется новое окно.
6. Укажите в нем имя, адрес электронной почты и пароль, а затем нажмите кнопку **Продолжить** (Continue).

   Во многих случаях программа Mozilla Thunderbird может автоматически определять нужные настройки (рис. 6.24).



Рис. 6.23. Установка приложения Mozilla Thunderbird

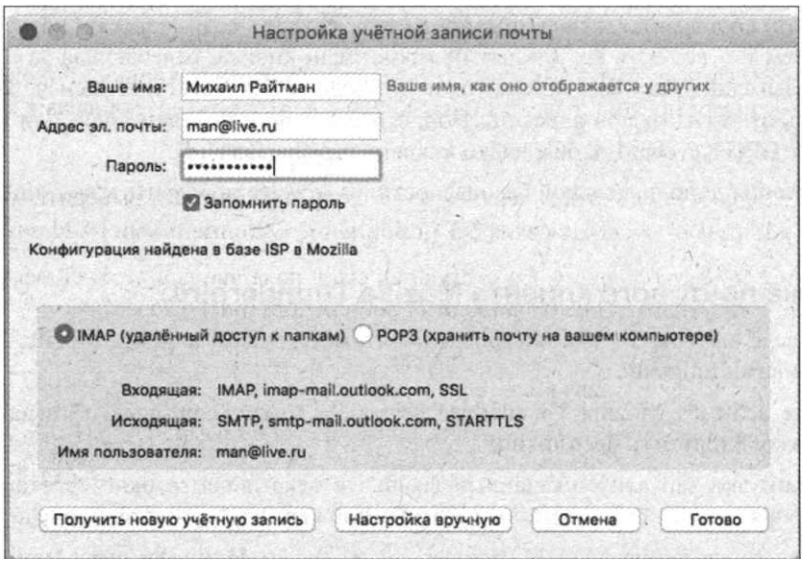


Рис. 6.24. Настройки учетной записи в программе Mozilla Thunderbird

Но иногда Mozilla Thunderbird недостаточно информации, тогда настраивать почту придется вручную. Далее показано, как это делается для учетной записи Gmail:

- Ваше имя (Your Name) — введите ваше имя или псевдоним;
- Адрес эл. почты (Email address) — укажите ваш полный адрес Gmail (в формате username@gmail.com);
- Пароль (Password) — ваш пароль Gmail;
- для сервера входящей почты IMAP:

[0] в раскрывающемся списке в

[0] имя сервера: imap.gmail.com;

- порт: 993;
- SSL: SSL/TLS;
- аутентификация: **Обычный пароль** (Normal password);

- для сервера исходящей почты SMTP:
  - имя сервера: **smtp.gmail.com;**
  - порт: 465 или 587;
  - SSL: SSL/TLS;
  - аутентификация: **Обычный пароль** (Normal password).
- **Имя пользователя** (Username): введите в оба поля ваш полный адрес Gmail (в формате **username@gmail.com).**

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Если для Google-аккаунта у вас включена двухфакторная аутентификация, то вы не сможете в Thunderbird использовать свой обычный пароль Gmail. Чтобы получить доступ к Gmail, вам придется создать новый пароль Gmail специально для Thunderbird. Более подробная информация содержится в справочной системе Google.

7. Когда все данные будут аккуратно введены, нажмите кнопку **Готово** (Done) — Thunderbird загрузит копии электронных писем с почтового сервера на ваш компьютер.

Теперь нужно установить Enigmail (GPG-плагин для Thunderbird).

1. Нажмите кнопку в правом верхнем углу окна Thunderbird и выберите пункт **Дополнения** (Add-ons) — откроется вкладка **Управление дополнениями** (Add-ons Manage).
2. Выполните поиск по слову enigmail, указав его в поле ввода в верхней части окна программы, — вы увидите список найденных дополнений (рис. 6.25).

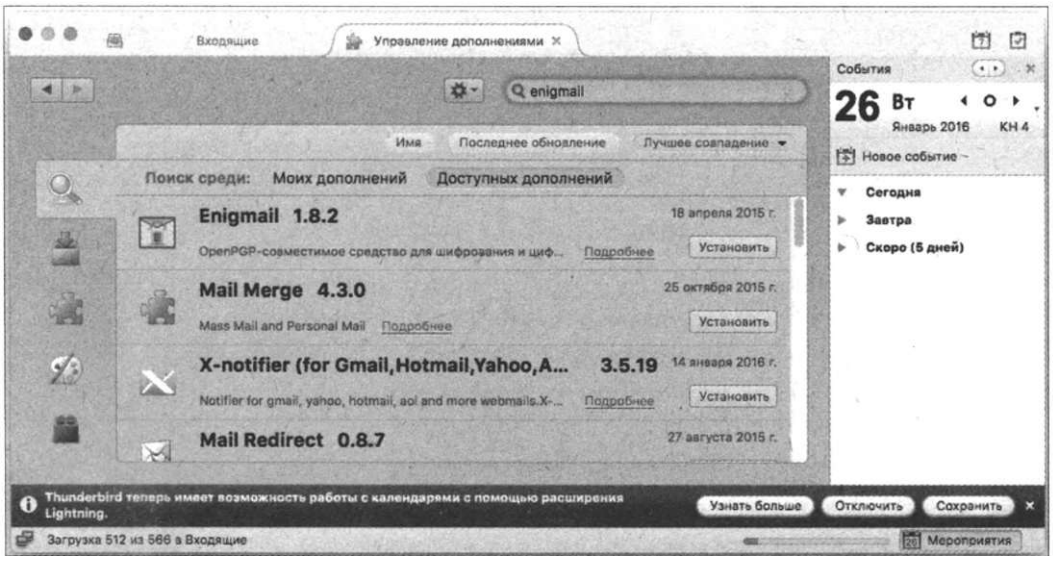


Рис. 6.25. Список найденных дополнений **в** программе Mozilla Thunderbird

3. В строке дополнения Enigmail нажмите кнопку **Установить** (Install) — после установки Enigmail браузер Mozilla Thunderbird предложит перезагрузиться, чтобы активировать Enigmail.
4. Щелкните мышью по ссылке **Перезапустить сейчас** (Restart Now) — после перезагрузки программы Mozilla Thunderbird появится дополнительное диалоговое окно с предложением настроить дополнение Enigmail.
5. Нажмите кнопку **Отмена** (Cancel) — мы настроим Enigmail вручную.
6. Нажмите кнопку в правом верхнем углу окна Thunderbird и выберите пункт **Настройки | Параметры учетной записи** (Options | Account Settings) — откроется одноименное диалоговое окно.
7. Выбрав вкладку **Защита OpenPGP** (OpenPGP Security), установите флажок **Включить поддержку OpenPGP (Enigmail) для этой учетной записи** (Enable OpenPGP support (Enigmail) for this identity).
8. Установите переключатель в положение **Использовать другой идентификатор OpenPGP-ключа** (Use specific OpenPGP key ID). Если ваш ключ не виден в этом поле по умолчанию, нажмите кнопку **Выбрать ключ** (Select Key) и выберите ключ вручную.
9. Флажки **Подписывать сообщения по умолчанию** (Sign messages by default), **подписать незашифрованное сообщение** (Sign non-encrypted message by default), **подписать зашифрованное сообщение** (Sign encrypted messages by default) и **Использовать PGP/MIME по умолчанию** (Use PGP/MIME by default) рекомендуется установить, а **Шифровать сообщения по умолчанию** (Encrypt messages by default) — сбросить (рис. 6.26).

   Идеальным вариантом было бы шифрование вообще всех исходящих сообщений, но это вряд ли возможно. Помните, что зашифрованное письмо можно отправлять только тому, кто пользуется PGP, и у вас должны быть открытые ключи этих людей. Оптимальный подход — вручную указывать, когда нужно зашифровать исходящее сообщение.
10. Нажмите кнопку OK, чтобы сохранить все настройки.

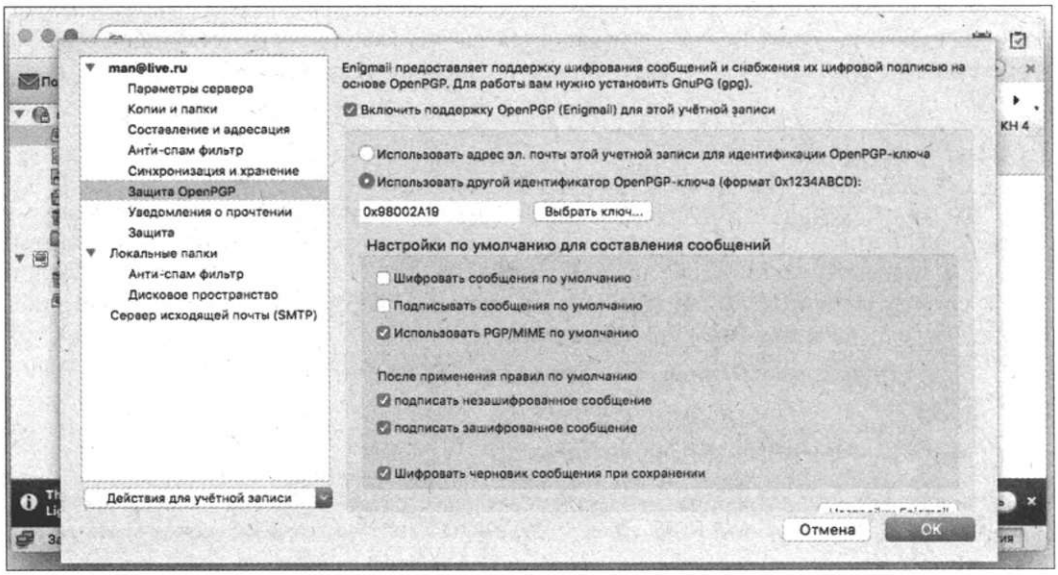


Рис. 6.26. Настройки OpenPGP **в** программе Thunderbird

На этом настройка Thunderbird и Enigmail завершена — теперь вы можете отправлять зашифрованные сообщения. При создании нового сообщения обратите внимание на две кнопки в верхней части окна: в виде карандаша (цифровая подпись сообщения) и замка (шифрование сообщения) (рис. 6.27).

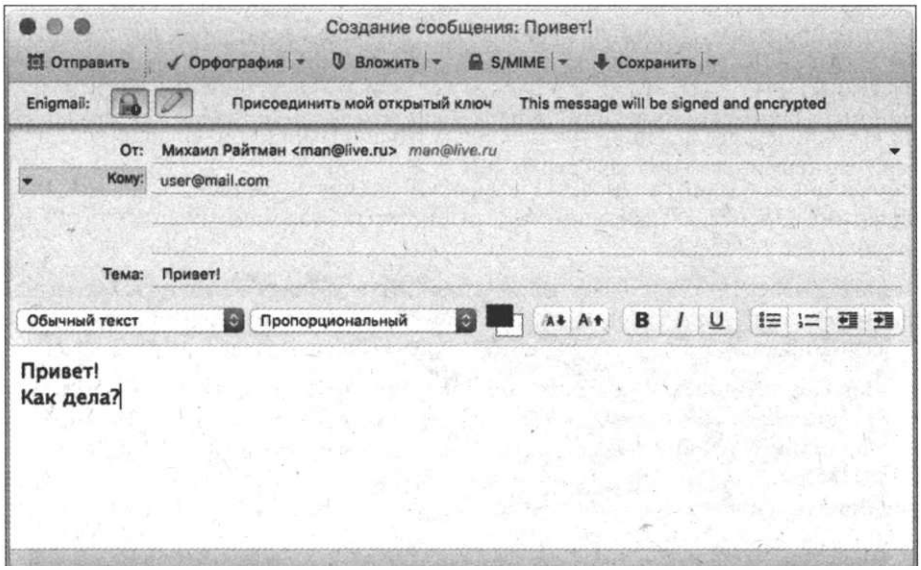


Рис. 6.27. Окно нового сообщения в программе Thunderbird

Если значок золотой, значит, соответствующая функция выбрана, если серебряный — нет. Нажимайте эти кнопки, чтобы включить/отключить подпись и шифрование.

В дальнейшем работа по оповещению других пользователей PGP, приему/отправке зашифрованной почты и отзыву PGP-ключей строится так же, как и в соответствующих разделах этой главы, посвященных PGP-шифрованию в операционной системе Windows.

PGP в Linux

Здесь мы рассмотрим, как использовать PGP в операционной системе Linux с популярным почтовым клиентом Mozilla Thunderbird. На данный момент нет возможности использовать PGP непосредственно с веб-сервисом электронной почты — таким как Gmail или Mail.ru. Но вы можете настроить PGP-шифрование для отправки писем со своего привычного почтового адреса в программе Mail или Thunderbird.

> ***ВНИМАНИЕ!***
>
> **Для ведения шифрованной переписки требуется, чтобы PGP-совместимые программы были установлены у каждого ее участника.**

Далее приведены приемы работы и настройки в операционной системе Linux Ubuntu, в других версиях Linux шаги могут несколько отличаться. В этом случае следует обратиться к справочной системе используемой операционной системы.

Установка Thunderbird, GnuPG и Enigmail

PGP — открытый стандарт, поддерживаемый во множестве различных программ. В этом разделе рассматривается программа GnuPG. Мы также установим дополнение Enigmail для программы Thunderbird, которое позволяет использовать PGP-шифрование в этом почтовом клиенте. Следующие шаги требуют выполнения некоторых команд в терминале.

1. Запустите программу Терминал (Terminal). Это можно сделать, нажав сочетание клавиш <Ctrl>+<Alt>+<T> или выполнив поиск по названию программы средствами операционной системы.
2. Если вы используете дистрибутив на основе Ubuntu (например, Ubuntu или Linux Mint), наберите в терминале команду (рис. 6.28):

```
sudo apt-get install gnupg thunderbird enigmail
```

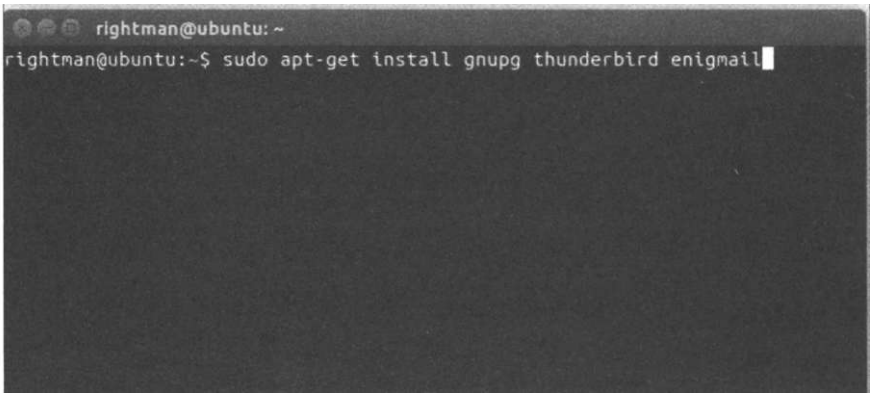


Рис. 6.28. Окно программы Терминал в операционной системе Ubuntu

Если вы используете дистрибутив на основе Red Hat (например, Red Hat или Fedora Core), наберите в терминале команду:

```
sudo yum install gnupg thunderbird thunderbird-enigmail
```

Если вы используете дистрибутив на основе Debian, наберите в терминале команду:

```
sudo apt-get install gnupg icedove enigmail
```

ПОЧТОВЫЙ КЛИЕНТ ICEDOVE

В дистрибутиве Debian почтовый клиент Thunderbird носит название Icedove. И далее я не буду писать в скобках Icedove всякий раз, когда упоминаю Thunderbird. Просто имейте в виду эту особенность.

Настройка Thunderbird

1. Запустите приложение Mozilla Thunderbird привычным вам способом (выберите из списка приложений или найдите с помощью поиска). Помимо окна самой программы в открывшемся диалоговом окне отобразится предложение получить новый адрес электронной почты.
2. Нажмите кнопку Пропустить это и использовать мою существующую почту (Skip this and use my existing email) — откроется новое окно.

3. Укажите в нем имя, адрес электронной почты и пароль, а затем нажмите кнопку Продолжить (Continue).

   Во многих случаях программа Mozilla Thunderbird может автоматически определять нужные настройки (рис. 6.29).

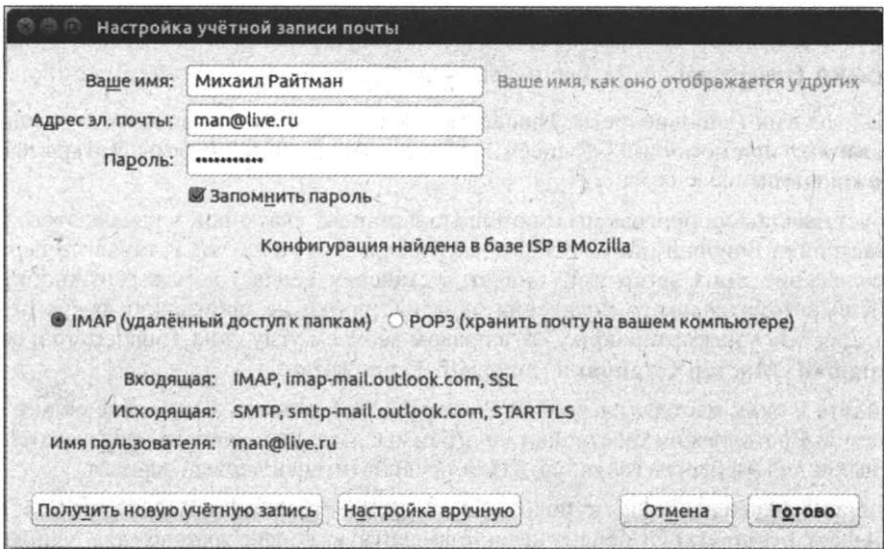


Рис. 6.29. Настройки учетной записи в программе Mozilla Thunderbird

Но иногда Mozilla Thunderbird недостаточно информации, тогда настраивать почту придется вручную. Далее показано, как это делается для учетной записи Gmail:

- Ваше имя (Your Name) — введите ваше имя или псевдоним;
- Адрес эл. почты (Email address) — укажите ваш полный адрес Gmail (в формате username@gmail.com);
- Пароль (Password) — ваш пароль Gmail;
- для сервера входящей почты IMAP:
  - в раскрывающемся списке выберите пункт IMAP;
  - имя сервера: imap.gmail.com;
  - порт: 993;
  - SSL: SSL/TLS;
- для сервера исходящей почты SMTP:
  - SSL: SSL/TLS;
  - аутентификация: Обычный пароль (Normal password).
- Имя пользователя (Username): введите в оба поля ваш полный адрес Gmail (в формате username@gmail.com).

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Если для Google-аккаунта у вас включена двухфакторная аутентификация, то вы не сможете в Thunderbird использовать свой обычный пароль Gmail. Чтобы получить доступ к Gmail, вам придется создать новый пароль Gmail специально для Thunderbird. Более подробная информация содержится в справочной системе Google.

4. Когда все данные будут аккуратно введены, нажмите кнопку **Готово** (Done).

Настройка Enigmail

Enigmail — плагин (дополнение) к Thunderbird. Его задача — шифрование и расшифровка закодированных при помощи PGP писем и обеспечение удобной работы с открытыми и закрытыми ключами.

Если вы устанавливали программы с помощью команды, указанной в начале этого раздела, мастер настройки Enigmail откроется автоматически. **В** этом случае установите переключатель в положение **Start setup now** (Начать установку сейчас) и нажмите кнопку **Далее** (Next). Если автоматического появления окна настройки не произошло, откройте мастер вручную. Для этого нажмите кнопку в правом верхнем углу окна Thunderbird и выберите пункт **Enigmail | Мастер установки** (Enigmail | Setup Wizard).

1. Перейдите к окну мастера настройки Enigmail — вы увидите диалоговое окно с предложением выбрать режим настройки программы: для начинающих пользователей, для опытных и для экспертов (вручную). Нам предпочтителен первый вариант.
2. Установите переключатель в положение **I prefer a standard configuration (recommended for beginners)** (Я предпочитаю стандартную конфигурацию (для начинающих)) и нажмите кнопку **Далее** (Next) — откроется диалоговое окно, в котором нужно указать пароль для защиты закрытого ключа (рис. 6.30).

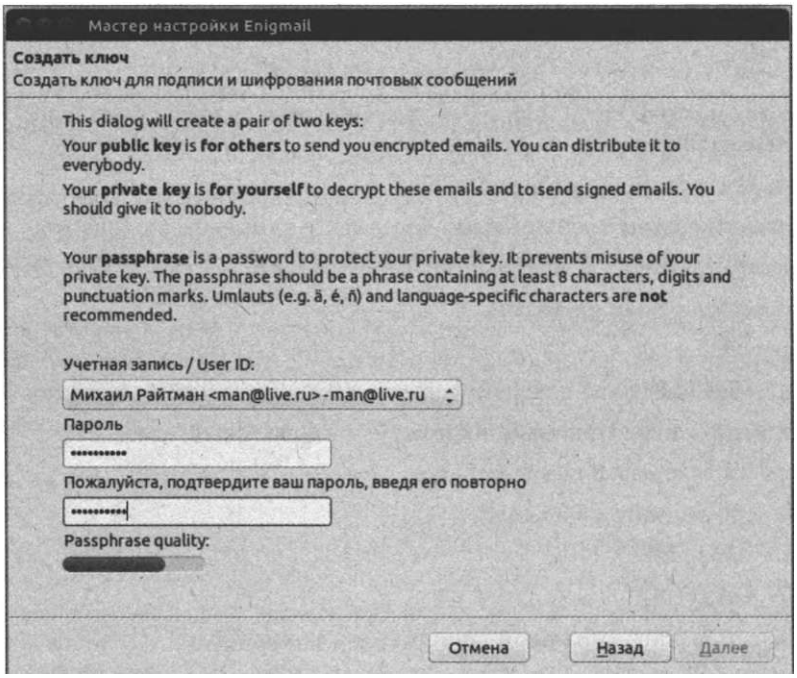


Рис. 6.30. Создание пароля для защиты закрытого ключа

3. Укажите желаемый пароль для защиты закрытого ключа — он должен состоять из не менее чем 8 символов и содержать латинские буквы, цифры и знаки пунктуации. Введите пароль в оба поля и нажмите кнопку **Далее** (Next).
4. Теперь помогите программе сгенерировать ключи, перемещая мышь и щелкая ее кнопками, нажимая клавиши клавиатуры и выполняя на компьютере другие активные действия, — плагин Enigmail создаст пару ключей. Когда этот процесс завершится, появится окно с сообщением и запросом о создании сертификата отзыва.
5. Такой сертификат может быть полезен, если возникнет необходимость отозвать прежние ключи. Обратите внимание — если вы просто удалите закрытый ключ, это не повлечет за собой неработоспособность парного открытого ключа. Люди по-прежнему смогут отправлять вам зашифрованные письма, но вы будете не в состоянии их расшифровать.
6. Нажмите кнопку **Создать сертификат отзыва** (Generate Certificate) — откроется диалоговое окно с запросом пароля, созданного на шаге 3.
7. Введите пароль к закрытому ключу, после чего откроется окно сохранения сертификата отзыва. Хотя вы можете сохранить файл и на компьютере, рекомендуется использовать для этого Flash-накопитель, который вы должны хранить в безопасном месте.

   Вот и все, что касается создания открытого и закрытого ключей.
8. Нажмите кнопку **Далее** (Next), а затем кнопку **Готово** (Finish).

Использовайие PGP/MIME

Последний шаг настройки программы Thunderbird — включение использования PGP/MIME. Этот способ позволяет упростить отправку зашифрованных писем с вложениями:

Вы можете найти эти настройки, нажав кнопку в правом верхнем углу окна Thunderbird и выбрав пункт **Настройки | Параметры учетной записи** (Options | Account Settings). Откроется одноименное диалоговое окно.

Выбрав в этом окне вкладку **Защита OpenPGP** (OpenPGP Security), установите флажок **Использовать PGP/MIME по умолчанию** (Use PGP/MIME by default). После нажатия кнопки OK использование PGP/MIME по умолчанию будет включено.

Использование Thunderbird с дополнением Enigmail позволяет легко шифровать и расшифровывать содержимое электронной почты. Но, как уже отмечалось, при этом информация об отправителе и получателе не шифруется, а если ее зашифровать, письмо не сможет быть отправлено.

В дальнейшем, работа по оповещению других пользователей PGP, приему/отправке зашифрованной почты и отзыву PGP-ключей строится так же, как и в соответствующих разделах этой главы, посвященных PGP-шифрованию в операционной системе Windows.

Теперь у вас есть все необходимые инструменты. Попробуйте самостоятельно отправить письмо, зашифрованное при помощи PGP.

ГЛАВА 7

Приватный обмен информацией

Основы безопасного общения

Угрозы безопасности сотовой связи

Приватная электронная почта

Приватное получение/отправка SMS-сообщений

Приватная голосовая связь

Приватный обмен мгновенными сообщениями

Благодаря современным телекоммуникационным системам и Интернету людям стало гораздо проще связываться друг с другом. И в то же время перехват коммуникаций в сетях связи упростился и распространился как никогда ранее в истории человечества. Если вы не принимаете никаких дополнительных мер для защиты своей частной жизни, любые ваши коммуникации (телефонный вызов, текстовое сообщение, электронное письмо, разговор в чате, IP-телефония, сеанс видеосвязи, сообщения в социальных сетях) могут быть подвержены перехвату.

Основы безопасного общения

Разумеется, самым безопасным видом связи является личная встреча — без компьютеров и телефонов. Но это не всегда возможно. Тогда лучшее, что можно сделать для собственной защиты при общении в сетях — использовать сквозное шифрование, при котором сообщение шифруется отправителем, а расшифровывается только конечным получателем, без привлечения третьих лиц.

Принцип работы сквозного шифрования

Допустим, два друга — назовем их Антон и Борис — поставили перед собой задачу защитить свои коммуникации. Тогда каждый из них должен создать пару шифровальных ключей. Перед тем как отправить письмо Борису, Антон шифрует его ключом адресата, и теперь только Борис сможет расшифровать послание. При этом, если злоумышленник контролирует канал связи и даже почтовую службу Антона (в том числе имеет доступ к его почтовому ящику), ему в руки попадут зашифрованные данные, и злоумышленник не смо-

жет их прочесть. А вот Борис, получив письмо, использует свой ключ и легко преобразует шифр в читаемое сообщение.

Сквозному шифрованию нужно научиться, но для собеседников это единственный способ обеспечить безопасность связи, не перепоручив ее защиту некой общей платформе. Создатели и владельцы сервисов наподобие Skype время от времени заявляют, что обеспечивают сквозное шифрование, а потом оказывается, что это не так. Чтобы сквозное шифрование действительно работало, любой пользователь должен иметь возможность убедиться в подлинности ключей своих собеседников. Если же программа связи не обладает таким функционалом, а злоумышленник надавит на разработчика (провайдера), он сможет прочесть ваши шифрованные сообщения.

Голосовые вызовы

Когда вы совершаете вызов по стационарному или мобильному телефону, никакого сквозного шифрования по умолчанию не предусмотрено. В сотовой связи ваш звонок еще может быть слабо зашифрован на участке от вашего телефона до базовой станции, но когда информация передается по сети, ее может перехватывать оператор связи, а значит, и любые злоумышленники, имеющие над ним власть. Самый простой способ обеспечения сквозного шифрования для голосовой связи — использование IP-телефонии (VoIP).

Внимание! Большинство популярных сервисов IP-телефонии (те же Skype, Google Hangouts и Facebook Messenger) хотя и шифруют каналы передачи данных и предлагают некоторую защиту трафика, которая не позволяет третьим лицам организовывать прослушивание переговоров, но *сами провайдеры, в принципе, способны осуществлять перехват* и считывать передаваемые данные[1]. Это может быть (или не быть) проблемой в зависимости от вашей модели угроз.

Далее приведен перечень некоторых приложений IP-телефонии, в которых реализовано сквозное шифрование:

- Brosix **(ru.brosix.com):** Windows, OS X, Linux, Android, iOS, веб-клиент;
- Cellcrypt **(cellcrypt.com):** Windows, Android, iOS, Blackberry;
- Ostel **(ostel.co):** Windows, OS X, Linux, Android, iOS, Blackberry;
- PrivateWave **(privatewave.com):** Android, iOS, Blackberry;
- Silent Phone **(tinyurl.com/nuopdly);**
- Signal **(whispersystems.org).**

Чтобы оценить преимущества VoIP и поддерживаемого им сквозного шифрования, оба участника разговора должны использовать одинаковые или совместимые программы.

Существуют также целые устройства, призванные решать вопросы безопасной связи владельца с другими людьми. Одним из таких устройств является смартфон Blackphone, который описывается далее в этой главе.

SMS- и MMS-сообщения

Привычные SMS- и MMS-сообщения не поддерживают сквозное шифрование. И если вы хотите обмениваться шифрованными посланиями с помощью телефона, вам скорее подойдет одна из программ для приватного обмена мгновенными сообщениями (см. далее), а не

[1] См. tinyurl.com/hsp9vzd.

система SMS. Некоторые такие программы работают по собственным протоколам. При этом пользователи, например, программы Signal могут общаться в защищенном режиме только с теми, кто также имеет эту программу на своем устройстве. А пользователи ChatSecure — мобильного приложения, которое шифрует поток данных с помощью сквозного шифрования в любой сети с поддержкой протокола XMPP, могут сами выбрать для связи какую-либо из независимых совместимых программ.

Мгновенные сообщения

Для обмена мгновенными сообщениями в реальном времени в различных программах и сервисах используется протокол сквозного шифрования Off-the-Record (OTR). Вот перечень некоторых программ, поддерживающих этот протокол:

- Adium **(adium.im):** OS X;
- ChatSecure **(chatsecure.org):** Android, iOS;
- Pidgin **(prdgin.im):** Windows, Linux.

Электронная почта

Большинство сервисов электронной почты позволяют подключаться к почтовому ящику через Веб-браузер. Многие из них поддерживают протокол HTTPS, осуществляющий шифрование трафика на транспортном уровне. Узнать, поддерживает ли протокол HTTPS используемый вами сервис можно, перейдя на его сайт и взглянув на интернет-адрес (URL), указываемый в соответствующем поле ввода (адресной строке) браузера. Там вместо HTTP вы должны увидеть HTTPS (например: **https://mail.google.com** или **https://mail.ru).**

Если провайдер поддерживает протокол HTTPS, но не по умолчанию, попробуйте в адресной строке заменить HTTP на HTTPS вручную и перезагрузите страницу, нажав клавишу <F5>. А чтобы страницы всегда (если эта возможность поддерживается сайтом) загружались через протокол HTTPS, установите дополнение HTTPS Everywhere для браузеров Firefox и Chrome (см. *главу 1).* Некоторые провайдеры веб-почты, такие как Hotmail, позволяют в настройках выбрать используемый по умолчанию протокол: HTTP или HTTPS.

Протокол HTTPS (иногда вы также можете встретить сокращения SSL или TLS) шифрует коммуникации так, что их не могут увидеть другие люди в вашей сети — например, пользователи подключения к той же точке доступа Wi-Fi в аэропорту или в кафе, коллеги по работе или одноклассники, системный администратор вашего интернет-провайдера и хакеры-злоумышленники. Если же связь происходит по протоколу HTTP, а не по HTTPS, то перехват и чтение всех данных, пересылаемых браузером, становится простой задачей. Это касается не только веб-страниц, но и содержания электронных писем, публикаций в блогах, всевозможных сообщений.

Но и протокол HTTPS имеет ограничения. Так, когда вы отправляете электронное письмо даже с использованием протокола HTTPS, ваш провайдер электронной почты все равно получает незашифрованную копию данных. И если у вас есть какие-либо причины препятствовать возможности провайдера передавать содержимое ваших электронных писем третьим лицам, задумайтесь об использовании сквозного шифрования вашей электронной почты, — таком, например, как PGP (см. *главу* 6).

Ограничения сквозного шифрования

Сквозное шифрование защищает лишь содержание вашей переписки, но не сам факт информационного обмена. Оно не защищает и метаданные: имя адресата, адрес его электронной почты, тему письма, дату, время. Кстати, когда вы звоните по мобильному телефону, *информация о вашем местонахождении* — тоже метаданные, и они позволяют все время следить за перемещениями владельца телефона.

Чтобы защитить метаданные, требуется не только сквозное шифрование, но и другие средства, — такие, например, как анонимная сеть Tor (см. *главу 17).*

Угрозы безопасности сотовой связи

На сегодняшний день мобильные телефоны (смартфоны) — одно из самых распространенных устройств связи. Они служат не только для телефонных звонков, но и для доступа к Интернету, передачи текстовых сообщений и записи всевозможных событий, происходящих в мире. Количество мобильных соединений превышает 7 млрд[1], по ним передается огромное количество различной информации: политической, финансовой, экономической, юридической, медицинской и личной. Использование этой информации злоумышленниками чрезвычайно опасно и может привести к катастрофическим последствиям, как для частных людей, так и для корпораций и государства. Далее приведен перечень некоторых потенциальных угроз, могущих возникнуть из-за отсутствия защиты сотовой связи:

- похищение людей (кидиеппинг) — этой угрозе особенно подвержены дети богатых родителей. Злоумышленники, фальсифицируя голос родителей при звонке ребенку по мобильному телефону, могут выманить его и похитить. Они рассчитывают при этом получить от родственников выкуп, а также принудить их к выполнению необходимых для похитителей действий;
- фальсификация голосов других людей (пранк) — такой угрозе чаще подвержены политические деятели и главы крупных компаний. Звоня им по мобильному телефону, злоумышленники имитируют голос знакомого им абонента с целью выведать у них конфиденциальные сведения и/или скомпрометировать;
- похищение корпоративных и конфиденциальных данных — большинство хакеров прослушивают мобильные телефоны влиятельных лиц, чтобы узнать пароли доступа к корпоративным базам данных и банковским счетам. В дальнейшем эти сведения могут использоваться для осуществления рэкета и вымогательства, а также с целью разорения конкурентов.

К сожалению, мобильные телефоны создавались без расчета на неприкосновенность частной жизни и неважно справляются с защитой коммуникаций. С технической точки зрения перехват GSM-переговоров сравнительно несложен по следующим причинам:

- стоимость несанкционированного перехвата и записи телефонных переговоров, ведущихся через сотовую связь, сравнительно невысока и составляет несколько тысяч долларов США за запись одного номера в течение месяца. Стоимость компьютерного моделирования голоса человека, говорящего по GSM, немного выше[2];

[1] **См. tinyurl.com/h5q65dd.**

[2] **См. tinyurl.com/z2cn5qv.**

- **размеры** аппаратуры для перехвата компактны — они немного больше портативного компьютера. Ее легко переносить и перевозить, а обнаружить практически невозможно из-за использования при прослушке т. н. *пассивного* режима.

Кроме того, мобильный телефон, как правило, предоставляет пользователю гораздо меньше возможностей контроля за его работой, чем настольный компьютер или ноутбук, — на мобильном телефоне труднее сменить операционную систему, исследовать атаки вредоносных программ, удалять нежелательные приложения, мешать посторонним лицам (например, оператору связи) следить за тем, как вы используете свое устройство. Более того, производитель телефона может объявить модель устаревшей и перестать обновлять программное обеспечение, в том числе и отвечающее за безопасность.

Некоторые проблемы можно решить с помощью сторонних программ для защиты приватности. Но это удается не всегда. Далее вы узнаете о том, как телефон может стать инструментом слежки и поставить под удар частную жизнь своего владельца.

Определение местонахождения

Самая серьезная угроза приватности, которую создает мобильный телефон, обычно не привлекает внимания, — телефон сообщает о том, где вы находитесь, причем передает сигналы об этом круглосуточно. Посторонним лицам доступно, по меньшей мере, четыре способа отследить местонахождение мобильного телефона.

Отслеживание сигнала по вышкам сотовой связи

Во всех современных мобильных сетях оператор может определить местонахождение телефона конкретного абонента, как только аппарат включится и зарегистрируется в сети. Этот метод отслеживания местонахождения телефона обычно называют *триангуляцией* — оператор измеряет уровень сигнала конкретного телефона на нескольких вышках, а потом по разности этого сигнала вычисляет местонахождение аппарата. Точность расчета зависит от многих факторов, в том числе от использованной оператором технологии и от числа вышек сотовой связи в окрестностях. Чаще всего координаты удается определить с точностью до городского квартала, но иногда можно достичь и более впечатляющих результатов.

Технически отслеживать местонахождение телефона может только сам оператор мобильной связи, осуществляя это в режиме реального времени или по сохраненным записям. Способа защиты от такого отслеживания нет, если ваш мобильный телефон включен и передает сигналы в сеть.

Отслеживание сигнала с помощью IMSI-ловушки

Злоумышленник, обладающий нужными техническими средствами, может собирать данные о местонахождении какого-либо телефона непосредственно с вышек сотовой связи. Для этого используется *IMSI-ловушка* (IMSI-кетчер) — портативное устройство, которое имитирует вышку сотовой связи (рис. 7.1). Задача та же — определить местонахождение конкретных мобильных телефонов и установить за ними слежку.

Сокращение IMSI происходит от англ. International Mobile Subscriber Identity (международный идентификатор мобильного абонента) — этот идентификатор записан на SIM-карте и уникален для каждой из них. Помимо отслеживания по IMSI, ловушка может отслеживать устройство с использованием и других его характеристик, — например, TMSI (Temporary Mobile Subscriber Identity) — временного идентификатора мобильного абонента, который

назначается ему после успешной аутентификации и используется в процессе установки звонка, регистрации в сети и т. д., или IMEI (International Mobile Equipment Identity) — международного идентификатора мобильного оборудования, уникального для каждого мобильного телефона.



Рис. 7.1. IMSI-ловушка

Такого рода трюк возможен по той причине, что мобильный телефон обязан аутентифицировать себя по запросу сети, а вот сама сеть (базовая станция) свою аутентичность подтверждать телефону не должна. Эта прореха в безопасности GSM-связи была внесена в архитектуру системы умышленно по настоянию спецслужб — для организации перехвата и мониторинга абонентов без ведома компаний-операторов мобильной связи. Поэтому, как только мобильный телефон принимает IMSI-ловушку в качестве своей базовой станции, этот аппарат-ретранслятор может деактивировать включенную абонентом функцию шифрования и работать с обычным открытым сигналом, передавая его дальше настоящей базовой станции. За редким исключением, GSM-телефоны не предупреждают владельца о принудительно отключенной функции шифрования, а во многих аппаратах функция шифрования вообще не реализована. В настоящее время надежной защиты от IMSI-ловушек нет.

Отслеживание сигнала с помощью Wi-Fi и Bluetooth

Кроме сотовой связи в современных смартфонах используются и другие беспроводные передатчики — на основе технологий Wi-Fi и Bluetooth. Их мощность меньше, чем у сотовой связи, вследствие чего их сигналы распространяются на небольшое расстояние (в пределах одной комнаты или здания). Как Bluetooth, так и Wi-Fi используют уникальный серийный номёр устройства — т. н. *MAC-адрес,* который устанавливает производитель устройства при его создании и который нельзя изменить с помощью предустановленных на смартфоне

программ. MAC-адрес включенного устройства может видеть любой пользователь, устройство которого принимает его сигнал.

К сожалению, MAC-адрес можно определить, даже если устройство не подключено к конкретной беспроводной сети (или подключено, но не передает данные), — смартфон с включенным Wi-Fi снова и снова передает сигналы, содержащие MAC-адрес. Так ваши соседи могут узнать, что где-то рядом находится ваше устройство.

По сравнению с мониторингом GSM-сетей, способы отслеживания сигналов Wi-Fi и Bluetooth не слишком пригодны по причине их распространения на малые расстояния, а также потому, что следящему необходимо заранее знать MAC-адрес устройства. Тем не менее, эти способы могут быть очень точными, если нужно определить, когда человек входит в здание и выходит из него. Чтобы избавиться от подобного риска, достаточно отключить на смартфоне Wi-Fi и Bluetooth.

Администраторы точек доступа Wi-Fi могут видеть MAC-адреса всех подключенных устройств. При этом администратор может выявить повторные подключения и подтвердить, что вы — тот самый человек, который подключался к сети ранее (даже если вы нигде не вводили имя или адрес e-mail и не использовали никакие сервисы).

На некоторых устройствах можно изменить MAC-адрес, и тогда устройство будет нельзя отследить по известному ранее номеру. Осуществляется это с помощью программ, специально предназначенных для смены MAC-адреса на смартфоне. Однако такая возможность сегодня не предусмотрена для большинства смартфонов и, как правило, требует root-доступа или джейлбрейка устройств.

Утечка данных о местонахождении при работе приложений и веб-серфинге

В современных смартфонах реализован функционал геолокации, позволяющий определять местонахождение аппарата. Обычно для этого используется GPS и/или ГЛОНАСС, а иногда и другие способы (по вышкам сотовой связи, с помощью Wi-Fi). Приложения могут запрашивать устройство о его координатах и использовать их для оказания некоторых услуг — например, для отображения на карте ближайших магазинов.

Некоторые приложения передают эти данные по сети оператору или разработчику устройства (программы), а тот, в свою очередь, позволяет другим людям узнавать ваше местонахождение, — разработчик, возможно, и не собирался следить за вами, но, в конечном счете, у него есть такая возможность, и она может оказаться в руках злоумышленников. В некоторых смартфонах можно определить приложения, которым разрешен доступ к данным о вашем местонахождении. С точки зрения защиты приватности рекомендуется ограничить набор таких приложений. Как минимум, следует убедиться, что ваше местонахождение известно только тем программам, которым оно необходимо и которым вы доверяете.

Речь необязательно идет о слежке в реальном времени. Слежка — это также сбор информации о действиях человека в прошлом, о его убеждениях, об участии в мероприятиях, о личных связях. Например, данные о местонахождении людей помогают узнать, приходил ли такой-то человек на определенную встречу.

Выключение телефона

Широко распространено мнение, что с помощью телефона можно отслеживать владельца, даже если тот по телефону и не говорит. Соответственно, для конфиденциального разговора рекомендуют полностью отключать телефоны и даже вынимать аккумуляторы.

В последнем варианте есть доля смысла, т. к. существуют вредоносные программы, которые способны эмулировать отключение телефона и демонстрировать пустой экран. При этом вы становитесь жертвой обмана, полагая, что телефон отключен, а программа тем временем записывает ваши разговоры или скрытно отправляет и принимает вызовы.

Подобные вредоносные программы на самом деле существуют, по крайней мере, для некоторых устройств, в частности, работающих под управлением операционной системы Android[1]. По сообщениям Эдварда Сноудена, спецслужбы совершенно точно могут использовать смартфон в своих целях и при необходимости задействовать отдельные его приложения. При этом для них не имеет значения, включен телефон или выключен, — получить доступ можно даже к неактивному смартфону[2].

Выключение телефонов имеет некоторый потенциальный минус — если многие люди в одном месте одновременно выключат свои телефоны, это само по себе может сигнализировать оператору связи о внезапном (подозрительном) изменении ситуации. Поэтому более разумный способ уменьшить утечку данных — оставить все телефоны в другой комнате, где их микрофоны не смогут подслушать разговоры.

Одноразовые телефоны

Это телефоны, которые покупают для временного использования, а потом выбрасывают. Люди, которые пытаются избежать прослушивания злоумышленниками, иногда прибегают к частой смене аппаратов (и номеров), чтобы их коммуникации было труднее отследить. Для этого им приходится использовать предоплаченный телефон, не связанный с его персональными данными или банковскими реквизитами. Важно, чтобы с конкретным пользователем нельзя было связать ни телефон, ни SIM-карту, чтобы обеспечить ему анонимную мобильную связь.

Одноразовые телефоны доступны во Всемирной паутине по цене от нескольких долларов США на таких сайтах, как Walmart.com и AIibaba.com, под названиями disposable и single use cell phones (рис. 7.2). Большинство из них привязаны к какому-либо оператору сотовой связи.



Рис. 7.2. Одноразовый телефон

[1] См. tinyurl.com/zhSgSwo.

[2] См. tinyurl.com/hzju9ny.

Впрочем, в использовании одноразовых телефонов существует и ряд ограничений. Во-первых, меняя SIM-карты или перемещая SIM-карту из одного устройства в другое, вы обеспечиваете лишь минимальную защиту. Мобильная сеть распознает как SIM-карту, так и устройство. Другими словами, оператор сотовой связи знает, в каких устройствах ранее использовались те или иные SIM-карты, и может отслеживать SIM-карты и устройства по отдельности или вместе. Во-вторых, существуют методики анализа местонахождения мобильных устройств, учитывающие вероятность работы одного и того же человека с несколькими устройствами.

Еще одна проблема, которая мешает анонимно использовать телефонную связь, — привычка человека звонить определенным абонентам. Эта привычка формирует легко узнаваемую картину. Например, вы обычно звоните членам семьи и коллегам по работе. Каждый из них получает звонки от множества других людей. Но вы, скорее всего, единственный человек в мире, кто звонит обеим группам с одного и того же номера. Если вы вдруг сменили номер, но сохранили привычки, то по картине звонков можно угадать ваш новый номер. Обратите внимание — не потому, что вы позвонили какому-то конкретному человеку, а по *уникальному сочетанию ваших звонков на разные номера.*

Одноразовый телефон называется также *выбрасываемым*, потому что владелец выбрасывает один аппарат, чтобы начать пользоваться другим. Но аналитические алгоритмы баз данных прослушивания позволяют установить связь между первым и вторым телефоном, поскольку оба используются для вызовов на примерно одни и те же номера.

Одноразовые телефоны могут быть эффективны, если соблюдаются минимальные условия:

- ни SIM-карты, ни аппараты не используются повторно;
- два устройства не используются вместе;
- нет связи между местами, где используются разные аппараты;
- владелец не звонит на один и тот же набор номеров (и не должен получать вызовы от них).

Спутниковые системы навигации

Система глобального позиционирования (GPS, Global Positioning System), как и ее российский аналог, глобальная навигационная спутниковая система (ГЛОНАСС), позволяют устройству в любой точке мира быстро и точно определить свои координаты. Системы навигации работают на основе анализа сигналов от спутников, которые доступны для публичного использования. Спутники систем навигации могут только передавать сигналы, но не получать их от телефона. Ни спутники, ни операторы навигационного оборудования не знают, где находится пользователь системы, и сколько людей использует ее.

GPS/ГЛОНАСС-приемник (например, в смартфоне) вычисляет *собственную позицию*, определяя, сколько времени потребовалось радиосигналам, чтобы преодолеть расстояние от разных спутников до него. Этими данными могут воспользоваться установленные на смартфоне приложения, которые запрашивают у операционной системы координаты телефона (определенные по GPS/ГЛОНАСС). Получив их, приложение может передавать эту информацию через Интернет, в том числе и злоумышленникам, если установленное программное обеспечение вредоносное.

Прослушивание сотовой связи

Сети сотовой связи изначально не были предназначены для использования технических средств защиты звонков абонентов от прослушивания. Другими словами, человек с соот-

ветствующей радиопринимающей аппаратурой способен прослушивать звонки. К настоящему времени ситуация улучшилась, но незначительно. К стандартам сотовой связи добавились технологии шифрования, призванные препятствовать прослушиванию, однако многие из них слишком слабые, распространены неравномерно и не у всех операторов связи. Так что и сегодня владелец подходящего радиоприемника может перехватывать голосовые вызовы и текстовые сообщения. Операторы и сами имеют возможность перехватывать и записывать всю информацию о том, кто, кому, когда звонил или отправил SMS-сообщение и какое. Кроме того, злоумышленник, находящийся рядом, может использовать IMSI-ловушку (см. ранее), имитируя вышку сотовой связи и перехватывая ваши коммуникации.

Ради собственной безопасности следует признать, что обычные звонки и текстовые сообщения не защищены от прослушивания или записи. Ситуацию можно изменить, если обеспечить более серьезную защиту коммуникаций (голосовых или текстовых) с помощью специальных программ стойкого шифрования. Надежность такой защиты во многом зависит от того, какие приложения вы используете и как они работают, обеспечивает ли ваша программа сквозное шифрование для защиты коммуникаций, есть ли у ее разработчика способ отменить или обойти установленную защиту.

Заражение телефона вредоносной программой

Телефон может пострадать от вредоносного кода. Зачастую пользователь сам устанавливает опасную программу, но есть и риск того, что злоумышленник взломает устройство, используя уязвимость в установленном программном обеспечении. Как и всюду, где речь идет о компьютерной технике, вредоносные программы обладают способностью шпионить за владельцем устройства. Вредоносная программа на мобильном телефоне может считывать персональные данные (например, сохраненные SMS-сообщения и фотографии) и активировать модули (скажем, микрофон, камеру, спутниковую навигацию), чтобы определить местонахождение телефона или следить за происходящими вокруг него процессами, практически превращая телефон в подслушивающее устройство. Вредоносная программа, как уже говорилось, может сымитировать даже отключение телефона, продолжая свою работу (экран при этом будет черным, чтобы убедить владельца, что телефон выключен).

Анализ содержимого телефона

Злоумышленник может выкрасть телефон и подключить его к специальному оборудованию, чтобы считывать данные, включая сведения о действиях на устройстве, телефонных звонках, SMS/MMS-сообщениях. Он может добраться даже до такой информации, доступ к которой обычному пользователю закрыт, — например, восстановить удаленные текстовые сообщения. Как правило, злоумышленник способен обойти простые формы защиты типа блокировки устройства с помощью пароля.

Существует немало программных функций и приложений для смартфонов, задача которых — помешать анализу определенных данных и записей. Информацию можно зашифровать, и она перестанет быть читаемой даже для специалиста. Кроме того, существуют программы для дистанционного стирания данных, — например, Найти iPhone (Find iPhone) в операционной системе iOS. Такая программа позволяет владельцу смартфона удаленно отправить на телефон команду стереть определенную информацию.

Подобные способы защиты данных могут оказаться полезны, если ваш телефон оказался в руках преступников.

Приватная электронная почта

В процессе серфинга по Всемирной паутине вам часто приходится регистрироваться на том или ином сайте для каких-либо целей. Обычно при регистрации требуется указать адрес электронной почты — для связи или, чаще, для подтверждения регистрации. Реальный рабочий или домашний электронный адрес в таких случаях указывать строго не рекомендуется — если только регистрация совершается не на тщательно проверенном сервисе, где реальный адрес необходим для продолжительной работы с использованием подтверждаемых персональных данных.

В идеале для таких авторизаций подойдет *временный* почтовый ящик, который вы, как правило, без заполнения серьезной формы регистрации создаете на специально предназначенном для этих целей сервисе и письма в котором хранятся от нескольких минут до нескольких месяцев. Тогда вы при регистрации на каком-либо сайте можете указать адрес электронной почты одного из своих временных ящиков. Получив на него письмо со ссылкой подтверждения регистрации, вы активируете учетную запись, перейдя по ссылке в письме, а временный почтовый ящик можно закрыть и забыть про него, — он будет автоматически удален через определенный промежуток времени.

Чаще всего на подобных сервисах вам достаточно указать лишь логин, т. е. первую часть электронного адреса, до символа @, после чего вы получаете доступ к содержимому ящика. Существуют также сервисы, позволяющие создать временный почтовый ящик, попадающая в который почта будет автоматически пересылаться на ваш реальный электронный адрес. Однако такой вариант небезопасен, поскольку в этом случае владельцу сервиса временной почты будет известен ваш реальный адрес электронной почты.

Стоит также обратить внимание, что на сайтах временной почты для доступа к временным ящикам не требуется пароль. Поэтому, если вы зарегистрируете, к примеру, ящик **temp@mailnesia.com,** любой другой пользователь сможет получить доступ к его содержимому, если также зарегистрирует ящик **temp@mailnesia.com.** И если срок хранения ваших писем в этом ящике еще не истек, он их увидит. Это особенно опасно, если на ваш ящик были высланы письма с вашими регистрационными данными (как это делают некоторые сайты). Поэтому, для повышения уровня безопасности рекомендуется создавать временные почтовые ящики с именами адресов (логинами) в виде хаотичного набора символов — например: **onssdD3543edyuhv7@mailnesia.com.**

> ***ПРОВЕРКА СУЩЕСТВОВАНИЯ АДРЕСА ЭЛЕКТРОННОЙ ПОЧТЫ***
>
> **В некоторых случаях может потребоваться опредепить, существует пи тот ипи иной адрес электронной почты. Сделать это можно на сайте 2ip.rU/mail4:hecker/.**

На рис. **7.3** приведен пример одного из таких веб-сервисов **(mailnesia.com),** позволяющих создать временный электронный почтовый ящик. В поле ввода нужно указать произвольное для этого почтового ящика имя (на рисунке— onssdf33543edyuhv7), а затем щелкнуть мышью на зеленой стрелке.

Внимательно рассмотрев свой открытый ящик, вы увидите указанное вами при регистрации имя в адресной строке браузера. В моем примере это **http://mailnesia.com/mailbox/** onssdf33543edyuhv7. Нетрудно догадаться, что, подставив вместо своего имени другое, вы откроете любой созданный на сервисе ящик. То же касается и многих других сервисов анонимной почты.

Стоит отметить, что некоторые подобные сервисы рассчитаны на то, что почтовый ящик используется здесь и сейчас, и окно браузера не будет закрываться, поэтому восстановление

содержимого ящика после закрытия окна не предусмотрено. Для вашего удобства далее приводится небольшая табл. 7.1 со списком некоторых доступных на момент подготовки книги сервисов временной почты.

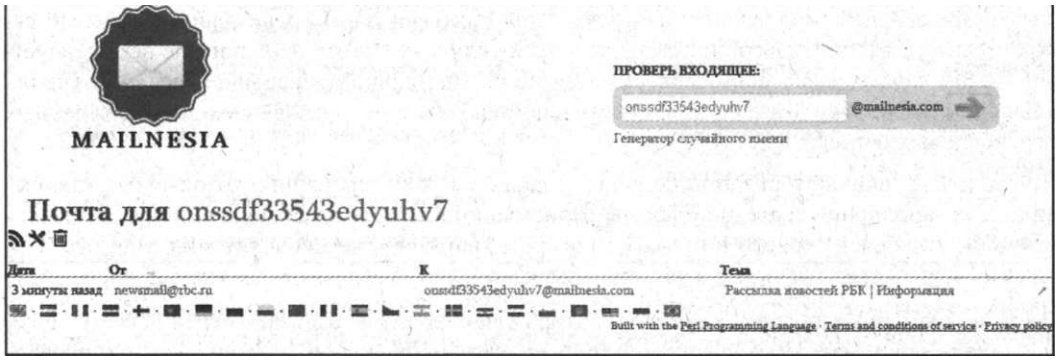


Рис. 7.3. Интерфейс сервиса временной электронной почты

Таблица 7.1. *15 бесплатных сервисов временной почты*

Название	Адрес	Комментарии
10MinuteMail	10minutemail.com	Почтовый ящик удаляется через 10 минут с возможностью пролонгации
Disposable Inbox	disposableinbox.com	Срок хранения сообщений — 24 часа. Есть возможность ответа на входящие сообщения
FilzMail	filzmail.com	Срок хранения сообщений — 24 часа
GuerrillaMail	guerrillamail.com/ru/	Почтовый ящик удаляется через 60 минут
Incognito Mail	incognitomail.com	Почтовый ящик удаляется через 60 минут
Jetable.org	jetable.org/en/index	Указывается реальный адрес и продолжительность жизни ящика: от 1 часа до месяца. Затем генерируется адрес временного почтового ящика, который вы указываете на любых сайтах. Почта, попадающая на адрес сгенерированного почтового ящика, автоматически пересылается на реальный
MailCatch	mailcatch.com/en/ disposable-email	Срок хранения сообщений — от нескольких часов до нескольких дней — зависит от трафика
MailforSpam	mailforspam.com	Используется любой логин. Ящик доступен по адресу mailforspam.com/mail/логин
Mailinator	mailinator.com	Ограничения до 10 одновременно сохраняемых сообщений. Также ограничен размер каждого сообщения — 120 Кбайт
Melt Mail	meltmail.com	Указывается реальный адрес и продолжительность жизни ящика: от 3 до 24 часов. Затем генерируется адрес временного почтового ящика, который вы указываете на любых сайтах. Почта, попадающая на адрес сгенерированного почтового ящика, автоматически пересылается на реальный

Таблица 7.1 *(окончание)*

Название	Адрес	Комментарии
myTrashMail.com	mytrashmail.com	Продолжительность жизни: от 5 дней до месяца. Лимит ящика — 4 Мбайт, до 2 Мбайт на одно письмо
Spamobox	spamobox.com	Почтовый ящик удаляется через 60 минут с возможностью пролонгации
TempEMail	tempemail.net	Почтовый ящик удаляется через 14 дней
Tempinbox	tempinbox.com	Обязательно следует установить флажок, что вы подтверждаете условия соглашения
TempMail	temp-maii.ru	Почтовый ящик удаляется через 120 минут

Помимо временных почтовых ящиков, которые необходимо создавать перед регистрацией, вы можете придумать определенные и уникальные имена/пароли, а затем зарегистрировать несколько постоянных почтовых ящиков. Дело в том, что временные адреса электронной почты удобны в тех случаях, когда необходимо выполнить несколько регистрации или периодически регистрироваться на сервере, чтобы получить несколько учетных записей.

Если же вы часто пользуетесь различными новостными веб-сайтами, предполагающими регистрацию для просмотра контента, тут несколько учетных записей не нужны. Достаточно завести ящик электронной почты вида **vasyapupkin@mail.ru** и указывать его при регистрации на всех таких веб-сайтах. Это очень удобно по нескольким причинам. Во-первых, вы всегда точно помните адрес электронной почты, когда его требуется указывать в виде логина (если же в качестве логина используется уникальное имя, то можно указывать, например, первую часть адреса электронной почты: **vasyapupkin).** Во-вторых, иногда адрес электронной почты используется при восстановлении пароля — а если регистрация была проведена на временный ящик, то письмо с данными восстановления пароля вы, скорее всего, уже не получите. Постоянный же адрес электронной почты будет существовать длительное время, пока вы им пользуетесь.

Разумеется, подобные временные, да и постоянные, ящики не обеспечивают защиту передаваемых данных, поэтому обмениваться через них конфиденциальными данными нельзя! Дня безопасной передачи важных данных следует использовать PGP-шифрование (см. *главу* 6), а также анонимные сети наподобие Tor (см. *главу 17).*

Приватное получение/отправка SMS-сообщений

При регистрации на некоторых сайтах требуется указывать номер своего мобильного телефона, на который впоследствии отправляется SMS-код, необходимый для активации учетной записи (аккаунта). Но, как правило, с целью создания аккаунта совсем не хочется «светить» реальный номер мобильника из-за угрозы безопасности персональных данных.

Для решения подобных проблем созданы сайты виртуальных мобильных номеров, позволяющие не только отсылать/получать SMS-сообщения, но даже и звонить. Чаще всего такие сервисы платные, но существуют и бесплатные, — например, Pinger. Этот сайт позволяет создавать виртуальные мобильные номера американского региона для обмена SMS-сообщениями. На момент подготовки книги отправка SMS на мобильные номера за пределами США была недоступна, но отображалась информация, что ведутся работы по решению этой проблемы.

Для регистрации и использования ресурса:

1. Перейдите на сайт pinger.com/tfw/ в своем браузере и щелкните мышью по ссылке Sign up (Регистрация) — вы увидите форму регистрации нового участника. Придумайте себе логин и пароль.
2. В поле Username (Логин) введите латинскими буквами логин, с которым вы будете авторизовываться на сайте Pinger.
3. В поля Password (Пароль) и Confirm Password (Подтвердить пароль) введите и подтвердите пароль.
4. В поле Email (Адрес электронной почты) укажите действующий адрес своей электронной почты — он понадобится для подтверждения регистрации аккаунта и может быть использован для оповещения о входящих SMS-сообщениях.
5. В поле Age (Возраст) введите свой возраст (или любое число больше 18).
6. Установите переключатель Gender (Пол) в одно из положений: Male (Мужчина) или Female (Женщина).
7. Введите CAPTCHA-код в поле Security Code (Секретный пароль).
8. Нажмите кнопку Create (Создать) — откроется форма, показанная на рис. 7.4, *слева.*
9. В соответствующее поле введите *американский* почтовый индекс (действующие индексы можно подсмотреть, к примеру, на сайте zip-area.com).

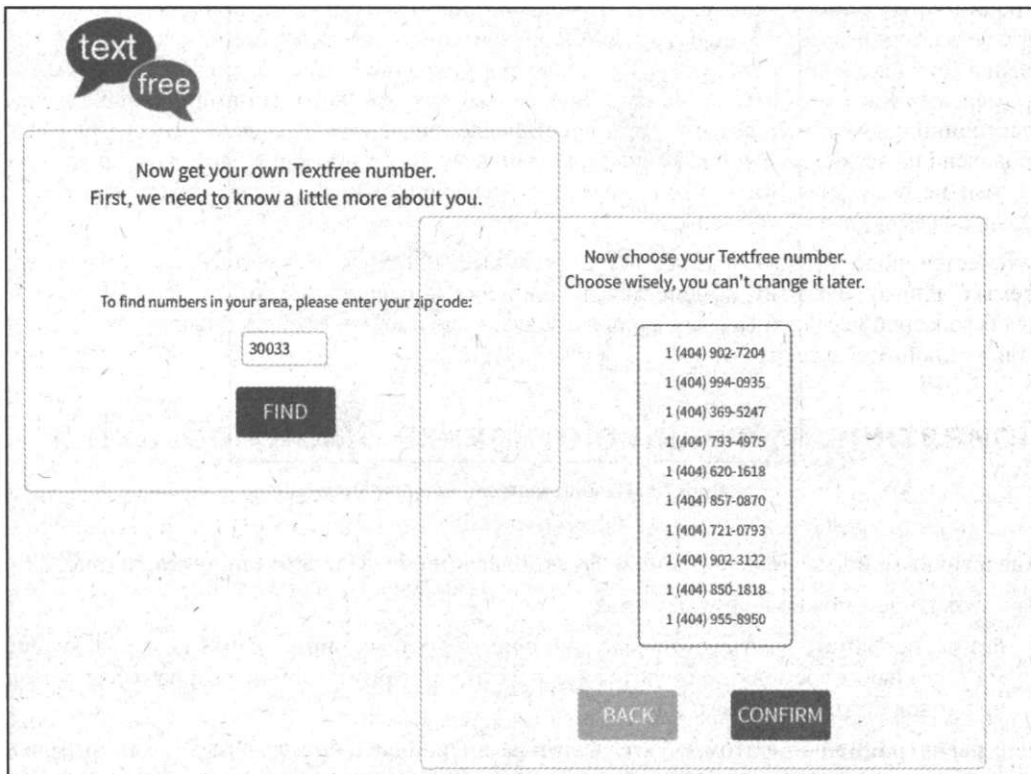


Рис. 7.4. Форма регистрации на сайте Pinger

10. Если указан верный почтовый индекс, то, нажав на кнопку Find (Найти), вы получите форму со списком доступных мобильных номеров на выбор (рис. 7.4, *справа).* В противном случае попробуйте указать другой действительный *американский* почтовый индекс.

ПРОБЛЕМЫ РЕГИСТРАЦИИ И ИСПОЛЬЗОВАНИЯ

Если возникает ошибка при регистрации на сайте Pinger, — возможно, причина в использовании российских почтовых сервисов, — укажите адрес электронной почты в системе Gmail или любой другой американской почтовой службы. Как уже отмечалось ранее, на момент подготовки книги возможность отправки SMS на номера за пределами США была недоступна.

11. Выберите номер телефона и нажмите кнопку Confirm (Подтвердить). Затем подтвердите аккаунт по ссылке из письма, полученного на указанный вами адрес электронной почты.

    После авторизации вы сможете получать и отправлять SMS-сообщения (повторяю — на момент подготовки книги пока только на мобильные номера США). Кроме того, ваш логин на сайте Pinger может использоваться в качестве адреса электронной почты, и вы можете получать/отсылать с его помощью электронные сообщения.

12. Увидеть присвоенные вам адрес электронной почты и номер мобильного телефона (рис. 7.5) можно, щелкнув мышью по ссылке Options (Параметры) в окне сервиса.



Рис. 7.5. Панель настроек на сайте Ртдег

Аналогичным, и даже более удобным, функционалом обладает сайт onIinesim.ru (рис. 7.6).

Работать на нем можно в двух режимах:

- без регистрации — открыто несколько общедоступных виртуальных номеров, которыми в реальном времени пользуются все посетители сайта. Удобный вариант для получения кодов подтверждения с сайтов;
- с регистрацией — в этом случае доступны индивидуальные номера для каждого пользователя, а также есть возможность просмотра SMS-сообщений, полученных ранее. Каждое сообщение оплачивается с личного счета пользователя.



Рис. 7.6. Интерфейс сайта onlinesim.ru

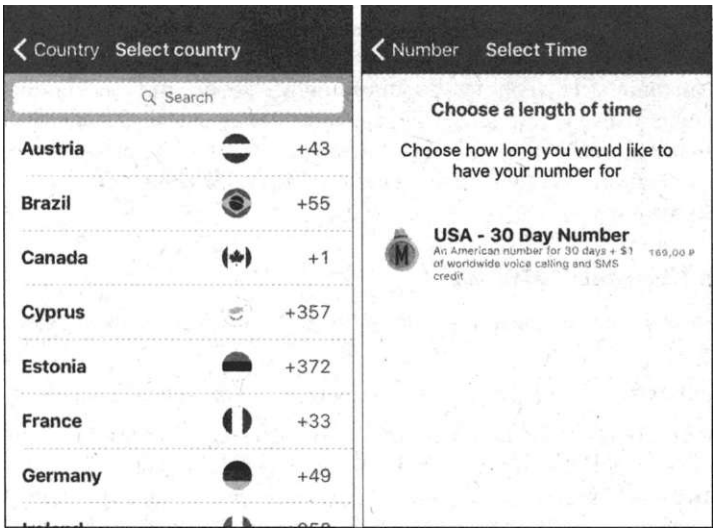


Рис. 7.7. Интерфейс приложения Hide My Phone

Для мобильных устройств также существуют разработки в плане обеспечения приватной связью. К примеру, для смартфонов под управлением операционной системы iOS создано приложение Hide My Phone, позволяющее получить виртуальный мобильный номер для обмена SMS-сообщениями и голосовых вызовов. Помимо ежемесячной абонентской платы за обслуживание номера тарифицируются сами вызовы и сообщения (рис. 7.7).

Разумеется, как и в случае с временной электронной почтой, подобные SMS-сервисы нельзя использовать для передачи конфиденциальных данных. После приема временного пароля или данных для входа на сайт следует сразу же изменить их в настройках профиля на сайте.

Приватная голосовая связь

Привычную голосовую связь, реализуемую через стационарные и сотовые телефонные сети, к сожалению, нет возможности зашифровать, и она остается доступной для прослушивания злоумышленниками. Но, благодаря развитию IP-телефонии, вы можете защитить переговоры, используя специальные программы или даже устройства, на которых установлены подобные специальные программы, а также другие инструменты для защиты передаваемых данных.

Одной из таких программ является мессенджер Signal, позволяющий, используя возможности IP-телефонии, безопасно разговаривать и обмениваться сообщениями (см. далее). В качестве альтернативы в этом разделе рассмотрена и система информационной безопасности Stealthphone — комплексное решение для защиты мобильной связи и компьютеров российской разработки. Здесь также описано несколько устройств, призванных обеспечить конфиденциальность переговоров владельцев.

Программа Signal

Signal **(whispersystems.org)** — бесплатная программа для устройств под управлением операционных систем iOS и Android, реализующая сквозное шифрование коммуникаций. С помощью программы Signal можно совершать защищенные телефонные и видеозвонки, обмениваться сообщениями и файлами. Для передачи данных (в том числе и голосовых) требуется подключение к Интернету устройств обоих собеседников. На обоих этих устройствах также должна быть установлена программа Signal, иначе совершить вызов не получится. Таким образом, при общении с помощью программы Signal вам не придется платить оператору сотовой связи за голосовую связь, SMS и MMS-сообщения,— оплачивается только интернет-трафик.

Установка и первый запуск

1. Скачайте и установите на свое устройство приложение Signal из магазина App Store или Google Маркет.
2. Запустите установленное приложение — вы увидите экран, показанный на рис. 7.8, *слева.*
3. Введите номер своего мобильного телефона и коснитесь кнопки **Подтвердите свое устройство** (Verify This Device). Действующий номер телефона необходим для совершения вызовов и отсылки/приема сообщений. Для подтверждения вы получите SMS-сообщение с шестизначным кодом. Если не получается принять SMS-сообщение, можно подтвердить свой номер с помощью голосового вызова (автоответчика).
4. Введите цифры шестизначного кода в соответствующее поле экрана программы Signal.

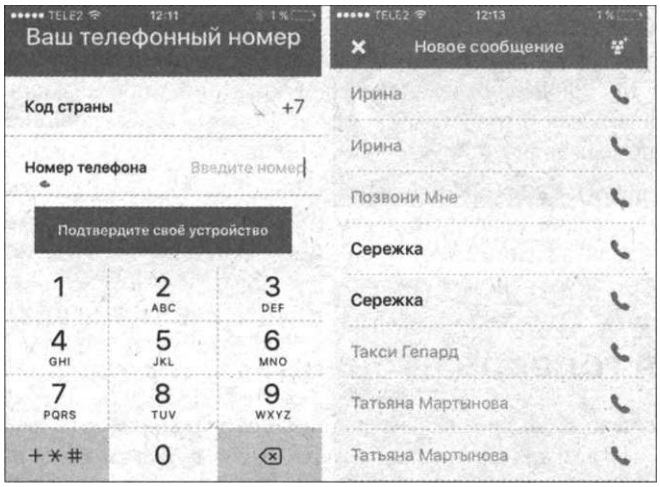


Рис. 7.8. Интерфейс приложения Signal (iOS)

5. Коснитесь кнопки **Отправить код подтверждения** (Submit Verification Code) — откроется экран с пустым списком контактов.

Чтобы использовать Signal, ваш собеседник должен также установить эту программу на свое устройство. Если вы попробуете позвонить или отправить сообщение человеку, у которого не установлена программа Signal, появится запрос, надо ли отправить вашему другу SMS-приглашение, но совершить голосовой вызов или отправить сообщение из Signal вы не сможете.

Делаем зашифрованный звонок

1. На главном экране программы Signal коснитесь кнопки — вы увидите свой список контактов (рис. 7.8, *справа).* Имена тех, кто уже пользуется программой Signal, будут выделены полужирным шрифтом, — вы можете звонить им и отправлять сообщения.
2. Коснитесь кнопки рядом с контактом нужного человека — программа выполнит вызов на номер выбранного абонента.

   Когда связь установлена, каждому собеседнику будет показана случайная пара слов (рис. 7.9, *слева),* — это позволит вам подтвердить свои личности и ключи шифрования, используемые для связи.

Самый надежный способ проверить личность собеседника — использовать для проверки слов альтернативный канал связи. Если вы узнаете собеседника по голосу, можете прочитать ему ключевые слова вслух (хотя злоумышленники могут и сымитировать голос вашего собеседника). Ключевые слова должны совпадать как у вас, так и у вашего собеседника.

Отправляем зашифрованное сообщение

Программа Signal позволяет отправить любой текст, изображение или видеофайл в зашифрованном виде напрямую адресату (рис. 7.9, *справа*), выбрав его номер в списке контактов.

Вы также можете зашифровать сообщение для группы людей. Для этого откройте список контактов, коснитесь кнопки в правом верхнем углу и создайте новую группу.

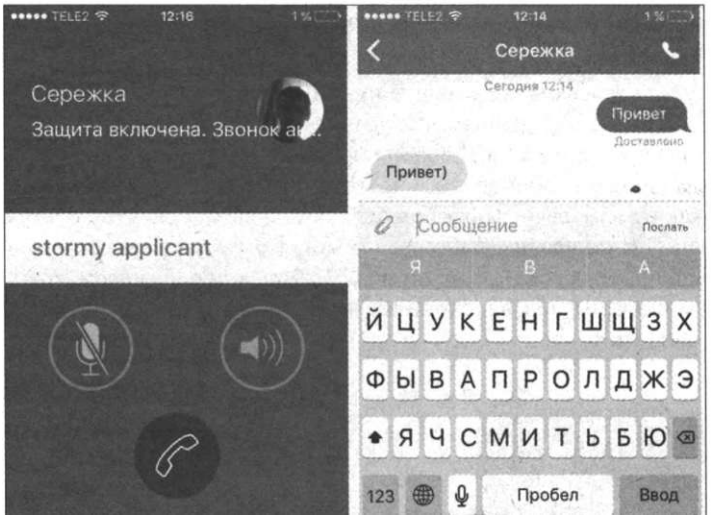


Рис. 7.9. Голосовые вызовы и сообщения в программе Signal (iOS)

Сквозное шифрование позволяет программе Signal заметно повысить уровень безопасности при обмене звонками и сообщениями. Но существуют и другие приложения для защиты переговоров по мобильному телефону — такие как Stealthphone Tell (tinyurl.com/gvotjm8), Silent Phone (tinyurl.com/nuopdly) и TopSec Phone (см. магазины Windows, Blackberry, App Store и Google Маркет).

Система Stealthphone

Stealthphone — это комплексное решение для защиты мобильной связи и компьютеров, состоящее из небольшого шифратора, подключаемого через интерфейс Bluetooth к мобильному телефону или компьютеру, и приложения Stealthphone Sec, работающего в связке с шифратором. Это решение позволяет шифровать любой тип передаваемых данных: речь (в том числе и IP-телефонию), SMS, MMS, электронную почту, переписку в социальных сетях и IM-мессенджерах, документы и файлы в мобильных телефонах и компьютерах стойким криптографическим алгоритмом. Оно также предоставляет возможность общаться в защищенном режиме в чатах и конференциях.

Шифратор Stealthphone (рис. 7.10, *слева*) совместим с любыми современными мобильными телефонами, а также планшетами или персональными компьютерами, он позволяет подключать через интерфейс Bluetooth одновременно до пяти устройств. Используемый в системе режим Voice Over GSM (VoGSM) служит для передачи зашифрованной речи через стандартный телефонный канал сотовой связи GSM. Это необходимо в тех случаях, когда мобильный телефон не имеет доступа к Интернету ни через Wi-Fi, ни через иные каналы передачи данных операторов сотовой связи (3G/4G, HSDPA, EDGE). При наличии доступа в Интернет голосовые вызовы можно вместо GSM переадресовать через IP-телефонию.

По запросу в системе устанавливается дополнительное программное обеспечение, которое формирует во время конфиденциального разговора речеподобные помехи. Тем самым исключается возможность снятия конфиденциальной информации через микрофон мобильного телефона, подключенного к шифратору. Шифрование речи производится с помощью от-

дельного устройства — аппаратного шифратора Stealthphone, который должен быть у каждого собеседника.

При краже или утере телефона злоумышленники не смогут получить доступ к хранящимся в программе Stealthphone Sec данным, потому что ключи шифрования хранятся в шифраторе. Каждому абоненту системы Stealthphone предоставляется уникальный набор ключей для связи с каждым другим абонентом, поэтому потеря или кража одного шифратора Stealthphone никак не влияет на защищенность остальных абонентов системы. Ключи шифрования соединений с конкретным абонентом могут быть удалены остальными абонентами системы Stealthphone из своих шифраторов. Набор ключей может быть легко изменен администратором системы при необходимости, а скомпрометированные ключи — удалены из базы ключей шифрования.



Рис. 7.10. Вид шифратора Stealthphone *(слева)* **и TopSec Mobile** *(справа)*

Узнать дополнительную информацию об устройстве можно на сайте ancort.ru. Среди аналогичных устройств можно отметить систему Stealthphone Hard, производимую швейцарской компанией Mobile Trust Telecommunications (tinyurl.com/zmqha6z), и TopSec Mobile, разработанную немецкой фирмой Rohde & Swartz (tinyurl.com/j7hhafw) (рис. 7.10, *справа).*

Blackphone 2

Несмотря на то, что аппарат Blackphone позиционировался компанией-разработчиком Silent Circle как самый защищенный смартфон, он был взломан за несколько минут на конференции DEF CON. Стремясь учесть упущения первой модели, разработчики выпустили вторую версию этого смартфона (рис. 7.11, *слева),* улучшив в ней практически все аппаратные характеристики и проведя работу над ошибками операционной системы устройства (PrivatOS). Впрочем, вряд ли можно быть уверенным в безопасности коммуникаций на этом гаджете, т. к. PrivatOS является не чем иным, как модифицированной операционной системой Android, одной из самых уязвимых мобильных платформ. Тем не менее, вторая версия

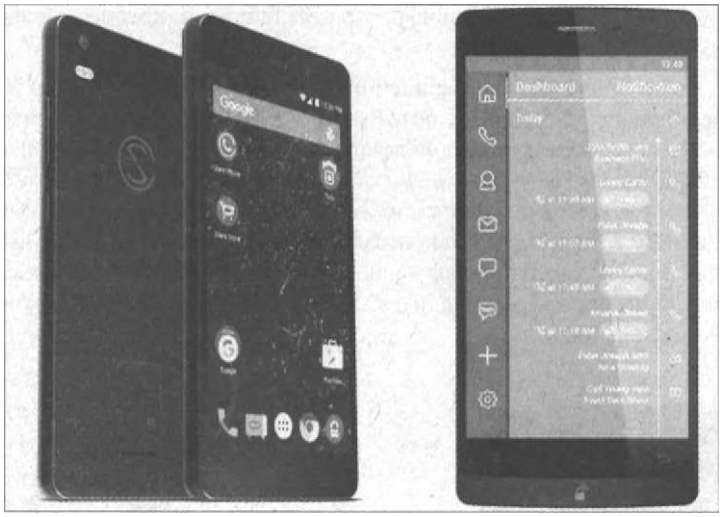


Рис. 7.11. Вид смартфона Blackphone 2 *(слева)* **и GranitePhone (***справа)*

смартфона вышла только в марте 2015 года, и подтвердить или опровергнуть доводы разработчика о защищенности устройства сможет только практическое использование.

Смартфон Blackphone появился как ответ на желание людей засекретить персональную информацию, которая нередко становится достоянием злоумышленников. Цель устройства — наделить пользователей доступом к полному контролю над конфиденциальностью персональных данных через набор безопасных приложений. В реализации этой цели на смартфоне установлен пакет Silent Suite, который состоит из следующих инструментов:

- Silent Phone — организует одноранговые зашифрованные вызовы через IP-телефонию;
- Silent Text — позволяет шифровать SMS-сообщения;
- Silent Contacts — защищает данные адресной книги, чтобы контакты не украли сторонние программы;
- Silent Meeting — реализует защищенную конференц-связь.

Все указанные приложения требуют платной подписки, и в стоимость устройства включен двухгодичный доступ к этим службам.

Как и в случае других подобных устройств, коммуникационные средства Blackphone 2 защищают информацию, только если абонент на другом конце провода пользуется такими же инструментами (доступными для операционной системы Android/iOS) или таким же смартфоном.

Разработчик устройства, компания Silent Circle, справедливо полагает, что далеко не вся связь нуждается в защите. Если вы заказываете по телефону пиццу, вряд ли злоумышленники станут подслушивать эти переговоры. Поэтому на смартфоне Blackphone 2 можно выбирать уровень конфиденциальности. В операционной системе PrivatOS доступны т. н. *пространства,* которые отделяют одни области Android-окружения от других путем размещения определенных частей системы в виртуальных контейнерах. Так, например, можно использовать одну учетную запись для всех коммуникационных приложений и другую для программ, работающих с документами. Смело отдавайте рабочий телефон в руки детям или гостям, и пусть они делают с. ним все, что угодно, — доступа к закрытым областям они не получат.

Помимо прочего, анонсирован запуск магазина одобренных приложений Silent Store и веб-инструмента Silent Manager — для управления устройствами сотрудников и разворачиваемыми на них приложениями. В качестве клиента электронной почты планируется выпуск приложения Dark Mail. Для хранения данных в зашифрованном виде выделяется 5 Гбайт пространства на облачном хранилище SpiderOak, а для обеспечения безопасности при веб-серфинге используется поисковый провайдер Disconnect, который через VPN-туннелирование анонимизирует запросы к интернет-службам. Все эти службы, разумеется, платные, поэтому по окончании двух лет эксплуатации подписку на них потребуется продлить.

Подавляющее число проблем с безопасностью и конфиденциальностью в операционной системе Android связано, как правило, с устанавливаемыми приложениями. Blackphone 2, будучи по сути Android-устройством, допускает установку программ из магазина Google Маркет, поэтому в смартфоне используется решение Security Center, необходимое для управления инсталлируемыми программами. Когда вы устанавливаете приложение, служба Security Center выводит список требуемых прав, и пользователь либо принимает, либо отклоняет их по отдельности. Права также регулируются в масштабе всей системы — к примеру, можно указать, что ни одно из приложений не располагает доступом к местоположению пользователя или его контактной информации. Такие настройки снижают типичные риски наподобие несанкционированной отправки персональных данных или звонков на платные номера. Встроенный центр управления сетями Wi-Fi отключает этот тип беспроводных соединений, если вы выходите из дома или офиса, чтобы остановить слежение за владельцем, основанное на географическом расположении точек доступа Wi-Fi. Если же смартфон был утерян или украден, по аналогии с iOS-девайсами вы сможете дистанционно стереть с него пользовательские данные.

Несмотря на перечисленные преимущества, смартфон подвержен потенциальным уязвимостям 0-day, а встроенный радиомодуль, выступающий промежуточным звеном между всеми беспроводными коммуникациями, располагает низкоуровневым доступом к микрофону, что опять же позволяет потенциальным злоумышленникам прослушивать владельца.

Другие устройства

Среди аналогичных устройств, предоставляющих владельцу средство для защищенных коммуникаций, можно отметить смартфон GranitePhone компании Sikur (рис. 7.11, *справа).* Никаких особенных подробностей о защите данных разработчики не приводят, однако известно, что аппарат предоставляет несколько степеней защиты, включая шифрование данных и облачное хранилище. Важно отметить, что устройство работает под управлением операционной системы Granite OS — собственной разработки компании, вместо платформы Android. Стоимость смартфона GranitePhone на февраль 2016 года составляла 999 долларов США, что дороже Blackphone 2 (799 долларов США). Приобрести устройство можно на сайтах **granitephone.com** и **silentcircle.com**/buy/ соответственно.

Помимо перечисленных устройств, существуют такие девайсы, как ANCORT A-7 — криптофон российской разработки, который изначально планировался для криптографической защиты. В этом устройстве используется специализированный крипточип, а также отсутствуют высокоизлучающие компоненты (сигнал которых можно перехватить): интерфейс Bluetooth, инфракрасный порт, съемная дополнительная память и приемопередатчик Wi-Fi. Реализация особой системы синхронизации обеспечивает надежную работу криптофона в роуминге, особенно на значительно удаленных расстояниях, где при передаче используются аналоговые средства передачи данных. В ANC0RT A-7 реализовано полноцен-

ное шифрование голоса и текстовых сообщений с соблюдением ГОСТ 28147-89[1]. Он также оснащается дополнительной аппаратной частью, которая позволяет не допустить несанкционированного прослушивания и удаленного включения микрофона. Расшифровать ранее зашифрованную в устройстве информацию невозможно, даже если им завладел злоумышленник, т. к. для каждого сеанса связи создается временный «сеансовый ключ», который в дальнейшем невозможно восстановить, — это обеспечивает сохранность разговоров, зашифрованных сообщений SMS и E-mail. Для обеспечения надежной криптографической связи смартфон ANCORT A-7 необходимо использовать обоим собеседникам. Приобрести смартфон можно на сайте **spectr-sks.ru,** стоимость аппарата на момент подготовки книги составляла 85 тыс. рублей.

Альтернативой ему представляется специальный сотовый телефон SMP-ATJIAC/2, в открытом режиме выполняющий все штатные функции стандарта GSM (голосовые вызовы и SMS-сообщения), а в защищенном — гарантированную криптографическую защиту речевой информации и аутентификацию абонентов. Приобрести устройство (стоимость аппарата на момент подготовки книги составляла 120 тыс. рублей) и узнать дополнительную информацию о нем можно на сайтах **stcnet.ru** и **tinyurl.com/z9faqgn.**

Стоит отметить, что согласно закону СОРМ-2, все переговоры с таких аппаратов могут напрямую протоколироваться в ФСБ, поэтому многие считают, что покупка отечественных аппаратов с криптозащитой лишена смысла, а ввоз подобных телефонов (не сертифицированных ФСБ) из-за границы запрещен. Ввиду этих уточнений, наиболее безопасным способом провести защищенные переговоры остается личная встреча без девайсов.

Приватный обмен мгновенными сообщениями

Уже не секрет, что ранее обеспечивавшая конфиденциальную и защищенную связь программа Skype перестала быть таковой. То же можно сказать и про системы обмена мгновенными сообщениями. Для решения проблемы обеспечения пользователей надежной и конфиденциальной связью стали разрабатываться различные альтернативные клиенты, такие как Telegram, Pidgin, Adium и др. Некоторые из них рассмотрим в этом разделе, а начнем мы, пожалуй, с Tox.

qTox

Tox — это VoIP-сервис, который позиционируется как безопасная альтернатива Skype. Как и Skype, Tox предлагает полный набор стандартных функций: голосовую и видеосвязь, режим конференции с несколькими участниками, возможность передачи мгновенных сообщений и файлов. По логике работы Tox напоминает схему взаимодействия клиентов пиринговой сети.

Решения для шифрования обычных телефонных переговоров давно существуют. Одними из самых востребованных являются ранёе рассмотренные приложения Signal **(whispersystems.org)** — для iOS и Android и Silent Circle **(silentcircle.com)** — для iOS и Android. Однако Tox может заменить собой как приватные мессенджеры, так и программные криптофоны. Существует несколько разновидностей клиентских приложений Tox: qTox — стандартная версия и pTox — максимально облегченная версия для пользователей Linux, Windows, OSX, BSD и Android, Toxic — аскетичный вариант для платформы UNIX,

[1] См. tinyurl.com/z5e4m3j.

Antox — мобильный вариант для операционной системы Android, а также Antidote — версия для iOS (пока еще не выпущена). Чтобы вам было проще разобраться в версиях клиентов Tox, в табл. 7.2 приведены некоторые уточняющие сведения.

Несмотря на разнообразие подходов при разработке клиентских приложений Tox, в'се они работают по общей схеме асимметричного шифрования: после установки приложения автоматически создается пара ключей, открытый ключ служит идентификатором для поиска собеседника, а закрытый — хранится только у владельца и подтверждает его подлинность, не раскрывая персональных данных.

Таблица 7.2. Клиентские приложения Tox

	Windows	GNU/Linux	BSD	OSX	Android	iOS
qTox	Да	Да	Да	Да	Нет	Нет
pTox	Да	Да	Да	Да	Минимально	Нет
Toxic	Нет	Да	Да	Да	Нет	Нет
Antox	Нет	Нет	Нет	Нет	Да	Нет
Antidote	Нет	Нет	Нет	Нет	Нет	Да

Познакомиться с возможностями программы и загрузить ее сборку на компьютер (поддерживаются операционные системы Windows, OS X, Android и Linux) можно на сайте **tox.chat.** На рис. 7.12 показан интерфейс программы qTox.

При первом запуске приложения понадобится выбрать имя пользователя, пароль и указать адрес электронной почты, после чего вы увидите главное окно qTox.

С помощью этой программы можно передавать по зашифрованным каналам текстовые сообщения и файлы, осуществлять голосовые и видеовызовы. Непременным условием при этом будет наличие приложения Tox на компьютере (устройстве) собеседника.

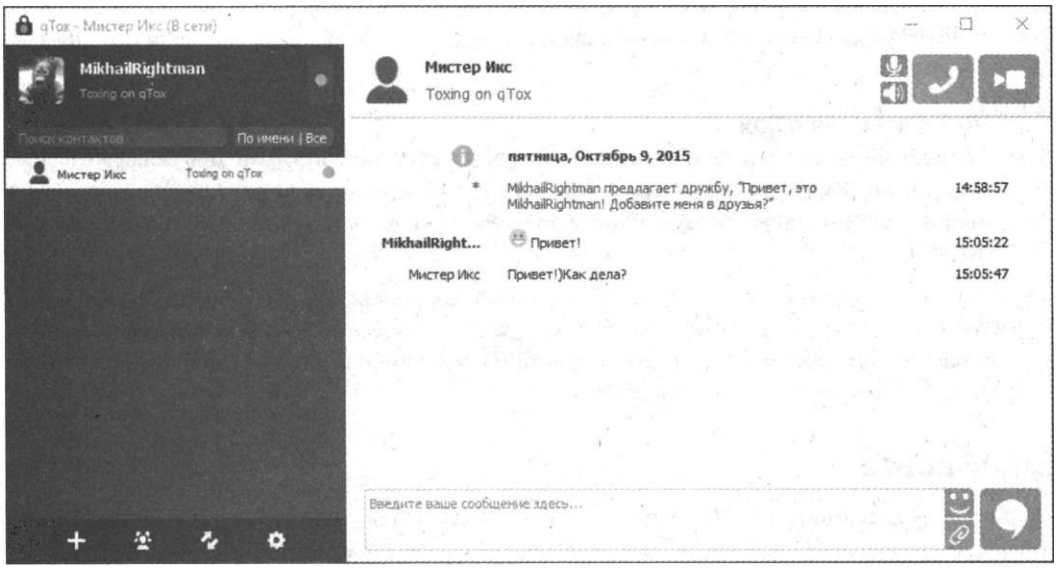


Рис. 7.12. Интерфейс программы qTox

Чтобы добавить собеседника, нужно узнать его Tox ID вида:

ВГЙЕ724ГСО6СВСС197126Е63АО30О7О62Е9Е42519ГА0Г084Е92790СС82Е5765Е57ЕВСГО4294Г

и ввести его в поле Tox ID, появляющееся после нажатия кнопки +.

Вы также можете предоставить собеседнику свой Tox ID, чтобы он включил вас в число своих контактов. Чтобы скопировать свой идентификатор, щелкните мышью по своему аватару или логину в левом верхнем углу окна программы qTox — вы увидите окно, показанное на рис. 7.13.

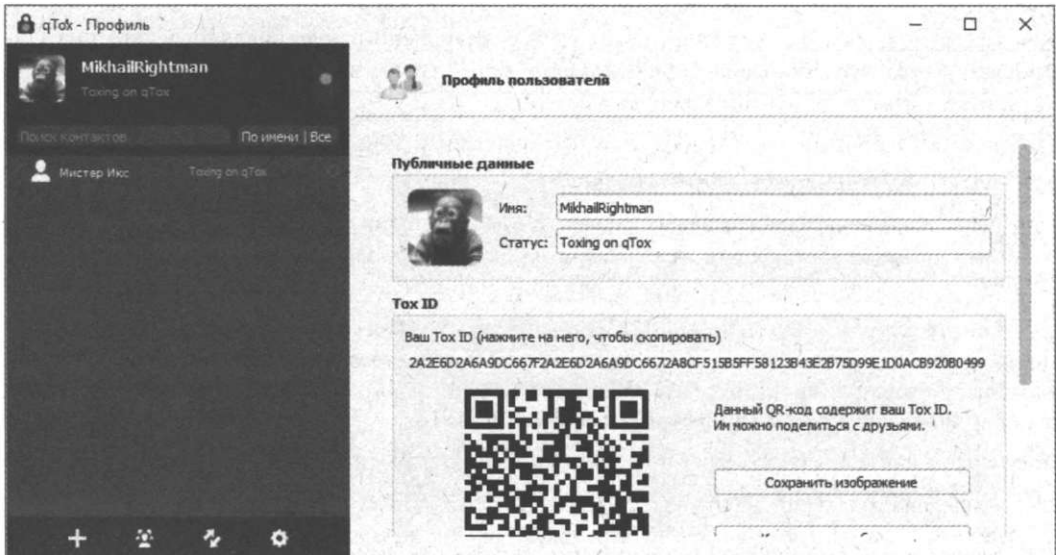


Рис. 7.13. Просмотр своего Tox ID

Щелкните в нем по своему Tox ID мышью, и он запишется в буфер операционной системы. Вместо Tox ID вы можете предоставить своим будущим собеседникам уникальный QR-код, показанный в том же окне.

ЛОКАЛИЗАЦИЯ QTOX

По умолчанию интерфейс qTox может оказаться на английском языке. Для выбора русского языка интерфейса щелкните мышью на кнопке____в нижней части окна программы, а затем

на вкладке General (Общие) выберите пуню* Русский в раскрывающемся списке Language (Язык).

Помимо Tox подобные сервисы для защищенной переписки разрабатываются и другими разработчиками. Среди них стоит отметить находящиеся в разработке Briar **(briarproject.org)** и Invisible.im **(invisible.im).** Оба эти клиента позиционируются как приватные аналоги WhatsApp, Viber и других мессенджеров.

ChatSecure

ChatSecure **(chatsecure.org)** — бесплатное приложение для смартфонов и планшетов под управлением операционной системы iOS и Android (доступное, соответственно, в магазинах App Store и Google Маркет), которое позволяет обмениваться зашифрованными мгновен-

ными сообщениями. Приложение поддерживает шифрование по криптографическому протоколу OTR (Off-the-Record) с обменом данными по протоколу XMPP (ранее известному как Jabber). Все сообщения, отправленные через ChatSecure, полностью приватны, при условии, что ваш собеседник также использует приложение с поддержкой протокола OTR (например, ChatSecure, Adium или Pidgin). ChatSecure позволяет пересылать и файлы: аудиосообщения, фотографии, текст и т. п. Что примечательно, при отправке сообщения из программы ChatSecure оно не сохраняется в системной памяти устройства.

Установка и настройка

Как уже отмечалось, приложение может быть установлено из официального магазина устройства: Apple App Store или Google Маркет. При первом запуске приложения после его установки вы увидите пустой экран **Чаты** (Chats).

Программа ChatSecure умеет работать с несколькими учетными записями. Для добавления учетной записи выполните следующие действия:

1. Коснитесь кнопки , а затем пункта **Новая учетная запись** (New account) — вам будет предложено создать новую или подключить существующую учетную запись (рис. 7.14, *слева).* В этом примере будет зарегистрирован новый аккаунт.
2. Коснитесь пункта **Создать новый** (Create New Account) — вы увидите экран, предназначенный для выбора способа подключения: с использованием сети Tor или нет.

   ПОДКЛЮЧЕНИЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ TOR

   Подключение с использованием сети Tor, что способно обеспечить еще большую защиту, доступно пока в качестве экспериментальной функции. На момент подготовки книги рекомендовалось использовать эту функцию с осторожностью.

3. Коснитесь пункта **XMPP (Jabber)** для подключения через один из публичных **XMPP**-серверов[1].
4. Укажите желаемое имя пользователя или адрес электронной почты и пароль (рис. 7.14, *справа).*

   FACEBOOK И GOOGLE TALK

   Вы можете авторизовать в программе ChatSecure аккаунты в социальных сетях Facebook и Google Talk и общаться со своими друзьями из этих сетей. Для этого нужно выбрать вариант подключения существующего аккаунта (см. рис. 7.14, *слева),* а затем указать данные своей учетной записи.

   Установка переключателей **Запомнить пароль** (Remember Password) и **Подключаться автоматически** (Login Automatically) в активное положение не рекомендуется, т. к. в этом случае снижается уровень защиты, — при утере или краже устройства злоумышленник сможет прочитать вашу переписку, автоматически авторизовавшись в приложении.

5. Коснитесь пункта **Создать** (Create) — через некоторое время вы увидите уведомление о созданном сертификате (рис. 7.15, *слева).*
6. Коснитесь пункта **Сохранить** (Save) — сертификат будет сохранен, а вы увидите экран настроек (рис. 7.15, *справа).*

[1] Список серверов приведен на сайте tinyurI.com/ptSkc4I.

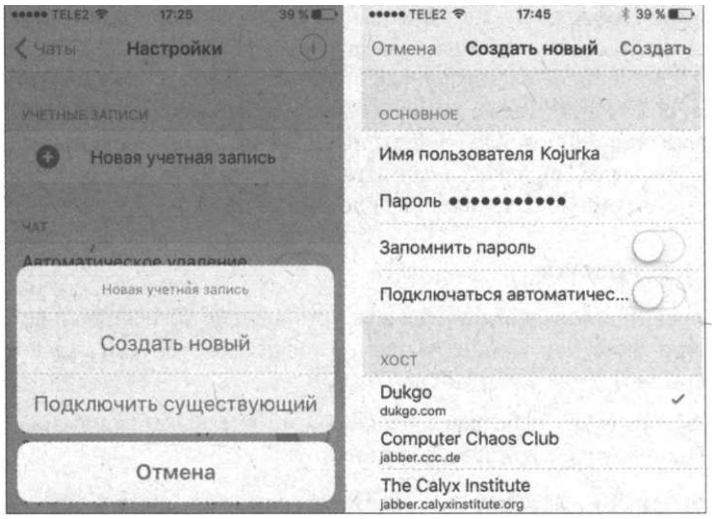


Рис. 7.14. ChatSecure: подключение аккаунта *(слева)* **и ввод данных** *(справа)*

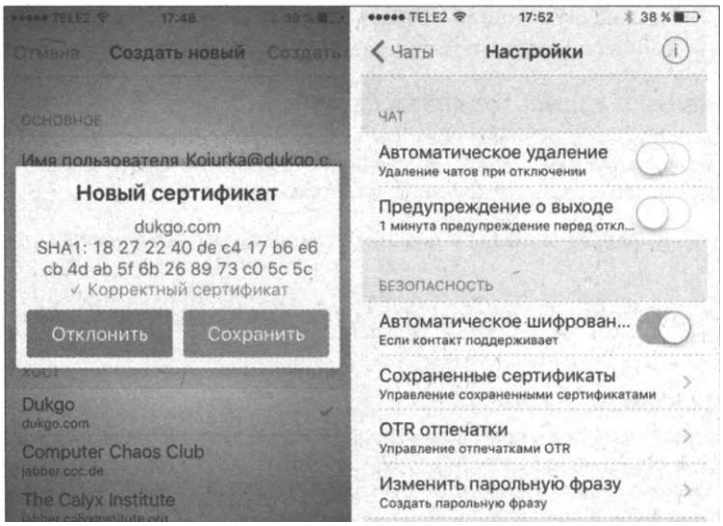


Рис. 7.15. ChatSecure: сохранение сертификата *(слева)* **и настройки программы** *(справа)*

Среди всех предлагаемых настроек важнейшим является переключатель Автоматическое удаление (Auto-delete). Как следует из описания, активное положение этого переключателя позволяет программе автоматически удалять чаты при выходе из приложения. Это полезно для обеспечения большей безопасности вашей переписки — никто не сможет прочитать ее, даже получив доступ к программе. На этом экране вы также можете настроить уведомление об автоматическом отключении аккаунта (происходит через некоторое время бездействия) и установить в активное положение переключатель Автоматическое шифрование (Auto-start Encryption). Последняя настройка должна быть активна, чтобы вы были уверены в безопасности переписки (при условии, что программа собеседника поддерживает шифрование). Другими опциями этого экрана осуществляется управление сохраненными сертификатами и OTR-отпечатками, а также парольной фразой для доступа к программе.

Работа в программе

После запуска программы и успешной авторизации аккаунта ваши собеседники смогут связаться с вами с помощью приложений для обмена мгновенными сообщениями.

Чтобы начать новый чат, выполните следующие действия:

1. Коснитесь кнопки в левом верхнем углу экрана **Чаты** (Chats) и выберите имя собеседника на экране, показанном на рис. 7.16, *слева.*

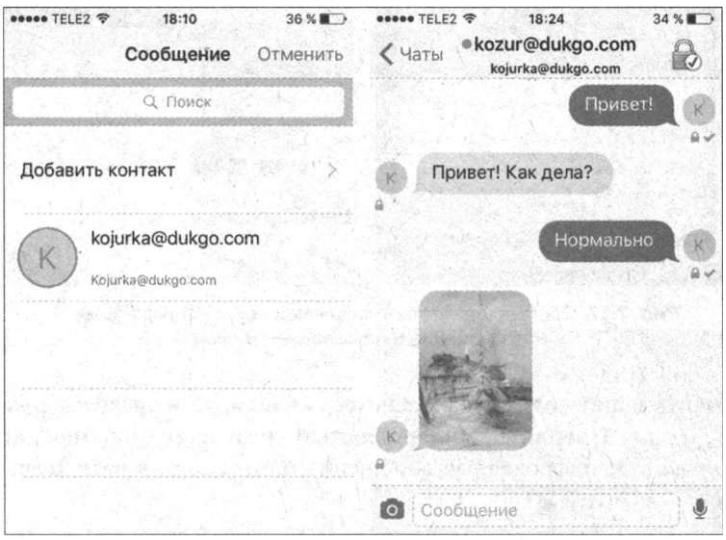


Рис. 7.16. ChatSecure: выбор контакта *(слева)* и чат (*справа)*

Если вы хотите добавить нового собеседника, коснитесь пункта **Добавить контакт** (Add Buddy) и введите адрес электронной почты собеседника. После подтверждения собеседником вашего запроса вы сможете начать с ним беседу.

2. После запуска чата (рис. 7.16, *справа)* с одним из собеседников коснитесь кнопки в правом верхнем углу экрана и выберите пункт **Начать шифрованный разговор** (Initiate Encrypted Chat). Если у собеседника установлено приложение с поддержкой криптографического протокола OTR, у вас появится возможность верифицировать отпечатки — ваш и вашего собеседника.

   Программа ChatSecure предлагает три варианта верификации отпечатков OTR. Если для общения используется программа на настольном компьютере, а не ChatSecure, для верификации отпечатка OTR лучше использовать альтернативный канал связи. Вы можете отправить свой отпечаток через SMS-сообщение, продиктовать его по телефону (если оба собеседника знают голоса друг друга), обменяться отпечатками по электронной почте (зашифрованной PGP-ключами) или при личной встрече.

3. Коснитесь кнопки в правом верхнем углу экрана и выберите пункт **Проверить** (Verification) — программа ChatSecure отобразит ваш отпечаток и отпечаток вашего собеседника (рис. 7.17, *слева).*

4. Если вы оба можете подтвердить, что имеющаяся у вас обоих информация совпадает, коснитесь кнопки **Проверен** (Verified).

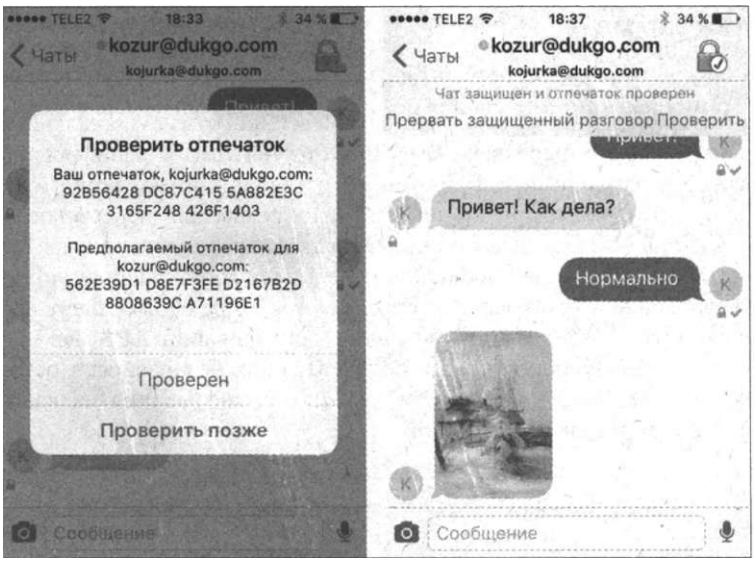


Рис. 7.17. ChatSecure: отпечатки ключей собеседников *(слева)* и отключение шифрования *(справа)*

5. Чтобы отключить защиту разговора, коснитесь кнопки в правом верхнем углу экрана и выберите пункт **Прервать шифрованный разговор** (Interrupt Encrypted Chat) (рис. 7.17, *справа*). Зашифрованные сообщения помечаются в чате значком , а незашифрованные — значком

Рассмотренное приложение, как мы уже отмечали, позволяет передавать мультимедиасообщения, фотографировать и безопасно отправлять фотографии и файлы, если собеседник тоже использует сквозное шифрование, и вы успешно верифицировали отпечатки.

ChatSecure также дает возможность создания новых учетных записей XMPP (Jabber), которые поддерживают шифрование OTR. Если вы еще не знакомы с XMPP, это хороший повод создать учетную запись и поэкспериментировать с открытыми протоколами обмена мгновенными сообщениями.

Telegram

Telegram — защищенное от прослушивания приложение для обмена сообщениями, выпущенное в 2013 году основателем социальной сети «ВКонтакте» Павлом Дуровым. Помимо отправки текстовых сообщений, приложение позволяет обмениваться мультимедийными файлами. Существенным достоинством Telegram является поддержка не только мобильных устройств (iOS, Windows Phone, Android и Blackberry), но и настольных платформ (Windows, OS X и Linux), а также веб-клиентов. Учетные записи пользователей привязываются к их телефонным номерам, а все сообщения (кроме секретных чатов) автоматически синхронизируются между устройствами. При регистрации в сервисе и последующих авторизациях новых устройств производится проверка телефонного номера через отправку SMS-сообщения с кодом или телефонный вызов.

В отличие от таких клиентов, как WhatsApp, Telegram работает в облаке, кроме того, шифрует весь трафик (в том числе и передаваемые файлы) и поддерживает функцию самоуничтожения сообщений. Благодаря распределенной инфраструктуре и мощным серверам,

программа Telegram гораздо безопаснее и быстрее, чем любое подобное приложение (WhatsApp, Viber и пр.).

Клиент Telegram основан на протоколе MTProto, созданном по проверенным алгоритмам, обеспечивающим высокую скорость и надежность. Программа поддерживает секретные чаты, сообщения в которых передаются между устройствами в зашифрованном виде и не хранятся на серверах разработчика, при этом по истечении определенного времени происходит их самоуничтожение, и они становятся недоступны для пересылки. Единственный минус такого подхода — если ваш собеседник отключен, сообщение не будет доставлено, — в режиме секретных чатов сообщения передаются только напрямую с устройства на устройство. Шифрование в программе осуществляется в два слоя (клиент-сервер и сервер-сервер) и основано на 256-битном симметричном шифровании AES, RSA 2048 и обмене ключами методом Диффи-Хеллмана. Для подтверждения безопасности общения производится верификация графического изображения ключа шифрования на вашем устройстве с изображением на устройстве собеседника.

Следует отметить, что программа Telegram гарантирует безопасность шифрования и передачи зашифрованных данных, однако не сможет уберечь вашу переписку от людей, имеющих физический доступ к устройству. В этом случае следует пользоваться только секретными чатами с включенным таймером самоуничтожения.

> ***НЕСКОЛЬКО СЕССИЙ***
>
> **Вы можете авторизоваться в программе Telegram на нескольких устройствах одновременно. Ограничений на количество одновременных сессий нет.**

Установите Telegram на своем устройстве, воспользовавшись поиском по слову `telegram` в соответствующем устройству магазине приложений. Для операционной системы Windows, OS X или Linux программу можно скачать по адресу **https://tlgrm.ru/apps.** Неофициальное приложение Telegram Web, в котором секретные чаты не поддерживаются, доступно по адресу **https://web.tlgrm.ru.**

Поддержка русского языка в Telegram

По умолчанию в программе Telegram русский интерфейс недоступен. Но чтобы установить русский или любой другой язык локализации, достаточно скачать и установить специальный файл с помощью робота. Для этого выполните следующие действия:

1. Запустите приложение Telegram и на вкладке **Contacts** (Контакты) коснитесь кнопки
2. В появившемся поле ввода укажите поисковый запрос `telerobot`, а затем выберите контакт **Робот Антон** (рис. 7.18, *слева).*
3. Откроется чат с выбранным контактом, в котором нужно указать команду, соответствующую указанному устройству (например, `ios` или `osx`) и устанавливаемому языку (к примеру, `ru` или `fr`). На рис. 7.18, *справа,* продемонстрирован чат с командой для устройств под управлением операционной системы Windows Phone. Далее приведены команды и порядок действий для разных устройств:
   - **iOS** — введите команду `locale ios ru` и коснитесь кнопки в виде стрелки в полученном ответном сообщении, чтобы скачать файл локализации. Затем коснитесь сообщения и в появившемся контекстном меню выберите пункт **Apply localization** (Применить локализацию). После выполнения указанных действий язык интерфейса приложения сменится на русский;

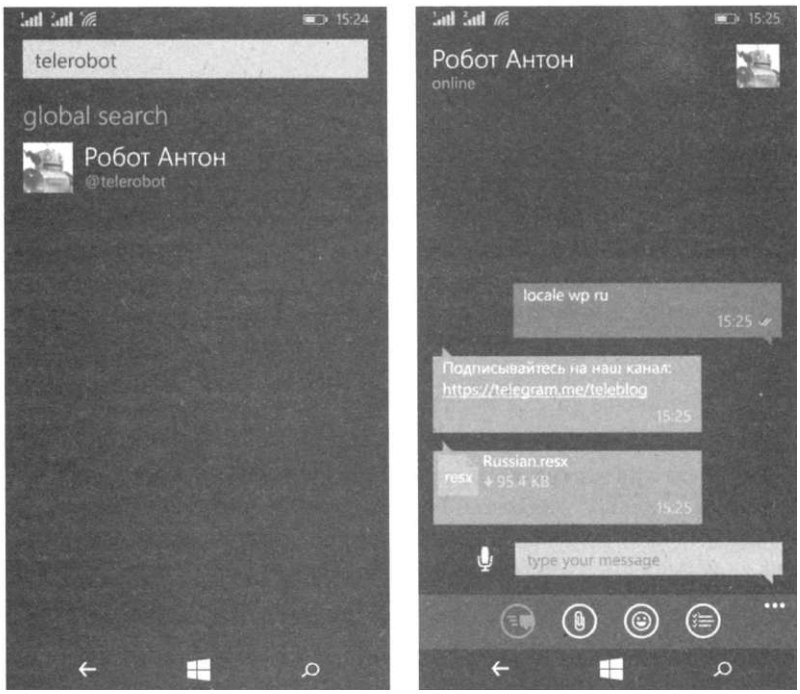


Рис. 7.18. Установка языка локализации в программе Telegram

Android — введите команду `locale android ru` и коснитесь кнопки в виде стрелки в полученномответном сообщении, чтобы скачать файл локализации. Затем коснитесь кнопки в правом верхнем углу сообщения и в появившемся контекстном меню выберите пункт **Apply localization file** (Применить файл локализации). Перейдите на экран настроек **(Settings | Language** (Настройки | Язык)) и выберите русский язык интерфейса. После выполнения указанных действий язык интерфейса приложения сменится на русский;

Windows Phone — на момент подготовки книги изменение языка интерфейса версии программы для операционной системы Windows Phone было недоступно. Тем не менее, команда `locale wp ru` позволяет запросить и скачать файл локализации. Возможно, в будущих версиях программы возможность русификации программы станет доступна и на устройствах под управлением операционной системы Windows Phone (Windows 10);

Telegram Desktop (Windows, OS `X`, Linux) — введите команду `locale tdesktop ru` и щелкните мышью на ссылке **Download** (Скачать) справа от полученного сообщения, чтобы скачать файл локализации. Затем перейдите на вкладку **Settings** (Настройки) на верхней панели и, нажав и удерживая сочетание клавиш <Shift>+<Alt>, щелкните мышью на ссылке **Change language** (Изменить язык). После выбора сохраненного файла локализации и перезапуска приложения язык интерфейса приложения сменится на русский;

Telegram для OS X— введите команду `locale osx ru` и сохраните файл локализации, полученный в ответном сообщении. Переименуйте полученный файл в **Localizable.strings.** Скопируйте этот файл в папку **/Applications/Telegram.app/Coritents/Resources/ru.lproj/,** заменив имеющийся там файл (потребуется ввести пароль адми-

нистратора). После перезапуска приложения язык интерфейса приложения сменится на русский.

Основы Telegram

Чтобы пригласить друзей в Telegram, достаточно отправить ссылку на скачивание программы любому вашему контакту через SMS-сообщение. Это можно сделать прямо из программы. Как только ваш друг установит приложение, он появится в вашем списке контактов. Далее приведены шаги для операционной системы Windows Phone, и на вашем устройстве они могут несколько отличаться.

1. Запустите приложение Telegram и перейдите на вкладку **Contacts** (Контакты) — вы увидите список всех контактов в вашем устройстве: в верхней части будут отображены контакты, у которых установлена программа Telegram, а ниже — все остальные (рис. 7.19, *слева)*.

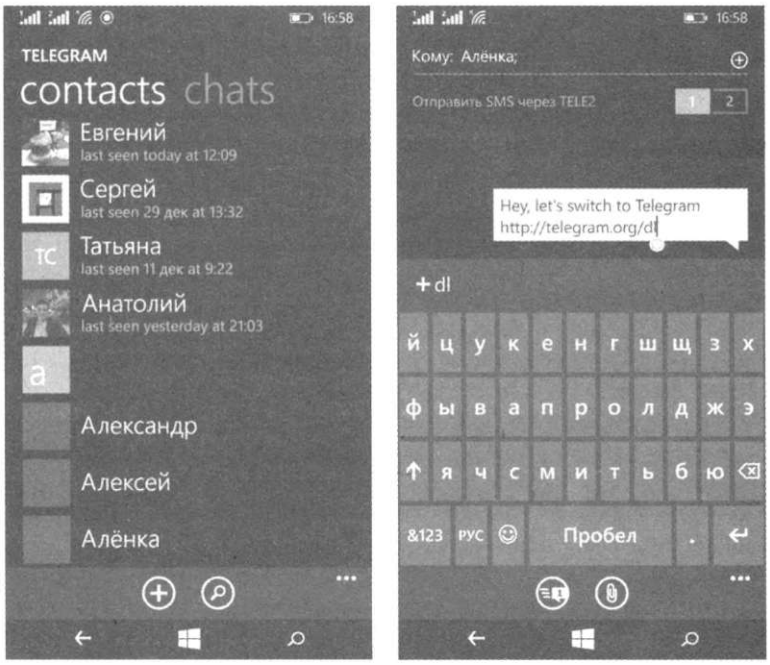


Рис. 7.19. Telegram: список контактов (слева) и SMS-сообщение с уведомлением (*справа)*

Если у контакта установлена программа Telegram, вы можете сразу начать общаться с ним, выбрав его имя из списка. Если ваш собеседник еще не пользуется Telegram, вы можете отправить ему SMS-сообщение с уведомлением.

2. Выберите имя контакта, у которого не установлена программа Telegram, — появится экран встроенного приложения, предназначенного для отправки SMS-сообщений (рис. 7.19, *справа)*.
3. При необходимости отредактируйте, а затем отправьте сообщение.

Чтобы другие пользователи могли найти вас с помощью поиска, нужно указать свое имя пользователя в настройках профиля. По умолчанию это имя не указывается, чтобы обеспе-

чить дополнительную безопасность пользователя и его коммуникаций (пользователь вне списка контактов может добавить вас, только указав ваш номер телефона, зарегистрированный в Telegram). Если же вам необходимо разрешить поиск своего профиля другими (любыми) пользователями, выполните следующие действия:

1. Перейдите на экран настроек профиля. На устройствах под управлением операционной системы Windows Phone это можно сделать, коснувшись кнопки Ц и выбрав пункт **Settings** (Настройки) (рис. 7.20, *слева),* — вы увидите экран настроек профиля, показанный на рис. 7.19, *справа.* На вашем устройстве доступ к настройкам профиля может быть иным (см. страницу **tinyurl.com/jdysr2r).**

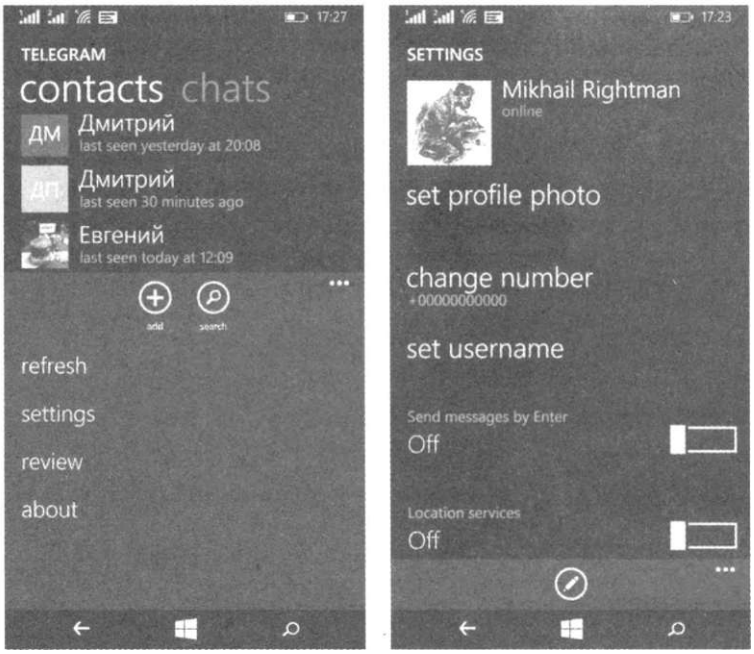


Рис. 7.20. Telegram: меню настроек *(слева)* и настройки профиля (*справа)*

2. Для указания (изменения) имени пользователя коснитесь ссылки **Set username** (Указать имя пользователя).
3. Введите имя, по которому пользователи будут находить вас в Telegram, и коснитесь кнопки

   Если вы создали себе имя пользователя, то можете поделиться ссылкой на свой профиль с другими пользователями, перейдя по ссылке **telegram.m***е/ВашеИмяПользователя*. Переход по этой ссылке автоматически запустит программу Telegram и откроет чат с вами.

На экране настроек профиля вы также можете сменить номер мобильного телефона (все контакты, сообщения, файлы и т. п. будут перемещены и связаны с новым номером), установить фото профиля (аватар), активировать службы геолокации (не рекомендуется для предотвращения отслеживания местонахождения) и выполнить некоторые другие настройки.

Общение в чате происходит таким же образом, как и во всех других подобных мессенджерах (см. рис. 7.18, *справа).*

В нижней части экрана расположены следующие кнопки:

- — служит для отправки набранного текста сообщения;
- — предназначена для передачи позиции геолокации, видеофайла, изображения или другого файла;
- —позволяет выбрать смайлик;
- — используется для выбора сообщений, которые нужно удалить касанием кнопки с изображением корзины.

После отправки сообщения на его облаке отображаются одна или две галочки: одна галочка информирует о том, что сообщение отправлено (и оно находится на сервере Telegram в ожидании, пока собеседник запустит программу), а собеседнику выслано уведомление о новом сообщении, две галочки означают, что сообщение прочитано (собеседник запустил программу Telegram и открыл чат с этим сообщением).

КОНФЕРЕНЦИИ И КАНАЛЫ

Если на вкладке Chats (Чаты) коснуться кнопки, а затем выбрать пункт New Group (Новая группа) или New Channel (Новый канал), можно создать новую конференцию или канал соответственно. Конференции позволяют привлечь в чат несколько участников из числа друзей, а каналы исполняют роль общедоступных массовых рассылок с неограниченным числом участников.

Секретные чаты

Секретные чаты подойдут пользователям, которые хотят общаться *действительно* безопасно. В таком случае весь трафик шифруется от устройства до устройства. Это означает, что только вы и ваш собеседник сможете прочитать ваши сообщения — никто не сможет их перехватить или расшифровать, включая разработчиков Telegram. Сообщения из секретного чата нельзя переслать. Более того -— можно задать промежуток времени, спустя который сообщения после прочтения их собеседником будут уничтожаться, причем они удалятся и с вашего устройства, и с устройства собеседника.

Когда создается секретный чат, участвующие в нем устройства обмениваются ключами шифрования по протоколу Диффи-Хеллмана.

ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА

Это криптографический протокол, позволяющий двум и более сторонам через незащищенный от прослушивания канал связи получить общий секретный ключ. Полученный ключ служит для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования. В чистом виде алгоритм Диффи-Хеллмана уязвим для модификации данных в канале связи, поэтому схемы с его использованием применяют дополнительные методы односторонней или двусторонней аутентификации. По последним данным алгоритм Диффи-Хеллмана может быть скомпрометирован АНБ[1].

После установления безопасного сквозного соединения создается изображение, визуализирующее ключ шифрования вашего чата (рис. 7.21, *справа*). Вы можете сравнить это изображение с тем, которое отображается у вашего собеседника, и если они идентичны, этот секретный чат безопасен, и атака посредника (см. соответствующее примечание в *главе 6)* в принципе невозможна.

[1] См. tinyurl.com/zfc25dk.

Создание секретного чата

Создать секретный чат можно двумя способами:

- на вкладке **Chats** (Чаты) программы Telegram коснитесь кнопки а затем выберите пункт **New Secret Chat** (Новый секретный чат). На появившемся экране **Add Member** (Добавить участника) выберите имя собеседника, чтобы начать с ним секретный чат;
- на вкладке **Contacts** (Контакты) программы Telegram выберите имя собеседника. На появившемся экране с обычным чатом коснитесь аватара пользователя (на устройствах под управлением операционной системы Windows Phone — в правом верхнем углу экрана), а затем выберите пункт **Create Secret Chat** (Создать секретный чат).

В любом случае вы увидите экран секретного чата, в котором сможете общаться с собеседником и пересылать ему файлы в безопасном режиме (рис. 7.21, *слева).*

Чтобы удостовериться, что вы общаетесь именно с тем человеком, которого представляет аккаунт в Telegram, и для проверки безопасности чата, вы можете проверить изображение, визуализирующее ключ шифрования вашего чата (см. рис. 7.21, *справа).* При сравнении этого изображения с тем, что отображается у вашего собеседника, они должны быть идентичны. Чтобы просмотреть это изображение, нужно коснуться аватара пользователя (на устройствах под управлением операционной системы Windows Phone — в правом верхнем углу экрана), а затем выбрать пункт **Encryption Key** (Ключ шифрования).

Помимо этого, в секретных чатах на обоих устройствах отображаются уведомления о действиях собеседника: если тот установил таймер самоуничтожения и, что может быть важно для обеспечения безопасности, сделал снимок экрана с чатом (см. рис. 7.21, *слева).*

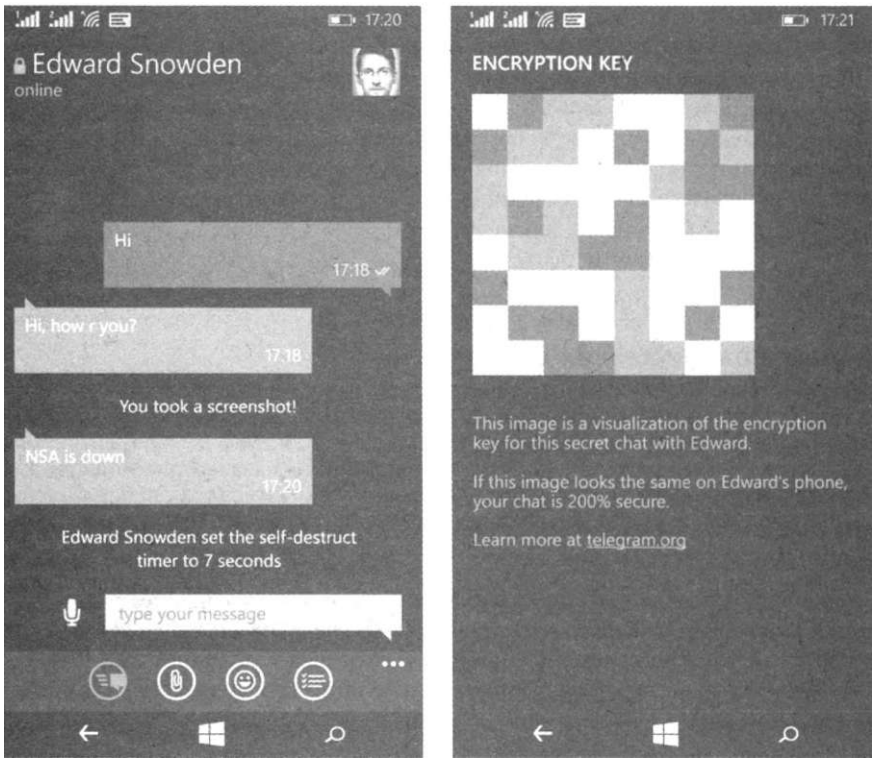


Рис. 7.21. Telegram: секретный чат *(слева)* и изображение ключа шифрования *(справа)*

Самоуничтожение сообщений

В секретных чатах доступен таймер самоуничтожения. Чтобы установить его, выполните следующие действия:

- **Windows Phone** — коснитесь аватара пользователя в правом верхнем углу экрана, а затем выберите промежуток времени в раскрывающемся списке **Self-destruct Timer** (Таймер самоуничтожения);
- **iOS** — коснитесь кнопки в поле ввода текста и выберите промежуток времени;
- **Android** — коснитесь кнопки на верхней панели и выберите промежуток времени.

Таймер запустится в момент, когда получатель прочтет сообщение (две зеленые галочки), и как только заданное время пройдет, сообщение будет удалено с *обоих* устройств. Фотографии, отправленные с включенным на короткий период таймером (менее 1 минуты), могут быть просмотрены, только пока вы их удерживаете. Обратите внимание, что таймер применяется только к сообщениям, отправленным *после* его установки. Он никак не повлияет на отправленные ранее сообщения.

Учитывайте, что секретные чаты привязаны к устройству. Если вы создадите секретный чат на одном из ваших устройств, он будет доступен только на нем, а когда вы выйдете из своего аккаунта, все секретные чаты будут удалены.

Удаление аккаунта

Для удаления аккаунта Telegram перейдите на страницу деактивации по адресу **tinyurl.com/qajy5cw** и укажите номер мобильного телефона, к которому привязан аккаунт. После этого вы получите на своем устройстве новое сообщение в системном чате Telegram с паролем, который необходимо ввести на странице деактивации.

Удалив аккаунт, вы безвозвратно удалите все сообщения, чаты и контакты. Это действие не может быть отменено: Тем не менее, ваши собеседники по-прежнему смогут переписываться в чатах, созданных вами, и будут иметь копии сообщений, которые вы им отправили. Поэтому, если вы хотите отправлять сообщения так, чтобы они не оставляли за собой следов, пользуйтесь таймером самоуничтожения.

Удаление аккаунта в Telegram необратимо. Если вы зарегистрируетесь вновь, то появитесь как новый пользователь и не сможете вернуть обратно историю переписки и контакты. Пользователям, у которых ваш номер записан в контактах, придет соответствующее уведомление, и переписка с вами будет далее вестись в новом диалоге.

Pidgin

Как уже говорилось в начале этой главы, OTR (Off-the-Record) — это протокол, позволяющий пользователям служб обмена мгновенными сообщениями и чатов вести конфиденциальную переписку. В этом разделе вы узнаете о том, как вести зашифрованную с помощью OTR переписку в чат-клиенте Pidgin — бесплатной программе с открытым исходным кодом для операционных систем Windows и Linux.

Протокол OTR повышает уровень безопасности при коммуникации следующим образом:

- шифрует чаты;
- позволяет убедиться, что ваш собеседник именно тот, за кого себя выдает;
- не позволяет серверу вести запись вашей беседы или получать к ней доступ иным способом.

По умолчанию программа Pidgin записывает чаты, но вы можете отключить запись. Однако при этом у вас нет контроля над собеседником — он может записывать разговор или делать снимки экрана, даже если с вашей стороны запись выключена.

В программе Pidgin вы можете авторизоваться, используя несколько учетных записей одновременно (например, Google Hangouts, Facebook и XMPP). Программа Pidgin позволяет общаться с помощью этих аккаунтов и без OTR, но защита ÖTR *работает, только если оба собеседника используют эту технологию.* Таким образом, даже если ваш собеседник не установил OTR, вы все равно можете общаться с ним с помощью Pidgin.

Если вы общаетесь в чате Google или Facebook, передаваемые данные *уже* шифруются с помощью протокола HTTPS. Но эти чаты, в отличие от чатов, защищенных OTR, *открыты* для сотрудников компаний Google или Facebook, которые имеют шифровальные ключи от вашего чата и могут передать их посторонним лицам или использовать для маркетинговых целей.

Программа Pidgin позволяет осуществлять верификацию собеседника, чтобы подтвердить личность собеседника и избежать атаки посредника. Для этого в каждом чате можно просмотреть отпечатки ключей (в виде последовательности символов) — как вашего, так и собеседника (как уже отмечалось ранее, короткие отпечатки позволяют проверять более длинные открытые ключи). Отпечатками следует обмениваться по альтернативному каналу связи (например, через сообщения в сети Twitter или по электронной почте). Если ключи не совпадают, вы не можете быть уверены, что говорите с нужным человеком. Впрочем, на практике пользователи часто используют несколько ключей или теряют и создают новые ключи, поэтому не удивляйтесь, если время от времени вам будет требоваться заново проверять ключи собеседников.

Несмотря на все перечисленные преимущества, важно отметить, что чат-клиент Pidgin довольно уязвим, т. к. при разработке этой сложной программы безопасность не ставили во главу угла, и имеющиеся в программе ошибки могут быть использованы злоумышленниками при целевой слежке. Шифрование данных в Pidgin обеспечивает хороший уровень защиты от нецелевой слежки, т. е. от попыток шпионить за всеми подряд, но если вы полагаете, что атака может быть направлена конкретно на вас, и что злоумышленник обладает серьезными ресурсами, следует рассмотреть более глубокие средства защиты, такие как PGP-шифрование электронной почты.

Установка и настройка Pidgin с OTR

Установка в Windows

Программу Pidgin для операционной системы Windows можно скачать со страницы проекта Pidgin, расположенной по адресу **pidgin.im.** Нам понадобится специальный инсталлятор, поэтому не торопитесь скачивать дистрибутив по первой попавшейся ссылке.

1. Перейдите на страницу **tinyurl.com/ab21c4n** и щелкните мышью на ссылке **offline installer** — вы попадете на новую страницу проекта Sourceforge. Через несколько секунд в диалоговом окне появится запрос, хотите ли вы сохранить файл. Если диалоговое окно не открылось, щелкните мышью на ссылке **direct link.**
2. Нажмите кнопку Сохранить файл (Save file) — будет скачан файл с именем вида pidgin-2.10.12-offline.exe (по умолчанию большинство браузеров сохраняет загруженные файлы в папку Загрузки).
3. Перейдите на страницу **tinyurl.com/pgagfs6** и в разделе OTR plugin for Pidgin щелкните мышью на ссылке **Win32 installer for pidgin 2.x (sig)** (рис. 7.22) — будет скачан файл с именем вида pidgin-otr-4.0.**1.exe.**

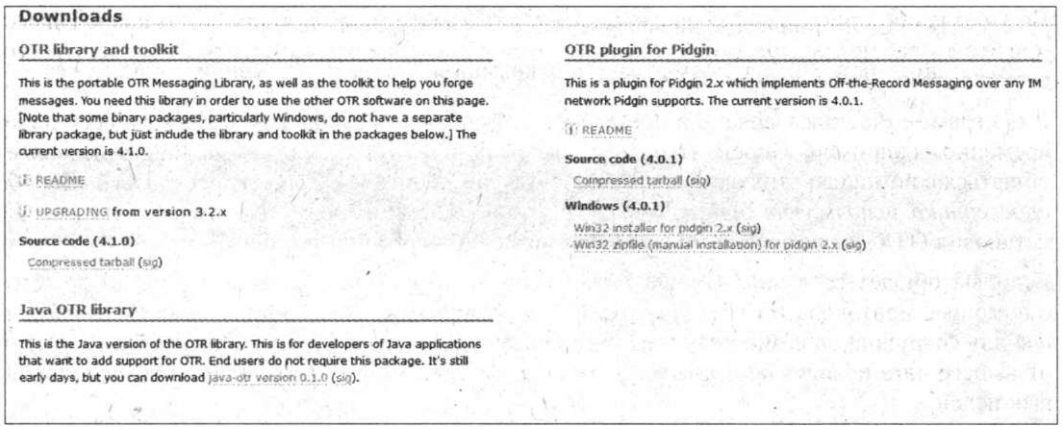


Рис. 7.22. Фрагмент страницы сайта **otr.cypherpunks.ca**

4. Запустите файл с именем вида **pidgin-2.10.12-offline.exe** и установите программу, не изменяя настроек инсталляции.
5. Повторите процесс установки для файла вида **pidgin**-otr-**4.0.1** .exe.
6. Если во время запуска файла установки появится окно с предупреждением, щелкните мышью на ссылке **Подробнее** (More info), а затем нажмите кнопку **Выполнить в любом случае** (Run anyway) (рис. 7.23).

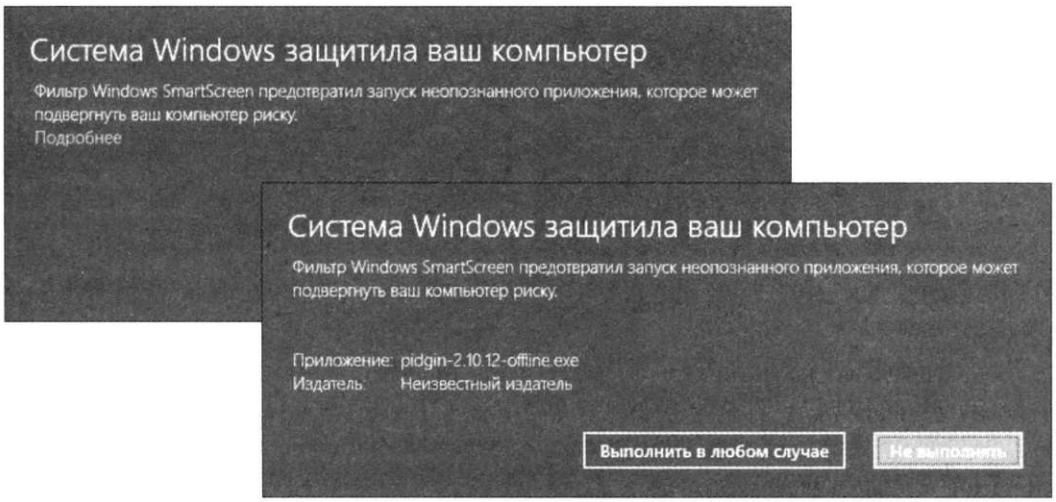


Рис. 7.23. Окно с предупреждением в операционной системе Windows

Для запуска программы в меню **Пуск** (Start) или на начальном экране щелкните мышью на ярлыке **Pidgin.**

Установка в Linux

Программа Pidgin и модуль OTR работают на всех дистрибутивах Linux аналогичным образом, но есть и некоторые различия. Основное из них связано с поиском и установкой Pidgin и OTR (в представленном далее примере использован дистрибутив Ubuntu):

1. Запустите центр приложений, нажав кнопку на боковой панели.
2. Выполните поиск по запросу `pidgin` в открывшемся окне вы увидите список результатов поиска (рис. **7.24**).

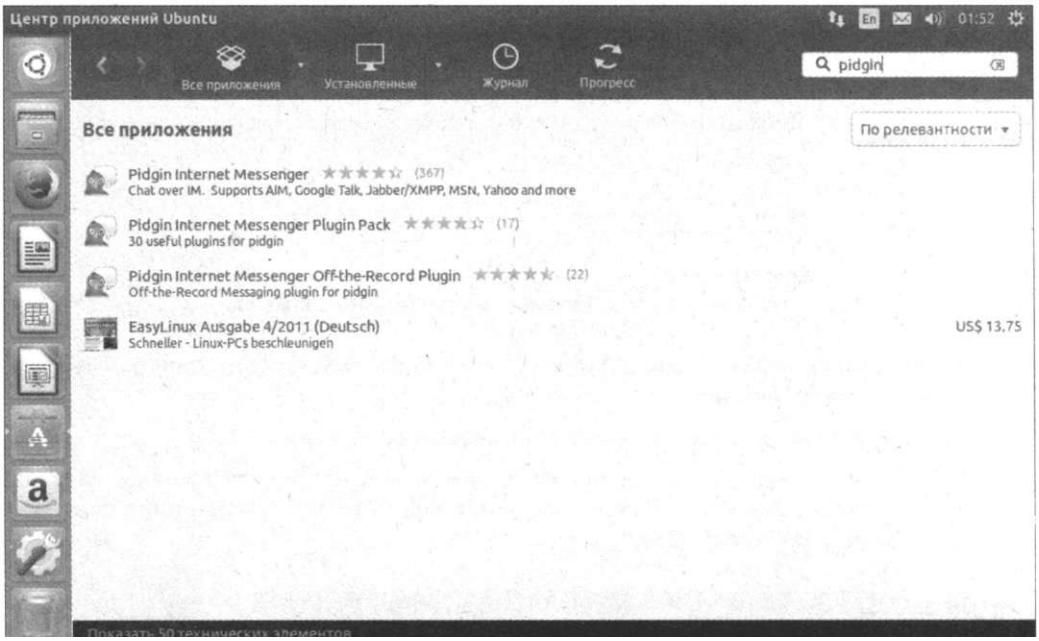


Рис. 7.24. Окно **Центр приложений Ubuntu** с результатами поиска

3. Установите приложения **Pidgin Internet Messenger** и **Pidgin Internet Messenger Off-the-Record Plugin.**
4. Введите пароль администратора для аутентификации и продолжения установки — значок мессенджера Pidgin появится на боковой панели.

Описанный далее процесс настройки Pidgin идентичен для операционных систем Windows и Linux.

Добавление учетной записи

При первом запуске Pidgin вы увидите окно приветствия с предложением добавить учетную запись. Так как учетной записи у нас еще нет, выполните следующие действия:

1. Нажмите кнопку **Добавить** (Add) — откроется диалоговое окно **Добавить учетную запись** (Add Account).

   Программа Pidgin позволяет работать со многими системами IM-сообщений, но мы остановимся здесь на системе XMPP, ранее известной как Jabber. Если вы не зарегистрированы в этой системе, то можете создать аккаунт на сайте **jabber.ru/user/register.**
2. В раскрывающемся списке **Протокол** (Protocol) выберите пункт **XMPP.**
3. **В** поле **Имя пользователя** (Username) введите свое имя пользователя **XMPP.**
4. В поле **Домен** (Domain) введите домен вашего аккаунта XMPP.

5. В поле **Пароль** (Password) введите свой пароль к аккаунту XMPP (рис. 7.25).

   Если установить флажок **Запомнить пароль** (Remember password), доступ к учетной записи упростится, но пароль будет сохранен на компьютере. Таким образом, любой пользователь, который имеет доступ к вашему компьютеру, будет иметь доступ и к вашей учетной записи Pidgin. Если такое опасение оправданно, не устанавливайте этот флажок, но тогда вводить пароль XMPP понадобится при каждом запуске программы Pidgin.

6. Нажмите кнопку **Добавить** — программа настроена и готова к работе.

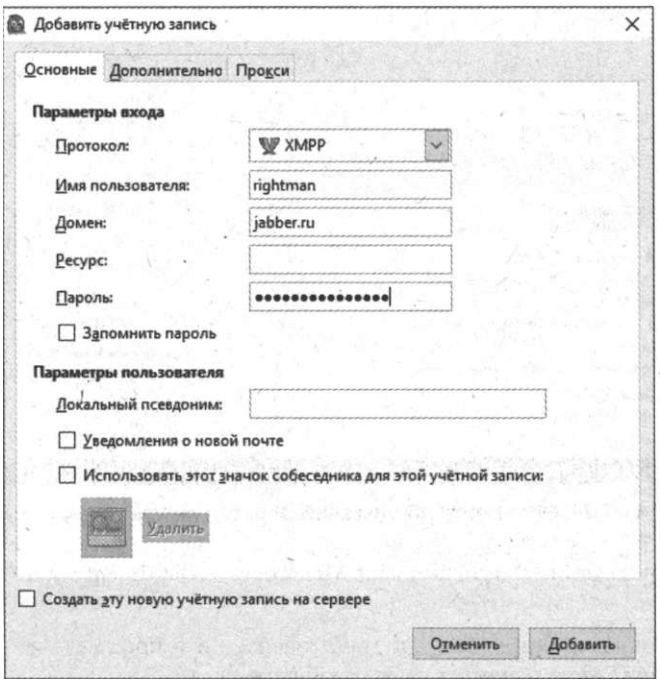


Рис. 7.25. Добавление аккаунта в программе Pidgin (Windows)

Добавление контакта

Теперь добавим собеседника:

1. Откройте меню **Собеседники** (Buddies) и выберите пункт **Добавить собеседника** (Add Buddy) — откроется одноименное окно. В нем нужно ввести имя или адрес электронной почты человека, с которым вы хотите общаться. Он необязательно должен присутствовать на том же сервере, но должен использовать тот же протокол (например, XMPP).
2. В поле **Имя пользователя собеседника** (Buddy's username) введите имя пользователя (в случае с XMPP — адрес электронной почты, связанный с аккаунтом собеседника).
3. Нажмите кнопку **Добавить** (Add).

После этого ваш собеседник получит сообщение с просьбой разрешить вам добавить его аккаунт. Когда он подтвердит и добавит ваш аккаунт, вы получите такой же запрос. Нажмите тогда кнопку **Авторизовать** (Authorize).

Настройка модуля OTR

Теперь настроим модуль OTR для безопасного общения. Для этого выполните следующие действия:

1. Выберите команду меню **Средства [Модули** (Tools | Plugins).
2. Установите флажок **Off-the-Record (OTR).**
3. Выделите пункт **Off-the-Record (OTR)** и нажмите кнопку **Настроить модуль** (Configure Plugin) (рис. 7.26, *слева*) — откроется окно с настройками модуля OTR. Обратите внимание на фразу **Ключ отсутствует** (No key present).

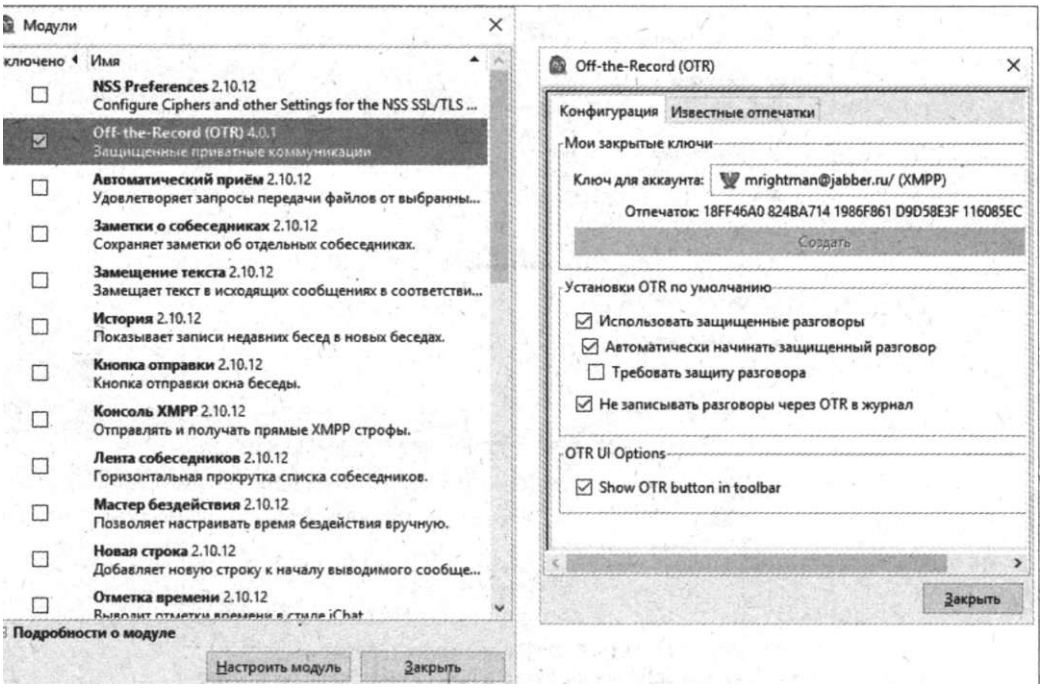


Рис. 7.26. Pidgin: список модулей *(слева)* **и настройки модуля OTR** *(справа)*

4. Нажмите кнопку Создать (Generate) — откроется небольшое окно и начнется генерация ключа.
5. По завершении процесса нажмите кнопку ОК — теперь в сответствующем поле окна представлен отпечаток ключа (рис. 7.26, *справа).*
6. Нажмите кнопку Закрыть (Close) в обоих диалоговых окнах.

Безопасное общение

Теперь вы с собеседником можете отправлять сообщения друг другу — для этого щелкните двойным щелчком на его имени в списке контактов. Однако это еще не защищенный чат — даже если вы подключились к серверу XMPP, ваши сообщения могут быть перехвачены. Обратите внимание на строку Не защищено (Not private) в правом нижнем углу окна чата.

1. Щелкните мышью на этой строке и в появившемся контекстном меню выберите пункт Начать защищенный разговор (Start private conversation) — появится сообщение, что выбранный контакт еще не аутентифицирован.
2. Снова щелкните мышью на строке, текст которой теперь гласит Не идентифицирован (Unverified).
3. В открывшемся контекстном меню выберите пункт **Аутентифицированный контакт** (Authenticate buddy) (рис. 7.27) — откроется окно с раскрывающимся списком **How would you like to authenticate your buddy?** (Каким образом вы хотите аутентифицировать контакт?). В раскрывающемся списке доступны три варианта:

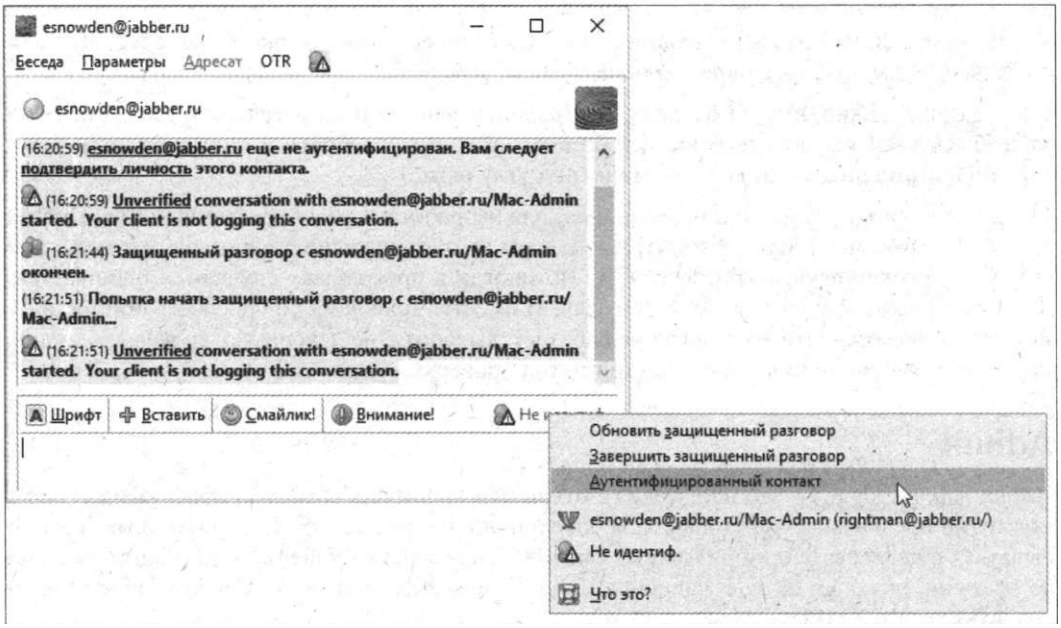


Рис. 7.27. Pidgin: аутентификация собеседника

- Shared secret (Общий секрет). В данном случае «общий секрет» — это текстовая строка, которая известна вам и вашему собеседнику. Вам следует предварительно договориться с ним о такой строке лично и никогда не передавать ее по незащищенным каналам связи, таким как электронная почта или Skype. Сейчас же вам и вашему собеседнику нужно ввести эту строку и нажать кнопку Authenticate (Аутентифицировать).

  Способ с общим секретом подходит, если вы со своим собеседником ранее договорились об общении в чате, но еще не создали отпечатки OTR на используемых вами компьютерах. Разумеется, оба собеседника должны использовать программу Pidgin;

- Manual fingerprint verification (Ручная проверка отпечатков) — способ подойдет, если на момент начала чата в программе Pidgin у вас уже есть отпечаток ключа собеседника (и наоборот). Этот способ не сработает, если собеседник сменит компьютер или создаст новый отпечаток. Если полученный ранее и отображаемый на экране отпечатки совпадают, выберите в раскрывающемся списке пункт Я проверил(а) (I have) и нажмите кнопку Authenticate (Аутентифицировать);

- **Question and answer** (Вопрос и ответ) — способ подойдет, если вы знакомы с собеседником, но не договорились об общем секрете и не успели поделиться отпечатками. Проверка основана на каком-либо знании, которым обладаете вы оба, — например, о событии или воспоминании. И в этом случае оба собеседника должны использовать программу Pidgin.

  Выбрав этот способ, введите вопрос, ответ на который известен вам обоим, и нажмите кнопку **Authenticate** (Аутентифицировать) — ваш собеседник увидит вопрос. После этого он должен ответить и также нажать кнопку **Authenticate** (Аутентифицировать). Ответ должен в точности совпадать с ожидаемым вами, и регистр также имеет значение. После аутентификации ваш собеседник получит сообщение о том, правильно ли он ответил.

4. Выберите способ аутентификации. Как только собеседник завершит процедуру аутентификации, вы получите окно с сообщением об этом.

Собеседнику нужно, в свою очередь, подтвердить ваш аккаунт, и только тогда вы оба сможете быть уверены, что пользуетесь безопасной связью. Обратите внимание на зеленую строку Защищено (Private) в правом нижнем углу окна.

Механизмы аутентификации, в принципе, должны работать между различными программами, такими как Jitsi, Pidgin, Adium, Kopete, и вы не обязаны использовать одну и ту же программу с функционалом XMPP и OTR. Но иногда в программах случаются ошибки. Так, в чат-программе Adium для OS X (см. далее) имеется проблема со способом Вопрос и ответ. Если окажется, что этот метод не работает, выясните, не использует ли ваш собеседник программу Adium, и попробуйте другой метод проверки.

Adium

Adium, как и Pidgin, — это программа с открытым кодом для обмена мгновенными сообщениями, но предназначенная только для операционной системы OS X. Она позволяет переписываться с пользователями различных протоколов обмена сообщениями в режиме реального времени, включая Google Hangouts, Yahoo! Messenger, Facebook, Windows Live Messenger, AIM, ICQ и XMPP.

В программе Adium вы можете авторизоваться, используя несколько учетных записей одновременно (например, Google Hangouts, Facebook и XMPP). Программа Adium позволяет общаться с помощью этих аккаунтов и без OTR, но защита OTR *работает, только если оба собеседника используют эту технологию.* Таким образом, даже если ваш собеседник не установил OTR, вы все равно можете общаться с ним с помощью Adium.

Если вы общаетесь в чате Google или Facebook, передаваемые данные *уже* шифруются с помощью протокола HTTPS. Но эти чаты, в отличие от чатов, защищенных OTR, *открыты* для сотрудников компании Google или Facebook, которые имеют шифровальные ключи от вашего чата и могут передать их посторонним лицам или использовать для маркетинговых целей.

Программа Adium позволяет осуществлять верификацию собеседника, чтобы подтвердить личность собеседника и избежать атаки посредника. Для этого в каждом чате можно просмотреть отпечатки ключей (в виде последовательности символов) — как вашего, так и собеседника (как уже отмечалось ранее, короткие отпечатки позволяют проверять более длинные открытые ключи). Отпечатками следует обмениваться по альтернативному каналу связи (например, через сообщения в сети Twitter или по электронной почте). Если ключи не совпадают, вы не можете быть уверены, что говорите с нужным человеком. Впрочем, на

практике пользователи часто используют несколько ключей или теряют и создают новые ключи, поэтому не удивляйтесь, если время от времени вам будет требоваться заново проверять ключи собеседников.

Несмотря на все перечисленные преимущества, важно отметить, что чат-клиент Adium довольно уязвим, т. к. при разработке этой сложной программы безопасность не ставили во главу угла, и имеющиеся в программе ошибки могут быть использованы злоумышленниками при целевой слежке. Шифрование данных в Adium обеспечивает хороший уровень защиты от нецелевой слежки, т. е. от попыток шпионить за всеми подряд, но если вы полагаете, что атака может быть направлена конкретно на вас, и что злоумышленник обладает серьезными ресурсами, следует рассмотреть более глубокие средства защиты, такие как PGP-шифрование электронной почты.

В этом разделе мы рассмотрим, как установить и настроить программу Adium и добавить в нее поддержку протокола OTR, который позволяет людям вести конфиденциальные беседы и использует сквозное шифрование.

Установка программы

1. Откройте в браузере ссылку **adium.im.**
2. Щелкните мышью на ссылке вида **Download Adium** 1.5.10.1 — на ваш компьютер (как правило, в папку **Загрузки)** будет скачан файл с расширением dmg.
3. Запустите скачанный файл двойным щелчком мыши — откроется окно мастера установки.
4. Перетащите значок Adium в правую часть окна на значок папки **Applications,** чтобы установить приложение. После установки запустите программу двойным щелчком мыши.

Если при запуске вы увидите сообщение, показанное на рис. 7.28, выполните указанные далее настройки.

1. Щелкните мышью по значку программы Adium, нажав и удерживая клавишу
2. В открывшемся контекстном меню выберите пункт **Открыть** (Open).
3. Нажмите кнопку **Открыть** (Open) в появившемся окне с предупреждением.

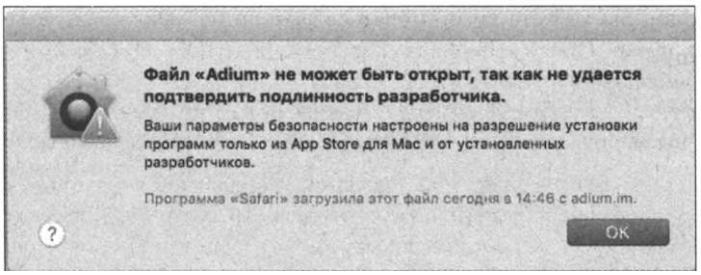


Рис. 7.28. Сообщение о невозможности запуска программы в OS X

Программа будет сохранена в списке исключений настроек безопасности, и в дальнейшем ее можно будет запускать двойным щелчком мыши, как любую проверенную программу.

Настройка учетной записи

Для разных сервисов/протоколов обмена мгновенными сообщениями настройки похожи, но не идентичны. В любом случае вам понадобятся имя пользователя и пароль. Мы остано-

вимся здесь на системе XMPP, ранее известной как Jabber. Если вы не зарегистрированы в этой системе, то можете создать аккаунт на сайте jabber.ru/user/register.

1. Чтобы настроить учетную запись, воспользуйтесь окном ассистента настройки Adium, показанным на рис. 7.29 и автоматически открывающемся при первом запуске программы.

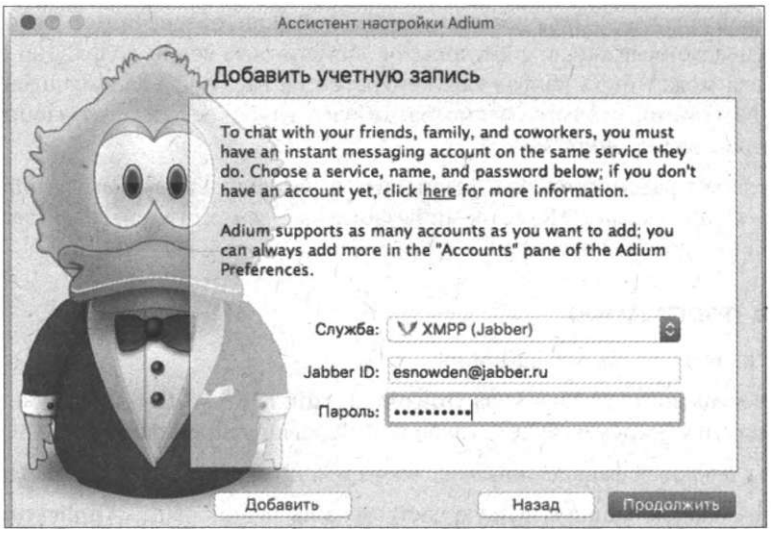


Рис. 7.29. Окно ассистента настройки Adium в OS X

Если окно ассистента настройки Adium автоматически не открылось, перейдите в меню Adium в верхней части экрана и выберите пункт Настройки (Preferences). В нижней части вкладки Учетные записи (Accounts) открывшегося окна нажмите кнопку + и выберите из меню пункт XMPP (Jabber) — вам будет предложено ввести имя пользователя и пароль.

2. В раскрывающемся списке Служба (Service) выберите пункт XMPP (Jabber).
3. В поле Jabber Ш введите свой адрес электронной почты, связанный с аккаунтом пользователя XMPP.
4. В поле Пароль (Password) введите свой пароль к аккаунту XMPP и нажмите кнопку Продолжить (Continue), а затем Готово (Finish), — программа настроена и готова к работе.

Защищенный чат

После активации в Adium одной или нескольких учетных записей можно безопасно общаться с кем-либо из зарегистрированных собеседников. При этом, чтобы вести защищенную беседу, оба собеседника должны использовать программы с поддержкой протокола OTR.

1. Выясните, кто из ваших собеседников использует протокол OTR, щелкните двойным щелчком на его имени и начните с ним беседу (рис-. 7.30).
2. Перед началом беседы обратите внимание на кнопку ^ в левом верхнем углу окна чата— нажмите эту кнопку и выберите пункт Начать шифрование чата (Initiate Encrypted OTR Chat). Кнопка сменит свой вид на — теперь ваш чат зашифрован.

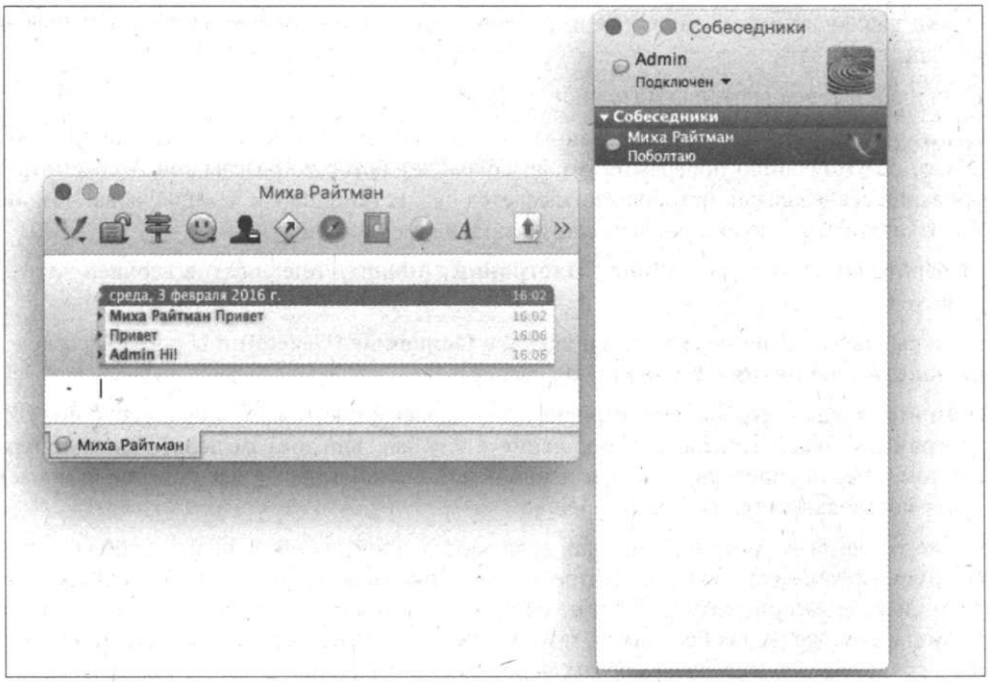


Рис. 7.30. Окно чата и списка контактов программы Adium в OS X

3. Хотя чат и зашифрован, собеседникам следует подтвердить личности друг друга (если только вы не сидите в одной комнате), — нажмите в окне чата Adium кнопку и выберите пункт Подтвердить (Verify). Вы увидите окно с ключами своим и вашего собеседника (рис. 7.31).

   Некоторые версии программы Adium поддерживают только подтверждение вручную. Тогда обоим собеседникам необходимо найти способ сверить отображенные на их экранах ключи и убедиться, что они полностью совпадают.

   Простейший способ — прочитать отпечатки ключей друг другу вслух, например, по телефону. Способ подходит, если вы способны узнать голоса друг друга. Другой вариант — передать ключи по иному каналу связи, например, по электронной почте (с PGP-шифрованием). Некоторые пользователи публикуют свои ключи на веб-сайтах, в сообщениях Twitter и даже на визитных карточках.



Рис. 7.31. Проверка ключа OTR в программе Adium

Очень важно внимательно проверить ключи на полное соответствие — все символы должны совпадать.

4. Если ключи совпадают, нажмите кнопку Да (Yes).

Итак, вы умеете открывать зашифрованный чат и подтверждать ключи собеседников. К сожалению, по умолчанию программа Adium сохраняет историю разговоров, — несмотря на шифрование сеанса связи, история записывается на жесткий диск в незашифрованном виде. Чтобы отключить эту функцию, выполните следующие действия:

1. Выберите команду меню Adium | Настройки (Adium | Preferences) в верхней части экрана.
2. В открывшемся окне перейдите на вкладку Основные (General) и сбросьте флажок Записывать сообщения в журнал (Log messages).

   Помните, однако, что вы не контролируете человека, с которым общаетесь, и его копия программы может записывать сообщения в журнал, или он сам делать снимки экрана с чатом. И если собеседник в этом плане не вполне вызывает у вас доверие, безопаснее будет пользоваться программой Telegram.

Кроме того, когда в программе Adium появляются оповещения о новых сообщениях, их содержимое может сохраняться в Центре уведомлений операционной системы OS X. Таким образом, даже если программа Adium не оставляет следов о переписке на вашем компьютере и компьютере вашего собеседника, зато операционная система может вести свои записи. В этом случае следует задуматься об отключении уведомлений.

Чтобы сделать это, запустите приложение Системные настройки (System Preferences) и в разделе Уведомления (Notification) выделите пункт Adium, после чего отключите уведомления, как показано на рис. 7.32.

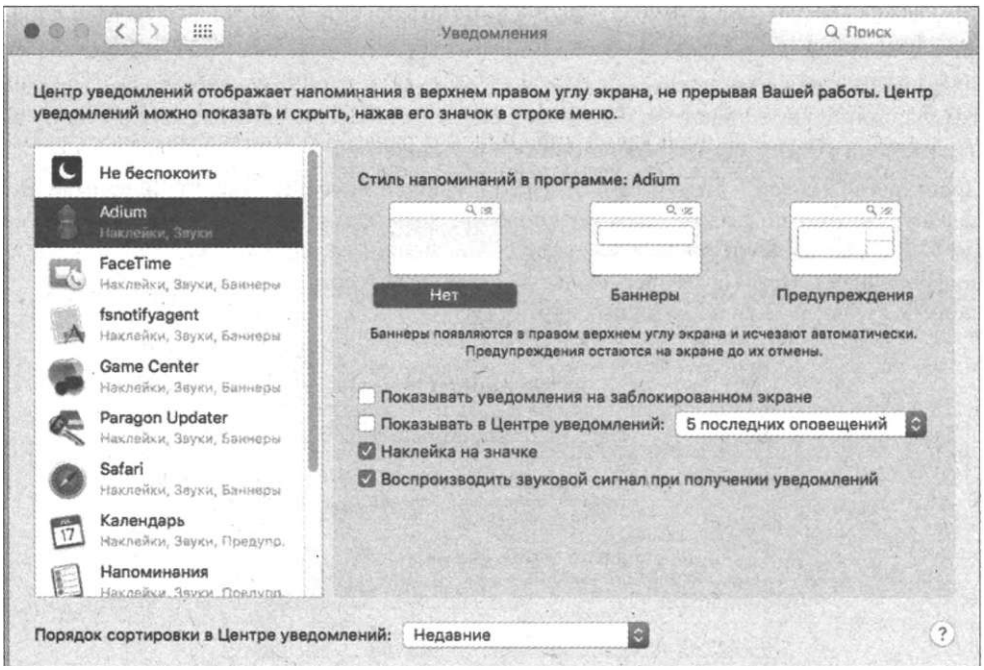


Рис. 7.32. Настройка уведомлений для программы Adium

Если же вы озабочены по поводу записей, которые были сохранены на вашем компьютере ранее, советую использовать шифрование диска — это защитит данные от посторонних.

Протокол cMix

Во время подготовки книги стало известно, что Дэвид Чом — создатель протокола Onion, на основе которого построен проект Tor (см. *главу 17),* — представил более надежную технологию анонимизации, которая лишена недостатков популярной анонимной сети в плане защиты и недостатков других аналогов смешанных сетей в плане производительности. Ею является новый криптографический протокол cMix для смешанных сетей.

Протокол cMix работает следующим образом. Приложение-мессенджер на смартфоне связывается с девятью серверами системы для формирования цепочки ключей, которыми затем обменивается с каждым из серверов. Потом, когда пользователь отправляет сообщение, данные этого сообщения шифруются путем умножения их на ключи из цепочки. Затем сообщение проходит через все девять серверов, и на каждом из них происходит отделение ключа шифрования, после чего данные сообщения умножаются на случайное число. Затем сообщение проходит по серверам по второму кругу и объединяется в группы с другими сообщениями. При этом на каждом сервере происходит перемешивание порядка сообщений в группах согласно алгоритму, известному только текущему серверу. Затем сообщения умножаются на другое случайное число, и процесс запускается в обратном порядке. Когда же сообщение в последний раз проходит по серверам, все случайные числа отделяются и заменяются ключами, уникальными по отношению к получателю сообщения.

Более высокий уровень анонимизации по сравнению с Tor обеспечивается тем, что в смешанной сети, в отличие от Tor, нельзя путем анализа трафика и времени доставки сообщений вычислить, какие узлы обмениваются сообщениями. В cMix также невозможно отследить путь сообщения, пока не будут взломаны все серверы системы (в данном случае — девять), даже если злоумышленнику удастся взломать восемь из девяти серверов.

В настоящее время все девять серверов системы находятся в облаке Amazon, что делает их беззащитными перед американскими спецслужбами. В конечной же версии системы авторы планируют запустить каждый из серверов в отдельной стране, чтобы весь путь сообщения не находился под юрисдикцией какой-либо одной страны. В ближайшее время разработчики планируют приступить к альфа-тестированию технологии.

Другие программы

Существует множество мессенджеров, как для открытого, так и безопасного общения. В табл. 7.3 приведены некоторые такие программы.

Таблица 7.3. *Мессенджеры для безопасного общения*

Название	Адрес	Платформа
Confide	getconfide.com	Windows, OS X, iOS (в т. ч. и Apple Watch)
Cryptocat	crypto.cat	Windows, OS X, iOS
Heml.is	tinyurl.com/on72kef	В разработке
SafeUM	safeum.com/ru/	Windows, OS X, Linux, iOS, Android, Blackberry
Sicher	shape.ag/en/	iOS, Android, Windows Phone
Silent Phone	tinyurl.com/nuopdiy	iOS, Android

Таблица 7.3 *(окончание)*

Название	Адрес	Платформа
SJ IM	**tinyurl.com/qx4edc4**	Windows, OS X, iOS, Android
TigerText	**tigertext.com**	Windows, Web, iOS, Android
Tor Messenger	**tinyurl.com/zfcl3lr**	Windows, OS X, Linux
VIPole	**vipole.com/ru/**	Windows, OS X, Linux, iOS, Android, Windows Phone
Wickr	**wickr.com**	Windows, OS X, Linux, iOS, Android

В июле 2015 года исследователи из Массачусетского технологического института (МТИ) продемонстрировали несовершенство анонимной сети Tor. Они определили местоположение анонимного сервера и источник отправленных конкретному пользователю Tor данных путем анализа зашифрованного трафика, проходящего всего лишь через один узел анонимной сети.

В конце 2015 года появилось сообщение, что ученые из МТИ создали самый надежный из существующих аналогов анонимный мессенджер. Система, более надежная, чем сеть Tor, и получившая название Vuvuzela, всячески запутывает следы и не позволяет злоумышленнику определить, какое сообщение какому адресату предназначено, даже если он взломает более 50% серверов.

Принцип работы системы Vuvuzela, как говорится в заявлении, лишен недостатка, позволившего исследователям МТИ деанонимизировать пользователей Tor: отправитель оставляет сообщение для адресата по определенному адресу в памяти интернет-сервера, а адресат затем забирает это сообщение. Помимо этого, клиент на компьютере пользователя регулярно отправляет на сервер сообщения вне зависимости от того, общается ли пользователь с кем-либо.

Каждое пересылаемое в системе сообщение имеет три уровня шифрования. Первый сервер, перед тем как отправить сообщение на следующий, снимает первый уровень шифрования. Второй сервер — второй уровень и т. д. На каждом сервере порядок адресатов перемешивается. То есть, к примеру, если на первый сервер поступили сообщения сначала для Алисы, потом для Бориса, а затем для Максима, то на второй сервер они будут отправлены в ином порядке — например, сначала для Максима, потом для Бориса, а затем Алисы. И только на третьем сервере становится известно, какие сообщения к какому адресу памяти прикреплены. Но даже если злоумышленник взломает этот последний сервер, он не сможет понять, является ли он последним. А чтобы защитить пользователей от попыток определить коммуникационную связь между двумя пользователями, разработчики сделали так, чтобы каждый сервер в момент передачи полученных сообщений, отправлял похожие сообщения по другим различным адресам.

На момент подготовки книги этот мессенджер еще находился в разработке. Следить за ходом разработки можно на странице проекта по адресу tinyurl.com/qb91any.

ЧАСТЬ II

Защищенные способы передачи данных

Глава 8.	**Использование прокси-серверов**
Глава 9.	**Виртуальные частные сети**
Глава 10.	**Подмена IP-адресов DNS-серверов**
Глава 11.	**Использование протокола IPV6**
Глава 12.	**Дополнительные способы альтернативной передачи данных**

Часто бывает, особенно при подключении к Интернету через локальную сеть, что некоторые веб-сайты не отображают свой контент должным образом. К примеру, выводится предупреждение, что IP-адрес пользователя не соответствует тем или иным требованиям, и страница попросту не отображается, или происходит перенаправление на какой-либо другой сайт, — например, на главную страницу портала компании. Так, во многих странах отсутствует возможность просмотра мультимедийного контента с сайтов Hulu.com и Pandora.com. Главы *второй части* книги направлены на решение этой проблемы.

ГЛАВА 8

Использование прокси-серверов

Использование альтернативных адресов веб-ресурсов

Использование анонимайзеров

Настройка браузеров для работы через прокси-серверы

Настройка мобильных устройств для работы через прокси-серверы

Использование цепочек прокси

Использование файлов автоконфигурации прокси-сервера

Использование файлов автоконфигурации прокси-сервера на мобильных устройствах

Из этой главы вы узнаете, как во Всемирной паутине посетить узлы с ограничением доступа к контенту — например, американские сайты Hulu.com и Pandora.com, — с IP-адресов за пределами США.

Наиболее часто встречаются следующие варианты ограничений:

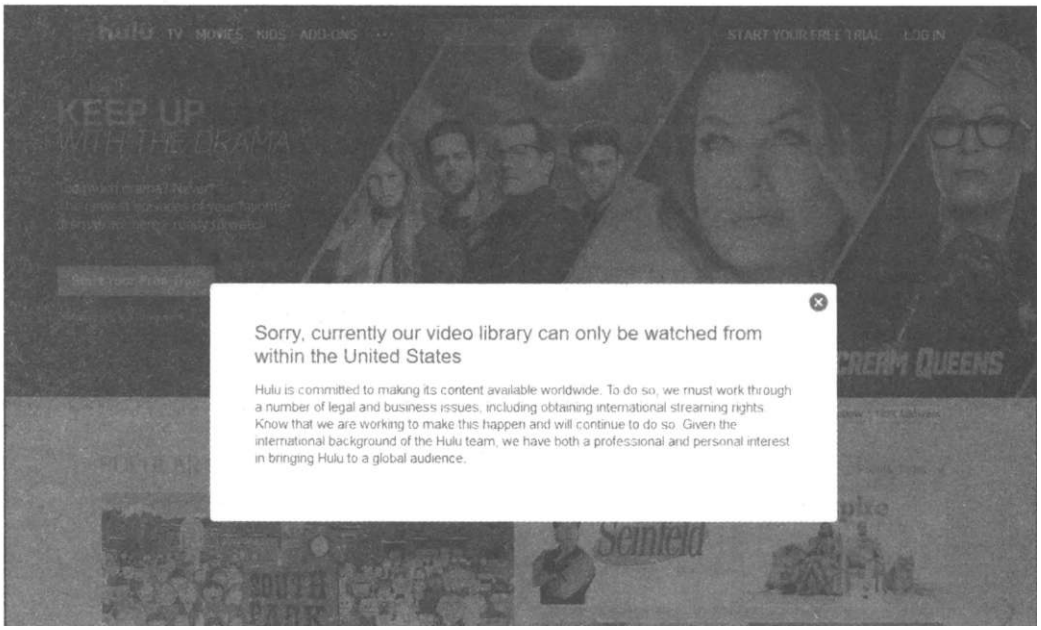
- доступ к тому или иному сайту страны не разрешается пользователям из других стран (местонахождение посетителя обычно определяется по IP-адресу его компьютера). Отличным примером (можете попробовать прямо сейчас) является сайт Hulu.com. Доступ к этому ресурсу разрешен только пользователям с IP-адресами, относящимися к США, а остальным (в том числе и российским) — закрыт. Точнее, посетить-то его можно, а вот просмотреть видеоролики — нет (рис. 8.1);

  ЗАПРЕТ ПРОСМОТРА ВИДЕОКОНТЕНТА

  Как можно видеть на рис. 8.1, посетитель, попытавшийся получить доступ к веб-сайту Ни1и, получил сообщение, что содержимое сайта может просматриваться только пользователями, находящимися в США. Такое ограничение обходится любым из описанных далее способов, самые простые из которых — использование анонимайзера, т. е. специализированного прокси-сервера, или специальных утилит.

- в ряде стран ограничивается доступ к определенным сайтам внутри страны (например, к оппозиционным в Иране, к Википедии в Китае и т. п.[1]) или вне ее (например, к УоиТиЬе в Пакистане). Определяется такая блокировка, как правило, настройками национального шлюза;

[1] **Интересную статью на эту тему можно найти по ссылке: tinyurl.com/6ea8edr.**



Рио. 8.1. Доступ к ресурсу заблокирован за пределами США

- из сети организации ограничивается доступ к конкретным веб-сайтам. Чаще всего компании посредством настройки прокси-сервера (представьте его как шлюз между локальной сетью компьютеров офисных работников и внешней Всемирной паутиной) блокируют доступ своих сотрудников к сайтам социальных сетей, развлекательным и XXX-ресурсам. К примеру, в одной из известных мне крупных компаний таким образом ограничивается доступ к сервису УоиТиЬе и некоторым другим;
- самой сложной ситуацией является та, когда прокси-сервер организации блокирует все веб-ресурсы, кроме определенных, — например, корпоративного сайта. Ситуация сложная, но не безвыходная.

Рассмотрим способы решения проблемы.

Использование альтернативных адресов веб-ресурсов

Первый и самый простой способ решения проблемы посещения узлов, недоступных по каким-либо причинам, заключается в указании в адресной строке браузера не адреса сайта как такового, а его альтернативного адреса или просто IP-адреса. К примеру, чтобы попасть на сайт социальной сети Facebook, можно ввести в адресной строке как сам адрес `facebook.com`, так и его IP-адрес `173.252.74.22`, — в любом случае вы попадете на сайт социальной сети Facebook (рис. 8.2).

В табл. 8.1 приведены IP-адреса основных запрещаемых в офисах веб-сайтов. Стоит отметить, что с прошествием времени некоторые альтернативные IP-адреса также могут быть заблокированы.

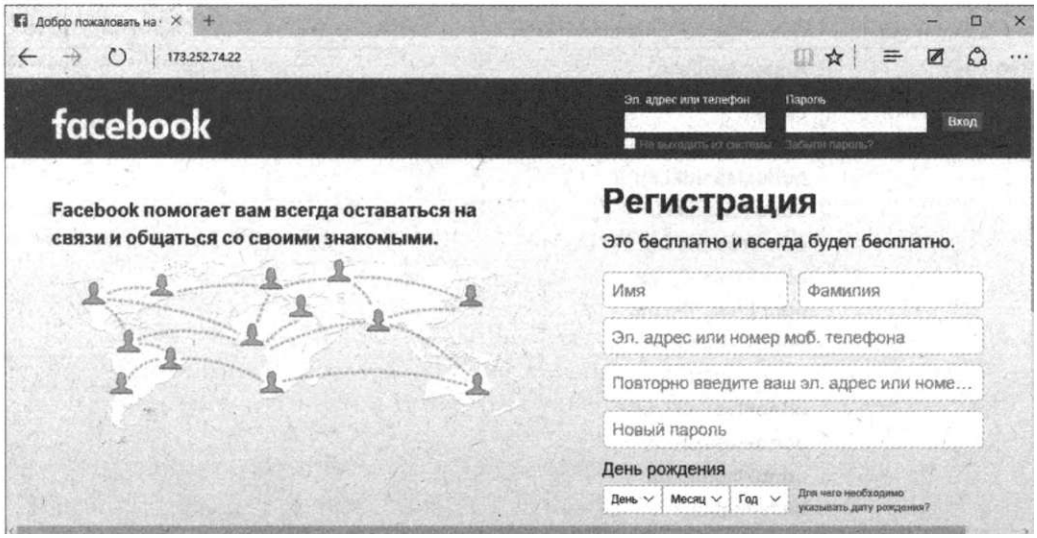


Рис. 8.2. Социальная сеть Facebook (173.252.74.22)

Таблица 8.1. *Альтернативные адреса веб-сайтов некоторых социальных сетей*

Веб-сайт	Адрес (адреса)[1]	IP-адреса	
Facebook	facebook.com	173.252.74.22	31.13.65.1
Google+ (а также и поисковая система Google)	plus.google.com t.co/CxmSYh5	173.194.32.128 173.194.32.129 173.194.32.130 173.194.32.131 173.194.32.132 173.194.32.133	173.194.32.134 173.194.32.135 173.194.32.136 173.194.32.137 173.194.32.142 173.194.71.199
MySpace	myspace.com	63.135.90.70	
YouTube	youtube.com youtube.ru youtubed.com yputube.com Youtu.be youtube.tv	173.194.32.128 173.194.32.129 173.194.32.130 173.194.32.131 173.194.32.132 173.194.32.133	173.194.32.134 173.194.32.135 173.194.-32.136 173.194.32.137 173.194.32.142 173.194.71.199
ВКонтакте	vk.com vkontakte.com bit.ly/cQnllY	87.240.131.97 87.240.131.99	87.240.143.242
Мой мир	my.mail.ru	94.100.180.25	94.100.180.26

[1] После верхнего — основного — адреса в таблице приводятся альтернативные адреса, при вводе которых происходит перенаправление на соответствующий сайт.

Таблица 8.1 *(окончание)*

Веб-сайт	Адрес (адреса)	IP-адреса	
Одноклассники.ги	**ok.ru** **odnoklassniki.ru** **odnoklassniki.eu** **odnoklasniki.ru** **odnoklassniki.tj** **odnoklassniki.kz** **odnoklassniki.md** **odnoklassniki.ua** **odnoklasniki.kz** **odnoklassniki.am** **odnokiassniki.lv** **odnoklasniki.ua** **bit.ly/4tq63j**	217.20.147.94 217.20.155.58	217.20.156.159

Вы также можете отредактировать файл hosts, расположенный в операционной системе Windows в каталоге %SYSTEMROOT%\System32\drivers\etcl. Надо только иметь в виду, что, как правило, этот файл нельзя редактировать в его исходном расположении. Его надо скопировать, к примеру, на рабочий стол, отредактировать, а затем заменить новой версией файла исходную в указанном каталоге. Альтернативные адреса сайтов заносятся в файл hosts следующим образом:

```
173.252.74.22  facebook.com
31.13.65.1  www.facebook.com
и т.п.
```

В случае блокировки доступа к тому или иному ресурсу с конкретного (вашего служебного) компьютера, в файле hosts могут присутствовать внесенные туда администратором локальной сети посторонние записи типа:

```
62.113.243.114  vk.com
62.113.243.114  odnoklassniki.ru
```

Подобные строки, в которых встречается название желаемого ресурса, вы можете аккуратно удалить. Однако, если вы точно не знаете, за что отвечает та или иная строка, вносить изменения в файл hosts не рекомендуется. И в любом случае перед изменением желательно сохранить резервную копию его исходной версии.

Разумеется, ваш провайдер или администратор локальной сети может заблокировать доступ и к другим социальным сетям (и прочим сайтам), которые вы привыкли посещать, и все их в книге не приведешь. Поэтому узнать IP-адрес определенного сайта можно так:

1. Откройте окно командной строки любым способом — например, нажав сочетание клавиш <Win>+<R>, указав значение **cmd** в поле ввода и нажав клавишу <Enter>.
2. В окне командной строки введите команду **nsiookup** и адрес искомого сайта— например:

   ```
   nslookup linkedin.com
   ```

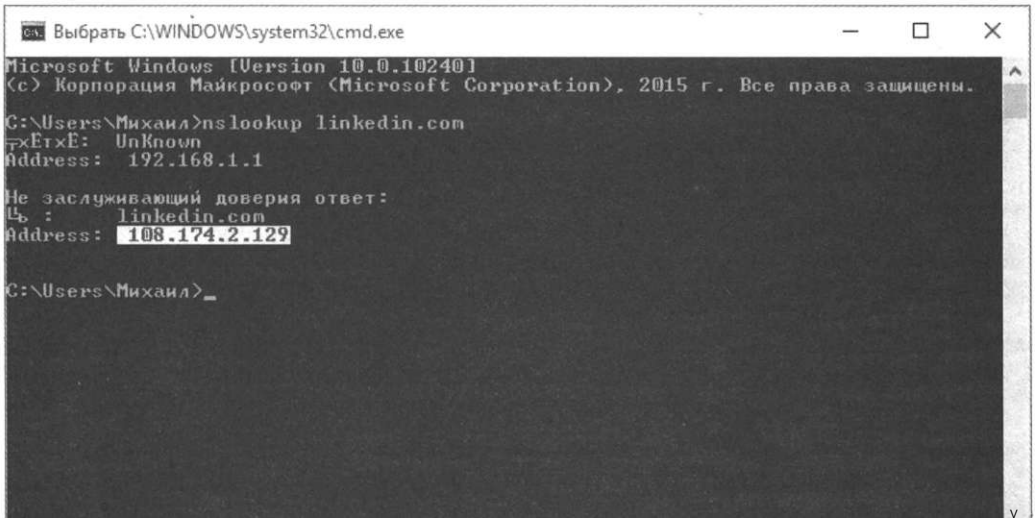


Рис. 8.3. Просмотр IP-адреса сайта LinkedIn

3. Нажмите клавишу <Enter> — вы увидите список посещенных узлов, их IP-адреса и некоторую другую информацию (рйс. 8.3).

Вы также можете узнать IP-адреса *посещенных* сайтов, просмотрев DNS-кэш на своем компьютере. Повторюсь — так вы сможете узнать адреса только тех узлов, которые недавно посещали на *том* компьютере, где выполняете команду. Итак, выполните следующие действия:

1. Откройте окно командной строки любым способом — например, нажав сочетание клавиш <Win>+<R>, указав значение cmd в поле ввода и нажав клавишу <Enter>.
2. Введите следующую команду:

```
ipeonfig /displaydns | more
```

3. Нажмите клавишу <Enter> — вы увидите список посещенных узлов, их IP-адреса и некоторую другую информацию (рис. 8.4). Прокручивать список можно, нажимая клавишу <Enter> (построчно) или <Пробел> (постранично).

На рис. 8.4 выделен IP-адрес сайта sailplay.ru, также доступного по IP-адресу 54.246.106.192. Чтобы скопировать IP-адрес из этого окна в буфер обмена, следует выделить его мышью и нажать клавишу <Enter>.

Кстати, можно вывести весь такой список в текстовый документ (в DOS-кодировке), выполнив команду:

```
ipeonfig /displaydns > "путь_к_текстовому_файлу\файл"
```

например:

```
ipeonfig /displaydns > "D:\sites.txt"
```

Созданный текстовый документ (файл sites.txt в нашем случае) можно открыть в любом редакторе, поддерживающем кодировку OEM 866, — например, в Notepad++.

Стоит отметить, что не все обнаруженные IP-адреса приведут на желаемый сайт, да и метод использования альтернативных адресов работает не на всех компьютерах (точнее, зависит

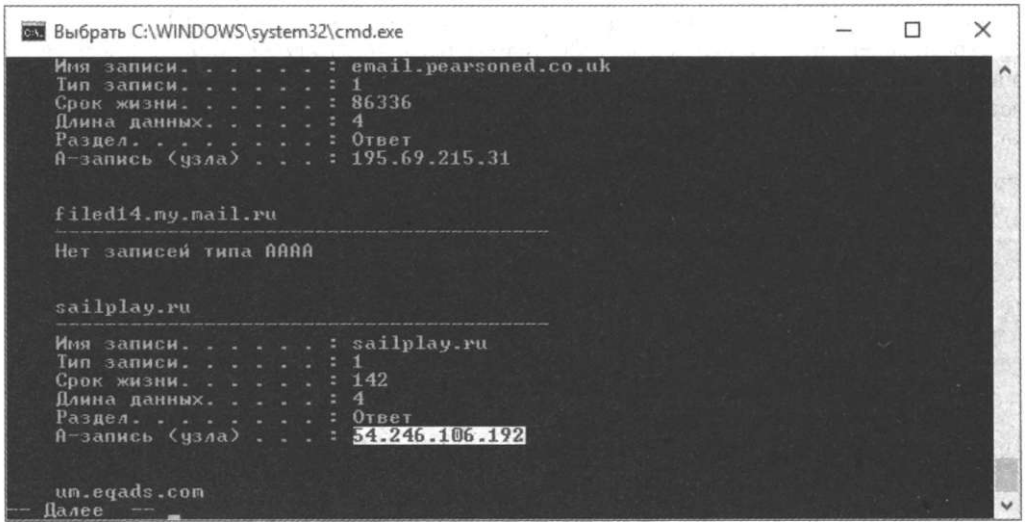


Рис. 8.4. Просмотр содержимого кэша РЫб

от настроек прокси-сервера в вашей организации). Если это так, попробуйте воспользоваться способом посещения ресурса через так называемый *анонимайзер* (см. далее).

Во Всемирной паутине также существуют сервисы, рекламирующие обход заблокированных сайтов. Суть их работы — вместо официального адреса социальной сети переводить вас на генерируемый, где вам предложат ввести данные своей учетной записи. Доверять таким сайтам не стоит. Скорее всего, генерируемые на этих веб-сайтах ссылки — не что иное, как прямой путь на *фишинговые* сайты, создаваемые с целью завладения вашими данными: логином, паролем и прочими сведениями (подробно про фишинг рассказано в *главе 3,* там же приведен скриншот поддельного веб-сайта, существовавшего на момент подготовки книги). Зачем это кому-то может быть нужно? Хотя бы для продажи рекламодателям — по содержимому ваших диалогов и учетных записей вполне можно составить ваш портрет: кто вы и что готовы приобрести. Впоследствии спам, приходящий на ваш электронный, да и почтовый ящики, будет рекламировать именно то, что вас интересовало в интернет-общении.

К тому же, представьте интерес, например, магазина электроники — «просканировав» предпочтения десятков и сотен тысяч пользователей социальных сетей, можно сформировать мнение, какие товары в первую очередь пользуются популярностью, на покупку каких товаров стоит привлечь скидкой и т. п.

Так что, будьте осторожны при посещении различных веб-сайтов, предполагающих ввод логина и пароля для активации аккаунта. Обязательно убедитесь, что содержимое в адресной строке браузера соответствует реальному адресу выбранного вами веб-сайта: odnoklassniki.ru, а не чему-нибудь типа odnaklassniki.ru, odnOklassniki.ru или вообще rtl-odnoshkolniki.ru.

Использование анонимайзеров

Этот способ может не подойти для получения доступа к некоторым ресурсам с высоким трафиком — таким как сервисы видеохостинга. Дело в том, что анонимайзеры далеко не всегда могут похвастаться высокой скоростью — вы попросту не сможете смотреть видео, или же сервис будет сильно тормозить его демонстрацию. Тем не менее, способ прост и

удобен для обхода ограничений доступа, к примеру, к социальным сетям из офиса, где прокси-сервер содержит «черный» список интернет-адресов (URL) веб-сайтов, — посещая сайт социальной сети, вы указываете адрес не ее, а анонимайзера. Кроме того, так можно попасть на какой-либо сайт, где и ваш IP-адрес по каким бы то ни было причинам занесен в «черный» список.

Нередки и ситуации, когда все компьютеры в организации работают через прокси-сервер — шлюз, имеющий определенный адрес. То есть, к примеру, для веб-сайта DepositFiles ваш компьютер определяется с IP-адресом (например) 123.123.123.123, компьютер коллеги за соседним столом — тоже с адресом 123.123.123.123 и т. д. Вы все определились с одним и тем же IP-адресом на сайте DepositFiles, а поскольку с одного IP-адреса может одновременно скачиваться только один файл, то... Правильно! Доступ получил и файл скачивает более проворный коллега, который успел сделать это первым, и теперь он злорадно улыбается, а вы ждете.

Вот во всех этих случаях может помочь анонимайзер, который попросту подменивает ваш IP-адрес (для того же сайта DepositFiles) и ваш пункт назначения (это уже для администратора вашей компании). Тут стоит оговориться, что многие файлообменники просекут вашу попытку зайти к ним через анонимайзер и файл скачать не дадут, но попытка — не пытка.

Итак, чтобы воспользоваться анонимайзером, требуется лишь перейти на веб-сайт одного из таких сервисов, содержащего поле ввода адреса и кнопку перехода на введенный интернет-адрес (URL).

Чтобы проверить, как это работает, воспользуемся сервисом определения IP-адреса пользователя — **whatismyipaddress.com** — и выбранным наугад анонимайзером.

Прежде всего, уточним свое «стандартное» состояние — без использования каких бы то ни было специальных средств (рис. 8.5). Как можно видеть из содержимого страницы, определен IP-адрес и местонахождение пользователя: Москва, Российская Федерация, а также указано и название его компании-провайдера (ISP).

> ***ОПРЕДЕЛЕНИЕ СОБСТВЕННОГО IP-АДРЕСА***
>
> Определить собственный IP-адрес вы можете также, например, на веб-сайтах **2ip.ru, ipgeobase.ru, myip.ru** или **whoer.net/ext.**

Теперь я попробую воспользоваться анонимным прокси-сервером, чтобы запрос от моего компьютера к серверу **whatismyipaddress.com** проложил свой путь через него. Таких прокси-серверов во Всемирной паутине тысячи, и располагаться они могут в самых различных государствах.

> ***СКРЫТЬСЯ НЕ УДАСТСЯ...***
>
> Вам также следует знать, что информация о том, что вы обращаетесь к прокси-серверу, тайной не является. Это я к тому, что по запросу шефа администратор проанализирует *логи* (log-файлы, или журналы, в которые заносится вся информация о том, кто, куда, где и как «путешествовал» с компьютера) и выяснит, что вы часами зависали на некоем «анонимайзер.ком». Был ли это сайт знакомств, морской бой или форум «Практика Буду» никто разбираться не станет, а вот доказывать, что вы не верблюд, а в худшем случае лишиться премии, получить выговор или написать заявление об увольнении, — придется.

Повторюсь, веб-сайт анонимайзера содержит строку, куда вводится адрес заблокированного узла, после чего он открывает соответствующую страницу. Множество ссылок на подобные сервисы можно получить, указав в строке поисковой машины запрос вида **proxy, прокси** или **анонимайзер.** На момент подготовки книги вполне нормально функционировали сайты **proxfree.com, proxer.ru, hideme.ru, anonymouse.org, g-tunnel.com, online-anonymizer.com**

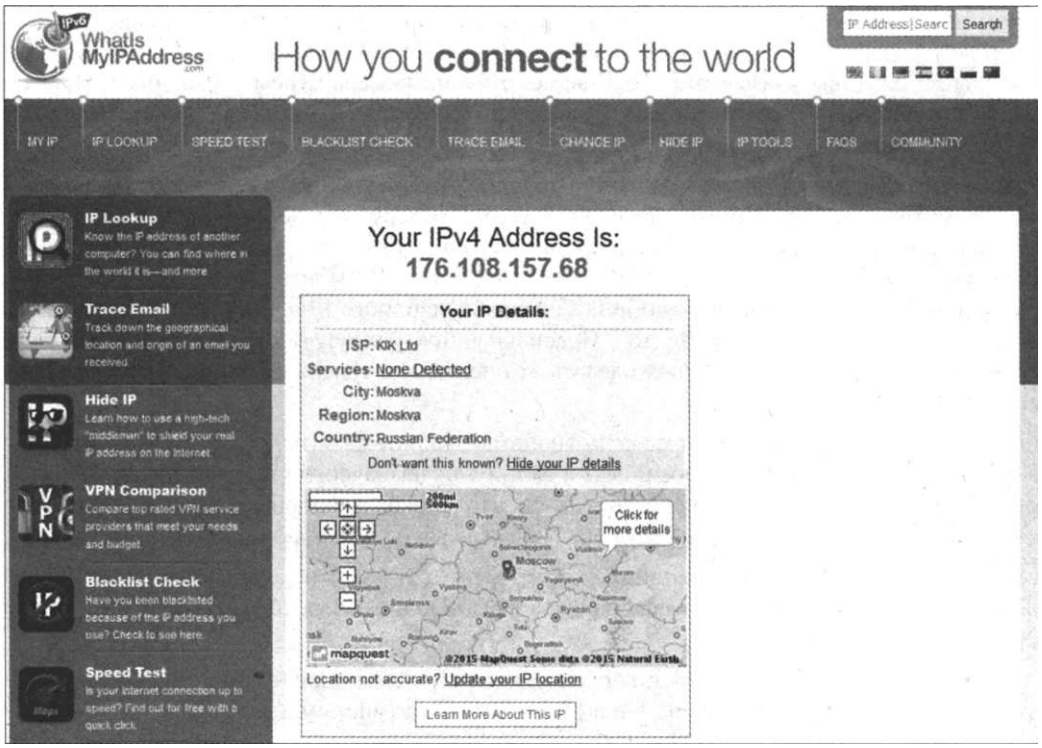


Рис. 8.5. Сервис whatismyipaddress.com определил местонахождение пользователя

и многие другие подобные сервисы. Кстати, в русском сегменте Всемирной паутины есть отличный, постоянно обновляющийся веб-сайт с форумом, содержащий информацию о свежих прокси-серверах, различных полезных программах и т. п. Его адрес: **freeproxy.ru/ru/index.htm.**

АДРЕСА ПРОКСИ-СЕРВЕРОВ

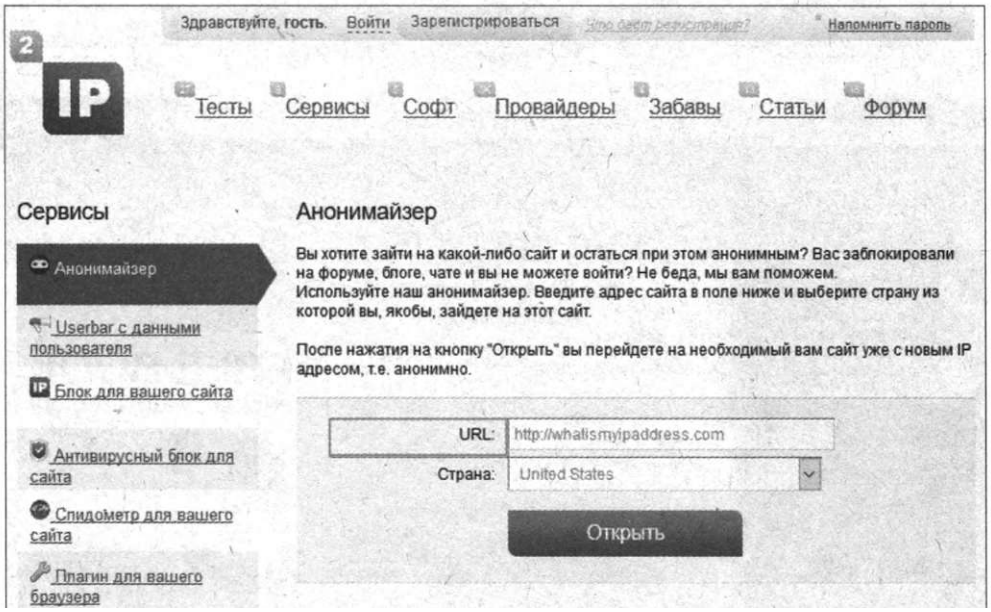
Вы можете просмотреть свежие списки адресов прокси-серверов на веб-сайте по ссылке tinyurl.com/q7vjb86.

Существуют как бесплатные, так и платные прокси-серверы. Недостаток бесплатных в том, что скорость их работы часто оставляет желать лучшего. Минус платных — приходится тратить деньги, причем от сбоев связи вы все равно не застрахованы. Иной раз вам придется перебрать не один десяток прокси, чтобы получить приемлемое качество соединения.

ОТСУТСТВИЕ ДОСТУПА к ПРОКСИ-СЕРВЕРАМ

Разумеется, доступ к прокси-серверам тоже может блокироваться системными администраторами, поэтому периодически возникает потребность в смене прокси. Думаю, это не проблема, поскольку их количество исчисляется десятками тысяч, а заблокировать все просто невозможно — кроме случаев, когда доступ разрешен лишь к определенным сайтам, а ко всем остальным автоматически запрещен.

Итак, я воспользуюсь русским анонимайзером 2IP, расположенным по адресу **https://2ip.ru/anonim/** (рис. **8.6).** Удобство этого веб-сайта в том, что, указав желаемый адрес (в моем случае: **http://whatismyipaddress.com),** вы также можете выбрать прокси подходящей страны в раскрывающемся списке ниже.



Рис, 8,6. Веб-сайт 2IP: услуга анонимайзера

Попробую прокси-сервер, расположенный, к примеру, в США, — выбираю в раскрывающемся списке пункт **United States** и нажимаю кнопку **Открыть.**

Через несколько секунд ожидания (не все прокси скоростные, тем более бесплатные) видим результат на сервисе **whatismyipaddress.com** (рис. 8.7). Комментарии тут, как говорится, излишни...

Как уже отмечалось, сам факт вашего обращения к прокси-серверу тайной для администратора не является, так же как и все остальные данные обращения (в том числе, какой заблокированный ресурс вы хотели просмотреть, и его содержимое), потому что обмен информацией происходит по незашифрованному каналу связи. То же касается и другого способа использования прокси, отличие которого от анонимайзеров заключается в необходимости указывать IP-адрес и порт в свойствах браузера (или любой другой программы, имеющей возможность работать через прокси-сервер), чтобы попадать на заблокированные веб-сайты напрямую (см. далее *разд. «Настройка браузеров для работы через прокси-серверы»).*

Для повышения уровня безопасности можно воспользоваться защищенным протоколом связи HTTPS (буква S здесь означает *Secure,* безопасный). При этом прокси-серверу передается только лишь команда подключения к определенному узлу, а прокси-сервер, в свою очередь, организует в обе стороны пассивную передачу зашифрованного трафика. В таком случае определить, что вы подключились к прокси-серверу, можно, но узнать, какой веб-сайт вы решили «нелегально» посетить, — затруднительно. Узлы, обеспечивающие подключение по протоколу HTTPS, можно определить по наличию префикса HTTPS в адресе — например, **https://2ip.ru/anonim/.**

Важно также выяснить, действительно ли предлагаемый прокси-сервер является анонимным и позволяет скрыть ваше реальное месторасположение. Для этого вы можете обратиться к веб-сайтам определения вашего IP-адреса (некоторые из них указаны ранее) или же просмотреть сведения о себе с помощью специализированных сайтов типа **tinyurl.com/ybszty.** После настройки подключения к прокси-серверу посетите один из подобных веб-



Рис. 8.7. IP-адрес изменен на американский

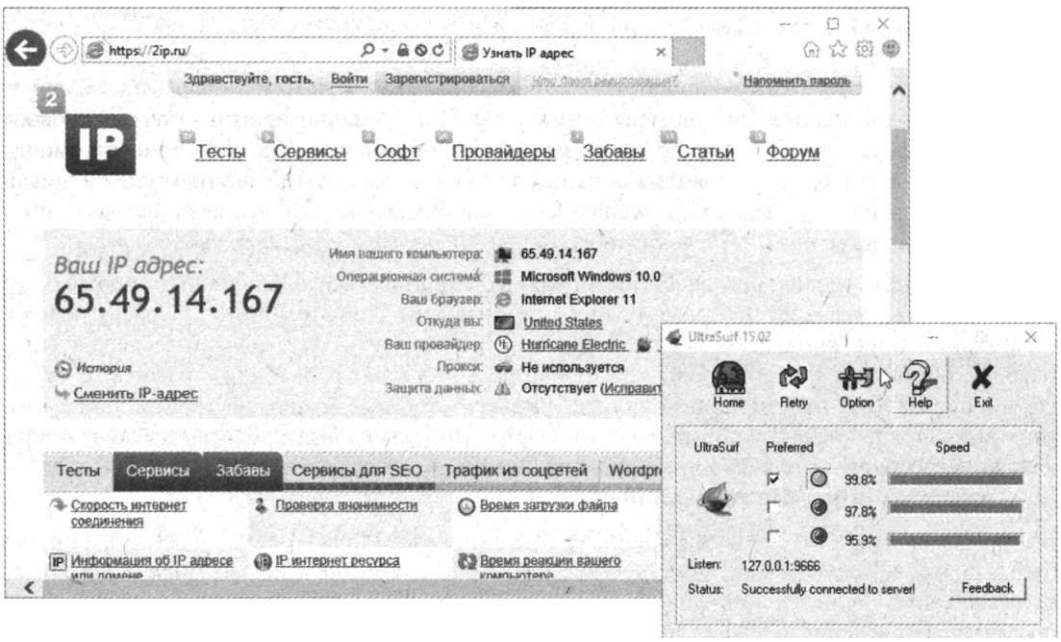


Рис. 8.8. Окна браузера Internet Explorer и программы UltraSurf

сайтов и посмотрите, насколько тщательно скрывается информация о вашем местоположении, IP-адресе, браузере и другие сведения.

Кроме того, можно попробовать в деле и такие приложения, как UltraSurf **(ultrasurf.us),** — оно обеспечивает и анонимность, и американский IP-адрес, поэтому с его помощью также можно получить доступ к содержимому многих веб-сайтов, просмотр которых в вашей стране по каким-либо причинам запрещен.

После скачивания и распаковки этого приложения его сразу можно запустить (без необходимости установки), после чего откроется окно программы с настройками и окно браузера Internet Explorer с доступом через прокси-сервер (рис. 8.8). Для доступа к окну настроек UltraSurf можно использовать большую кнопку в виде замка, располагающуюся в правом нижнем углу экрана браузера, однако, как правило, никаких дополнительных настроек обычно производить не требуется.

Настройка браузеров для работы через прокси-серверы

Альтернативой использованию анонимайзеров является настройка браузера таким образом, чтобы подключение осуществлялось через сайт прокси-сервера. Прежде всего, вам понадобится актуальный список прокси-серверов, который вы без труда найдете во Всемирной паутине, — например, здесь: **tinyurl.com/q6edfr7.** Далее мы рассмотрим, как настроить подключение через прокси-сервер в различных браузерах.

Браузер Internet Explorer

Для начала настроим самый распространенный браузер — Internet Explorer. Выполните следующие действия:

1. В правом верхнем углу окна программы Internet Explorer нажмите кнопку и выберите команду меню **Свойства браузера** (Browser Options). Можно пройти и через основное меню — нажмите клавишу <Alt>, а затем выберите в появившейся строке меню команду **Сервис | Свойства браузера** (Tools [Browser Options) — откроется одноименное диалоговое окно.
2. Перейдите на вкладку **Подключения** (Connections) — содержимое диалогового окна **Свойства браузера** (Browser Options) изменится (рис. 8.9, *слева).*
3. Нажмите кнопку **Настройка сети** (LAN Settings) — откроется диалоговое окно **Настройка параметров локальной сети** (Local Area Network (LAN) Settings) (см. рис. 8.9, *справа).*
4. Чтобы назначить подключение через прокси-сервер, установите флажок **Использовать прокси-сервер для локальных подключений** (Use a proxy server for your LAN), а затем укажите в поле ввода **Адрес** (Address) IP-адрес прокси-сервера (HTTP или HTTPS) вида 124.205.71.238, а в поле ввода **Порт** (Port) — порт подключения, например, 8909.

ОГРОМНЫЙ СПИСОК ПРОКСИ-СЕРВЕРОВ

Список прокси-серверов доступен на сайте spys.ru/free-proxy-list/. Имеется возможность отфильтровать прокси определенной страны, а также анонимные прокси и прокси с поддержкой SSL.

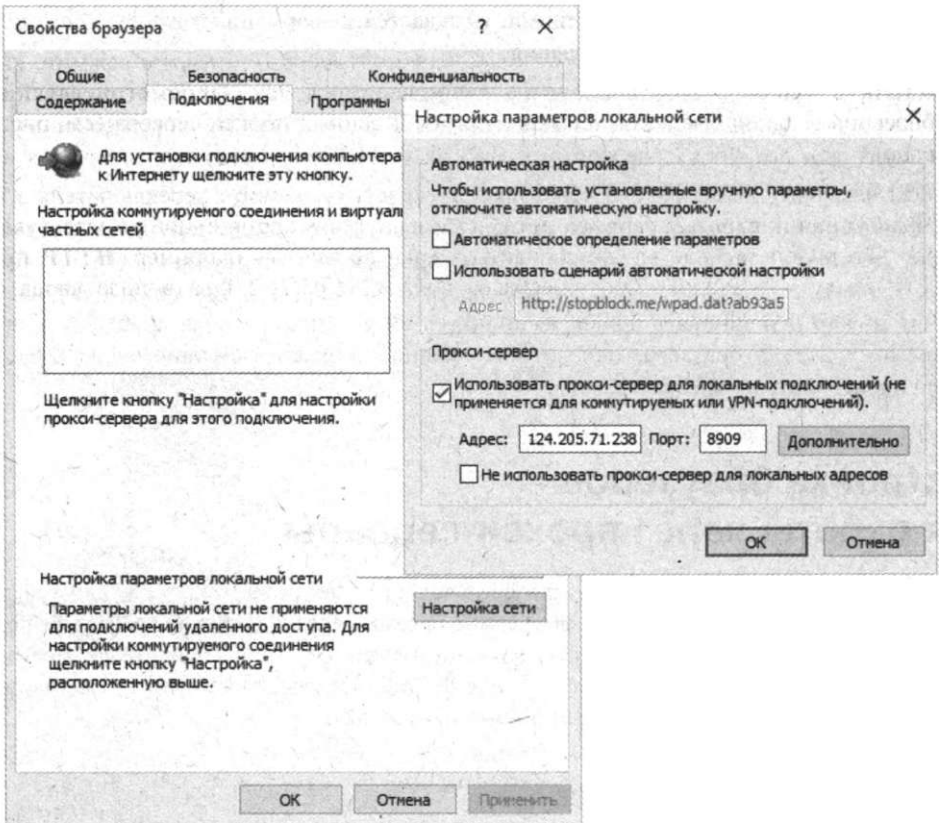


Рис. 8.9. Настройка параметров прокси-сервера в браузере Internet Explorer

5. При необходимости установите флажок Не использовать прокси-сервер для локальных адресов (Bypass proxy server for local addresses).

> ***ПРИМЕЧАНИЕ для ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ***
>
> **Если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения, указанные шаги недоступны. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке Подключения (Connections) диалогового окна Свойства браузера (Browser Options), и нажать кнопку Настройка (Settings).**

6. Нажимайте последовательно кнопки ОК, чтобы закрыть открытые диалоговые окна.

Вы также можете нажать кнопку Дополнительно (Advanced) и в открывшемся диалоговом окне указать адреса различных прокси-серверов для разных протоколов.

Браузер Mozilla Firefox

В браузере Firefox настройка прокси происходит аналогично настройке Internet Explorer:

1. В правом верхнем углу окна программы Firefox нажмите кнопку и выберите команду меню Настройки (Settings). Или же, нажав клавишу <Alt>, выберите команду меню Инструменты | Настройки (Tools | Options). В любом случае откроется страница Настройки (Options).

2. Перейдите на вкладку Дополнительные (Advanced).
3. Выберите дополнительную вкладку Сеть (Network) (рис. 8.10, *слева)* и нажмите кнопку Настроить (Setup). Открывшееся после этого диалоговое окно Параметры соединения (Connection settings) предназначено для указания данных прокси-сервера (см. рис. 8.10, *справа).*
4. Чтобы назначить подключение через прокси-сервер, установите переключатель в положение Ручная настройка сервиса прокси (Manual proxy configuration), а затем укажите в соответствующем поле ввода (зависит от типа прокси) — например, HTTP прокси (HTTP Proxy), — IP-адрес прокси-сервера вида 124.205.71.238, а в поле ввода Порт (Port) — порт подключения, например, 8909.

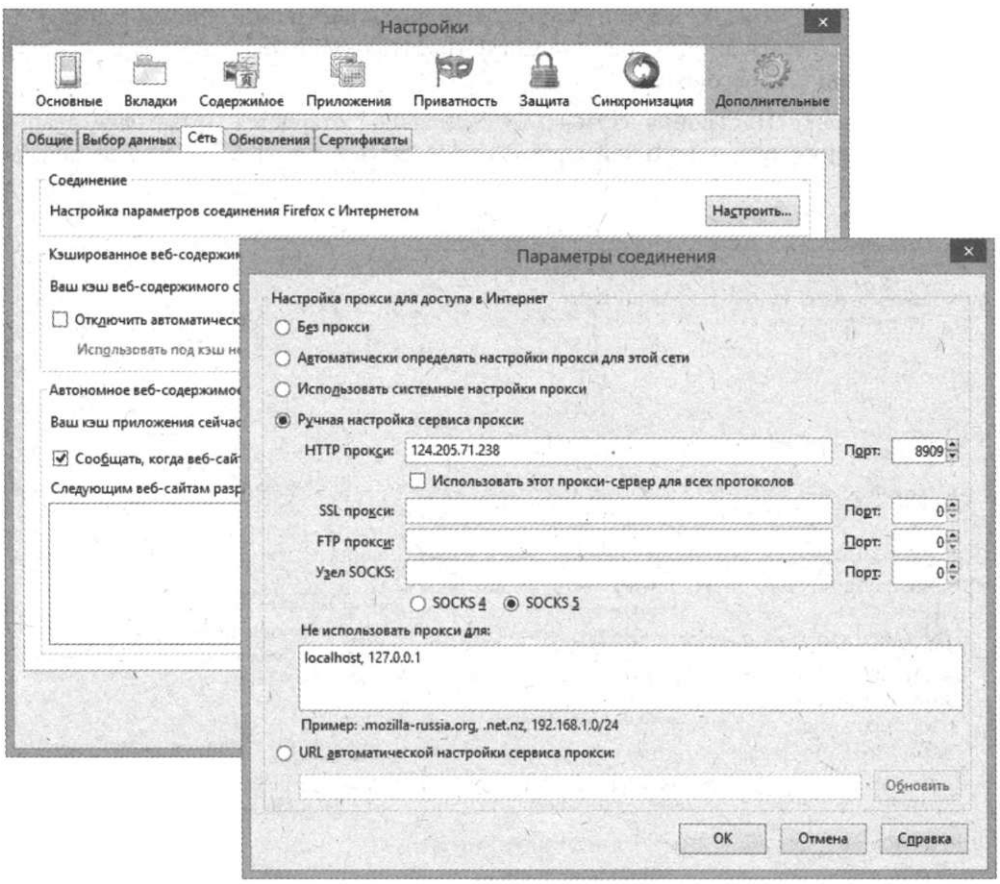


Рис. 8.10. Настройка параметров прокси-сервера в браузере Mozilla Firefox

ПРОВЕРКА ПРОКСИ-СЕРВЕРОВ НА РАБОТОСПОСОБНОСТЬ

Прокси-серверы имеют привычку очень быстро переставать работать, поэтому имеет смысл проверить их перед настройкой браузера. Для проверки существуют специальные программы, а также онлайн-формы. Первые вы можете найти по ссылке tinyurl.com/qz5ftwf, **а пару онлайн-форм проверки здесь:** tinyurl.com/42zk38u.

5. Закройте открытые диалоговое окно и страницу настроек.

В операционной системе OS X настройка браузера Firefox осуществляется аналогичным образом, только доступ к пункту Настройки (Options) осуществляется из меню Firefox.

Браузер Opera

Далее приводятся шаги настройки браузера Opera в версии для операционных систем Windows и OS X.

В Windows выполните следующие шаги:

1. Выберите команду меню Opera | Настройки (Opera | Preferences) — откроется вкладка Настройки (Preferences) (рис. 8.11, *слева).*
2. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси (Change proxy settings) — откроется диалоговое окно Свойства: Интернет (Internet Options) на вкладке Подключения (Connections).
3. Нажмите кнопку Настройка сети (LAN Settings) — откроется диалоговое окно Настройка параметров локальной сетн (Local Area Network (LAN) Settings) (рис. 8.11, *справа).*

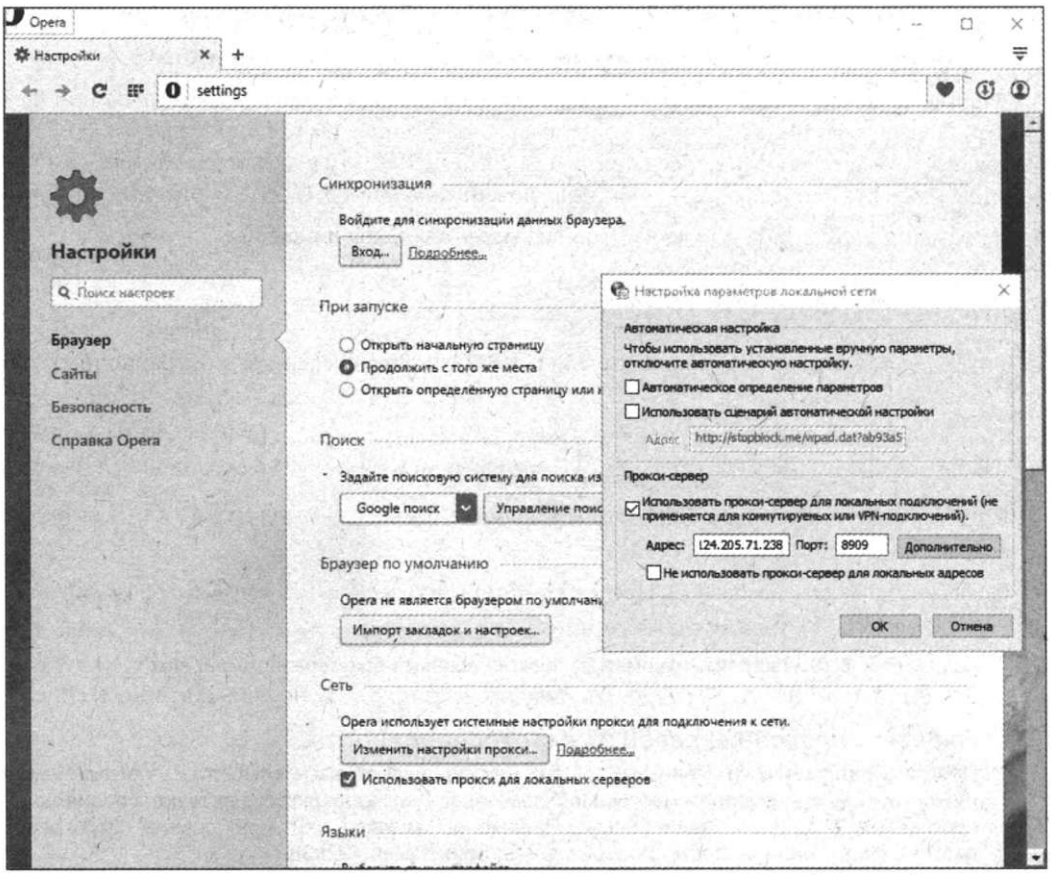


Рис. 8.11. Настройка параметров прокси-сервера в браузере Opera

4. Чтобы назначить подключение через прокси-сервер, нужно установить флажок **Использовать прокси-сервер для локальных подключений** (Use a proxy server for your LAN), а затем указать в поле ввода **Адрес** (Address) IP-адре'с прокси-сервера (HTTP или HTTPS) вида 124.205.71.238, а в поле ввода **Порт** (Port) — порт подключения, например, 8909.
5. При необходимости установите флажок **Не использовать прокси-сервер для локальных адресов** (Bypass proxy server for local addresses).

> ***ПРИМЕЧАНИЕ для ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ***
>
> Если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения, указанные шаги недоступны. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке **Подключения** (Connections) диалогового окна **Свойства браузера** (Browser Options), и нажать кнопку **Настройка** (Settings).

6. Нажимайте последовательно кнопки ОК, чтобы закрыть открытые диалоговые окна.

В операционной системе OS X настройка осуществляется несколько иначе:

1. Выберите команду меню **Opera | Настройки** (Opera | Preferences) — откроется вкладка **Настройки** (Preferences) (см. рис. 8.11, *слева).*
2. **В** разделе **Сеть** (Network) нажмите кнопку **Изменить настройки прокси** (Change proxy settings) — откроется панель **Сеть** (Network) на вкладке **Прокси** (Proxy).
3. Установите флажок **Автонастройка прокси** (Automatic Proxy Configuration).
4. Чтобы назначить подключение через прокси-сервер, установите соответствующий флажок (зависит от типа прокси) — например, **Веб-прокси (HTTP)** (Web proxy (HTTP)), введите IP-адрес прокси-сервера вида 124.205.71.238 в поле **Сервер веб-прокси** (Web proxy server), а в поле правее — порт подключения, например, 8909 (см. рис. 8.13, *справа).*
5. Нажимайте кнопки ОК и **х**, чтобы закрыть открытые окна и панели.

Браузер Google Chrome

Далее приводятся шаги настройки браузера Google Chrome в версии для операционных систем Windows и OS X.

Настройка прокси-сервера в браузере Google Chrome для операционной системы Windows производится идентично настройке программы Opera после доступа к странице параметров:

1. В правом верхнем углу окна программы Google Chrome нажмите кнопку и выберите команду меню **Настройки** (Settings).
2. Щелкните мышью **по** ссылке **Показать дополнительные настройки** (Show advanced settings) — вид страницы изменится (рис. 8.12).
3. В разделе **Сеть** (Network) нажмите кнопку **Изменить настройки прокси-сервера** (Change proxy settings) — откроется диалоговое окно **Свойства: Интернет** (Internet Options) на вкладке **Подключения** (Connections).
4. Нажмите кнопку **Настройка сети** (LAN Settings) — откроется диалоговое окно **Настройка параметров локальной сети** (Local Area Network (LAN) Settings) (см. рис. 8.12, *справа).*
5. Чтобы назначить подключение через прокси-сервер, нужно установить флажок **Использовать прокси-сервер для локальных подключений** (Use a proxy server for your LAN),

а затем указать в поле ввода Адрес (Address) IP-адрес прокси-сервера (HTTP или HTTPS) вида 124.205.71.238, а в поле ввода Порт (Port) — порт подключения, например, 8909.

6. При необходимости установите флажок Не использовать прокси-сервер для локальных адресов (Bypass proxy server for local addresses).

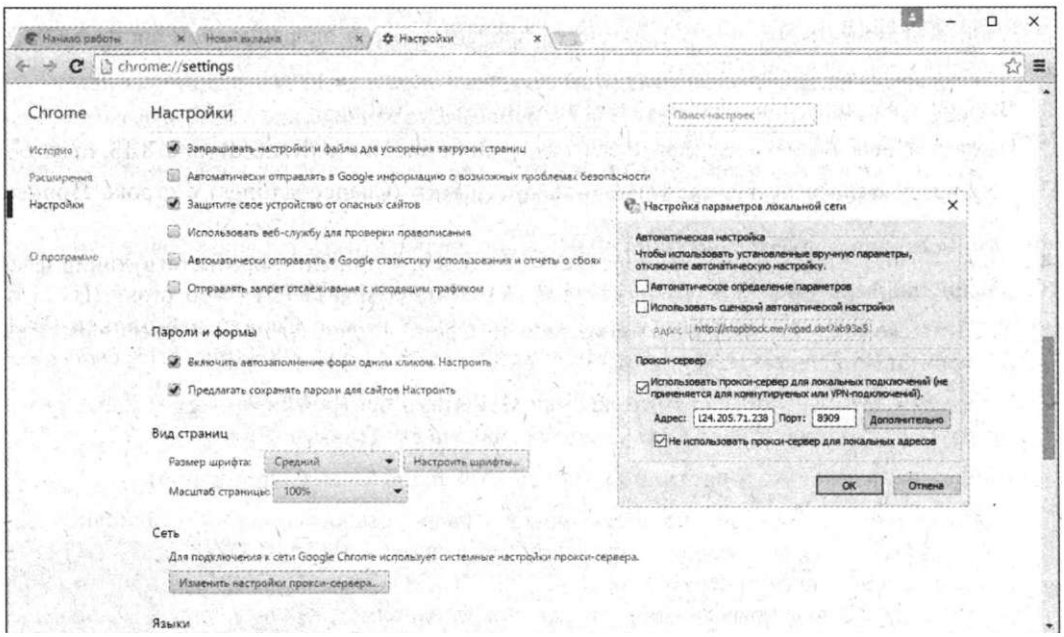


Рис. 8.12. Настройка параметров прокси-сервера в браузере Google Chrome

ПРИМЕЧАНИЕ для ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ

Если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения, указанные шаги недоступны. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке Подключения (Connections) диалогового окна Свойства браузера (Browser Options), и нажать кнопку Настройка (Settings).

7. Нажмите кнопку ОК, чтобы закрыть диалоговое окно, и закройте вкладку Настройки (Preferences) щелчком мыши по значку **x**.

В операционной системе OS X настройка браузера Google Chrome осуществляется несколько иначе:

1. Выберите команду меню Chrome | Настройки (Chrome | Preferences) — откроется вкладка Настройки (Preferences).
2. Щелкните мышью по ссылке Показать дополнительные настройки (Show advanced settings) — вид диалогового окна изменится (см. рис. 8.12).
3. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси-сервера (Change proxy settings) — откроется панель Сеть (Network) на вкладке Прокси (Proxy).
4. Установите флажок Автонастройка прокси (Automatic Proxy Configuration).
5. Чтобы назначить подключение через прокси-сервер, установите соответствующий флажок (зависит от типа прокси) — например, Веб-прокси (HTTP) (Web proxy (HTTP)),

введите IP-адрес прокси-сервера вида 124.205.71.238 в поле Сервер веб-прокси (Web proxy server), а в поле правее — порт подключения, например, 8909 (рис. 8.13, *справа).*

6. Нажимайте кнопки OK и x, чтобы закрыть открытые окна и панели.

Браузер Safari

Настройка браузера Safari для работы через прокси-сервер в операционной системе OS X производится следующим образом:

1. Выберите команду меню Safari | Настройки (Safari | Settings).
2. На открывшейся панели перейдите на вкладку Дополнения (Advanced) (рис. 8.13, *слева).*
3. Щелкните мышью по кнопке Изменить настройки (Change settings) в строке Прокси (Proxy).
4. Чтобы назначить подключение через прокси-сервер, установите соответствующий флажок (зависит от типа прокси) — например, Веб-прокси (HTTP) (Web proxy (HTTP)), введите IP-адрес прокси-сервера вида 124.205.71.238 в поле Сервер веб-прокси (Web proxy server), а в поле правее — порт подключения, например, 8909 (рис. 8.13, *справа).*
5. Нажимайте кнопки OK и **x**, чтобы закрыть открытые окна и панели.

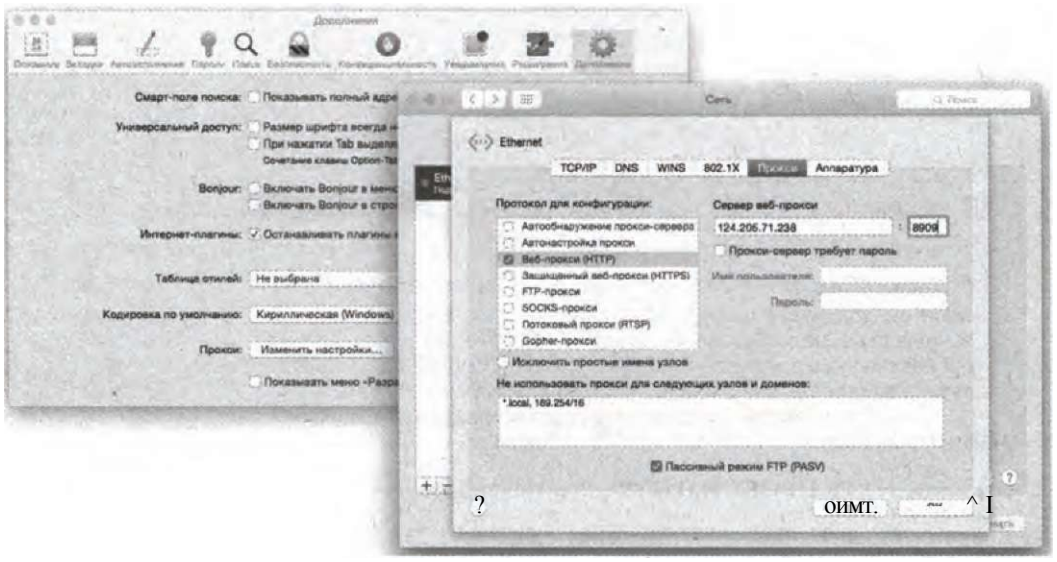


Рис. 8.13. Настройка параметров прокси-сервера в браузере Safari

Настройка мобильных устройств для работы через прокси-серверы

Здесь мы рассмотрим способы работы через прокси-серверы с мобильных устройств под управлением операционных систем iOS (таких, как iPad и iPhone), Windows Phone, Android и Blackberry.

Операционная система iOS

Настройка устройств iPhone, iPad и iPod Touch для работы через прокси-сервер в сетях Wi-Fi производится следующим образом:

1. Коснитесь значка Настройки (Settings).
2. На открывшемся экране коснитесь пункта Wi-Fi, а затем значка (T) справа от названия подключенной сети — вы увидите экран, показанный на рис. 8.14.

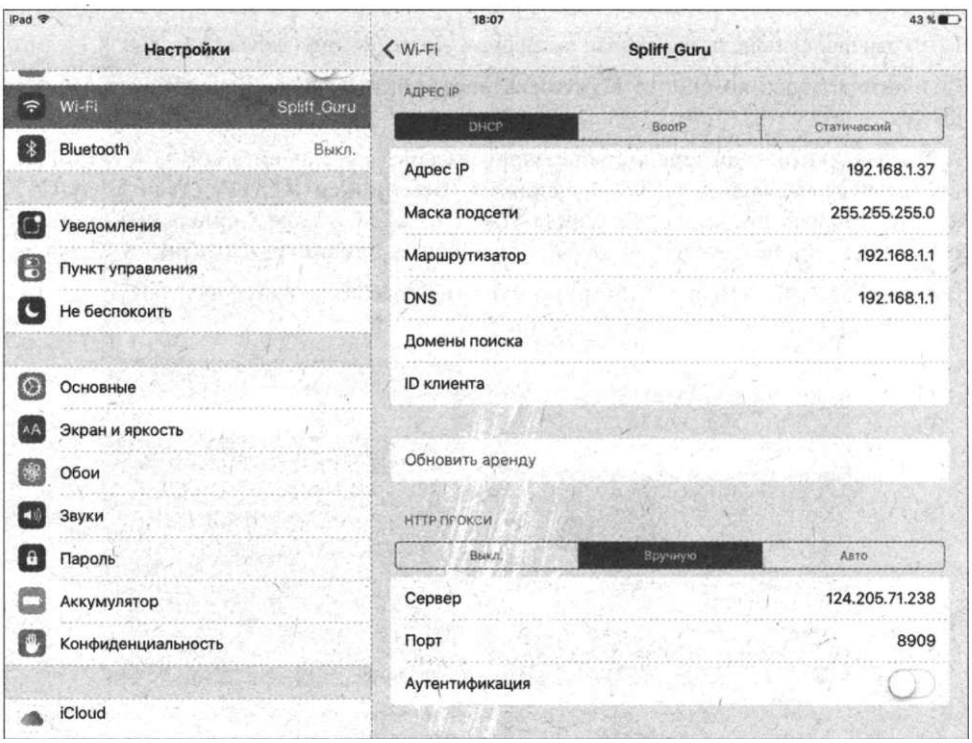


Рис. 8.14. Настройка параметров прокси-сервера в операционной системе iOS 9

3. В разделе HTTP ПРОКСИ (HTTP-proxy) коснитесь пункта Вручную (Manual).
4. Введите IP-адрес прокси-сервера вида 124.205.71.238 в поле Сервер (Server), а в поле Порт (Port) — порт подключения, например, 8909 (см. рис. 8.14).
5. Если на прокси-сервере необходима авторизация, установите переключатель Аутентификация (Authentication) в активное положение и введите логин и пароль в соответствующие поля (появятся при активации параметра).

Теперь вы можете пользоваться доступом в Интернет через прокси-сервер. Настройки прокси-сервера для каждой сети Wi-Fi указываются отдельно.

Операционная система Windows Phone

Сети Wi-Fi

Настройка устройств под управлением операционной системы Windows Phone для работы через прокси-сервер в сетях Wi-Fi производится следующим образом:

1. Смахните главный экран влево и коснитесь пункта **Настройки** (Settings).
2. На открывшемся экране коснитесь пункта Wi-Fi, а затем названия подключенной сети — вы увидите экран, показанный на рис. 8.15, *слева.*

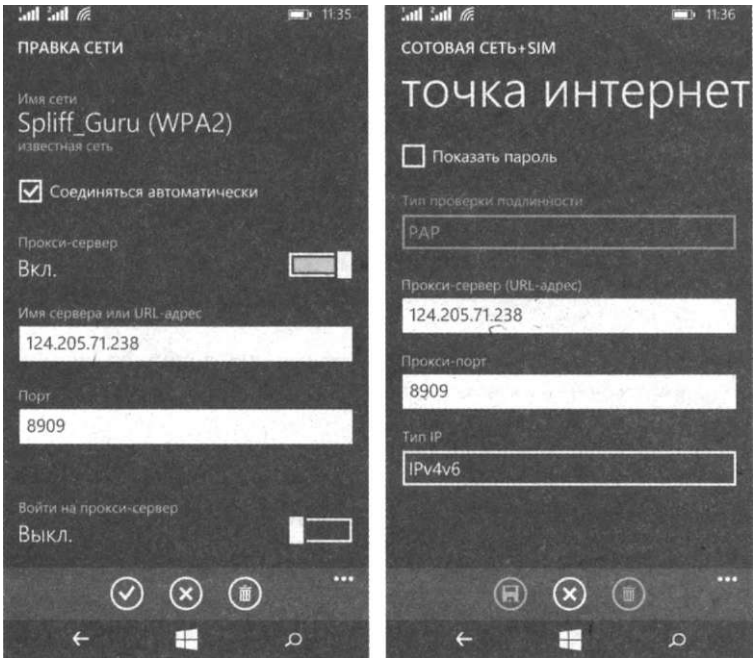


Рис. 8.15. Настройка параметров прокси-сервера в операционной системе Windows Phone 8 для Wi-Fi *(слева)* и для сотовой сети *(справа)*

3. Установите переключатель **Прокси-сервер** (Proxy server) в активное положение.
4. Введите IP-адрес прокси-сервера вида 124.205.71.238 в поле **Имя сервера** (Server), а в поле **Порт** (Port) — порт подключения, например, 8909 (см. рис. 8.15, *слева).*
5. Если на прокси-сервере необходима авторизация, установите переключатель **Войти на прокси-сервер** (Authentication) в активное положение и введите логин и пароль в соответствующие поля (появятся при активации параметра).
6. Коснитесь кнопки , чтобы подтвердить настройки.

Настройки прокси-сервера для каждой сети Wi-Fi указываются отдельно.

Сотовые сети для передачи данных

Если же требуется осуществить доступ через прокси-сервер с использованием сотовой сети для передачи данных, выполните следующие действия:

1. Смахните главный экран влево и коснитесь пункта **Настройки** (Settings).
2. На открывшемся экране коснитесь пункта **Сотовая сеть + SIM** (Cellular + SIM).

   Опционально для смартфона с двумя SIM-картами: коснитесь пункта **Настройки SIM-карты 1** (SIM 1 settings) или **Настройки SIM-карты 2** (SIM 2 settings), — в зависимости от того, какую SIM-карту вы используете для подключения к Интернету.
3. Установите переключатель **Настройка точки доступа вручную** (APN manual settings) в активное положение — вы увидите экран, показанный на рис. 8.15, *справа.*
4. Введите адрес, логин и пароль для доступа к точке согласно сведениям, полученным от вашего оператора сотовой связи.
5. Введите IP-адрес прокси-сервера вида 124.205.71.238 в поле **Прокси-сервер** (Proxy server), а в поле **Прокси-порт** (Proxy port) — порт подключения, например, 8909 (см. рис. 8.15, *справа).*
6. Коснитесь кнопки , чтобы подтвердить настройки.

Теперь вы можете пользоваться доступом в Интернет через прокси-сервер.

Операционная система Android

Сети Wi-Fi

К любой добавленной на устройство под управлением операционной системы Android сети Wi-Fi можно подключиться через прокси-сервер. Вот как это сделать:

1. Откройте экран **Настройки** (Settings).
2. **В** разделе **Беспроводные средства и сети** (Wireless & networks) коснитесь пункта **Wi-Fi.**
3. Коснитесь и удерживайте название нужной сети Wi-Fi.
4. Выберите пункт **Изменить сеть** (Modify network) — вы увидите экран, показанный на рис. 8.16, *слева.*
5. Установите флажок **Показать расширенные функции** (Show advanced options).
6. В разделе **Параметры прокси-сервера** (Proxy Settings) в раскрывающемся списке выберите пункт **Вручную** (Manual).
7. Введите IP-адрес прокси-сервера вида 124.205.71.238 в поле **Имя хоста прокси-сервера** (Server), а в поле **Порт прокси-сервера** (Port) — порт подключения, например, 8909 (см. рис. 8.16, *слева).*
8. Коснитесь кнопки **Подключить** (Connect), чтобы подтвердить настройки.

Настройки прокси-сервера для каждой сети Wi-Fi указываются отдельно.

Сотовые сети для передачи данных

Если же на устройстве под управлением операционной системы Android требуется осуществить доступ через прокси-сервер с использованием сотовой сети для передачи данных, выполните следующие действия:

1. Откройте экран **Настройки** (Settings).
2. В разделе **Беспроводные средства и сети** (Wireless & networks) коснитесь пункта **Еще** (More).

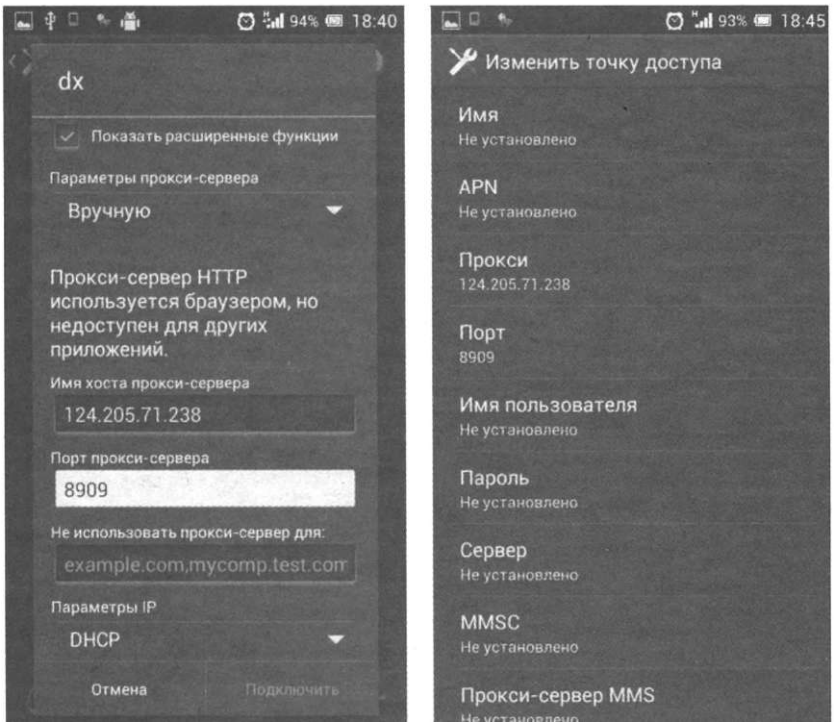


Рис. 8.16. Настройка параметров прокси-сервера в операционной системе Android 4 для Wi-Fi *(слева)* **и для сотовой сети** *(справа)*

3. На открывшемся экране коснитесь пункта Сети мобильной связи (Cellular), а затем пункта Точки доступа (APN) (APN)
4. В контекстном меню выберите пункт Создать APN (Create APN) — вы увидите экран, показанный на рис. 8.16, *справа.*
5. Введите адрес, логин и пароль для доступа к точке согласно сведениям, полученным от вашего оператора сотовой связи.
6. Введите IP-адрес прокси-сервера вида 124.205.71.238 в поле Прокси (Proxy), а в поле Порт (Port) — порт подключения, например, 8909 (см. рис. 8.16, *справа).*
7. Коснитесь кнопки ОК, чтобы подтвердить настройки.

Теперь вы можете пользоваться доступом в Интернет через прокси-сервер.

Операционная система Blackberry OS

Сети Wi-Fi

К любой добавленной на устройство под управлением операционной системы Blackberry OS сети Wi-Fi можно подключиться через прокси-сервер. Вот как это сделать:

1. Откройте экран Настройки (Settings) и коснитесь пункта Сети и подключения (Network and Connections).
2. КоснитесьпунктаWi-Fi.

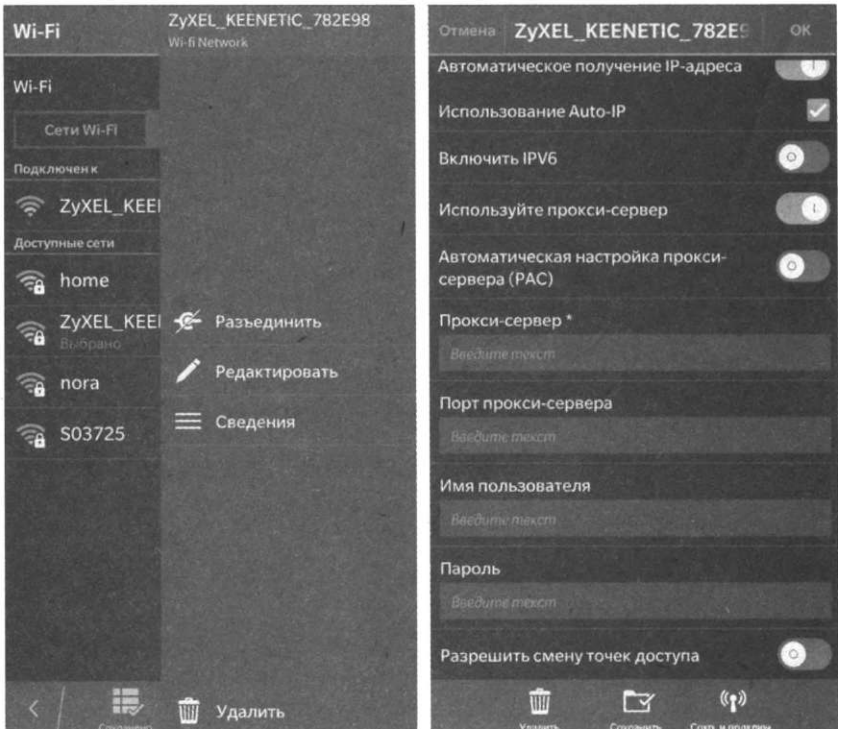


Рис. 8.17. Настройка параметров прокси-сервера в операционной системе Blackberry OS 10

3. Коснитесь и удерживайте название нужной сети Wi-Fi — вы увидите экран, показанный на рис. 8.17, *слева.*
4. Выберите пункт Редактировать (Modify) — вы увидите экран, показанный на рис. 8.17, *справа.*
5. Установите переключатель Используйте прокси-сервер (Use proxy Server) в активное положение.
6. Введите IP-адрес прокси-сервера вида 124.205.71.238 в поле Прокси-сервер (Proxy Server), а в поле Порт прокси-сервера (Proxy server port) — порт подключения, например, 8909 (см. рис. 8.17, *справа).*
7. Если на прокси-сервере необходима авторизация, введите логин и пароль в соответствующие поля ниже.
8. Коснитесь кнопки Сохранить и подключить (Save & connect), чтобы подтвердить настройки.

Настройки прокси-сервера для каждой сети Wi-Fi указываются отдельно.

Сотовые сети для передачи данных

Если же на устройстве под управлением операционной системы Blackberry OS требуется осуществить доступ через прокси-сервер с использованием сотовой сети для передачи данных, выполните следующие действия:

1. Откройте экран Настройки (Settings) и коснитесь пункта Сети и подключения (Network and Connections).

2. Выберите пункт **Мобильная сеть** (Mobile Network). Одноименный переключатель должен находиться в активном положении.
3. Коснитесь кнопки
4. На открывшемся экране введите данные адрес, логин и пароль для доступа к точке согласно сведениям, полученным от вашего оператора сотовой связи.
5. Введите IP-адрес и порт прокси-сервера в соответствующее поле в формате *Адрес: Порт,* — например, 124.205.71.238:8909.
6. Сохраните настройки.

Теперь вы можете пользоваться доступом в Интернет через прокси-сервер.

Использование цепочек прокси

Настроив в свойствах браузера подключение через прокси, вы сможете несколько безопаснее чувствовать себя во Всемирной паутине и посещать заблокированные администратором узлы. Для пущей же анонимности можно использовать цепочки прокси, например, осуществив подключение так, как показано на рис. 8.18.

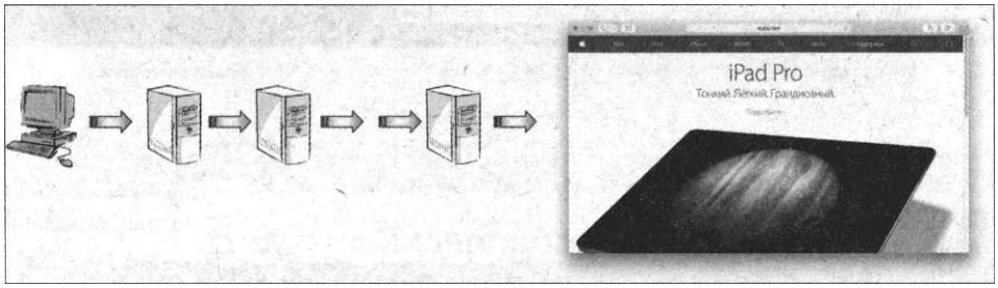


Рис. 8.18. Цепочка прокси

Прокси-серверов между вашим компьютером и целевым веб-узлом может быть сколько угодно — так обнаружить вас будет еще сложнее. Только подбирать следует достаточно скоростные прокси-серверы, иначе, если хотя бы одно звено будет работать слишком медленно, загрузки требуемой веб-страницы вам придется ждать очень долго, или же произойдет обрыв соединения.

Для организации цепочек прокси обычно используются специальные программы, превращающие совокупность узлов в один «виртуальный прокси». Чтобы воспользоваться цепочкой прокси, вам понадобится прописать в настройках такой программы только лишь адрес такого «виртуального прокси». Самое важное при построении цепочки — определиться, прокси-серверы какого типа вы станете использовать и в какой последовательности, иначе ваш «виртуальный туннель» не будет работать. И чтобы все пошло штатно, вам нужно придерживаться следующих правил чередования типов серверов:

- SOCKS —• HTTPS —• CGI;
- SOCKS —• HTTPS;
- HTTPS —• SOCKS;
- SOCKS —• CGI;
- HTTPS —• CGI;

- HTTPS -• SOCKS -• CGI;
- CGI • SOCKS;
- CGI • HTTP.

В каждом звене может быть несколько прокси-серверов одного типа — например, SOCKS • HTTPS • HTTPS.

Самый простой способ использования цепочки следующий:

1. Перейдите на сайт анонимайзера — к примеру, на 2ip.ru/anonim/.
2. В адресной строке анонимайзера укажите адрес сайта другого прокси-сервера (например, online-anonymizer.com), руководствуясь правилами, приведенными ранее, и перейдите на него.
3. Повторите шаг 2 нужное число раз.
4. В адресной строке последнего анонимайзера цепочки введите целевой адрес и перейдите по нему — браузер будет выглядеть весьма несчастно, но цепочка прокси функционирует (рис. 8.19).



Рис. 8.19. Просмотр сайта whatismyipaddress.com через цепочку прокси-серверов

Как можно видеть на рис. 8.19, мы начали путешествие с немецкого анонимайзера (на что указывает домен **.de** в адресной строке браузера), потом перешли на чешский (домен **.cz** в поле ввода ниже), затем посетили анонимайзер с замечательным названием **Hide My Ass!** (его название отображено в серой (для меня желтой) полосе над сайтом для проверки IP-адреса) и, наконец, перешли на искомый сайт **What is my IP-address,** сообщивший, что мы с компьютером находимся где-то в Аризоне.

Тема использования специальных программ организации цепочек прокси достойна отдельной книги, и информацию о них вы сможете найти во Всемирной паутине, в том числе и на странице **tinyurl.com/qz5ftwf.**

Цепочки анонимных прокси-серверов, особенно бесплатных, не смогут обеспечить высокую скорость работы. Не стоит рассчитывать и на загрузку объемных файлов, а также на прослушивание аудио- и просмотр видеоконтента. Тем не менее, анонимно просматривать содержимое веб-страниц вы сможете.

Использование файлов автоконфигурации прокси-сервера

Можно настроить браузер и на использование специального PAC-файла (файла автоконфигурации прокси-сервера), в котором содержится список ограниченных веб-адресов. При попытке доступа к какому-либо из таких адресов, браузер автоматически отправляет трафик через один из указанных в PAC-файле прокси-серверов. Запросы к другим адресам выполняются обычным образом.

Рассмотрим использование такого файла на примере сервиса «ПростоVPN» применительно к различным веб-браузерам.

Браузер Internet Explorer

Настройка браузера Internet Explorer на использование PAC-файла сервиса «ПростоVPN» в операционной системе Windows осуществляется следующим образом:

1. В правом верхнем углу окна программы Internet Explorer нажмите кнопку §J§ и выберите команду меню Свойства браузера (Browser Options). Можно пройти и через основное меню: нажмите клавишу <Alt>, а затем выберите в появившейся строке меню команду Сервис | Свойства браузера (Tools | Browser Options), — откроется одноименное диалоговое окно.
2. Перейдите на вкладку Подключения (Connections) — содержимое диалогового окна Свойства браузера (Browser Options) изменится.
3. Нажмите кнопку Настройка сети (LAN Settings) — откроется диалоговое окно Настройка параметров локальной сети (Local Area Network (LAN) Settings) (рис. 8.20, *справа).*
4. Установите флажок Использовать сценарий автоматической настройки (Use automatic configuration script).
5. В поле Адрес (Address) укажите адрес **http://antizapret.prostovpn.org/proxy.pac** (см. рис. 8.20, *справа).*
6. Закройте открытые диалоговые окна, последовательно нажимая в них кнопки OK.
7. Перейдите на заблокированный сайт для проверки соединения.

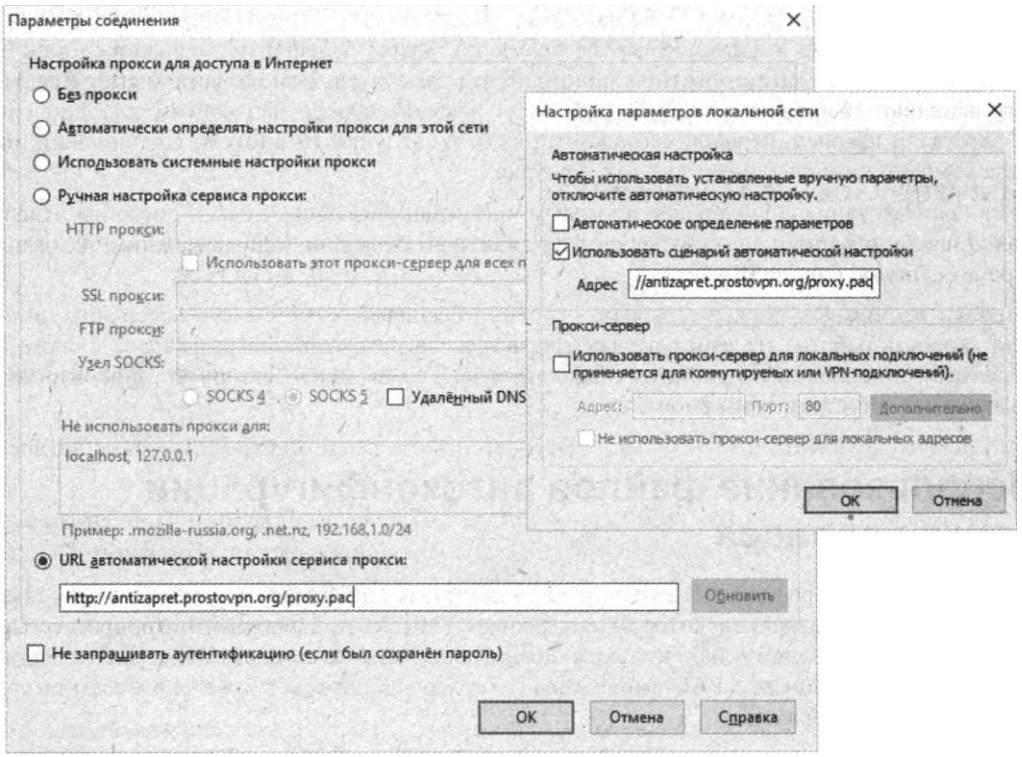


Рис. 8.20. Настройка браузеров Mozilla Fjrefox *(слева)* и Internet Explorer/Chrome/Opera *(справа)*

Для отмены использования PAC-файла повторите первые три шага и сбросьте флажок **Использовать сценарий автоматической настройки** (Use automatic configuration script).

Браузер Mozilla Firefox

Настройка браузера Mozilla Firefox на использование PAC-файла сервиса «npocToVPN» в операционной системе Windows осуществляется следующим образом:

1. В правом верхнем углу окна программы Firefox нажмите кнопку и выберите команду меню **Настройки** (Settings). Или же, нажав клавишу <Alt>, выберите команду меню **Инструменты** I **Настройки** (Tools | Options). В любом случае откроется страница **Настройки** (Options).
2. Перейдите на вкладку **Дополнительные** (Advanced), а затем в раздел **Сеть** (Network).
3. Нажмите кнопку **Настроить** (Configure) — откроется окно **Параметры соединения** (рис. 8.20, *слева).*
4. Установите переключатель в положение **URL автоматической настройки сервиса прокси** (Automatic proxy configuration URL) и в поле ниже укажите адрес **http:// antizapret.prostovpn.org/proxy.pac** (см. рис. 8.20, *слева).*
5. Закройте открытые диалоговые окна и страницу настроек.
6. Перейдите на заблокированный сайт для проверки соединения.

В операционной системе OS X настройка осуществляется аналогичным образом, только доступ к пункту Настройки (Options) выполняется из меню Firefox.

Для отмены использования PAC-файла повторите первые три шага и установите переключатель в положение Без прокси (No proxy).

Браузер Google Chrome

Далее приводятся шаги настройки браузера Google Chrome на использование PAC-файла сервиса «ПростоVPN» в версии для операционных систем Windows и OS X.

В Windows выполните следующие шаги:

1. В правом верхнем углу окна программы Google Chrome нажмите кнопку и выберите команду меню Настройки (Settings).
2. Щелкните мышью по ссылке Показать дополнительные настройки (Show advanced settings) — вид диалогового окна изменится.
3. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси-сервера (Change proxy settings) — откроется диалоговое окно Свойства: Интернет (Internet Options) на вкладке Подключения (Connections).
4. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси-сервера (Change proxy settings) — откроется диалоговое окно Свойства: Интернет (Internet Options) на вкладке Подключения (Connections).
5. Нажмите кнопку Настройка сети (LAN Settings) — откроется диалоговое окно Настройка параметров локальной сети (Local Area Network (LAN) Settings) (см. рис. 8.20, *справа)*.
6. Установите флажок Использовать сценарий автоматической настройки (Use automatic configuration script).
7. В поле Адрес (Address) укажите адрес **http://antizapret.prostovpn.org/proxy.pac** (см. рис. 8.20, *справа)*.
8. Закройте открытые окна.
9. Перейдите на заблокированный сайт для проверки соединения.

В операционной системе OS X настройка осуществляется несколько иначе:

1. Выберите команду меню **Chrome** | Настройки (Chrome | Settings).
2. Щелкните мышью на ссылке Показать дополнительные настройки (Show advanced settings) — вид диалогового окна изменится.
3. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси-сервера (Change proxy settings) — откроется панель Сеть (Network) на вкладке Прокси (Proxy) (рис. 8.21).
4. Установите флажок Автонастройка прокси (Automatic Proxy Configuration).
5. В поле ввода адреса укажите значение **http://antizapret.prostovpn.org/proxy.pac** (см. рис. 8.21) и нажмите кнопку ОК.
6. Закройте открытые окна, не забыв нажать кнопку Применить (Apply).
7. Перейдите на заблокированный сайт для проверки соединения.

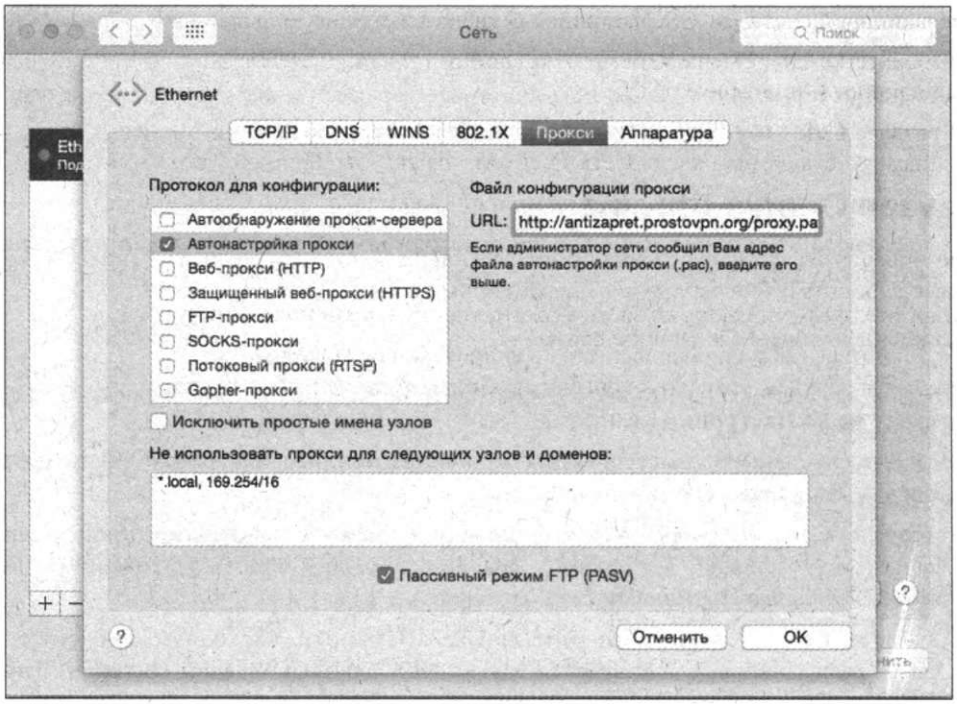


Рис. 8.21. Настройка параметров прокси-сервера для работы с сервисом «прострVPN» в OS X

Для отмены использования PAC-файла повторите первые три шага и сбросьте соответствующий флажок.

Браузер Opera

Настроим браузер Opera на использование PAC-файла сервиса «ПростоVPN».

В операционной системе Windows выполните следующие шаги:

1. Выберите команду меню Opera | Настройки (Opera | Preferences) — откроется вкладка Настройки (Preferences).
2. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси (Change proxy settings) — откроется диалоговое окно Свойства: Интернет (Internet Options) на вкладке Подключения (Connections).
3. Нажмите кнопку Настройка сети (LAN Settings — откроется диалоговое окно Настройка параметров локальной сети (Local Area Network (LAN) Settings) (см. рис. 8.20, *справа).*
4. Установите флажок Использовать сценарий автоматической настройки (Use automatic configuration script).
5. В поле Адрес (Address) укажите адрес http://antizapret.prostovpn.org/proxy.pac (см. рис. 8.20, *справа).*
6. Нажимайте последовательно кнопки ОК, чтобы закрыть открытые диалоговые окна.
7. Перейдите на заблокированный сайт для проверки соединения.

В операционной системе OS X настройка осуществляется несколько иначе:

1. Выберите команду меню Opera | Настройки (Opera | Preferences) — откроется вкладка Настройки (Preferences).
2. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси (Change proxy settings) — откроется панель Сеть (Network) на вкладке Прокси (Proxy) (см. рис. 8.21).
3. Установите флажок Автоиастройка прокси (Automatic Proxy Configuration).
4. В поле ввода адреса укажите значение http://antizapret.prostovpn.org/proxy.pac и нажмите кнопку ОК.
5. Закройте открытые окна, не забыв нажать кнопку Применить (Apply).
6. Перейдите на заблокированный сайт для проверки соединения.

Для отмены использования PAC-файла повторите первые два шага и сбросьте соответствующий флажок.

Браузер Safari

Настроим браузер Apple Safari на использование PAC-файла сервиса «ПростоVPN» в операционной системе OS X.

1. Выберите команду меню Safari | Настройки (Safari | Preferences).
2. В открывшейся панели перейдите на вкладку Дополнения (Advanced) и нажмите кнопку Изменить настройки (Change Settings) в строке Прокси (Proxies) (рис. 8.22).
3. В открывшемся окне установите флажок Автонастройка прокси (Automatic Proxy Configuration).
4. В поле ввода адреса укажите значение http://antizapret.prostovpn.org/proxy.pac (см. рис. 8.21).

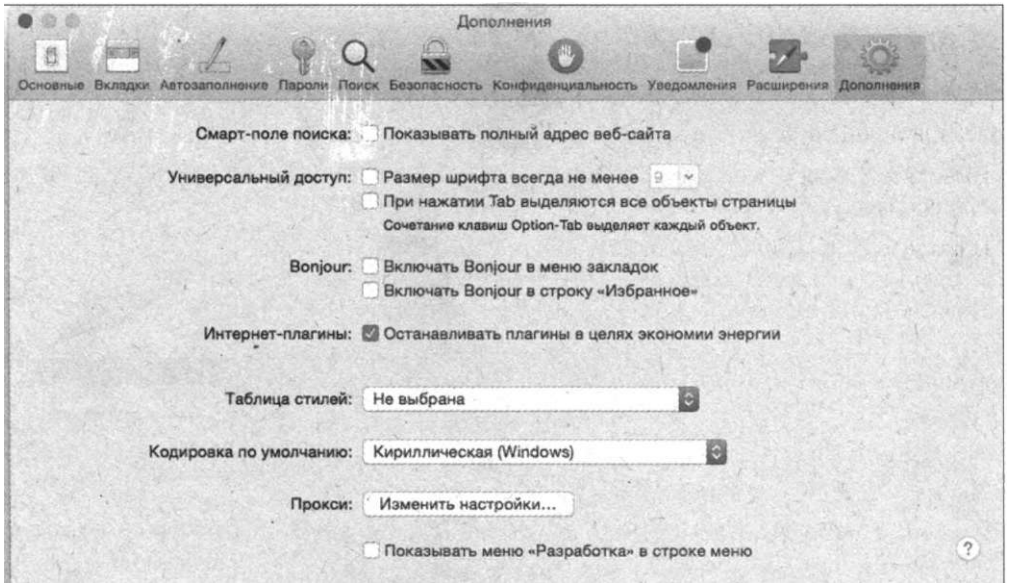


Рис. 8.22. Окно настроек браузера Safari: Вид вкладки Дополнения окна настроек браузера Safari

5. Закрой те открытые окна, не забыв нажать кнопку **Применить** (Apply).
6. Перей дите на заблокированный сай т для проверки соединения.

Для отмены использования PAC-фай ла повторите первые два шага и сбросьте соответствующий флажок.

Использование файлов автоконфигурации прокси-сервера на мобильных устройствах

Здесь мы рассмотрим способы применения фай ла автоконфигурации прокси-сервера на мобильных устрой ствах под управлением операционных систем iOS (iPad и iPhone) и Android.

Операционная система iOS

Настрой ка устрой ств iPhone, iPad и iPod Touch для работы через прокси-сервер с применением фай ла автоконфигурации производится следующим образом:

1. Коснитесь значка **Настрой ки** (Settings).
2. На открывшемся экране коснитесь пункта **Wi-Fi,** а затем значка справа от названия подключенной сети, — вы увидите экран, показанный на рис. 8.23.

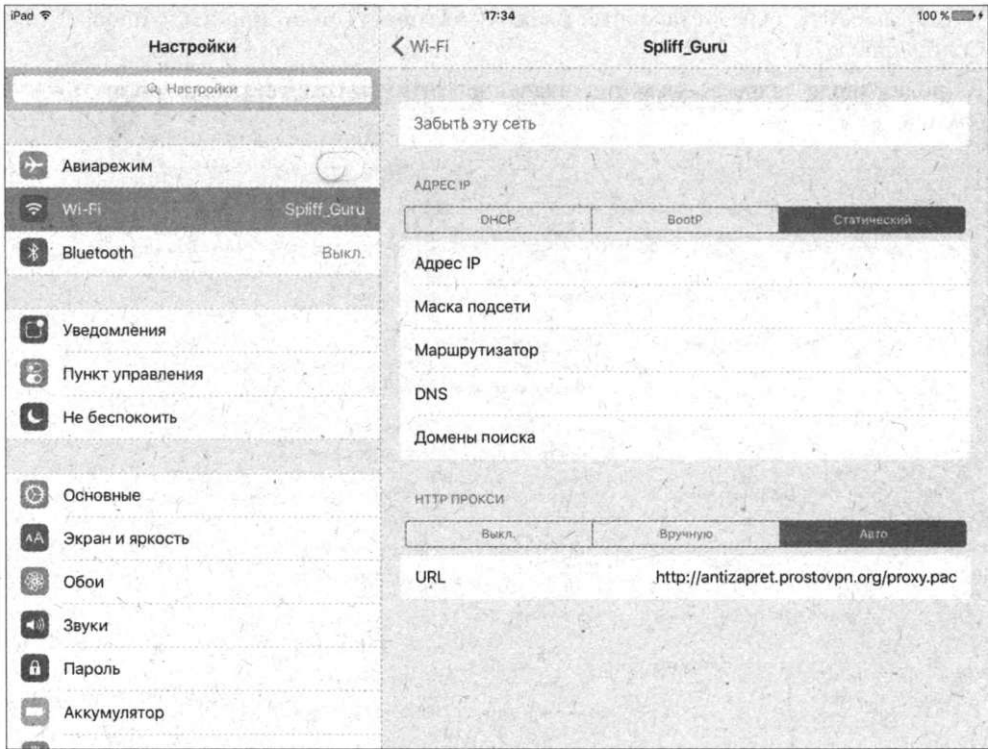


Рис. 8.23. Настройка параметров прокси-сервера для работы с сервисом «ПростоVPM» в операционной системе IOS

3. В разделе HTTP ПРОКСИ (HTTP-proxy) коснитесь пункта Авто (Auto).
4. В поле ввода URL укажите значение http://antizapret.prostovpn.org/proxy.pac (см. рис. 8.23).

Теперь вы можете пользоваться доступом в Интернет через прокси-сервер «ПростоVPN». Настройки прокси-сервера для каждой сети Wi-Fi указываются отдельно.

Операционная система Android

Устройства на платформе Android (как и на Windows Phone, и на Blackberry) не поддерживают использование файлов автоконфигурации прокси-сервера, но можно установил, на них и настроить на использование PAC-файлов браузер Firefox. Для этого выполните следующие действия:

1. Установите приложение Firefox for Android через магазин Google Маркет на свое устройство под управлением операционной системы Android.

> ***FIREFOX FOR IOS***
>
> **Браузер Firefox на устройствах под управлением операционной системы iOS на момент написания книги не поддерживал команду** `about :config`

2. Запустив браузер Firefox, в его адресной строке введите команду `about :config`, чтобы перейти к настройкам браузера.
3. В поле поиска введите слово `proxy`, чтобы отобразить список настроек, относящихся к прокси (рис. 8.24).

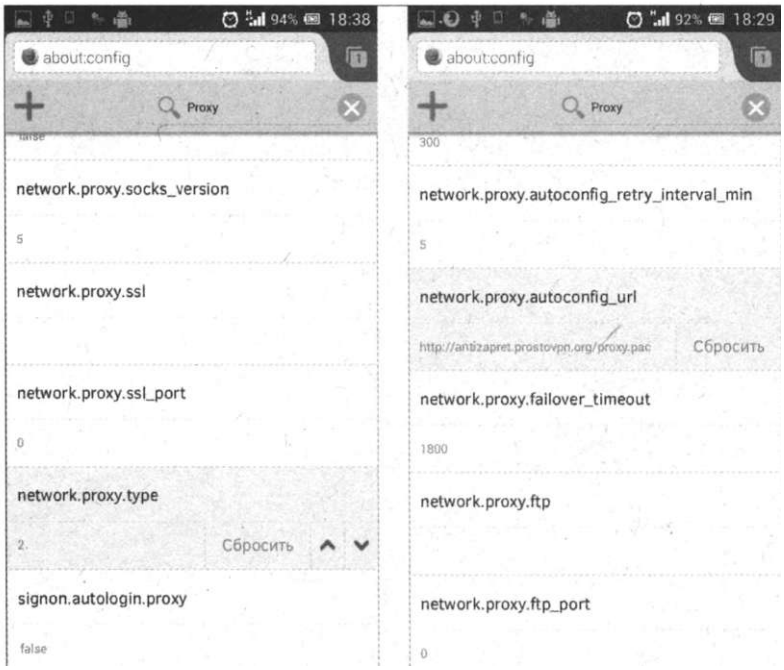


Рис. 8.24. Настройка параметров прокси-сервера для работы с сервисом «ПростоVPN» операционной системе Android

4. Найдите параметр network.proxy.type и, дважды коснувшись поля ниже, присвойте ему значение 2 (рис. 8.24, *слева).*
5. Найдите параметр network.proxy.autoconfig_url и, дважды коснувшись поля ниже, присвойте параметру значение http://antizapret.prostovpn.org/proxy.pac (рис. 8.24, *справа).*
6. Закройте страницу about:config — браузер Firefox должен работать с использованием PAC-файла для автоматической настройки подключения через прокси-сервер.

Теперь вы можете пользоваться доступом в Интернет через прокси-сервер.

Все описанное в разделах, посвященных прокси-серверам, относится к веб-серфингу через браузеры. Что же касается работы приложений электронной почты, ICQ и других программ — настройка прокси в них происходит схожим с браузерами способом (если только выполненные настройки не влияют глобально на подключение всего компьютера).

ГЛАВА 9

Виртуальные частные сети

Программа Hotspot Shield

Универсальное решение ZenMate

Настройка VPN-туннелей через протокол SSTP

SSH-туннель к серверу Amazon

Виртуальные частные сети (Virtual Private Network, VPN), организованные в виде зашифрованного туннеля, «тянутся» поверх Интернета[1]. Такое VPN-соединение состоит из виртуального пирингового канала, который подразумевает связь между двумя компьютерами, и создается через общественную сеть, например через Интернет (рис. 9.1).

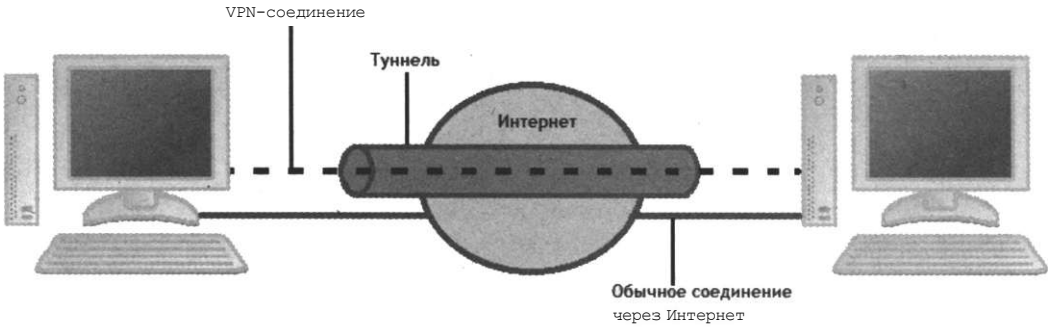


Рис. 9.1. Схема построения VPN-соединения

Каждый *пир* (узел сети) отвечает за шифрование данных до входа в туннель и их расшифровку при выходе. Хотя VPN-соединение всегда устанавливается между двумя пирами, каждый из них может создавать дополнительные туннели с другими узлами, причем для всех таких узлов пир на стороне сервера может быть одним и тем же. Это становится возможным благодаря тому, что узел может шифровать и расшифровывать данные от имени всей сети. В таком случае узел VPN называется *VPN-шлюзом,* с которым пользователь устанавливает соединение и получает доступ в сеть за ним, называемую *доменом шифрования.* Каждый

[1] **Подробнее об этом см.** ru**.wikipedia**.org**/wiki/VPN.**

раз, когда соединение сетей обслуживают два VPN-шлюза, используется *туннелирование.* Это означает, что шифруется весь IP-пакет, после чего к нему добавляется новый заголовок, содержащий IP-адреса двух VPN-шлюзов, которые и доступны при перехвате трафика. Таким образом, невозможно определить компьютер-источник в первом домене шифрования и компьютер-получатель во втором.

Программа Hotspot Shield

Вы можете спросить, а как же в эпоху широкополосного подключения к Интернету смотреть заблокированные видеоролики на сервисах YouTube или Hulu и слушать радио на Pandora? Ведь бесплатные и многие платные прокси-серверы, как и утверждалось в *главе 8,* не потянут такие скорости передачи данных. Ответом на такой вопрос станет использование VPN-туннелей.

Этот способ наиболее актуален для ситуаций, когда контент того или иного сайта или доступ к нему полностью ограничены. Так, уже упоминавшиеся ранее американские сайты Pandora и Hulu не позволяют иностранным (в том числе и российским) пользователям прослушивание своих радиостанций (Pandora) и просмотр видеороликов (Hulu). Суть способа — в организации виртуальной частной сети (VPN), для чего можно воспользоваться бесплатной программой Hotspot Shield.

Итак, вернемся к сайту hulu.com. Чисто американское детище любит радовать российских посетителей, желающих посмотреть тот или иной видеоролик, надписями такого содержания (рис. 9.2).

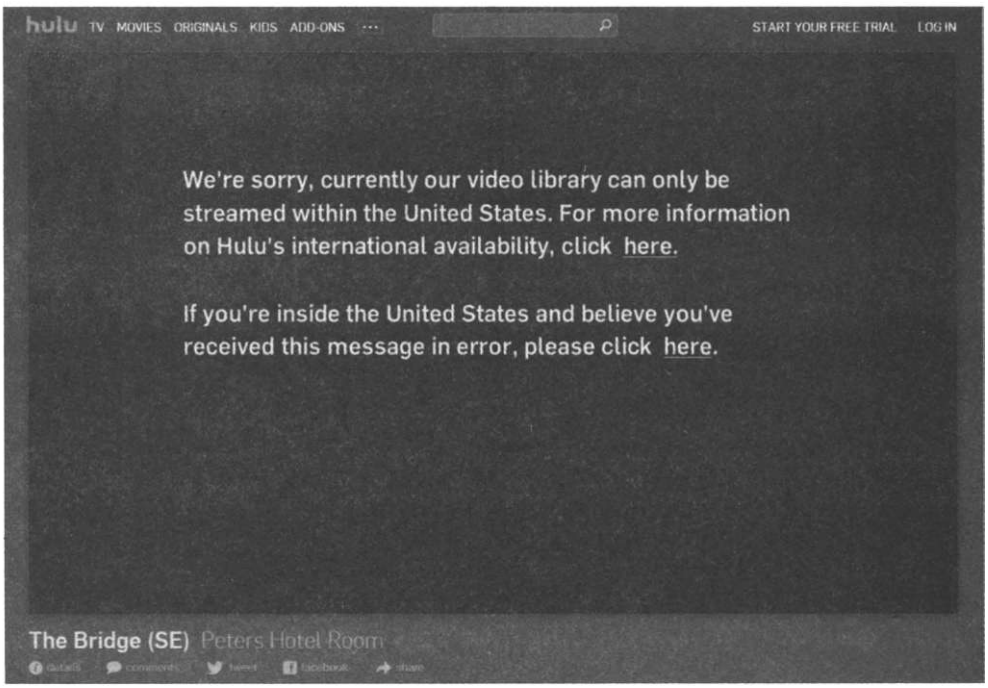


Рис. 9.2. **Сообщение, что просмотр видеоролика доступен только гражданам США**

Попробуем решить проблему с помощью программы Hotspot Shield.

1. Перейдите на веб-сайт hotspotshield.com/ru.

> ***БЕЗОПАСНОСТЬ СОЕДИНЕНИЙ WI-FI***
>
> **Особенно полезна программа Hotspot Shield в плане обеспечения безопасности соединения Wi-Fi, поскольку она организует шифрованное соединение, защищающее данные от прослушивания.**

2. Скачайте дистрибутив бесплатной версии программы (доступны версии как для настольных операционных систем Windows и OS X, так и для мобильных платформ iOS и Android).
3. После успешной загрузки выполните установку программы, подтверждая инсталляцию драйверов для новых сетевых устройств. По окончании процесса установки в области уведомлений появится значок щита зеленого цвета, информирующего, что программа функционирует должным образом, и откроется страница с подпиской на демонстрационную версию. Откроется также и диалоговое окно с настройками, которое можно сразу закрыть.
4. Укажите свой адрес электронной почты и пароль, чтобы активировать подписку на демонстрационную версию. В дальнейшем вы сможете пользоваться бесплатной версией с ограничениями и рекламой или приобрести платную подписку.
5. В диалоговом окне, открываемом щелчком мыши по значку программы в области уведомлений, вы можете изменить настройки защиты (все сайты или выбранные), выбрать страну вашей виртуальной локации, а также просмотреть объемы входящего/исходящего трафика (рис. 9.3).

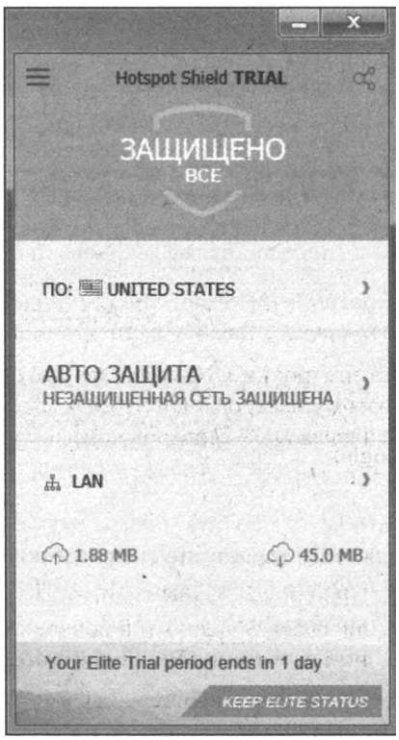


Рис. 9.3. **Панель приложения Hotspot Shield**

На этом, собственно, все — программа установлена и запущена.

Перейдем на страницу сайта hulu.com, чтобы убедиться, что программа Hotspot Shield решила проблему (рис. 9.4).

Теперь вы можете, как пользователь с американским IP-адресом, просматривать страницы сайтов с контентом, который из-за параноидальности защитников авторских прав заблокирован к показу во всех странах, кроме США.

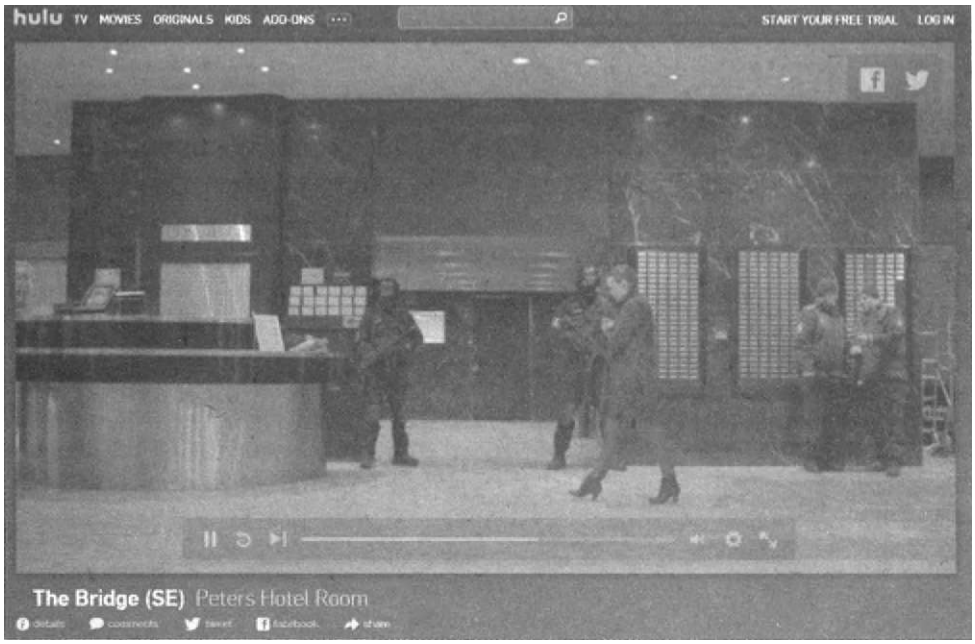


Рис. 9.4. Тот же самый ролик теперь воспроизводится

ПЛАТНЫЕ СЕРВИСЫ VPN

За небольшую абонентскую плату в месяц вы можете воспользоваться услугами компании, предоставляющей скоростной VPN-доступ к серверу нужной страны, — например, **v-p-n.ru.**

Программу Hotspot Shield по идее можно использовать и для других сайтов, в том числе и для прослушивания радиостанций Pandora.

НИШ БЛОКИРУЕТ АНОНИМАЙЗЕРЫ

В 2015 году ресурс **Hulu.com** стал блокировать анонимайзеры, в том числе и доступ через Hotspot Shield. Поэтому для доступа к этому сайту необходимо пробовать использовать другие способы, например, подмену IP-адресов DNS-сервера (см. далее).

Чтобы отключить программу, следует щелкнуть на кнопке в окне, показанном на рис. 9.3, или щелкнуть правой кнопкой мыши по значку программы в области уведомлений и выбрать команду меню **Изменить режим защиты | Выкл** (Change protection mode | Stop).

Подробная инструкция на русском языке по установке и работе с программой Hotspot Shield опубликована на странице по ссылке **tinyurl.com/oqkrt4a.**

Далее приводится небольшой список других бесплатных VPN-сервисов (табл. 9.1).

***Таблица 9.1. 15** бесплатных VPN-сервисов и цена за премиум-подписку*

Название VPN-сервиса	URL-адрес	Цена за месяц платной подписки, от[1]
Ace VPN	**acevpn.com**	**4,58 $**
CyberGhost	**cyberghostvpn.com**	**4,16 €**

[1] Как правило, самая низкая цена в месяц получается при оплате за год.

Таблица 9.1 (окончание)

Название VPN-сервиса	URL-адрес	Цена за месяц платной подписки, от
Hideninja	hideninja.com	125 Р
Hotspot Shield	hotspotshield.com/ru	2,49$
ItsHidden	itshidden.com	6,66$
PrivateTunnel	privatetunnel.com	12,00 $ (оплата за трафик)
proXPN	proxpn.com	6,25$
SecurityKISS Tunnel	securitykiss.com	1,99 €
Spotflux	spotflux.com	2,49$
SurfEasy	surfeasy.com	2,49$
TorVPN	torvpn.com	3,00 €
TunnelBear	tunnelbear.com	4,16 €
VPN Gate	vpngate.net	отсутствует
Your Freedom	your-freedom.net	0,50 €
ZenMate	zenmate.com	6,49 €

Универсальное решение ZenMate

Универсальный плагин ZenMate пока еще бесплатен и доступен в версиях для браузеров Firefox, Opera, Chrome, а также в виде приложений для платформ Windows, OS X, iOS и Android. Плагин предоставляет доступ в Интернет по защищенному зашифрованному каналу на основе VPN (виртуальной частной сети), обеспечивая пользователю и анонимность, и безопасность. К тому же он маскирует адрес расположения пользователя под жителя Соединенных Штатов, Великобритании, Германии, Румынии, Швейцарии или Гонконга (в бесплатном варианте), а также еще и Великобритании, Франции, Канады и Сингапура (в варианте «премиум»). Вот это его свойство и поможет вам при необходимости достучаться до запрещенных в вашей стране сайтов, а также до тех ресурсов, где вас дискриминируют по местожительству.

Установка плагина проста.

1. Перейдите в браузере на сайт **https://zenmate.com** и нажмите кнопку **Add to...** (Добавить в...) (рис. 9.5).
2. Нажмите кнопку Разрешить (Allow), а затем Установить (Install) — все остальное (загрузку инсталлятора и установку плагина) браузер выполнит автоматически, после чего на панели браузера появится соответствующий значок и отобразится предложение активировать плагин.
3. Нажмите кнопку **Activate ZenMate** (Активировать ZenMate) — значок плагина в панели браузера приобретет зеленый цвет и, как видно из рис. 9.6, выведет вас в Интернет через другой сервер, в моем случае — румынский.

Попробуем теперь по установившейся традиции посетить закрытый для всех, кроме американцев, сайт радиостанции **pandora.com** и убедимся, что и румынам туда тоже хода нет.

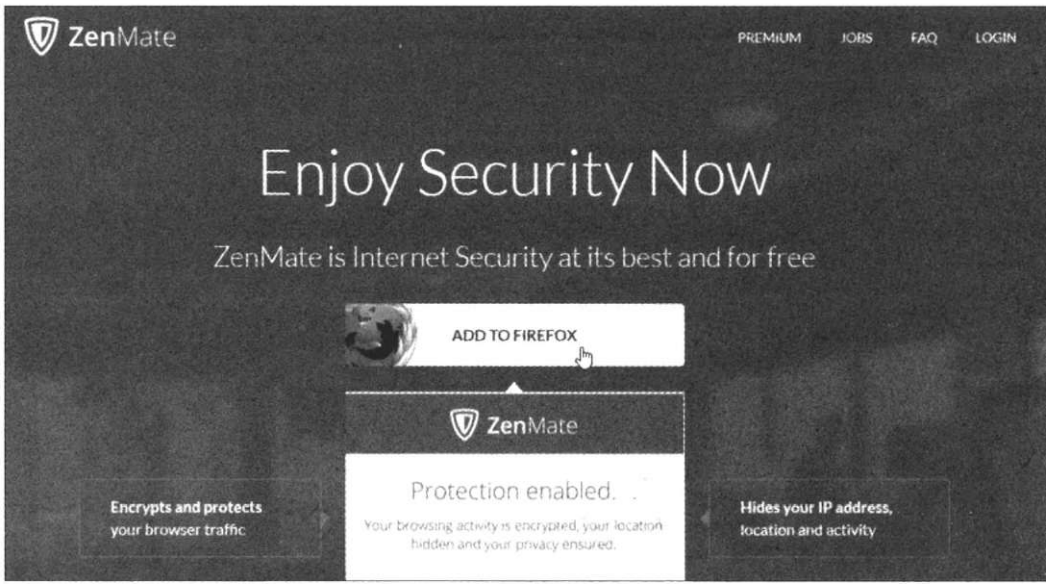


Рис. 9.5. Главная страница сайта плагина ZenMate

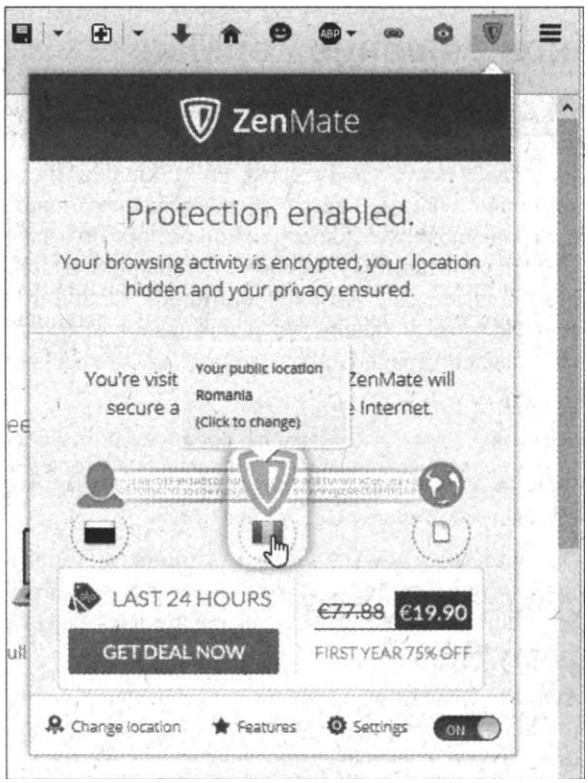


Рис. 9.6. Плагин ZenMate установлен

Что ж, остается только сменить место жительства — нажмите на панели ZenMate кнопку в виде флага страны публичной локации (в центре, на которую наведен указатель мыши на рис. 9.6), выберите из открывшегося списка New York, United States и обновите страницу браузера (рис. 9.7).

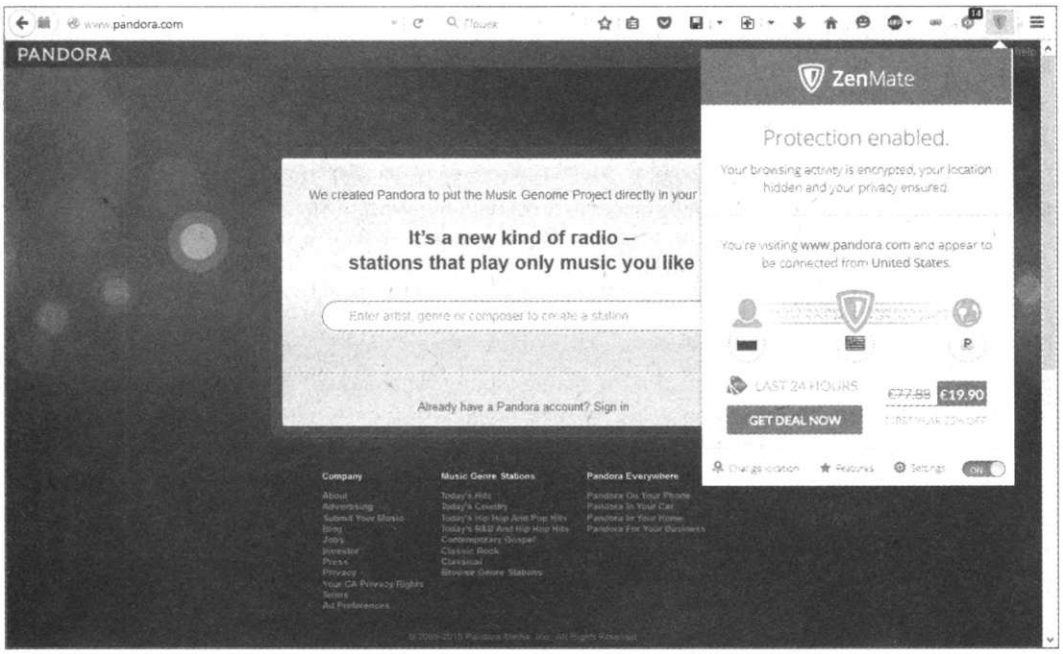


Рис. 9.7. Открытие страницы сайта Pandora.com

Надо также отметить, что включенный плагин слегка притормаживает интернет-серфинг, и если нет надобности открывать закрытые ресурсы, то его лучше отключить, щелкнув по его значку в панели браузера и нажав в открывшейся панели плагина (см. рис. 9.6) переключатель ON — плагин отключится, а переключатель получит надпись OFF. Включить его в случае надобности также просто — нажатием переключателя OFF.

КНОПКА GET ZENMATE FREE

Если в момент установки плагина ZenMate вы обнаружите, что бесплатным он быть перестал (вам могут быть предложены на выбор бесплатный, но ограниченный, вариант и платный премиальный), прокрутите стартовую страницу сайта ZenMate до самого конца вниз, и там вы найдете вожделенную кнопку Get ZenMate Free.

Настройка VPN-туннелей через протокол SSTP

Еще один способ попадания на закрытые для вас сайты заключается в настройке специального VPN-протокола под названием SSTP (Secure Socket Tunneling Protocol, протокол безопасного туннелирования сокетов), который разработан корпорацией Microsoft, основан на SSL и включен в состав операционных систем Windows версий 2008/XP SP3/Vista SP.1 и выше.

Рассмотрим пример подключения через SSTP-лротокол в операционной системе Windows 10 (в других версиях порядок шагов может быть несколько иным) с использованием сервиса freesstpvpn.com.

1. Щелкните правой кнопкой мыши на значке сетевого подключения (локальной сети или беспроводной, не важно) в области уведомлений и выберите в контекстном меню команду Центр управления сетями и общим доступом (Network and Sharing Center).
2. В центральной части открывшегося окна щелкните мышью на ссылке Создание и настройка нового подключения или сети (Set up a new connection or network).
3. Выберите пункт Подключение к рабочему месту (Proxy) и нажмите кнопку Далее (Next).
4. Если появится запрос о создании нового подключения или использования текущего, установите переключатель в положение Нет, создать новое подключение (No, create a new connection) и нажмите кнопку Далее (Next).
5. Выберите пункт Использовать мое подключение к Интернету (VPN) (Use my connection to Internet (VPN)).
6. В открывшемся диалоговом окне в обоих предусмотренных там полях укажите адрес SSTP VPN-сервера, к которому вы хотите подключиться, в зависимости от страны: для США — us.freesstpvpn.com, для Великобритании — uk.freesstpvpn.com или для Нидерландов — NL nl.freesstpvpn.com (рис. 9.8, *слева).* Это значение необходимо указать в обоих полях и нажать кнопку Создать (Create).

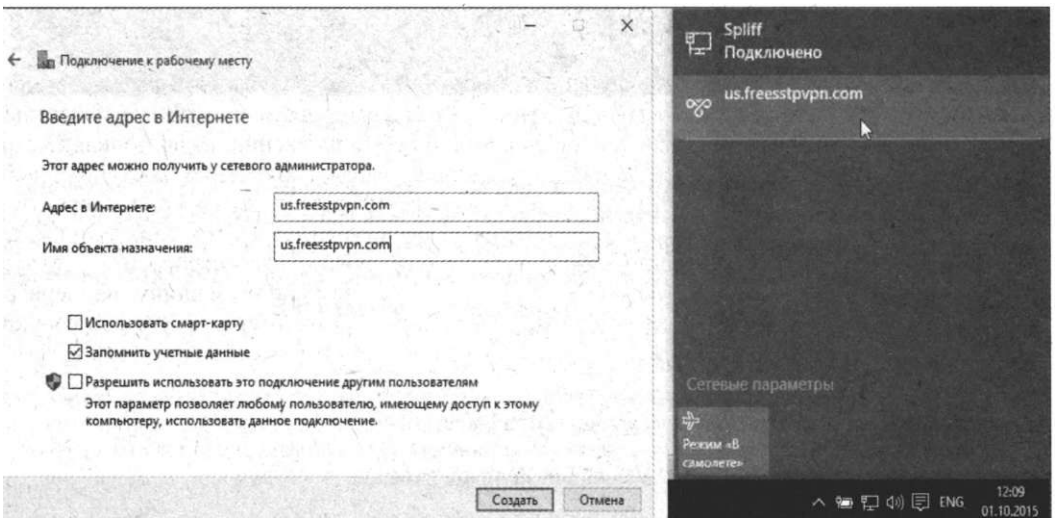


Рис. 9.8. Создание подключения к SSTP VPN-серверу в операционной системе Windows

7. Щелкните мышью по значку сетевого подключения (локальной сети или беспроводной, не важно) в области уведомлений — вы увидите список доступных подключений, среди которых будет значиться только что созданное — freesstpvpn.com (рис. 9.8, *справа).*
8. Щелкните мышью по этому подключению — откроется окно параметров Windows на вкладке VPN.
9. Щелкните по кнопке Подключить (Connect) подключения freesstpvpn.com.

10. В полях ввода открывшегося диалогового окна укажите значения vpn и freesstp и нажмите кнопку **ОК** (рис. **9.9).**

После нажатия кнопки **ОК** произойдет подключение к указанному SSTP VPN-серверу.

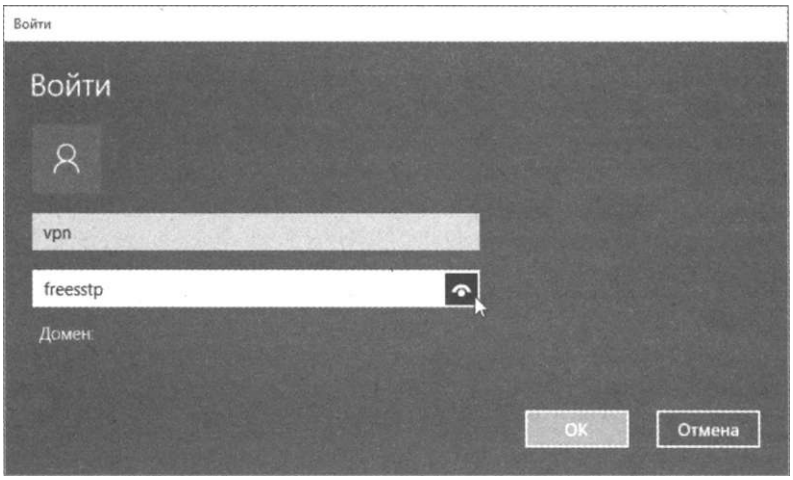


Рис. 9.9. Ввод данных авторизации для подключения к SSTP VPN-серверу

SSH-туннель к серверу Amazon

Amazon Web Services (AWS) — это облачные вычислительные службы, которые вместе составляют целую платформу и позволяют хранить и анализировать публичные и частные данные, а также размещать динамические веб-сайты и веб-приложения. Использование сервера Amazon представляет собой довольно сложный способ получения доступа к веб-сайтам, тем не менее позволяющий обходить блокировку ресурсов без потерь в скорости и за небольшую плату (при регистрации вы получаете бесплатный доступ к ряду услуг в течение 12 месяцев). Для организации такого доступа вам нужно зарегистрировать учетную запись (аккаунт) AWS, затем настроить и запустить виртуальную машину на сервере Amazon, после чего настроить подключение к ней на своем компьютере и получить необходимый доступ.

Регистрация учетной записи AWS

Для регистрация учетной записи AWS выполните следующие действия:

1. Откройте браузер и перейдите по адресу **aws.amazon.com/ru/.**

   Если у вас уже есть аккаунт на сайте **Amazon.com,** введите свой адрес электронной почты (или номер телефона) и пароль, а затем нажмите кнопку **Войти в систему через безопасный сервер** (Sign in using our secure server). Если аккаунта нет, создайте новый, следуя приведенным далее шагам.

2. Нажмите кнопку **Регистрация** (Sign In to the Console)
3. Установите переключатель в положение **Я — новый пользователь** (I am a new user).
4. Нажмите кнопку **Войти в систему через безопасный сервер** (Sign in using our secure server).

5. Заполните открывшуюся форму, указав свое имя, адрес электронной почты и желаемый пароль. Нажмите кнопку Создать учетную запись (Create account) — вы увидите форму дополнительных сведений об учетной записи (рис. 9.10).

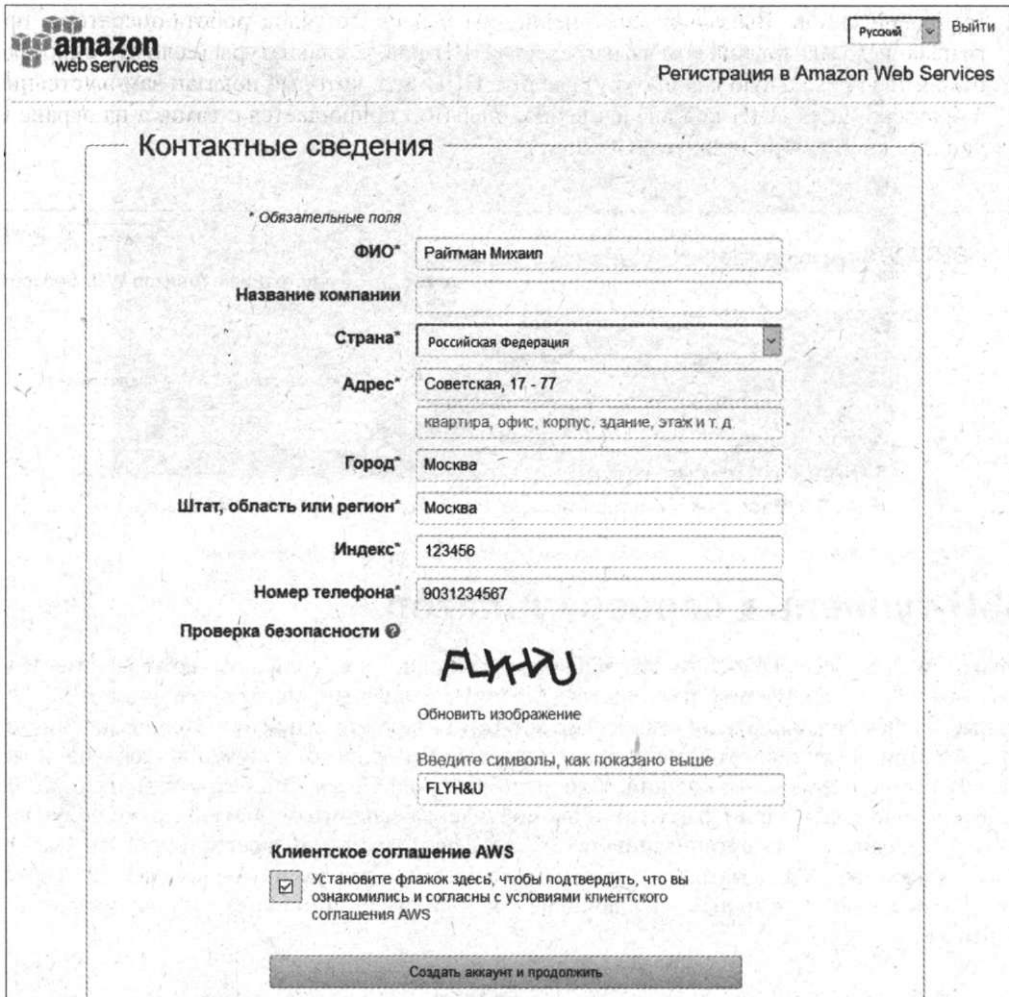


Рис. 9.10. Ввод контактных сведений при создании аккаунта AWS

6. Заполните форму. Обязательно введите функционирующий номер мобильного телефона, т. к. с его помощью будет подтверждаться создание аккаунта.
7. Нажмите кнопку Создать аккаунт и продолжить (Create account & continue).
8. В открывшейся форме укажите данные своей банковской карты (подойдет любая карта, за исключением Electron[1]): номер карты, дату истечения срока действия и фамилию/имя держателя карты. Нажмите кнопку Продолжить (Continue).

[1] **Карты типа Electron (например, Сбербанк Социальная) не поддерживаются при оплате интернет-покупок, поскольку не имеют CVV-кода на обратной стороне.**

9. Вы увидите форму, показанную на рис. 9.11, в которой следует проверить указанный номер телефона и нажать кнопку Позвонить мне сейчас (Call me now).

10. Вы увидите ПИН-код из четырех цифр и через некоторое время на телефон поступит голосовой вызов. Выполнив соединение, вы услышите голос робота-оператора, приглашающего (на английском языке) ввести ПИН-код. С клавиатуры (если это смартфон, откройте виртуальную клавиатуру) введите ПИН-код, который показан вам на странице в браузере. Если ПИН-код введен верно, оператор попрощается с вами, а на экране вы увидите кнопку Продолжить (Continue).

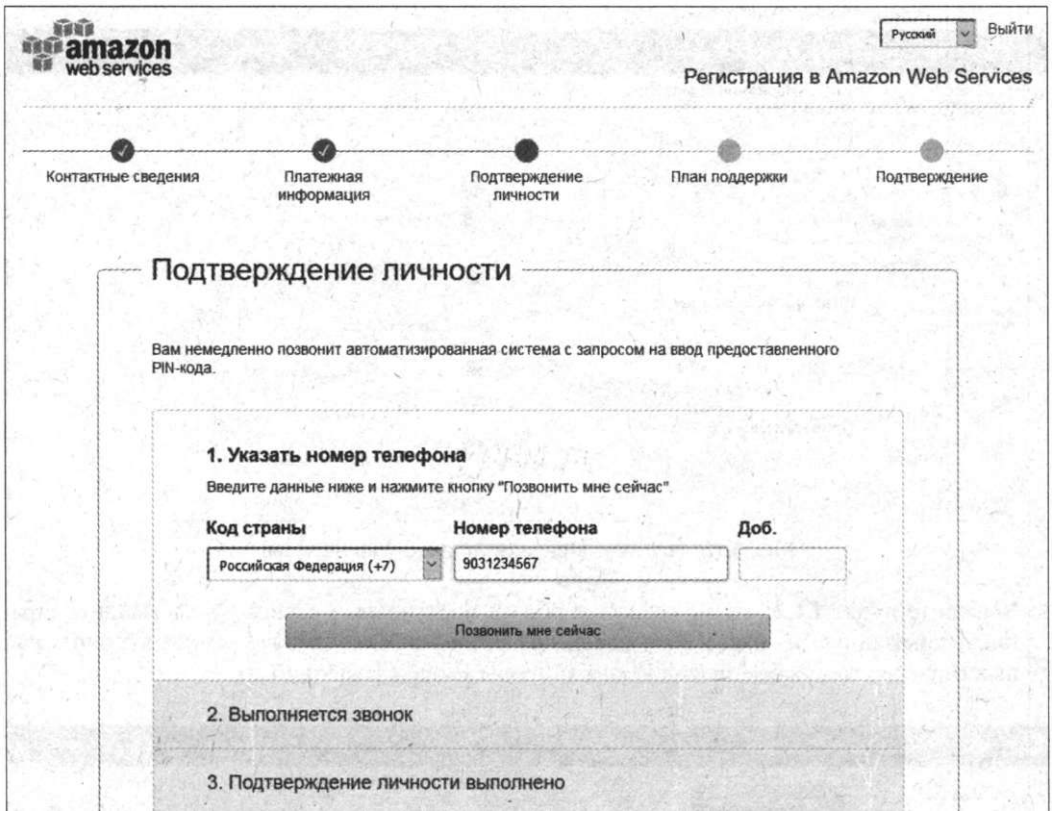


Рис. 9.11. Ввод контактных сведений при создании аккаунта AWS

11. Нажмите кнопку Продолжить (Continue), чтобы отобразить страницу, предназначенную для выбора плана поддержки.

12. Оставьте переключатель в положении, установленном по умолчанию: Базовый (Бесплатно) (Basic (Free) и нажмите кнопку Продолжить (Continue) — вы увидите страницу с благодарностью за создание аккаунта AWS.

Через некоторое время вы получите по электронной почте уведомление, что ваш аккаунт активирован (Your AWS Account is Ready). Теперь вы можете пользоваться возможностями службы AWS.

Создание виртуального сервера

Для настройки SSH-туннеля выполните следующие действия:

1. Перейдите по адресу aws.amazon.com/ru/ и нажмите кнопку Вход в консоль (Sign in to the Console).
2. На открывшейся странице введите свой адрес электронной почты (или номер телефона) и пароль, а затем нажмите кнопку Войти в систему через безопасный сервер (Sign in using our secure server). Вы увидите страницу со множеством служб, которые доступны вам как владельцу аккаунта AWS (на рис. 9.12 показан фрагмент этой страницы).

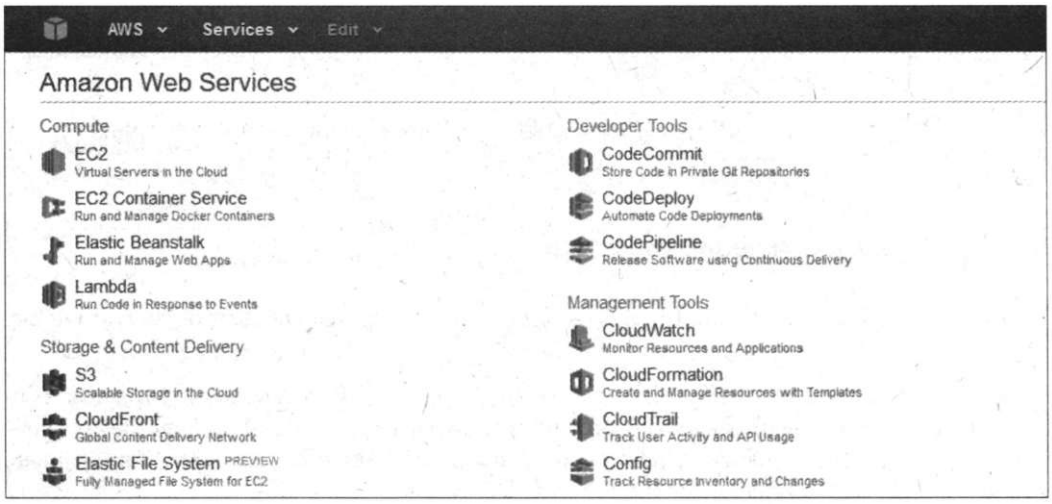


Рис. 9.12. Фрагмент страницы Amazon Web Services

3. Выберите пункт EC2, чтобы создать в облаке виртуальный сервер, — вы увидите страницу, показанную на рис. 9.13 и предназначенную для создания экземпляров виртуальных серверов в службе Amazon Elastic Compute Cloud (Amazon EC2).



Рис. 9.13. Фрагмент страницы службы Amazon EC2

4. Нажмите кнопку Launch instance (Запустить экземпляр) — откроется страница, предназначенная для выбора операционной системы, под управлением которой будет работать сервер (рис. 9.14).

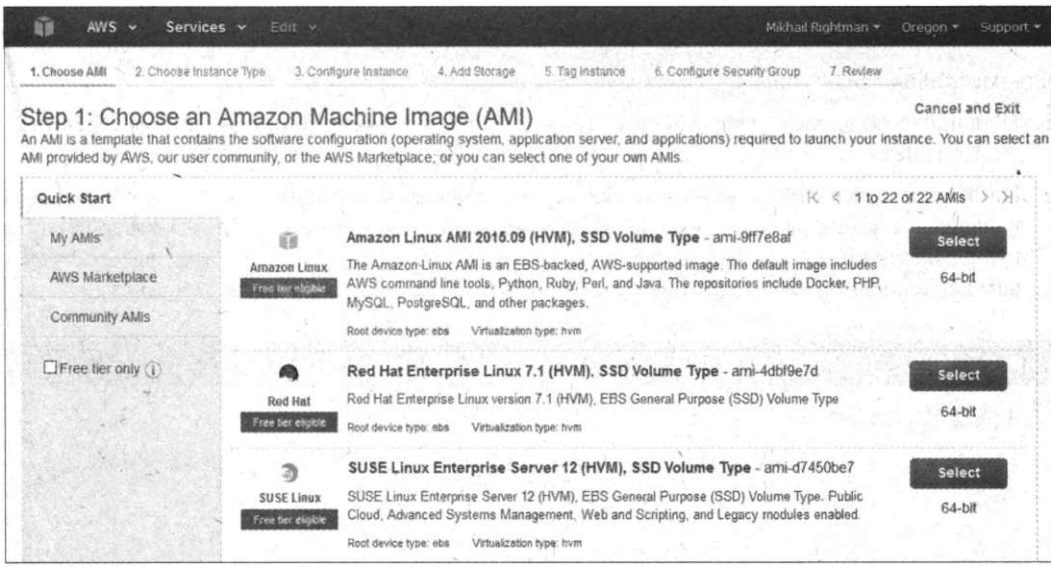


Рис. 9.14. Выбор операционной системы виртуального сервера

5. Выберите операционную систему (например, Ubuntu), нажав соответствующую кнопку Select (Выбрать).
6. На открывшейся странице (рис. 9.15) выберите пункт Micro instances (Микроэкземпляры) в раскрывающемся списке Filter by (Фильтровать по), чтобы отфильтровать список доступных типов экземпляров и отобразить только микроэкземпляры. Как правило, список сократится до одного пункта.

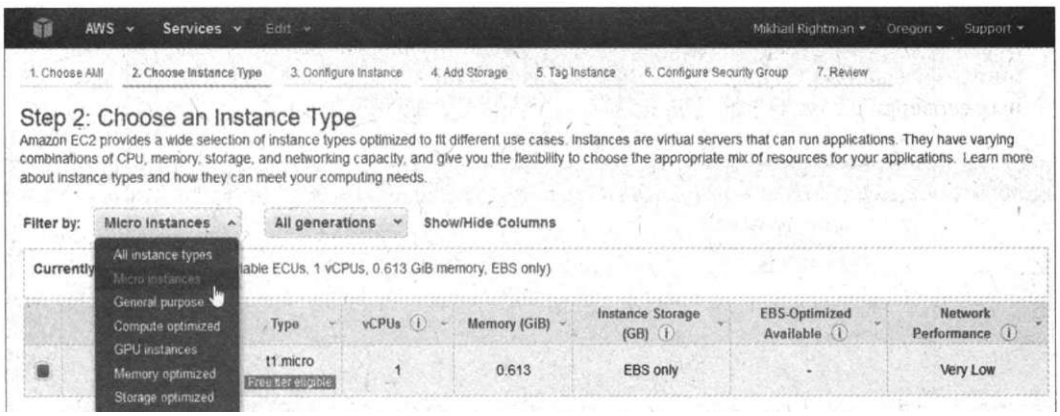


Рис. 9.15. Выбор типа экземпляра виртуального сервера

7. Выбрав тип экземпляра виртуального сервера, нажмите кнопку Review and Launch (Проверить и запустить) — вы перейдете сразу к шагу под номером 7, отображающему страницу со сводной информацией об экземпляре виртуального сервера (рис. 9.16).
8. Нажмите кнопку Launch (Запустить) — вы увидите окно (рис. 9.17), предназначенное для выбора существующих и создания новых пар ключей.

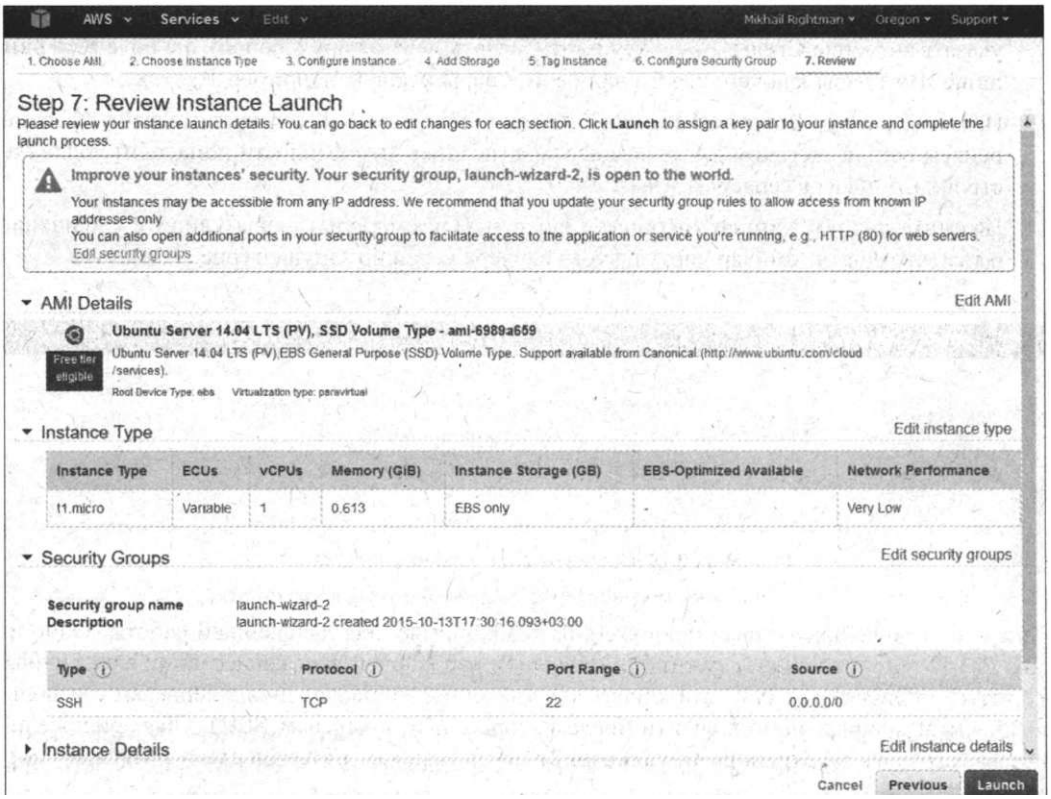


Рис. 9.16. Сводная информация об экземпляре виртуального сервера

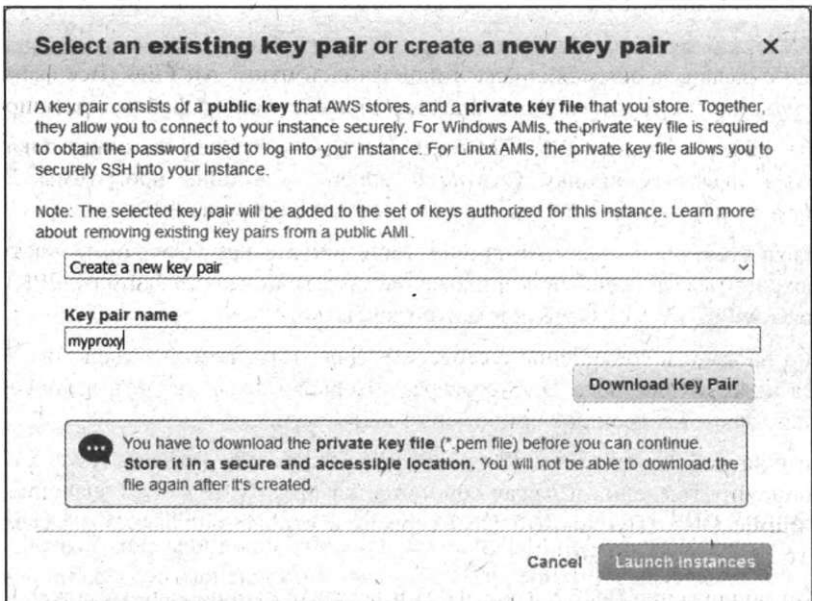


Рис. 9.17. **Окно управления парами ключей**

9. Если вы не создавали ранее пару ключей, в верхнем раскрывающемся списке следует указать значение Create a new key pair (Создать новую пару ключей), а в поле Key pair name (Имя пары ключей) ввести любое имя пары ключей, например `щуrгоху`.
10. Нажмите кнопку Download Key Pair (Скачать пару ключей) и сохраните файл с расширением pern на жестком диске компьютера (позднее этот файл нам понадобится для настройки туннеля с сервером Amazon).
11. Нажмите кнопку Launch Instances (Запустить экземпляры) — вы увидите сообщение о том, что ваш экземпляр виртуального сервера успешно запущен (рис. 9.18).

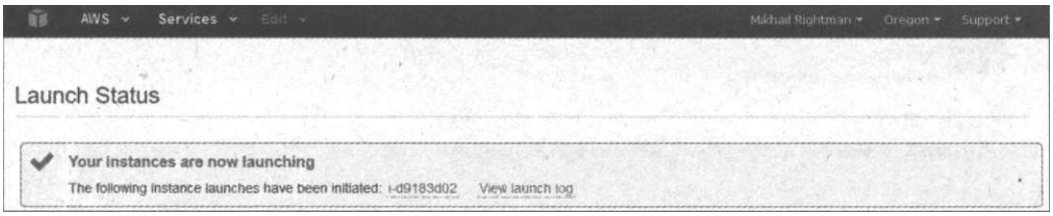


Рис. 9.18. Сообщение о состоянии запуска

Теперь нам понадобится пара приложений, необходимых для дальнейшей работы. Одно из них, PuTTY Key Generator, служит для генерации пар ключей и их конвертации в различные форматы. Второе, PuTTY, — это клиент для удаленного подключения к серверам с использованием различных протоколов (в числе которых и нужный нам SSH). Оба приложения можно загрузить на странице tinyurl.com/2r4w по ссылкам puttygen.exe и putty.exe соответственно.

Загрузив указанные приложения, выполните следующие действия:

1. Запустите приложение Putty Key Generator и нажмите в его окне (рис. 9.19) кнопку Load (Загрузить).
2. Выберите в раскрывающемся списке типов файлов пункт All Files (Все файлы), т. к. по умолчанию окно загрузки частного ключа отображает только файлы с расширением ppk.
3. Выберите ранее сохраненный PEM-файл (он был сохранен из окна, показанного на рис. 9.17) и нажмите кнопку Открыть (Open) — в окне программы PuTTY Key Generator вы увидите сведения о загруженном ключе (см. рис. 9.19).
4. Не изменяя настройки, нажмите кнопку Save private key (Сохранить частный ключ), чтобы сохранить загруженный в приложение закрытый ключ в формате PPK. После этого программу PuTTY Key Generator можно закрыть.

Далее нужно настроить соединение с сервером. Для этого, помимо закрытого PPK-ключа, понадобится адрес публичного DNS-сервера, который можно увидеть в консоли AWS, и выполнить кое-какие настройки в приложении и браузере.

1. Перейдите на вкладку Instances (Экземпляры) на странице консоли AWS в окне браузера и скопируйте (выделив и нажав сочетание клавиш <Ctrl>+<C>) значение, указанное в поле Public DNS (Публичный DNS-сервер) в строке запущенного экземпляра виртуального сервера (рис. 9.20).
2. Запустите приложение PuTTY (рис. 9.21) и вставьте скопированный адрес в поле Host Name (Имя хоста). Остальные настройки оставьте без изменений.



Рис. 9.19. Интерфейс утилиты PuTTY Key Generator

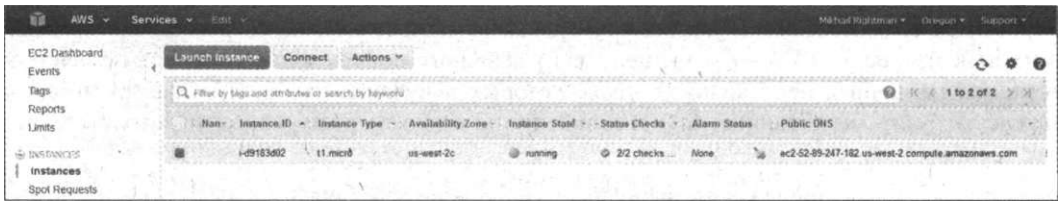


Рис. 9.20. Просмотр DNS-адреса запущенного экземпляра виртуального сервера

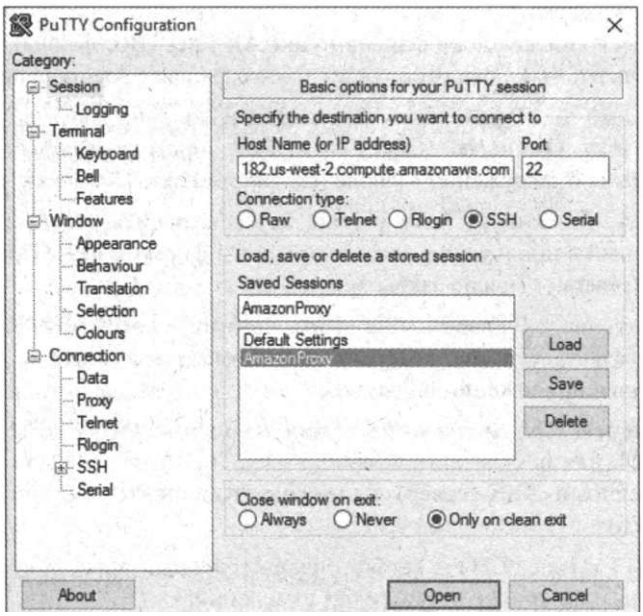


Рис. 9.21. Ввод IP-адреса в приложении PuTTY

3. Перейдите на вкладку SSH | Auth (SSH | Авторизация) и, нажав кнопку Browse (Обзор), выберите и загрузите в PuTTY ранее сохраненный файл закрытого ключа в формате PPK (рис. 9.22, *слева).*

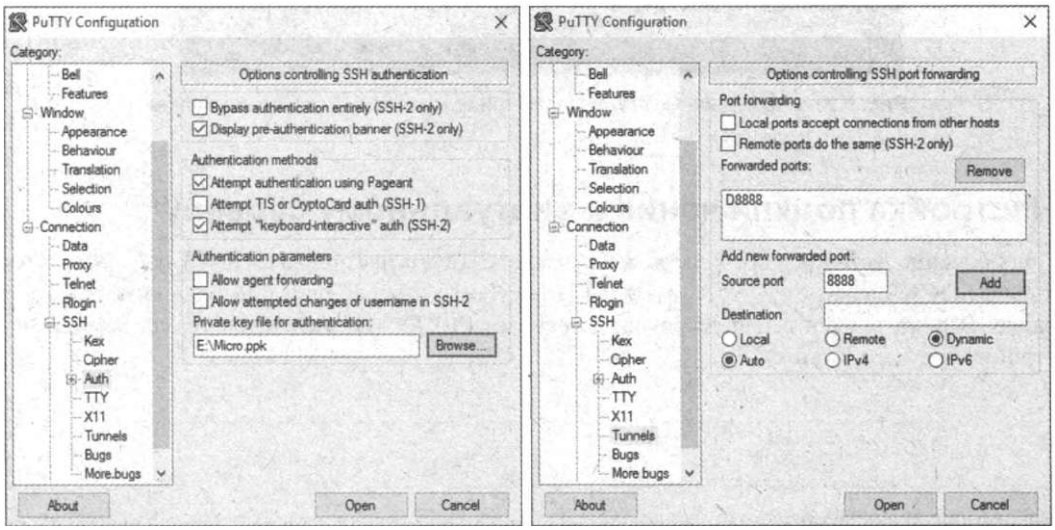


Рис. 9.22. PuTTY: указание пути к PPK-ключу (слева) и настройка порта перенаправления (*справа)*

4. Перейдите на вкладку SSH | Tunnels (SSH | Туннели).
5. В поле Source port (Исходный порт) укажите значение любого свободного порта, к которому будет обращаться браузер, — например, 8888.
6. Установите переключатель в положение Dynamic (Динамичный) и нажмите кнопку Add (Добавить) — в поле Forwarded ports (Порты перенаправления) появится значение выбранного порта (рис. 9.22, *справа).*

> ***СОХРАНЕНИЕ НАСТРОЕК В PUTTY***
>
> **Вы можете сохранить настройки PuTTY в качестве сессии, чтобы не указывать их каждый раз вновь, перейдя на вкладку Session (Сессия) окна этой программы, введя название сессии в поле Saved Session (Сохраненные сессии) и нажав кнопку Save (Сохранить). В дальнейшем, вместо ввода адреса сервера вручную, вы сможете выбрать название сессии и нажать кнопку Load (Загрузить) для загрузки настроек.**

7. Нажмите кнопку Open (Открыть) — при первом запуске с данным ключом появится запрос на запись ключа в реестр. Подтвердите запрос, нажав кнопку Да (Yes) — вы увидите окно командной строки, приглашающее к авторизации (строка Login as:).
8. Введите имя пользователя для авторизации. Это может быть имя `root`, `ec2-user` или любое другое, зарегистрированное на сервере, экземпляр которого вы запустили. В случае, если требуется использовать какое-либо определенное имя, система оповестит вас об этом, например, так:

```
Please login as the user "Ubuntu" rather the user "root"
```

(Пожалуйста, авторизуйтесь под именем `user`, а не `root`).

9. В случае успешной авторизации вы увидите в окне сообщение об успешной авторизации с открытым ключом и некоторую другую информацию (рис. 9.23).

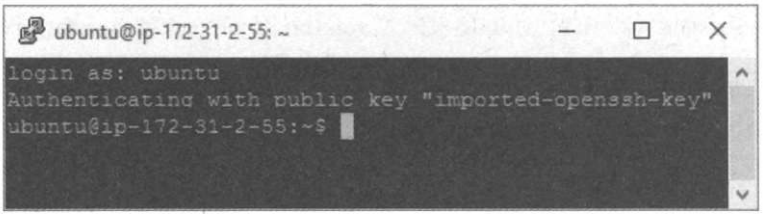


Рис. 9.23. Сообщение PuTTY об успешной авторизации с открытым ключом

Настройка подключения к виртуальному серверу

Подключение установлено, теперь в браузере следует настроить SOCKS-прокси, указав в поле SOCKS адрес 127. о. о. i, а в поле Порт (Port) — адрес порта, выбранного на шаге 5 ранее. В роли прокси в нашем случае выступает PuTTY (на рис. 9.24 показан пример настройки браузера Firefox).

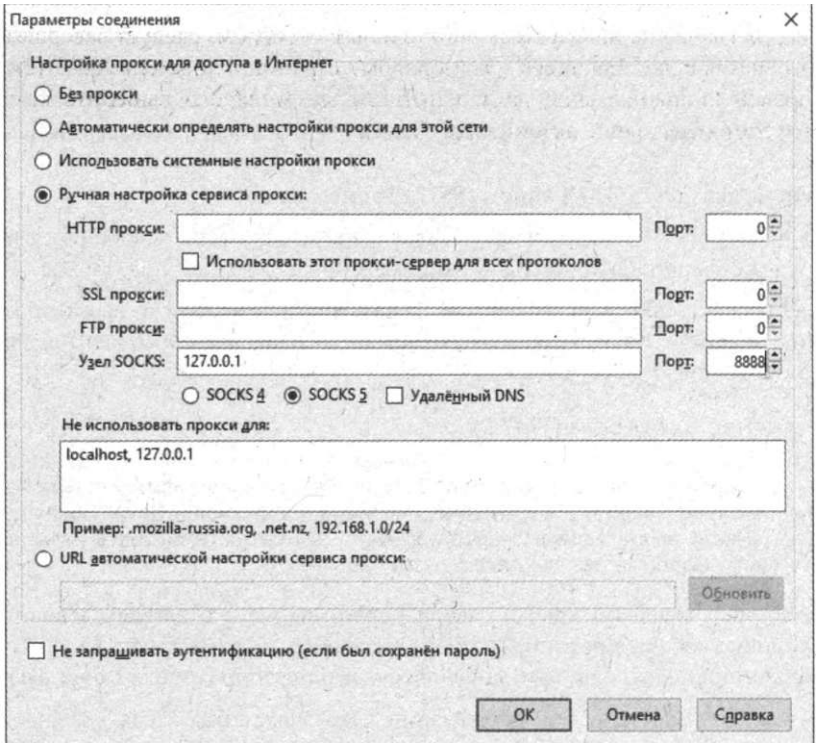


Рис. 9.24. Настройка в браузере Firefox доступа через PuTTY-прокси

Теперь попробуйте перейти на заблокированный сайт или сервис, определяющий ваше местонахождение, например, **2ip.ru** (рис. 9.25).

Как можно видеть, настройка SSH-туннеля к серверу Amazon успешно завершена. Тем не менее, важно помнить, что этот способ не обеспечивает анонимности при веб-серфинге.

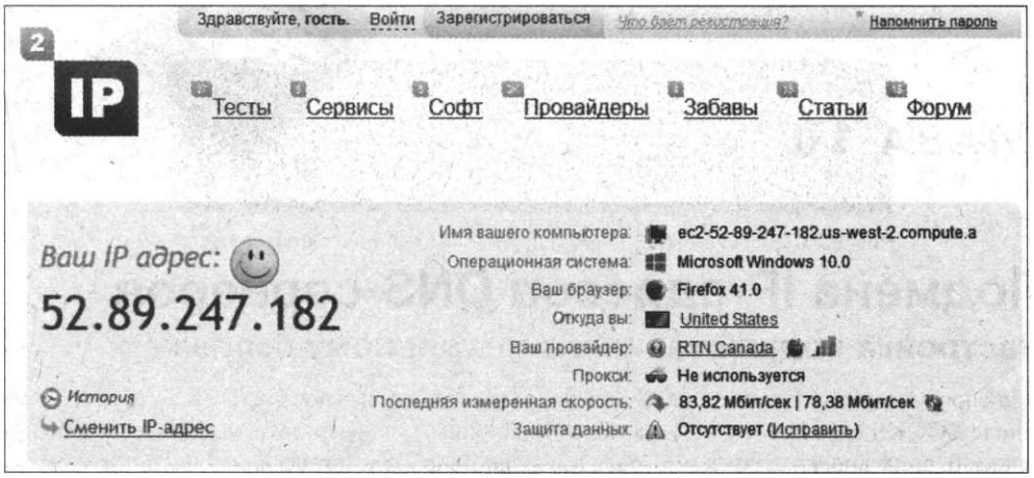


Рис. 9.25. Настройка SSH-туннеля к серверу Amazon успешно завершена

В тех случаях, когда вы не пользуетесь виртуальным сервером, следует завершать его работу. Для этого на вкладке Instances (Экземпляры) страницы консоли AWS (см. рис. 9.20) щелкните правой кнопкой мыши на запущенном экземпляре и выберите команду меню Instant State | Stop (Состояние экземпляра | Стоп).

ГЛАВА 10

Подмена IP-адресов DNS-серверов

Подмена IP-адресов DNS-серверов в операционной системе Windows
Подмена IP-адресов DNS-серверов в операционной системе OS X
Подмена IP-адресов DNS-серверов в операционной системе iOS
Подмена IP-адресов DNS-серверов в операционной системе Android
Подмена IP-адресов DNS-серверов на маршрутизаторе Zyxel Keenetic

Существует простой способ получения доступа к таким сайтам, как **Hulu.com,** без использования стороннего софта. Заключается он в указании подменных адресов DNS-сервера в настройках сетевого подключения.

В качестве примера ресурса, обспечивающего такую подмену, выберем сервис Tunlr, расположенный по адресу **tunlr.net** (аналогичным функционалом обладает сервис **unlocator.com** и ряд других).

> ***GOOGLE DNS***
>
> Вы также можете использовать IP-адреса бесплатных DNS-серверов Google: `8.8.8.8` и `8.8.4.4`. Для их установки в окне командной строки нужно выполнить команду:
>
> ```
> netsh interface ip set dns "Local Area Connection" static 8.8.8.8
> ```
>
> а затем:
>
> ```
> ipconfig /flushdns
> ```
>
> Подробная инструкция по использованию бесплатных DNS-серверов Google представлена по ссылке **tinyurl.com/chrvmwt.** Однако учтите, что Google перманентно сохраняет для анализа информацию о вашем провайдере и местоположении. Ваш IP-адрес также хранится у него в течение 24 часов. Чтобы избежать этого, вы можете воспользоваться услугами других DNS-провайдеров (см. **tinyurl.com/gnschwl).**

После регистрации (указания адреса электронной почты и пароля) и авторизации вы увидите страницу (рис. 10.1), предлагающую выбрать устройство, на котором следует настроить подмену IP-адресов DNS-серверов.

> ***РЕГИСТРАЦИЯ НА TUNLR***
>
> На главной странице сервиса следует ввести адрес электронной почты и желаемый пароль. Стоит отметить, что адреса не всех российских почтовых сервисов поддерживаются, поэтому при возникновении ошибок пробуйте другие почтовые сервисы — например, Gmail. После успешной авторизации и подтверждения адреса электронной почты сервис предло-

жит вам пригласить через социальную сеть друга, чтобы тот тоже воспользовался услугами сервиса. В последнем случае вы сможете пользоваться сервисом бесплатно.

Далее мы рассмотрим процесс настройки такой подмены на компьютерах под управлением операционных систем Windows и OS X, в устройствах на платформах Android и iOS, а также на наиболее популярном маршрутизаторе Zyxel Keenetic. Помимо этого, на сайте Tunlr доступны инструкции для игровых приставок PlayStation, Nintendo и Xbox, мультимедийных проигрывателей Apple TV и Roku, а также маршрутизаторов Apple, Netgear, Cisco и др.

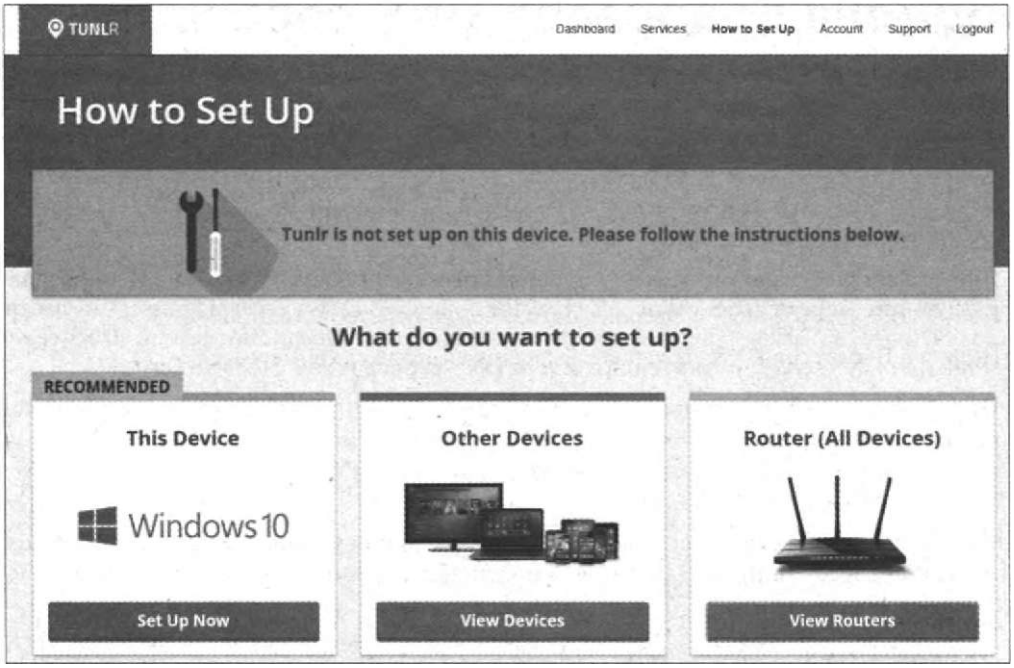


Рис. 10.1. Сервис **turilr.net**

УСТРОЙСТВА НА ПЛАТФОРМЕ WINDOWS PHONE 8

В устройствах на платформе Windows Phone 8 также есть поле ввода IP-адреса DNS-сервера, но оно затенено и недоступно для редактирования. Возможно, эта недоработка будет устранена в 10-й версии этой мобильной операционной системы.

IP-АДРЕСА

Если устройство требует ввода трех цифр после точки, добавляйте 0 к каждой группе цифр, — например: 045.033.081.176 вместо 45.33.81.176.

Прежде чем приступить к настройке, запишите на случай необходимости отката текущие адреса DNS-серверов (как правило, устройства настроены на автоматическое получение адресов DNS-серверов, но в некоторых случаях они указываются).

Сервис Tunlr поддерживает только определенный список сайтов и, в частности, Hulu. Для всех остальных запросов он будет работать как обычный DNS-сервер. В случае если по каким-то причинам подмена DNS-серверов не работает, посетите страницу со сведениями по решению проблем по адресу **tinyurl.com/osgnc5t.**

Подмена IP-адресов DNS-серверов в операционной системе Windows

Записав на всякий случай текущие адреса DNS-серверов, приступим к настройке их подмены:

1. Щелкните правой кнопкой мыши на значке сетевого подключения в области уведомлений (локальной сети или беспроводной, не важно) и выберите в контекстном меню команду Центр управления сетями и общим доступом (Network and Sharing Center).
2. В левой части открывшегося окна щелкните мышью на ссылке Изменение параметров адаптера (Change adapter settings).
3. Щелкните правой кнопкой мыши на активном подключении и выберите пункт Свойства (Properties).
4. В открывшемся диалоговом окне сбросьте флажок IP версии 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6)).
5. Выберите пункт IP версии 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4)) и нажмите кнопку Свойства (Properties).
6. В открывшемся диалоговом окне установите переключатель в положение Использовать следующие адреса DNS-серверов (Use the following DNS server addresses) и укажите полученные на сайте Tunlr IP-адреса в полях ввода Предпочитаемый DNS-сервер (Preferred DNS server) и Альтернативный DNS-сервер (Alternate DNS server).
7. Перезапустите сетевое подключение (последовательность перечисленных шагов показана на рис. 10.2).

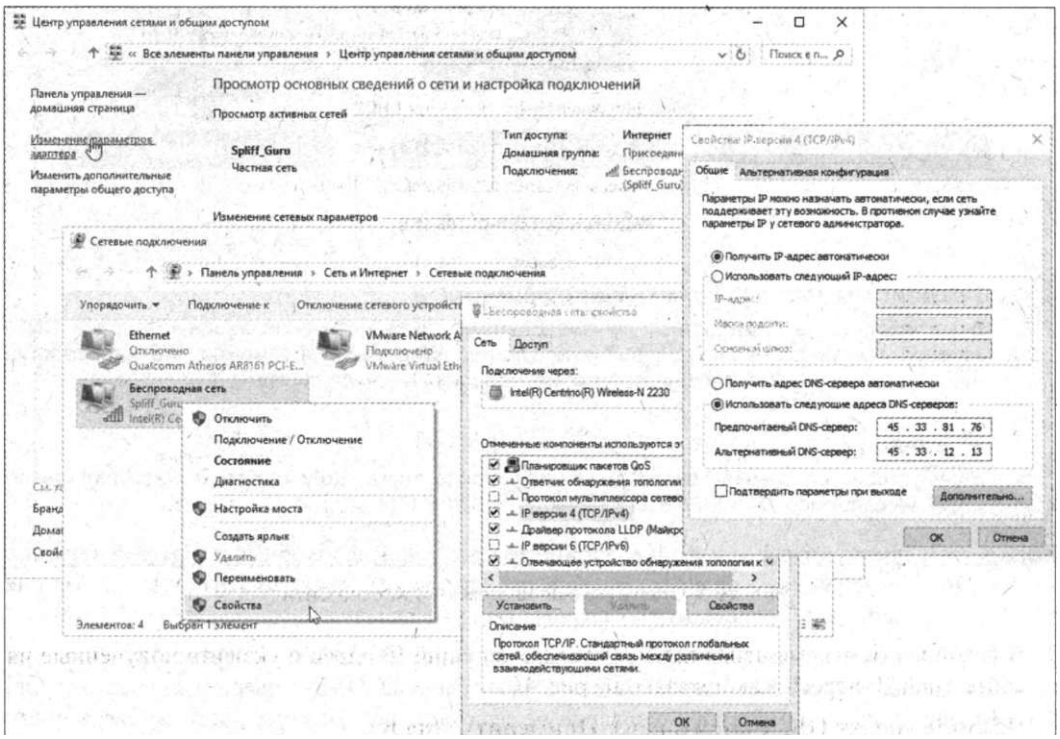


Рис. 10.2. Указание IP-адресов DNS-серверов в операционной системе Windows 10

После этого подключение будет осуществляться через серверы компании Тип1г.

Как уже отмечалось, сервис поддерживает только определенный список сайтов и, в частности, Ни1и. Для всех остальных запросов он будет работать как обычный DNS-сервер. В случае если по каким-то причинам подмена DNS-серверов не работает, посетите страницу со сведениями по решению проблем по адресу **tinyurl.com/osgnc5t.**

Подмена IP-адресов DNS-серверов в операционной системе OS X

Прежде чем приступить к настройке, запишите текущие адреса DNS-сервера на случай от-

1. Выберите команду меню | **Системные настройки** (| System preferences), а затем щелкните мышью на разделе настроек **Сеть** (Network).
2. Щелкните мышью на активном подключении в левой части окна, а затем нажмите кнопку **Дополнительно** (Advanced) (рис. 10.3).

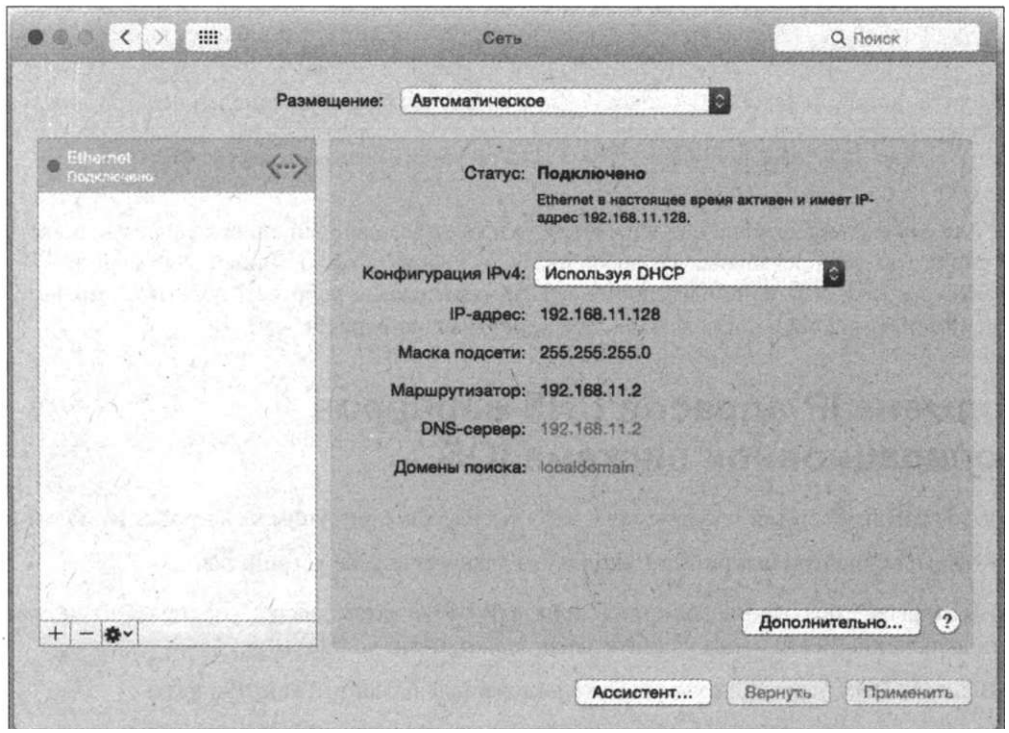


Рис. 10.3. Операционная система OS X: окно Сеть

3. В левой части открывшейся панели удалите текущий IP-адрес и укажите полученные на сайте Tunlr IP-адреса, как показано на рис. **10.4.**
4. Нажмите кнопку **ОК,** а затем кнопку **Применить** (Apply).

После этого подключение будет осуществляться через серверы компании Tunlr.

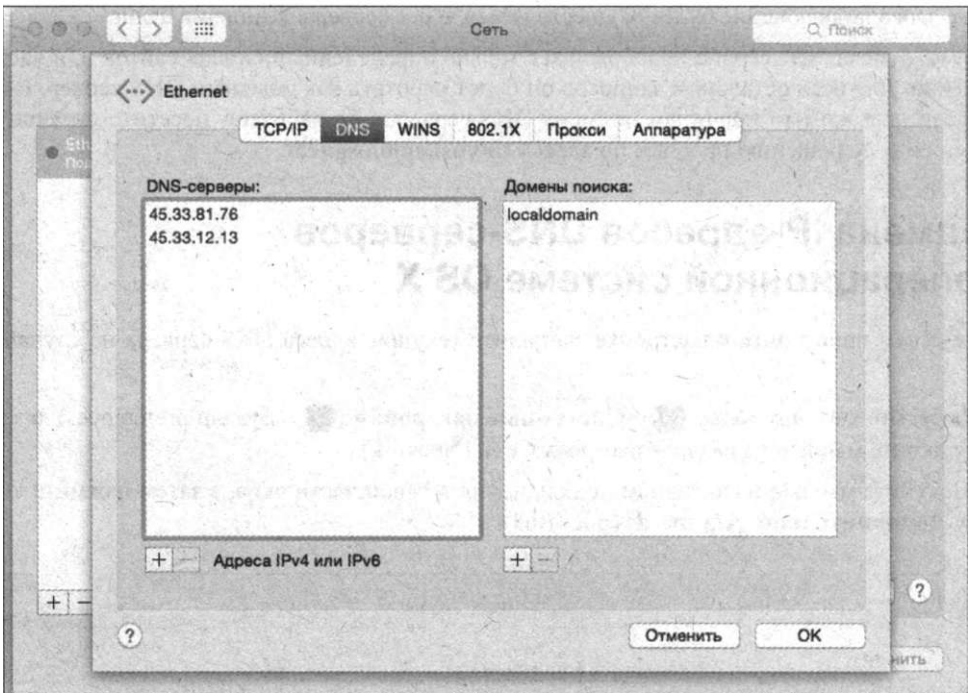


Рис. 10.4. Указаны новые IP-адреса DNS-серверов в операционной системе OS X

Как уже отмечалось, сервис поддерживает только определенный список сайтов и, в частности, Hulu. Для всех остальных запросов он будет работать как обычный DNS-сервер. В случае если по каким-то причинам подмена DNS-серверов не работает, посетите страницу со сведениями по решению проблем по адресу **tinyurI.com/osgnc5t.**

Подмена IP-адресов DNS-серверов в операционной системе iOS

Записав на всякий случай текущие адреса DNS-серверов, приступим к настройке их подмены:

1. Коснитесь значка **Настройки** (Settings) на главном экране устройства.
2. На открывшемся экране коснитесь пункта **Wi-Fi,** а затем значка справа от названия подключенной сети — вы увидите экран, показанный на рис. 10.5.
3. В строке **DNS** через запятую укажите полученные на сайте Tunlr IP-адреса.
4. Коснитесь пункта **Wi-Fi,** чтобы сохранить настройки.

После этого подключение будет осуществляться через серверы компании Tunlr.

Как уже отмечалось, сервис поддерживает только определенный список сайтов и, в частности, Hulu. Для всех остальных запросов он будет работать как обычный DNS-сервер. В случае если по каким-то причинам подмена DNS-серверов не работает, посетите страницу со сведениями по решению проблем по адресу **tinyurl.com/osgnc5t.**

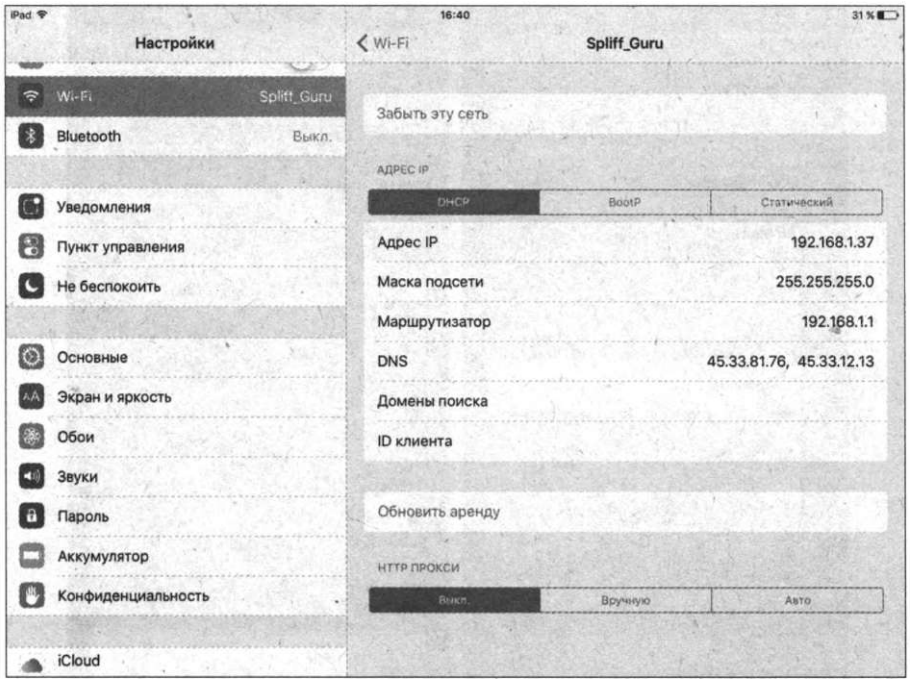


Рис. 10.5. Указаны новые IP-адреса DNS-серверов в операционной системе iOS

Подмена IP-адресов DNS-серверов в операционной системе Android

Записав на всякий случай текущие адреса DNS-серверов, приступим к настройке их подмены:

1. Откройте экран Настройки (Settings).
2. В разделе Беспроводные средства и сети (Wireless & networks) коснитесь пункта Wi-Fi.
3. Коснитесь и удерживайте название нужной сети Wi-Fi.
4. Выберите пункт Изменить сеть (Modify network).
5. Установите флажок Показать дополнительные параметры (Show advanced options).
6. Среди появившихся элементов управления найдите раскрывающийся список Настройка IP (IP settings) и выберите в нем пункт Статический (Static) (рис. 10.6, *слева).*
7. Найдите элементы управления. DNS 1 и DNS 2. В поле DNS 1 введите первый IP-адрес DNS-сервера, полученный на сайте Tunlr, а в поле DNS 2 — второй (рис. 10.6, *справа).*
8. Прежде чем вы сможете сохранить настройки, нужно заполнить поле IP-адрес (IP address). Можно указать тот же адрес, что указан серым цветом, — просто введите его заново. После этого коснитесь кнопки Сохранить (Save).

Теперь подключение будет осуществляться через серверы компании Tunlr.

Как уже отмечалось, сервис поддерживает только определенный список сайтов и, в частности, Hulu. Для всех остальных запросов он будет работать как обычный DNS-сервер.

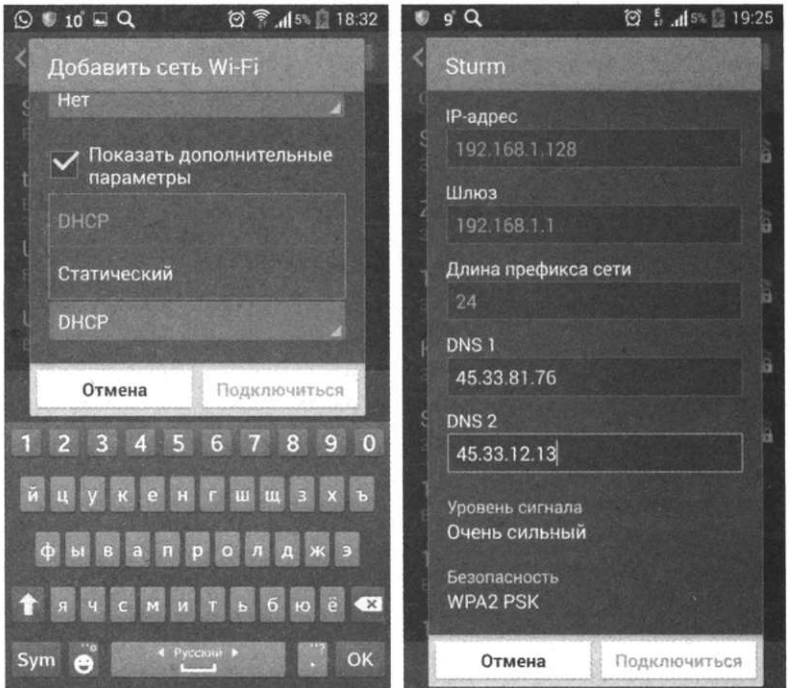


Рис. 10.6. Установка статичного IP-адреса *(слева)* **и ввод новых IP-адресов DNS-серверов** *(справа)*

В случае если по каким-то причинам подмена DNS-серверов не работает, посетите страницу со сведениями по решению проблем по адресу tinyurl.com/osgnc5t.

Подмена IP-адресов DNS-серверов на маршрутизаторе Zyxel Keenetic

Подмену IP-адресов DNS-серверов на маршрутизаторах мы рассмотрим здесь на примере популярного маршрутизатора Zyxel Keenetic.

Прежде чем приступить к настройке, запишите текущие адреса DNS-сервера на случай отката (как правило, устройство настроено на автоматическое получение адресов DNS-сервера, но в некоторых случаях они указываются).

1. Откройте в браузере панель администратора маршрутизатора. Для этого в адресной строке браузера следует указать IP-адрес маршрутизатора, узнать который вы можете из руководства пользователя. Впрочем, иногда он приводится и на наклейке на корпусе устройства (там же указываются логин и пароль по умолчанию). В большинстве маршрутизаторов панели администратора присваиваются IP-адреса 192.168.0.1, 192.168.1.1 или 192.168.2.1.
2. Введите логин и пароль для доступа к панели администратора.
3. Перейдите на вкладку Интернет (Internet) и щелкните мышью на строке, соответствующей подключению к вашему провайдеру. Для провайдера Дом.ги, к примеру, это соединение PPPoE.
4. Укажите полученные на сайте Tunlr IP-адреса в полях ввода DNS 1 и DNS 2 (рис. 10.7).

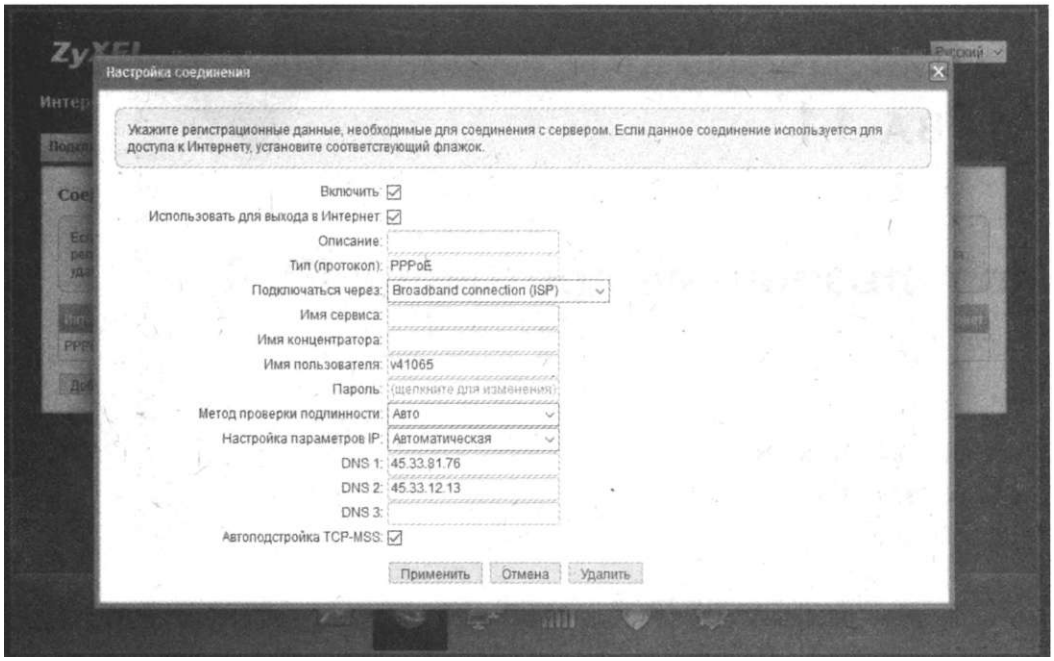


Рис. 10.7. Добавление IP-адресов подменных DNS-серверов в настройках Маршрутизатора

5. Нажмите кнопку Применить (Apply).
6. Перезапустите маршрутизатор.

После этого подключение будет осуществляться через серверы компании Tunlr.

Как уже отмечалось ранее, сервис поддерживает только определенный список сайтов и, в частности, Hulu. Для всех остальных запросов он будет работать как обычный DNS-сервер. В случае если по каким-то причинам подмена DNS-серверов не работает, посетите страницу со сведениями по решению проблем по адресу tinyurl.com/osgnc5t.

ГЛАВА 11

Использование протокола IPv6

Основы IPv4, IPv6 И NAT

Настройка протокола IPv6/Teredo

Использование туннельных брокеров

Использование протокола 1PУ6 также позволяет обойти ограничения при посещении сайтов типа Hulu.com путем проброски любого трафика через IPv6-туннель. К примеру, в корпоративной сети может быть заблокирован какой-либо определенный тип трафика (например, BitToггent), но IPv6 при этом пропускается. После подключения IPv6 ВЫ сможете скачивать торренты, и администратору обнаружить нежелательный трафик в такой ситуации очень сложно. Но прежде чем перейти к настройке протокола IPv6, рассмотрим немного теории.

Основы IPv4, IPv6 и NAT

Как вы, возможно, знаете, каждому сетевому устройству присваиваются IP-адреса. Протокол IPv4, на основе которого изначально осуществлялось и до сих пор осуществляется объединение отдельных устройств в компьютерные сети, а последних — в сеть Интернет, и одной из задач которого является адресация в сети (присваивание IP-адресов ее узлам), исчерпал запасы нераспределенных IP-адресов. В протоколе IP 4-й версии IP-адрес представляет собой 32-битовое число, обычно записываемое в виде разделенных точками четырех десятичных чисел со значением от 0 до 255, — например, 192.168.0.3. Адресное пространство IPv4 ограничивается примерно 4,3 млрд адресов (2^{32}), и с учетом того, что IP-адреса присваиваются каждому сетевому устройству, практически все они уже задействованы.

Чтобы решить проблему нехватки сетевых адресов, в сетях TCP/IP (стек сетевых протоколов передачи данных, используемых в сетях, включая Интернет) в 1994 году был реализован механизм NAT (от англ. Network Address Translation, преобразование сетевых адресов), позволяющий преобразовывать IP-адреса транзитных пакетов. Этот механизм сейчас и обеспечивает подключение к Интернету вашей и других локальных сетей. Как уже упоминалось, IPv4 ограничен примерно 4,3 млрд адресов — даже если бы у каждого жителя планеты был всего один компьютер, адресов бы уже не хватило (что и говорить обо всех остальных сетевых устройствах). Тут и выходит на сцену NAT. По большому счету, этот механизм подменяет *локальный* («серый», приватный — используемый в вашей и любой другой домашней или корпоративной сети) адрес устройства, — например, 192.168.1.1, на

глобальный («белый», публичный — используемый в глобальной сети, Интернете), — например, 176.15.1.1.

Принимая пакет от локального компьютера (имеющего, например, адрес 192.168.1.1), маршрутизатор анализирует IP-адрес назначения. И если это локальный адрес (например, 192.168.1.2), то пакет пересылается локальному компьютеру с соответствующим адресом в вашей сети. А если— нет (например, 176.15.1.10), то пакет следует переслать наружу, в Интернет. Если попытаться отправить с локального адреса запрос к веб-серверу, находящемуся в Интернете, то сам запрос теоретически дойдет, т. к. веб-сервер имеет глобальный адрес, а вот ответ от сервера не вернется, поскольку обратный адрес, на который этот ответ надо слать, — локальный. Поэтому маршрутизатор «на лету» транслирует (подменяет) обратный IP-адрес (192.168.1.1) пакета на свой внешний, видимый из Интернета, IP-адрес (например, 176.15.1.1) и меняет номер порта (чтобы различать ответные пакеты, адресованные разным локальным компьютерам). Теперь у пакета и адрес отправителя, и адрес получателя — глобальные, и всему Интернету кажется, что именно маршрутизатор отправил этот пакет, поэтому и ответные пакеты отправляются на адрес этого же маршрутизатора. Маршрутизатор же имеет именно тот единственный глобальный IP-адрес, который дал ему провайдер при подключении его к Интернету.

При попадании на маршрутизатор из Интернета обратного пакета система NAT понимает, что хоть адресом назначения и является адрес маршрутизатора, на самом деле пакет предназначается локальному компьютеру. Тогда на этом пакете адрес назначения меняется на внутренний приватный адрес (например, 192.168.1.1) в вашей локальной сети, и маршрутизатор передает его соответствующему локальному компьютеру. Чтобы обеспечить точную внутреннюю адресацию, система NAT запоминает, какой из компьютеров локальной сети инициализировал подключение, и по таблицам подключений возвращает обратные пакеты.-

В качестве локальных в IPv4 выделены следующие адреса:

- 10.0.0.0— 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

Одним из существенных недостатков системы NAT является снижение производительности сети из-за дополнительных действий на маршрутизаторе, связанных с необходимостью трансляции (подмены) адресов. Возникают проблемы и с работой некоторых протоколов, а также сложности при организации туннелей и входящих соединений извне. Огорчает и то, что устройство с локальным адресом не может полноценно работать в сети, — на компьютере с локальным адресом нельзя организовать сервер и напрямую обмениваться файлами и т. п. Многие провайдеры предлагают возможность использования на локальном компьютере глобального адреса, но, как правило, за это взимается отдельная плата (рис. 11.1).

Проблемы ограничения адресного пространства и трансляции адресов призван решить протокол IPv6. В нем используются 128-битовые числа (вместо 32-битовых в IPv4) и отображаются они в виде восьми групп по четыре шестнадцатеричных символа, разделенных двоеточием: 2001:0db8:lla3:09d7:lf34:8a2e:07a0:765d. Количество допустимых адресов IPv6 в 10^{28} раз превышает количество адресов IPv4[1].

Когда адресное пространство в IPv4 закончится (по разным расчетам это произойдет в 2017 году), два стека протоколов — IPv6 и IPv4 — станут использоваться параллельно, с постепенным увеличением доли IPv6. Такая ситуация допускается из-за наличия в эксплуатации

[1] По ссылке tinyurl.com/n46jkn5 вы найдете подробное сравнение этих двух версий протокола 1P.

огромного количества устройств, в том числе устаревших, не поддерживающих IPv6 и требующих специального преобразования для работы с устройствами, использующими только IPv6.

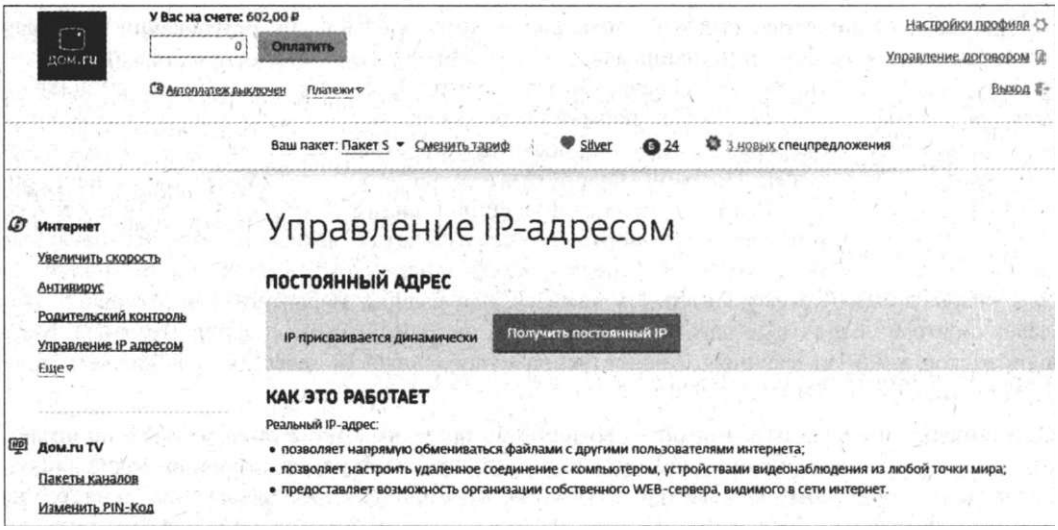


Рис. 11.1. Услуга подключения глобального IP-адреса на странице провайдера Дом.ru

В настоящее время протокол IPv6 только начинает использоваться, и трафик по нему составляет не более нескольких процентов от всего сетевого трафика. Тем не менее, существуют узлы, которые уже сейчас можно посещать с использованием протокола IPv6, и в плане рассматриваемых в этой книге тем соединение по протоколу IPv6 может быть задействовано для посещения по альтернативным **IPv6**-адресам сайтов, заблокированных в вашей организации.

Провайдеры постепенно начинают осуществлять поддержку протокола IPv6, допуская его активацию в личном кабинете пользователя. Как правило, никаких дополнительных настроек для этого производить не требуется — современные операционные системы готовы к использованию протокола. Уточнить наличие поддержки, настроить (при необходимости) и активировать протокол можно на сайте вашего провайдера.

В случае же, если провайдер не предоставляет поддержку протокола IPv6, вам придется настроить сетевой протокол Teredo, предназначенный для передачи пакетов IPv6 через сети IPv4. Подробнее о Teredo можно узнать по ссылке tinyurl.com/pnjocp9.

> ***ПРОТОКОЛ TEREDO***
>
> **Описанный здесь способ настройки IPv6/Teredo не обеспечивает полноценную работу на компьютере протокола IPv6. Teredo рекомендуется задействовать лишь в том случае, если с его помощью планируется только посещение IPv6-сайтов и загрузка торрентов (использование Teredo позволит добавить как новых сидов, так и повысить рейтинг для трекеров с учетом статистики).**

Существует несколько способов настроить на компьютере протокол IPv6:

- осуществить прямое подключение по протоколу IPv6 через провайдера, официально предоставляющего IPv6-доступ. К таким относятся Дом.ру, МГТС, Ростелеком и некоторые другие (при этом доступ предоставляется не во всех городах). Полный список провайдеров, предоставляющих **IPv6**-доступ, вы найдете на странице tinyurl.com/jech57b;

- использовать выделенный или виртуальный сервер — этот способ достаточно сложный и требует финансовых затрат: абонентскую плату за предоставление VPS и т. п. (см. например, сайт vstoike.ru);
- задействовать механизм 6to4, позволяющий передавать [**IPv6-**пакеты через IPv4-сети. Для реализации этого способа требуется *глобальный* (белый) статический IP-адрес! Такую услугу за дополнительную абонентскую плату можно получить у провайдера;
- реализовать IPvö-туннель, настроив должным образом протокол IPv6/Teredo,— этот способ описан далее. Можно воспользоваться как готовым BAT-файлом (создан под русскую версию Windows 7/8 и прекрасно работает в Windows 10), так и выполнить настройки самостоятельно (необходима профессиональная версия Windows). В Linux используется протокол Miredo — аналог протокола Teredo (см. инструкцию на сайте tinyurl.com/zszg4je);
- использовать туннельного брокера — этот способ также описан далее.

Настройка протокола IPv6/Teredo

Суть работы протокола Teredo — в передаче **IPv6-**пакетов через **IPv**4-сети путем их инкапсуляции в UDP-дейтаграммы и передачи их через устройства, использующие NAT. Технология была разработана корпорацией Microsoft и очень проста в настройке.

Если вы пользуетесь программой ^Torrent, то можете прямо в ее настройках активировать поддержку IPv6/Teredo. Для этого в окне программы выберите команду меню Настройки | Настройки программы (Options | Preferences) и на вкладке Общие (General) нажмите кнопку Установить IPv6/Teredo (Install IPv6/Teredo) (рис. 11.2).

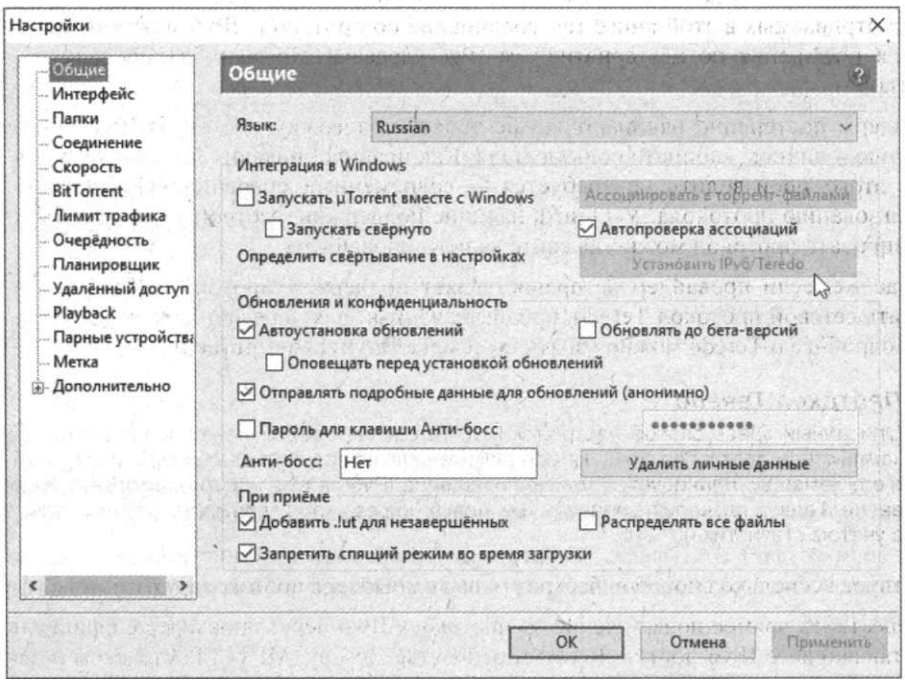


Рис. 11.2. Установка IPv6\Teredo в программе mTorrent

Не потребуется никаких регистрации — это работает, что называется, «из коробки». Все клиенты, подключенные к Интернету аналогичным образом, соединяются друг с другом напрямую (Teredo лишь помогает обойти ограничения NAT), практически отсутствуют и потери в скорости.

Следует все же отметить, что Teredo-aflpeca, по сравнению с прямым или 6to4-nofliuno-чением, каждый раз генерируются, исходя из текущего IP-адреса и используемого UDP-порта, т. е. являются *динамическими.* **Но хуже всего, что Teredo Может обойти не каждый NAT. И если после настройки IPv6-сайт — например, ipv6.google.com, не открывается, запустите командную строку[1] и введите команду:**

```
netsh int ipv6 show teredo
```

Если в ответ на эту команду появится сообщение: Ошибка: клиент за симметричным NAT — Teredo использовать нельзя. В таком случае остается последний (но не худший) вариант — использовать туннельного брокера (см. далее).

С помощью BAT-файла

Необходимый для активации протокола IPv6/Teredo BAT-файл вы можете скачать по адресу tinyurl.com/ngvhf8u. На случай, если сайт не будет доступен, далее приведено содержимое этого файла:

```
Pause
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Dnscache\Parameters /v
AddrConfigControl /t REG_DW0RD /d 0
timeout /T 3
se config iphlpsvc start= auto
net start iphlpsvc
timeout /T 10
netsh interface ipv6 reset
timeout /T 3
netsh interface ipv6 set dns "Подключение по локальной сети" static
2001:4860:4860::8888 primary validate= no
netsh interface isatap set state disabled
netsh interface 6to4 set state disabled
netsh interface teredo set state type=enterpriseclient servername=teredo.trex.fi
refreshinterval=default clientport=default
timeout /T 3
netsh int ipv6 delete route : :/0 Teredo
netsh int ipv6 add route : :/0 Teredo
timeout /T,3
ipconfig /flushdns
Pause
```

По необходимости, строку `"Подключение по локальной сети"` **нужно заменить на реальное название подключения на вашем компьютере (кодировка OEM 866).**

Скачав (или создав) BAT-файл, запустите его с правами администратора — щелкните по файлу правой кнопкой мыши и выберите команду Запуск от имени администратора (Run as Administrator).

[1] **Нажмите сочетание клавиш <Win>+<R>, введите** `cmd` **и нажмите кнопку ОК.**

Настройка вручную

Напомню, что этот способ подойдет только для профессиональных выпусков операционной системы Windows, поскольку в домашних версиях Windows компонент «Редактор локальной групповой политики» отсутствует.

Итак, если вы используете профессиональную (а также корпоративную или максимальную) версию Windows, сначала включите службу Вспомогательная служба IP (IP Helper) — если она выключена.

1. Откройте панель управления и запустите компонент Службы (Services) из папки Администрирование (Administration).
2. Щелкните правой кнопкой мыши по службе Вспомогательная служба IP (IP Helper) и выберите в контекстном меню пункт Свойства (Properties).
3. В раскрывающемся списке Тип запуска (Startup Type) выберите пункт Автоматически (Auto) и нажмите кнопку Запустить (Run) (рис. 11.3).

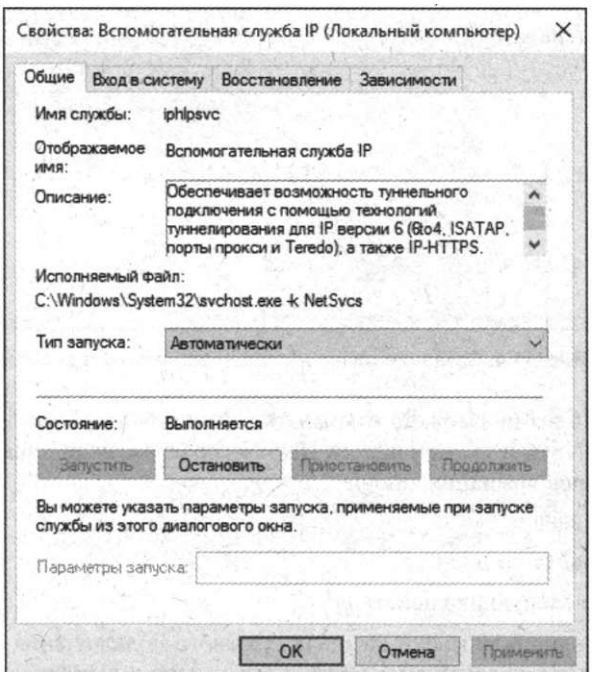


Рис. 11.3. Настройки службы Вспомогательная служба IP

4. Закройте диалоговое окно нажатием кнопки OK, а также окна папки Администрирование (Administration) и панели управления.

Далее нужно внести некоторые изменения в системный реестр:

1. Запустите редактор реестра, нажав сочетание клавиш <Win>+<R>, указав в поле ввода значение `regedit` и щелкнув мышью на кнопке OK.
2. Откройте раздел `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Dnscache\Parameters` и создайте DWORD-ключ с именем `AddrConfigControl`, равный нулю. Для этого щелкните правой кнопкой мыши в правой части окна редактора реестра и выбери-

те команду **Создать | Параметр DWORD (32 бита)** (New | DWORD (32-bit) Value) в контекстном меню (рис. 11.4).

3. Завершите работу редактора реестра.

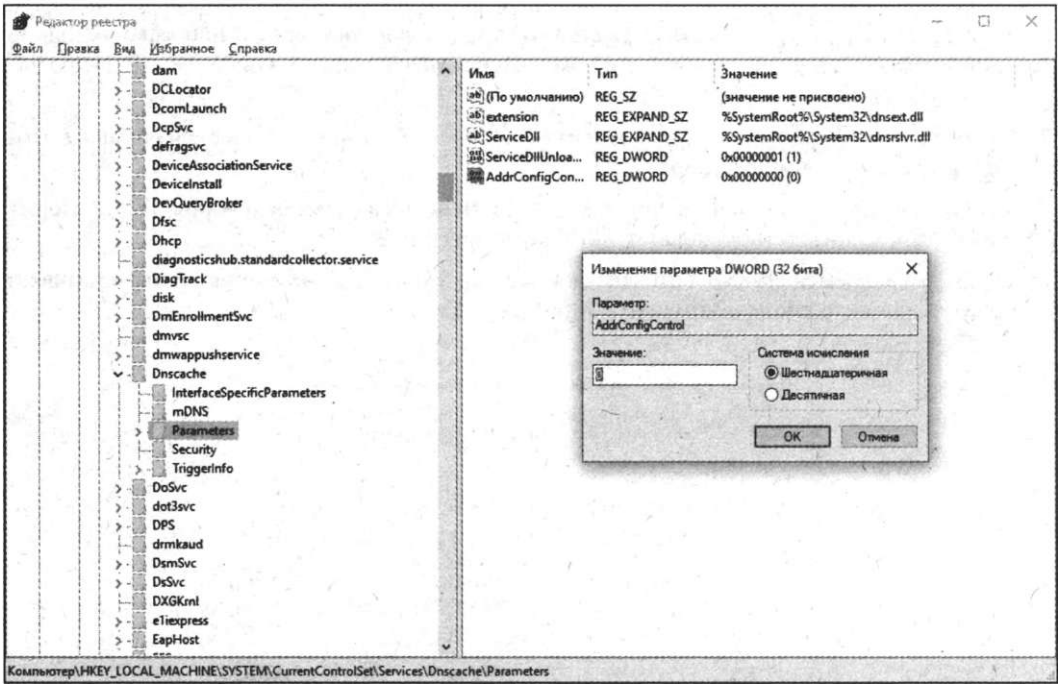


Рис. 11.4. Создание ключа AddrConfigControl в реестре

Без настройки DNSv6 вы не сможете открывать сайты в браузере по их доменному имени, поэтому настроим DNSv6 и укажем адреса DNSv6-**серверов,** использовав в качестве примера адреса DNS-серверов компании Google:

- 2001:4860:4860:•:8888
- 2001:4860:4860::8844

Для этого выполните следующие действия:

1. Щелкните правой кнопкой мыши на значке сетевого подключения в правой части панели задач Windows и в появившемся контекстном меню выберите пункт **Центр управления сетями и общим доступом** (Network and Sharing Center).
2. Щелкните мышью на ссылке **Изменение параметров адаптера** (Change adapter settings) в левой части окна.
3. Щелкните правой кнопкой мыши на сетевом соединении (которое используется для подключения к Интернету) и выберите в контекстном меню пункт **Свойства** (Properties).
4. **В** открывшемся диалоговом окне настроек соединения выберите пункт **IP версии 6 (TCP/IPv6)**[1] (Internet Protocol Version 6(TCP/IPv6)) (рис. 11.5, *слева).*

[1] **В версиях операционной системы Windows ранее Windows 10 название пункта может несколько отличаться.**

5. Установите переключатель в положение **Использовать следующие адреса DNS-серверов** (Use the following DNS server addresses) и укажите приведенные ранее адреса DNS-серверов компании Google (рис. 11.5, ***справа).***
6. Последовательными нажатиями кнопок OK закройте открытые диалоговые окна.

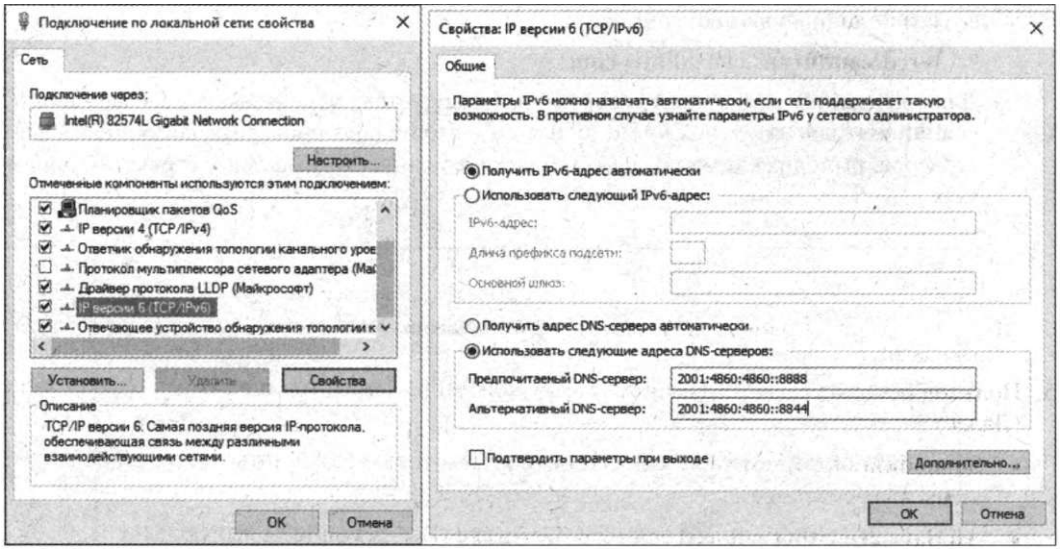


Рис. 11.5. Настройка протокола IPv6: добавление адресов DNS-сервера

Теперь нужно запустить редактор локальной групповой политики и активировать/настроить протокол Teredo. Напомню, что редактор локальной групповой политики доступен только в профессиональных выпусках операционной системы Windows.

1. Запустите редактор локальной групповой политики, нажав сочетание клавиш <Win>+<R>, указав в поле ввода значение gpedit.msc и щелкнув мышью на кнопке **ОК.**
2. Откройте раздел **Конфигурация компьютера | Административные шаблоны | Сеть | Параметры TCP/IP | Технологии Туннелирования IPv6** (Computer Configuration | Administrative Templates | Network | TCPIP Settings | IPv6 Transition Technologies).
3. Двойным щелчком щелкните по каждом из указанных далее пунктов и настройте их следующим образом:
   - **Установить квалификацию Teredo по умолчанию** (Teredo Default Qualified) — установите переключатель в положение **Включено** (Enabled) и выберите в раскрывающемся ниже списке пункт **Включенное состояние** (Enabled State) (рис. 11.6);
   - **Установить частоту обновления Teredo** (Teredo Refresh Rate) — установите переключатель в положение **Включено** (Enabled) и выберите в раскрывающемся ниже списке пункт **10;**
   - **Установить состояние Teredo** (Teredo State) — установите переключатель в положение **Включено** (Enabled) и выберите в раскрывающемся ниже списке пункт **Корпоративный клиент** (Corporate Client);
   - **Установить имя сервера Teredo** (Teredo Server Name) — установите переключатель в положение **Включено** (Enabled) и укажите в поле ввода одно из следующих значений:

- teredo.remlab.net
- teredo.trex.fi
- teredo.ipv6.microsoft.com
- teredo.ngix.ne.kr
- teredo.managemydedlcom
- teredo.autotrans.consulintel.com

Для надежной и быстрой работы рекомендуется использовать сервер teredo.remlab.net или *teredo.trex.fi.* Но лучше самостоятельно проверить доступность всех серверов, выполняя команду `ping` для каждого из них в командной строке, — например: `ping teredo.remlab.net;`

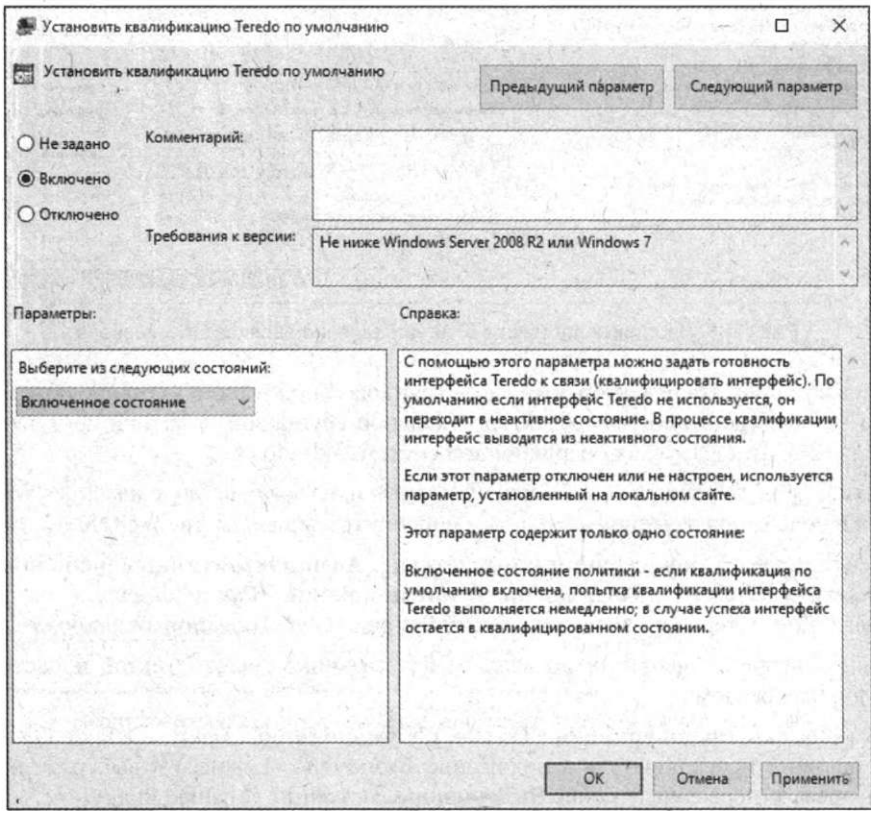


Рис. 11.6. Настройка политики Установить квалификацию Teredo по умолчанию

- Установить имя ретранслятора 6to4 (6to4 Relay Name) — установите переключатель в положение Отключено (Enabled);
- Установить интервал разрешения имен ретранслятора 6to4 (6to4 Relay Name Resolution Interval) — установите переключатель в положение Отключено (Enabled);
- Установить состояние 6to4 (6to4 State) — установите переключатель в положение Включено (Enabled) и выберите в раскрывающемся ниже списке пункт Отключенное состояние (Disabled State);

- Установить состояние IP-HTTPS (IP-HTTPS State) — установите переключатель в положение Отключено (Enabled);
- Установить имя маршрутизатора ISATAP (ISATAP Router Name) — установите переключатель в положение Отключено (Enabled);
- Установить состояние ISATAP (ISATAP State) — установите переключатель в положение Включено (Enabled) и выберите в раскрывающемся ниже списке пункт Отключенное состояние (Disabled State).

После выполнения всех указанных настроек окно редактора локальной групповой политики должно выглядеть так, как показано на рис. 11.7.

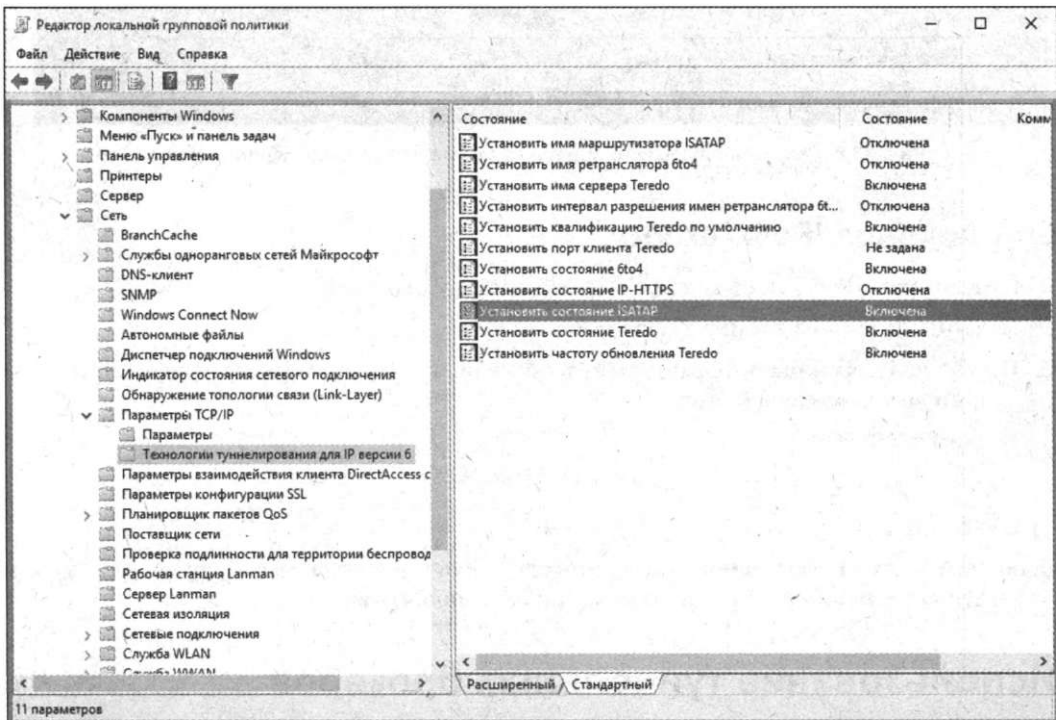


Рис. 11.7. Окно редактора **локальной групповой политики** после настройки

Осталось проверить работоспособность протокола Teredo:

1. Откройте окно командной строки любым способом — например, нажав сочетание клавиш <Win>+<R>, указав значение `cmd` в поле ввода и нажав клавишу <Enter>.
2. Введите следующую команду, нажав после ввода клавишу <Enter>:

   ```
   ping ipv6.nnm-club.me
   ```

   Вы должны увидеть результат успешного обмена пакетами с ресурсом ipv6.**nnm-club.me** (рис. 11.8).

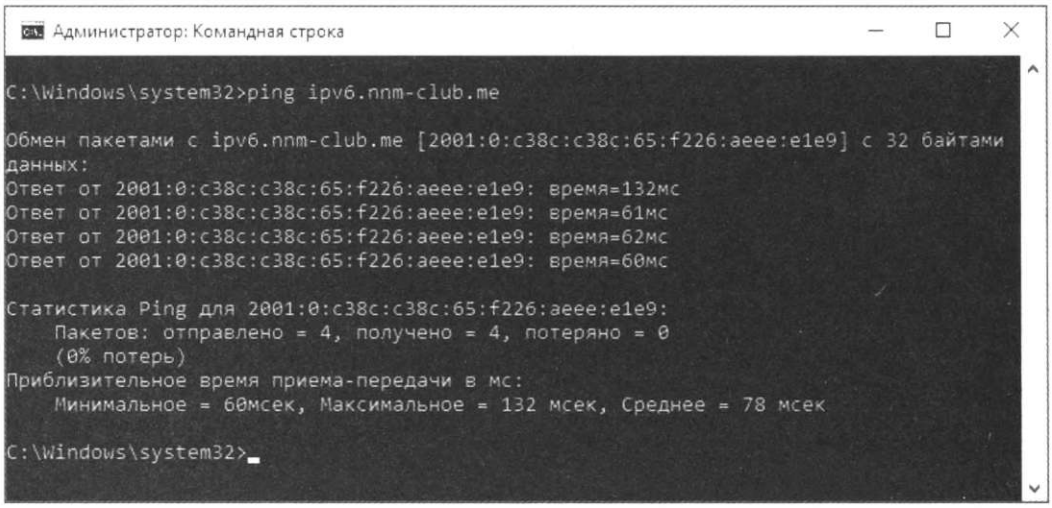


Рис. 11.8. Результат успешного обмена пакетами с ресурсом ipv6.nnm-club.nie

Отключение IPv6/Teredo

Для отключения IPv6/Teredo следует выполнить следующие шаги:

1. Нажмите сочетание клавиш <Win>+<R>.
2. В поле ввода Открыть (Open) укажите значение cmd и нажмите клавишу <Enter>. Вы увидите окно командной строки.
3. Введите команду:

   ```
   netsh interface teredo set state disabled
   ```

   и нажмите клавишу <Enter>.

Дополнительная информация по протоколу IPv6 доступна на форуме по адресу tinyurl.com/noewxlq и на сайте по ссылке tinyurl.com/ol4jk6e.

Использование туннельных брокеров

Использование туннельных брокеров — это универсальный вариант, подходящий как пользователям с глобальным **IPv**4-адресом, так и работающим без него. Туннельные сервисы реализуют туннели в **IPv6**-сеть и часто задействуют шлюзы в разных странах, выбирать из которых нужно ближайший, чтобы минимизировать задержки передачи данных. Туннельный брокер, как правило, выдает не один, а целый диапазон **IPv6**-адресов, которые не меняются при смене **IPv**4-адреса компьютера и привязываются к аккаунту пользователя. Одним из наиболее простых туннельных брокеров является tunnelbroker.net.

IPv6 через *tunnelbroker.net*

Регистрация и использование сервиса tunnelbroker.net осуществляются совершенно бесплатно. После заполнения формы для регистрации аккаунта на странице tinyurl.com/olanjk9 пароль будет автоматически сгенерирован и выслан на указанный адрес электронной почты.

После авторизации на сайте с указанным логином и высланным паролем необходимо создать туннель. Дня этого выполните следующие действия:

1. Авторизуйтесь на сайте tunnelbroker.net со своим логином и паролем.
2. Щелкните мышью на ссылке Create Regular Tunnel (Создать обычный туннель) в левой части страницы.
3. На открывшейся странице в строке You are viewing from: укажите свой текущий IP-адрес — на рис. 11.9 показано, что используется адрес 46.147.207.53. Там же вы можете увидеть сообщение о распространенной ошибке: блокировке соединений по протоколу ICMP.

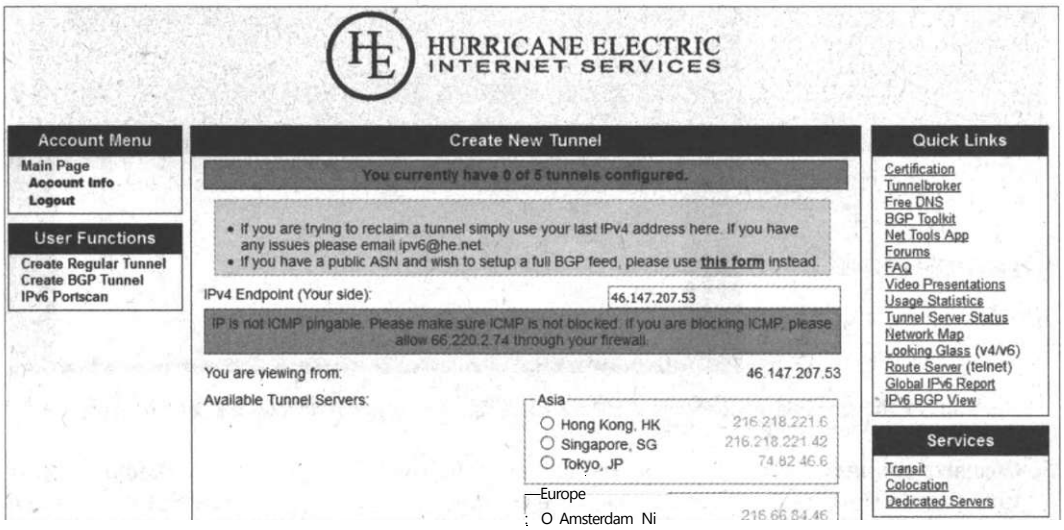


Рис. 11.9. Создание туннеля на сайте tunnelbroker.net

Если в вашем случае также отображается эта ошибка, необходимо разблокировать подключения по протоколу ICMP в настройках брандмауэра. В случае, если компьютер напрямую подключен к Интернету, изменения необходимо проводить в настройках брандмауэра Windows или антивирусного приложения. Если же подключение к Интернету осуществляется через маршрутизатор — в настройках устройства. К сожалению, в рамках одной книги нельзя привести универсальную инструкцию или последовательность шагов для настройки каждого брандмауэра. Вы можете выполнить поиск по запросу `как настроить ICMP` или `настройка ICMP` с добавлением названия программы или устройства. Например: `как настроить ICMP в брандмауэре Windows`, `настройка ICMP в Kaspersky Internet Security` или `настройка ICMP на Zyxel Keenetic` (рис. 11.10).

4. После указания IP-адреса установкой переключателя в одно из положений выберите ближайший к вам туннельный сервер.

   В списке также указаны IP-адреса этих серверов, поэтому перед выбором можно проверить время отклика и маршрут до каждого из них с помощью команды `ping` или `traceroute`. Дня пользователей из России оптимальным сервером будет один из находящихся в Европе.

5. Нажмите кнопку Create Tunnel (Создать туннель).

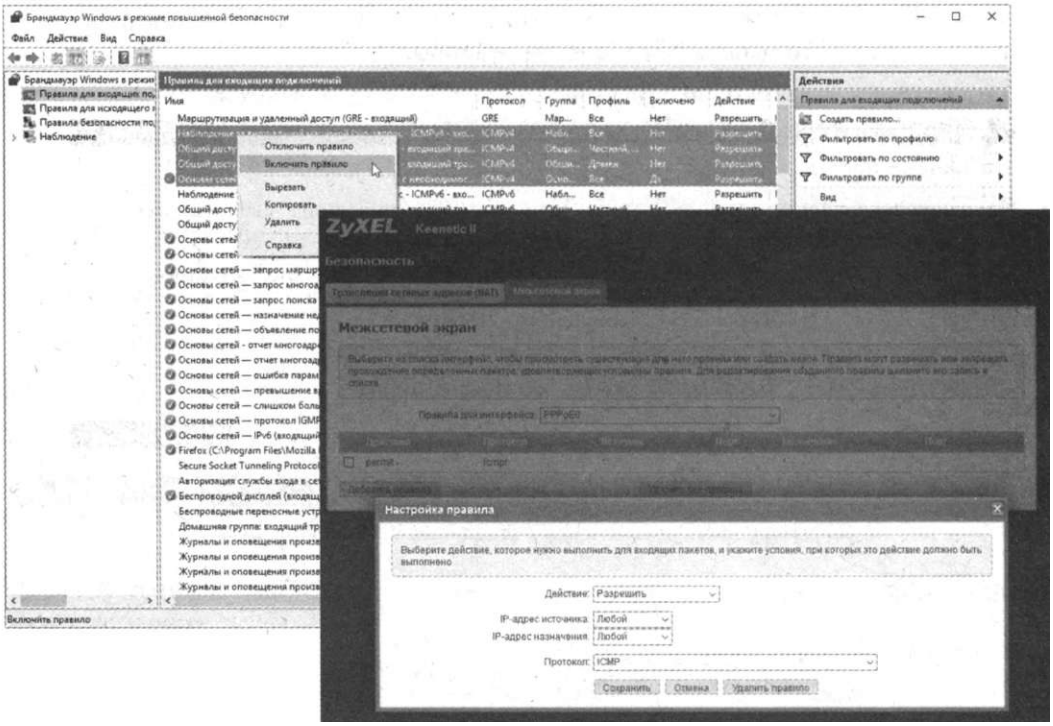


Рис. 11.10. Настройка протокола ICMP в разных брандмауэрах (Windows и Zyxel Keenetic)

6. Создав туннель, для его настройки перейдите на главную страницу сайта tunnelbroker.net и щелкните мышью по названию туннеля в группе Configured Tunnels (Настроенные туннели) (рис. 11.11) — вы увидите страницу с настройками туннеля.

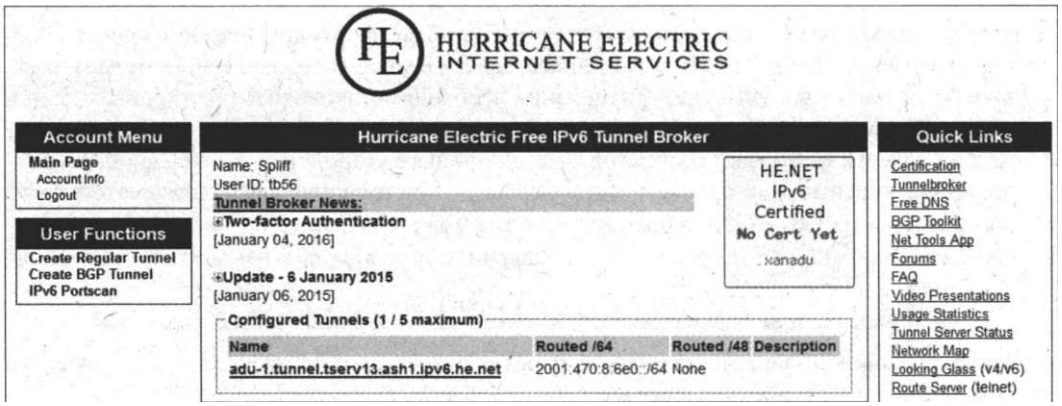


Рис. 11.11. Главная страница со списком созданных туннелей

7. Перейдите на вкладку Example Configurations (Примеры настройки) и в раскрывающемся списке выберите используемую вами операционную систему. После этого вы увидите список конкретных команд, которые нужно поочередно выполнить (в окне программы cmd), чтобы настроить у себя только что созданный туннель (рис. 11.12).

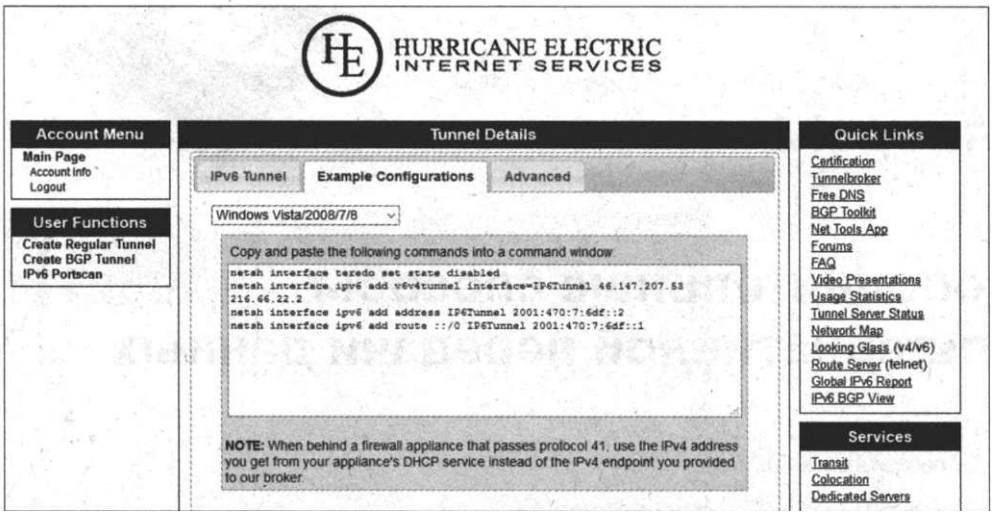


Рис. 11.12. Страница со списком команд для настройки туннеля

Очень удобно, что сервер брокера выдает сразу готовые к выполнению команды, без необходимости размышлять, какие значения куда нужно подставить. После выполнения всех команд IPv6 должен заработать.

Существуют и другие туннельные брокеры:

- Gogonet/Freenet6 (gogonet.gogo6.com) — один из самых доступных туннельных брокеров, предлагающий различные типы туннелей, в том числе собственный протокол для обхода NAT. Подключение осуществляется через удобное приложение;
- SixXS (sixxs.net) — сервис позволяет создавать туннели разных типов и выбирать среди свыше 40 серверов по всему миру для подключения.

Список туннельных брокеров также доступен на странице tinyurl.com/zdwdeed.

После выполнения настройки перейдите на сайт test-ipv6.com, чтобы протестировать IPv6-подключение (рис. 11.13).

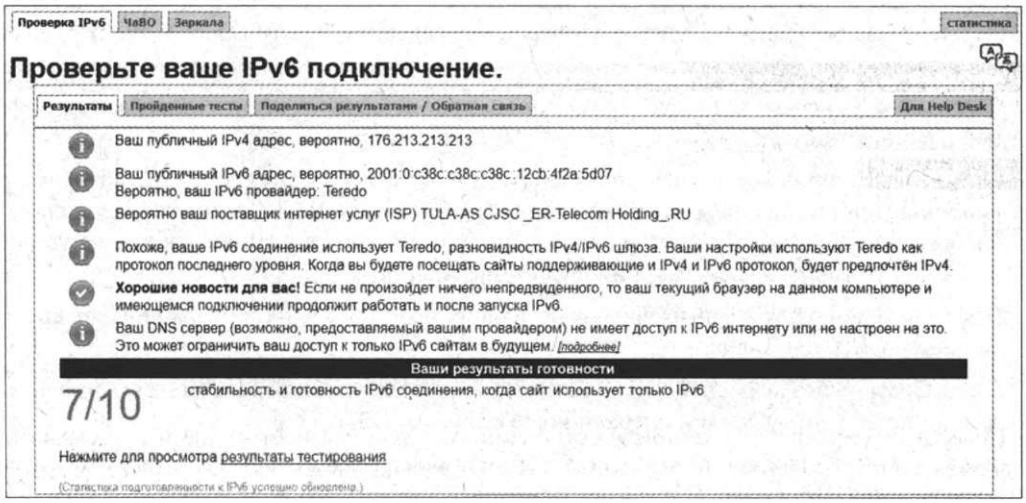


Рис. 11.13. Результаты теста подключения по протоколу IPv6

ГЛАВА 12

Дополнительные способы альтернативной передачи данных

- Э Turbo-режимы в браузерах
- Э Использование систем онлайн-переводов
- Э Использование специальных расширений браузеров
- О Подключение к Интернету через мобильные устройства
- Э Внешние устройства и подключения

В этой главе описаны дополнительные способы получения доступа к сайтам типа Hulu.com, в том числе и через мобильные устройства.

Turbo-режимы в браузерах

Браузер Opera

В браузере Opera доступен режим Opera Turbo, который, прежде всего, создан с целью экономии трафика и ускорения загрузки данных. В этом режиме размер страниц уменьшается, за счет чего ускоряется их загрузка без ущерба для контента. Режим Opera Turbo поддерживается в следующих продуктах:

- **Opera Mini — версия браузера, совместимая практически со всеми моделями смартфонов и планшетов;**
- **Opera Max — приложение для управления трафиком и экономии трафика, которое при использовании мобильного подключения к Интернету или Wi-Fi сжимает видеоролики и изображения. Браузер Opera Max специально разработан для удобной работы на устройствах под управлением операционной системы Android;**
- **Opera — браузер для компьютеров, работающих под управлением операционных систем Windows, OS X или Linux;**
- **Opera Coast — браузер, специально разработанный для удобной работы на смартфонах и планшетах под управлением операционной системы iOS.**

Помимо экономии трафика, режим Opera Turbo позволяет в некоторых случаях просматривать сайты типа Hulu.com. При включении этого режима все запрашиваемые страницы проходят через серверы Opera, предназначенные для экономии трафика, поэтому и осуще-

ствляется доступ к заблокированным сайтам (по сути, вы обращаетесь к серверу Opera, а не к недоступному сайту).

Для активации режима в настольной версии браузера следует выбрать команду меню Opera | Opera Turbo (рис. 12.1, *слева).*

На мобильных устройствах, как правило, режим включен автоматически (в Opera Mini настройка недоступна, а на iOS-гаджетах нужно перейти на экран Настройки (Settings), выбрать приложение Opera Coast и убедиться, что режим включен (рис. 12.1, *справа).*



Рис. 12.1. Выбор режима Opera Turbo в Windows-версии браузера *(слева)* **и настройка режима в iOS (***справа)*

Яндекс.Браузер

Режим Турбо также доступен и в приложении Яндекс.Браузер, поддерживающем работу в операционных системах Windows, QS X, Linux, iOS и Android. По умолчанию этот режим

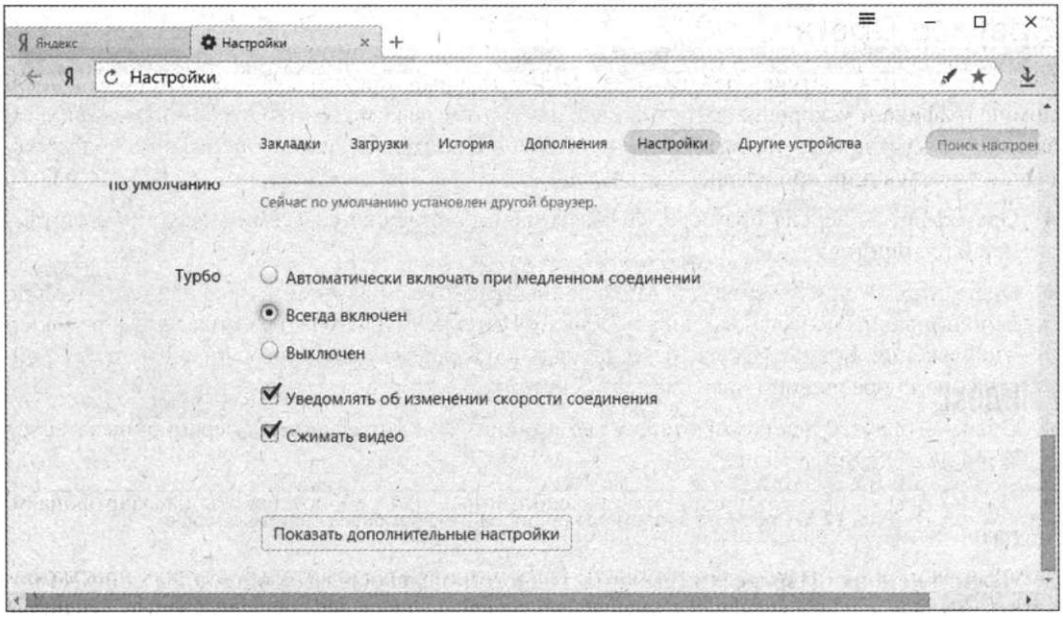


Рис. 12.2. Настройка режима Турбо в Windows-версии программы Яндекс Браузер

включается при скорости ниже 128 Кбит/с, однако, как правило, скорость подключения сейчас выше, поэтому для получения доступа к сайтам типа Hulu.com режим Турбо следует включить на постоянной основе. Для этого нажмите в браузере кнопку_____и выберите команду меню **Настройки** (Settings), после чего в разделе **Турбо** (Turbo) установите одноименный переключатель в положение **Всегда включен** (Always on) (рис. 12.2).

О включенном режиме Турбо информирует значок в адресной строке браузера.

Использование систем онлайн-переводов

Предлагаемый метод доступа на сайты типа Hulu.com довольно прост, но подойдет в основном для просмотра текстовой информации, т. к. сколь-нибудь затратный в плане трафика мультимедийный контент на некоторых таких ресурсах отсекается. Впрочем, с помощью систем онлайн-переводов реально попасть даже на ресурс Pandora, разве что при этом могут возникнуть трудности с трансляцией потокового радио. Прием работает за счет того, что, по сути, вы обращаетесь к сайту онлайн-переводчика, проксирующего нужный сайт, а не к заблокированному ресурсу.

Воспользоваться методом можно следующим образом:

1. Перейдите на сайт **translate.google.ru.**
2. Введите в поле ввода адрес заблокированного ресурса.

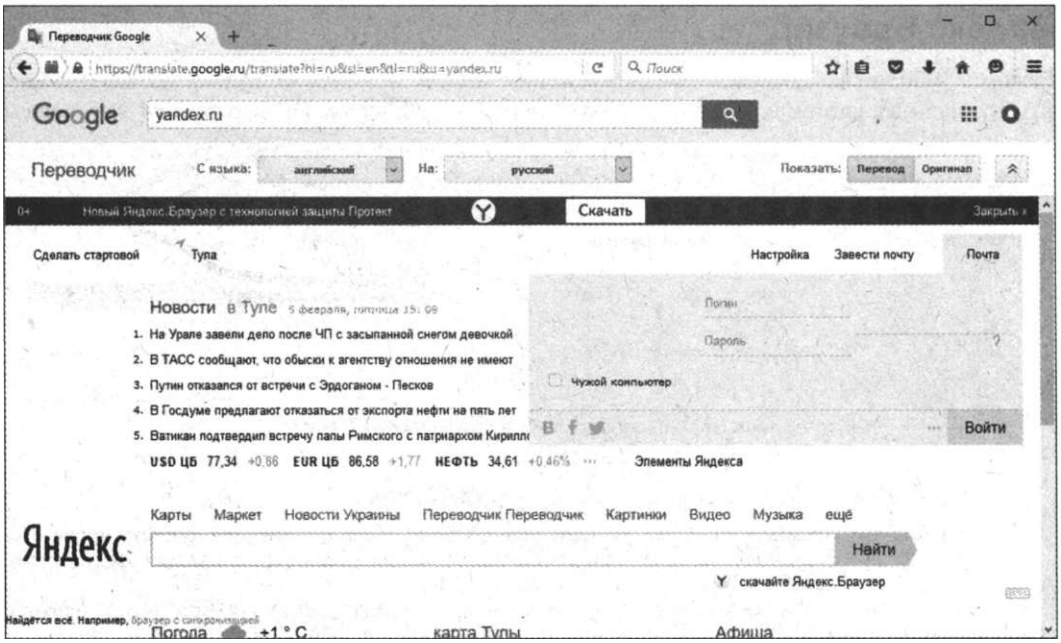


Рис. 12.3. Просмотр заблокированного сайта с помощью системы Google

3. Нажмите кнопку **Перевести** (выбор исходного и целевого языков разницы не имеет) — вы увидите содержимое веб-сайта. Если сайт оказался переведенным на иностранный язык, нажмите кнопку **Оригинал** в правом верхнем углу страницы (рис. 12.3).

Окно переводчика Google позволяет переходить по ссылкам на разделы текущего и других сайтов.

Аналогичным функционалом обладает сервис Яндекс.Переводчик, доступный по адресу **translate.yandex.ru.**

Использование специальных расширений браузеров

Помимо прочего, вы можете использовать и специальные расширения браузеров. Например, friGate — именно оно открыло доступ к сайтам **Hulu,** Netflix и Pandora с моего компьютера. Расширение доступно для браузеров Firefox, Opera и Chrome по адресу **https://frigate.org/ru/.** Никакой дополнительной настройки после установки расширения не требуется. Принцип его действия, по словам разработчика, заключается в том, что при обращении к одному из поддерживаемых сервисов запрос автоматически отправляется через прокси-сервер, в то время как все другие соединения происходят обычным образом. Это позволяет обойти проверку расположения компьютера и в то же время работать во Всемирной паутине без снижения скорости.

Сразу после установки расширения вы можете проверить его работу, перейдя на вкладку **Проверить IP** (Check IP) на сайте проекта (рис. 12.4).

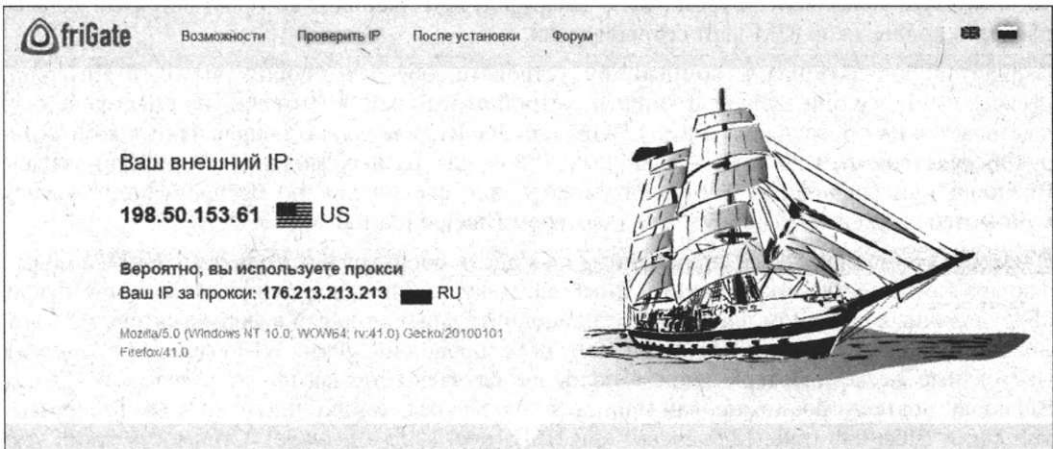


Рис. 12.4. Проверка работы расширения friGate

ПРОСМОТР ЗАБЛОКИРОВАННОГО ВИДЕО НА YOUTUBE

Существует специальный сайт (tinyurl.com/bh2wl44), созданный для разблокировки на сайте YouTube видеороликов, которые были запрещены к просмотру в той или иной стране.

Среди аналогичных расширений можно назвать плагин ProxTube для браузеров Chrome **(tinyurl.com/9x9wkbk)** и Firefox, который автоматически обрабатывает и позволяет просматривать все недоступное видео, расширение Hide My Ass! Web Proxy для браузеров Chrome **(tinyurl.com/o5jbh44)** и Firefox **(tinyurl.com/ottevgq),** Browsec для Firefox **(tinyurl.com/pdrn4uf),** универсальный плагин-приложение ZenMate **(zenmate.com)** и расширение HTTPS Everywhere **(tinyurl.com/38sqvb9),** поддерживаемое, кроме прочих, и браузерами Opera и Firefox на платформе Android. Существует также обеспечивающий высокую скорость пере-

дачи данных плагин, но доступный только для браузера Chrome, — Google SPDY Proxy (tinyurl.com/ojqzyy3).

ПЛАГИН/ПРИЛОЖЕНИЕ ZENMATE

Подробное описание плагина/приложения ZenMate, предоставляющего доступ в Интернет по защищенному зашифрованному каналу на основе VPN (виртуальной частной сети) и маскирующего адрес расположения пользователя по его выбору под жителя Соединенных Штатов, Великобритании, Германии, Румынии, Швейцарии или Гонконга, приведено в *главе 9.*

Для браузеров Internet Explorer, Chrome и Firefox и устройств под управлением операционной системы Android также разработан бесплатный плагин Hola (hola.org), который не только позволяет заходить на недоступные в вашей стране медиасервисы, но и ускоряет загрузку страниц и другого контента. Кроме того, в группе HolaUnblockerScripts на сайте социальной сети Facebook вы найдете новые скрипты для разблокирования самых разных сайтов (tinyurl.com/orhajgr).

Подключение к Интернету через мобильные устройства

Еще один способ добраться до нужных сайтов, если в вашей сети доступ к ним заблокирован администратором или провайдером, — подключиться к другой сети. Проще всего это сделать через мобильное устройство — смартфон или планшет, который при этом должен обладать поддержкой SIM-карт сотовой связи.

Вариантов подключения к компьютеру устройств, обеспечивающих выход в Интернет, множество, и все они зависят от модели устройства. Выход в Интернет на смартфоне осуществляется по протоколам GPRS (EDGE) или 3G/4G, а затем его подключают к компьютеру посредством кабеля USB (различных типов для разных моделей устройств), канала Bluetooth или соединения Wi-Fi. Разумеется, для соединения по беспроводному каналу компьютер должен быть оборудован адаптером Bluetooth и/или Wi-Fi.

С ноутбуками проще — все современные их модели оборудованы модулями Wi-Fi, а подавляющее большинство также имеет и Bluetooth-модуль. Для относительно старых ноутбуков, оборудованных разъемом для установки дополнительных модулей в форм-факторе PC Card, можно приобрести соответствующий модуль беспроводной связи Wi-Fi (рис. 12.5, *справа).* Настольные же компьютеры лишь в половине случаев оснащаются адаптерами Wi-Fi или Bluetooth, поэтому, возможно, вам придется обзавестись тем или иным модулем беспроводной связи Bluetooth (рис. 12.5, *слева)* или USB (рис. 12.5, *в центре).* Стоимость таких устройств начинается с пары сотен рублей.

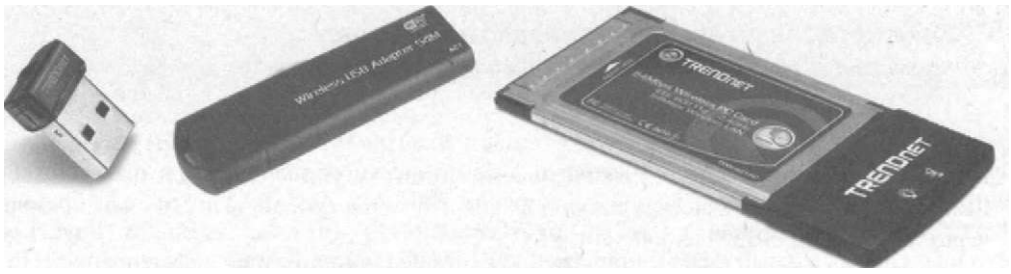


Рис. 12.5. Слева направо: USB-адаптер Bluetooth, USB-адаптер Wi-Fi, адаптер Wi-Fi в форм-факторе PC Card (PCMCIA)

Рассмотрим далее способы настройки точки доступа Wi-Fi на смартфонах/планшетах под управлением операционных систем Android, Windows Phone, iOS и Blackberry. Для осуществления доступа к Интернету на смартфоне/планшете должен быть обязательно включен режим передачи данных через сотовую сеть и, при необходимости, подключена соответствующая услуга у оператора.

Операционная система Android

На устройствах под управлением операционной системы Android (на разных моделях устройств и версиях операционной системы Android интерфейс меню может выглядеть иначе) настройка осуществляется следующим образом:

1. Перейдите в настройки устройства — обычно для этого нужно коснуться значка **Настройки** (Settings) на главном экране. Вы увидите соответствующий экран (рис. 12.6, *слева).*
2. На экране настроек коснитесь пункта Ещё (More settings). На некоторых устройствах этот пункт может называться иначе — например, **Беспроводные сети** (Wireless & Networks). Откроется экран с параметрами беспроводных сетей (рис. 12.6, *в центре).*
3. Выберите пункт **Режим модема** (Tethering and Portable Hotspot), тем самым открыв одноименный экран (рис. 12.6, *справа).*

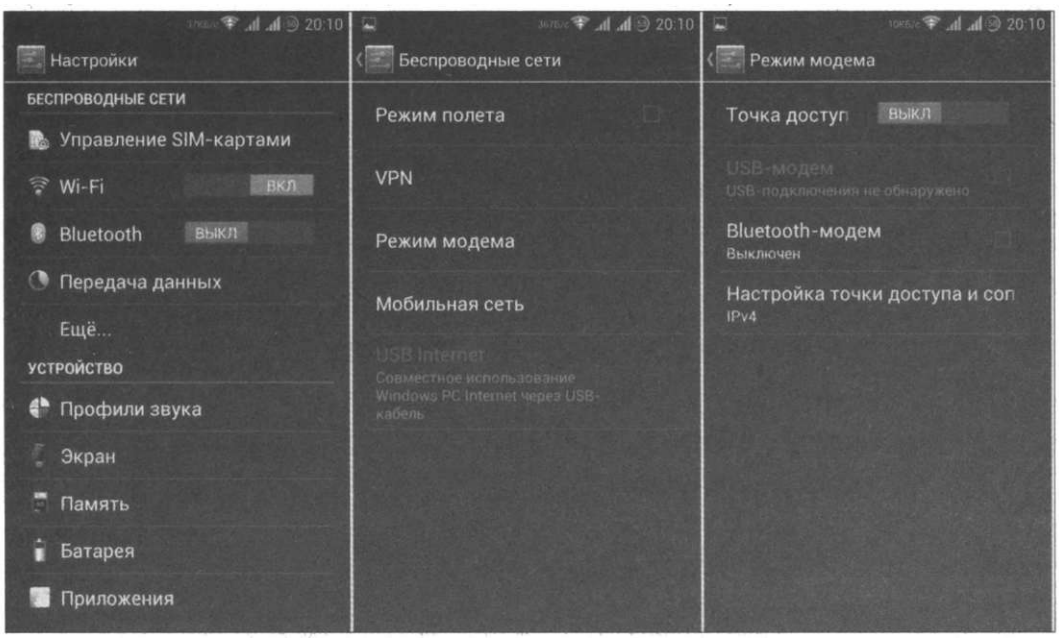


Рис. 12.6. Настройка точки доступа на смартфоне под управлением Android 4

Как можно видеть, на экране **Режим модема** (Tethering and Portable Hotspot) вы можете настроить смартфон в качестве точки доступа к Интернету и связать его с компьютером через интерфейс USB, Bluetooth или Wi-Fi.

4. Коснитесь пункта **Точка доступа** (Portable Wi-Fi hotspot), чтобы получить доступ к настройкам точки доступа на устройстве (рис. 12.7, *слева).*

5. Чтобы продолжить настройку, коснитесь пункта **Настройка точки доступа** (Configure) — вы увидите экран, показанный на рис. 12.7, *в центре.*

   Здесь можно изменить имя сети, режим защиты сети (обычно используется режим WPA2) и назначить пароль, ввод которого потребуется для подключения компьютера к точке доступа на устройстве.

   В общем-то, вы можете и не задавать никакого пароля, чтобы не возиться потом с его вводом, но так поступать не рекомендуется, поскольку в этом случае к вашему смартфону/планшету сможет подключиться любой желающий, устройство которого находится в радиусе действия вашей точки доступа, а это противоречит правилам безопасности, обсуждаемым в книге.

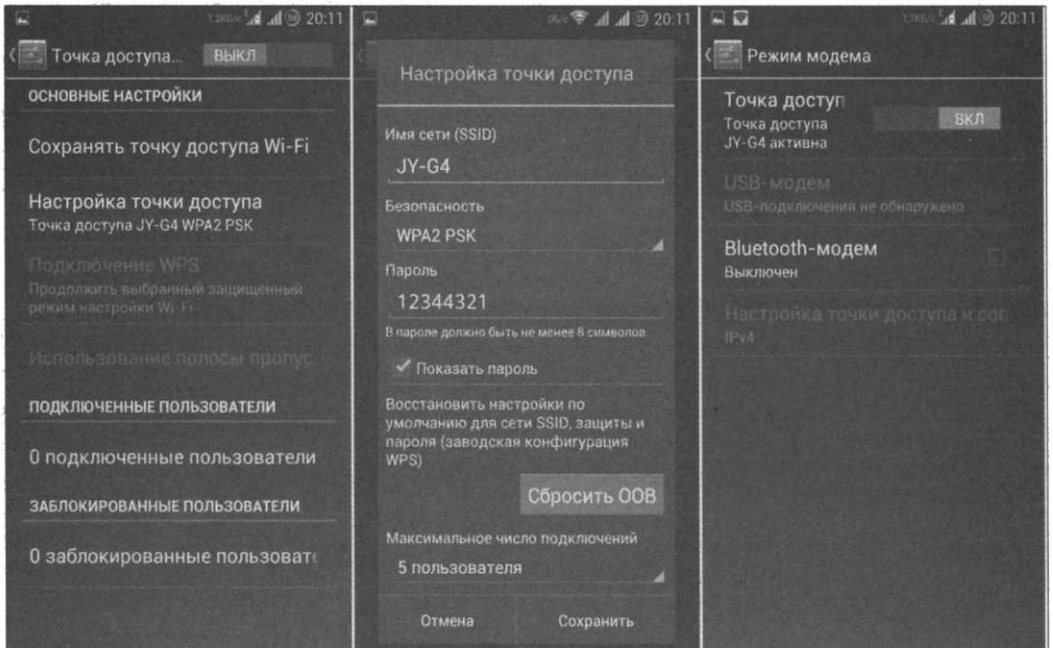


Рис. 12.7. Настройка точки доступа на смартфоне под управлением Android 4 (*продолжение)*

6. После изменения настроек сети следует коснуться переключателя **Точка доступа** (Portable Wi-Fi hotspot) и перевести его в активное состояние (рис. 12.7, *справа).*

   На этом экране есть также возможность, установив соответствующий флажок, разрешить подключение к смартфону/планшету через интерфейс USB или Bluetooth.

Теперь осталось только выполнить на компьютере поиск доступных сетей Wi-Fi и подключиться к созданной точке доступа для осуществления соединения с Интернетом.

Операционная система Windows Phone

В операционной системе Windows Phone настройка смартфона в качестве точки доступа к Интернету осуществляется очень просто. Для этого выполните следующие действия:

1. Смахнув главный экран влево, прокрутите список и коснитесь пункта **Настройки** (Settings), чтобы отобразить интерфейс, показанный на рис. 12.8, *слева.*

2. Найдите в списке пункт **Общий интернет** (Internet Sharing) и коснитесь его — вы увидите экран, показанный на рис. 12.8, *в центре*. Для включения режима точки доступа достаточно установить переключатель **Общий доступ** (Sharing) в активное положение.

   Базовые настройки завершены, а данные по умолчанию для доступа к сети указаны на экране.

3. Чтобы изменить имя сети, по которому точка доступа будет обнаруживаться компьютером, а также настроить пароль, коснитесь кнопки **Установка** (Setup), — вы увидите экран, показанный на рис. 12.8, *справа*.

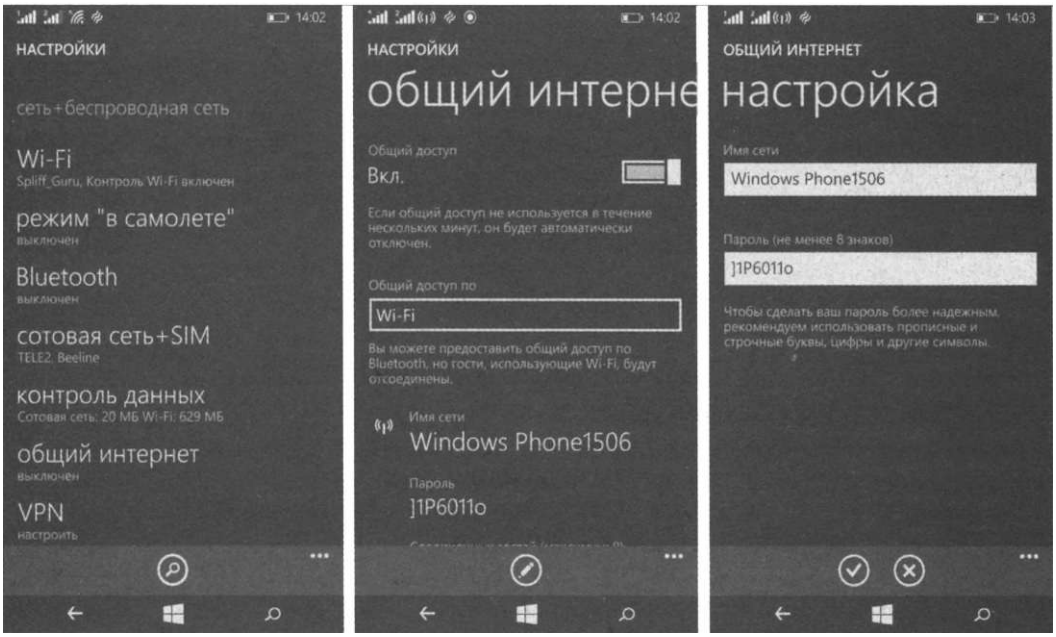


Рис. 12.8. Настройка точки доступа на смартфоне под управлением Windows Phone 8

Теперь осталось только выполнить на компьютере поиск доступных сетей Wi-Fi и подключиться к созданной точке доступа для осуществления соединения с Интернетом.

Операционная система iOS

На устройствах под управлением операционной системы iOS — таких, как смартфон iPhone и планшет iPad с поддержкой сотовых сетей, процедура активации девайса в качестве точки доступа максимально упрощена:

1. На главном экране коснитесь значка **Настройки** (Settings).
2. На экране настроек iPhone/iPad выберите пункт **Режим модема** (Personal Hotspot) (рис. 12.9).
3. Установите переключатель **Режим модема** (Personal Hotspot) в активное положение.

   Как можно видеть, на экране **Режим модема** (Personal Hotspot) вы можете настроить смартфон в качестве точки доступа к Интернету и связать его с компьютером через интерфейсы USB, Bluetooth или Wi-Fi. Необходимые инструкции отображены на экране.

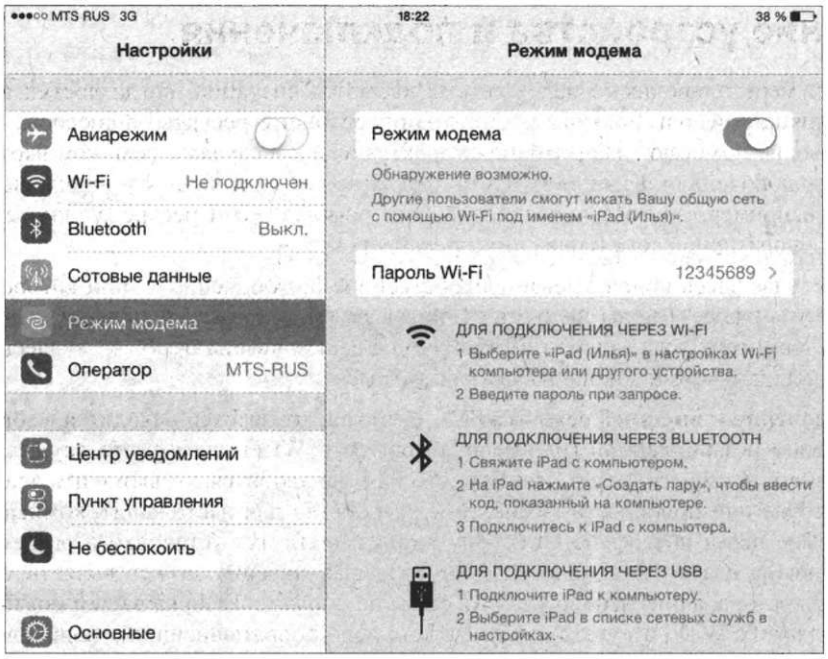


Рис. 12.9. Настройка точки доступа на устройстве Под управлением iOS

4. Чтобы изменить сетевой пароль, с которым к точке доступа Wi-Fi сможет подключаться компьютер, коснитесь пункта **Пароль Wi-Fi** (Wi-Fi Password).

Теперь осталось только выполнить на компьютере поиск доступных сетей Wi-Fi и подключиться к созданной точке доступа для осуществления соединения с Интернетом.

Операционная система Blackberry OS

На устройствах под управлением операционной системы Blackberry также доступна функция раздачи Интернета другим девайсам. Она носит название **Мобильная точка доступа** (Mobile Hotspot) и настраивается следующим образом:

1. Смахните главный экран от верхнего края вниз.
2. Коснитесь кнопки **Настройки** (Settings) и перейдите на экран **Сети и подключения | Мобильная точка доступа** (Networks and Connections | Mobile Hotspot).

   Если вы ранее не пользовались режимом мобильной точки доступа, следуйте инструкциям на экране, а также запомните предложенный системой пароль к мобильной точке доступа.
3. Установите переключатель **Мобильная точка** (Mobile Hotspot) в активное положение.

Пользователю устройства, подключающегося к созданной вами точке доступа, осталось выполнить на компьютере поиск доступных сетей Wi-Fi и подключиться к созданной точке для осуществления соединения с Интернетом.

Внешние устройства и подключения

В большей мере приводимые далее советы касаются ситуаций, когда доступ в Интернет вовсе заблокирован, или доступны только корпоративные ресурсы, а способы, описанные в этой главе, не помогают. Информация эта актуальна и в случаях, если компьютер вообще не имеет подключения к Интернету. Суть предлагаемых способов — в подключении к другой сети (например, другого провайдера). Они помогут, если ресурс блокируется только в вашей корпоративной сети или вашим провайдером.

В любом случае здесь подразумевается собственное подключение — при котором администратор сети в офисе, где вы находитесь, никак не сможет отследить ваши действия, если только не посмотрит логи (временные файлы) на вашем компьютере, — но здесь надо подчищать за собой, о чем подробно рассказано в *главе 1.*

- **Подключение к внешней сети Wi-Fi — если ваш компьютер находится в зоне вещания какой-либо незащищенной (или бесплатной) сети Wi-Fi, вы можете осуществить подключение к Интернету через нее. Все, что вам понадобится, — включить адаптер Wi-Fi на ноутбуке или приобрести компактное устройство для настольного компьютера, подключаемое через интерфейс USB. Внутренняя плата для установки в разъем PCI-E на материнской плате тоже подойдет, но торчащая антенна может вызвать подозрения администратора, а оперативно удалить ее вы не сможете. Если на вашем ноутбуке встроенный адаптер Wi-Fi отсутствует, вы можете использовать внешний, подключаемый как в виде карты PCMCIA (PC Card) (см. рис. 12.5), так и через интерфейс USB.**
- **Подключение через 3G/4G-модем — практически все операторы сотовой связи предлагают сейчас компактные 3G/4G-модемы, подключаемые через интерфейс USB (рис. 12.10). Их стоимость варьируется в диапазоне от 800 до 6000 руб. за устройство, а доступ в Интернет обойдется в сумму от 0 до 4500 руб. в месяц. Такой модем вы можете подключить к любому компьютеру и посещать любые веб-сайты в свое удовольствие.**

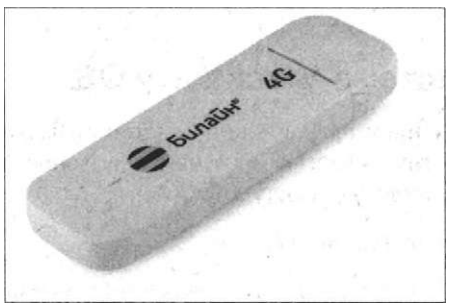


Рис. 12.10. 4G-модем

ЧАСТЬ III

Анонимные сети: защищенная работа в Интернете

Глава 13.	Основные анонимные сети
Глава 14.	Freenet: концепция свободной сети
Глава 15.	I2P: проект невидимого Интернета
Глава 16.	Платформа RetroShare
Глава 17.	Tor: луковая маршрутизация

Часть III **этой книги посвящена разнообразным анонимным сетям, позволяющим, как следует из их названия, анонимизировать (защитить от перехвата) весь трафик, передаваемый и получаемый вами из Интернета. Некоторые из анонимных сетей позволяют получать доступ и к заблокированным сайтам. Так, сеть Tor допускает посещение недоступных на вашем компьютере сайтов, поскольку организует, по сути, зашифрованное многоузловое VPN-соединение. А сеть I2P позволяет посещать заблокированные ресурсы, разместившие свои зеркала на сайтах этой невидимой сети. Сети Freenet и RetroShare в основном предназначены для зашифрованного и анонимного общения и обмена файлами.**

ГЛАВА 13

Основные анонимные сети

Основы анонимных сетей

Децентрализованные анонимные сети

Гибридные анонимные сети

Java Anonymous Proxy

Анонимные сети — это компьютерные сети, созданные для достижения анонимности в Интернете и работающие поверх глобальной сети. Особенность таких сетей заключается в многоуровневом шифровании и распределенном характере построения (т. е. в отсутствии главного узла системы), позволяющем сделать перехват трафика или даже взлом части узлов сети не критическим событием. Крупные анонимные сети, такие как RetroShare, Tor, I2P и др., достойны отдельных глав, которые вы найдете в этой книге далее. А сейчас мы познакомимся с понятием об анонимных сетях и основными их представителями.

Основы анонимных сетей

Здесь мы рассмотрим десятку наиболее крупных так называемых *анонимных сетей* и способы доступа к ним. Надо отметить, что обеспечение анонимности не означает повышения безопасности, — наоборот, при работе под их прикрытием возрастает риск установки вредоносного программного обеспечения или возможности подвергнуться еще какой-либо угрозе. Обязательно учитывайте, что одно только использование анонимной сети не обеспечивает вам скрытности и безопасности, — подлинная анонимность складывается из многих факторов. Поэтому незаконные действия, выполняемые с применением анонимных сетей, рано или поздно будут пресечены.

В анонимных сетях скрывается множество нелегальных торговых площадок оружия, наркотиков, порнографии (в том числе и детской), ворованных аккаунтов и реквизитов банковских карт. Стоит иметь в виду, что все это относится к разряду запрещенного законом, — за приобретение незаконных товаров или услуг можно надолго лишиться свободы. В анонимных сетях обретается также множество хакеров, фрикеров и тому подобных субъектов, поэтому здесь (как и в целом в Интернете) вы не должны указывать любые свои персональные данные, банковские реквизиты и пр.

В дальнейшем изложении ссылки на подобные ресурсы не публикуются, а вся информация приведена лишь с ознакомительной целью. Итак, познакомимся с анонимными сетями.

ВКРАТЦЕ ОБ АНОНИМНЫХ СЕТЯХ

Анонимными **называются компьютерные сети, созданные для достижения анонимности в Интернете и работающие** ***поверх*** **Всемирной паутины. Специфика таких сетей заключается в том, что их разработчики вынуждены идти на компромисс между степенью защиты и простотой использования. Важен также и аспект сохранения анонимности и конфиденциальности в условиях какого-либо давления на оператора сервера. При этом, в зависимости от наличия или отсутствия в сети центральных серверов, анонимные сети условно подразделяются на децентрализованные и гибридные. Многоуровневое шифрование и распределенный характер анонимных сетей устраняют единую точку отказа и лишают смысла однонаправленный вектор атак, что позволяет сделать перехват трафика или даже взлом части узлов сети не критическим для сети в целом событием. Однако за анонимность приходится расплачиваться увеличением времени отклика, снижением скорости, а также большими объемами сетевого трафика.**

Децентрализованные анонимные сети

В децентрализованной сети любой компьютер может установить соединение с другим компьютером, а также послать ему запрос на предоставление ресурсов. Каждый компьютер сети выступает при этом в роли сервера, обрабатывая запросы других компьютеров и отсылая им ответы, а также выполняя другие вспомогательные и административные функции. Гарантии постоянного соединения с любым из компьютеров сети нет — соединение может прерваться в любой момент времени. Но когда сеть достигает определенного размера, в ней одновременно начинает существовать множество серверов с одинаковыми функциями, между которыми могут происходить переключения.

Далее будет рассмотрен ряд современных децентрализованных анонимных сетей, а с тремя из них: Freenet, I2P и RetroShare — вы познакомитесь детальнее в *главах 14-16.*

ANts P2P

ANts P2P — файлообменная пиринговая сеть 3-го поколения, созданная в 2003 году и отличающаяся, благодаря механизму туннелирования и двухуровневому шифрованию AES, повышенной безопасностью. В этой сети, в отличие от BitTorrent, участники обмениваются трафиком не напрямую, а через несколько узлов. Каждому участнику известен только IP-адрес его непосредственного соседа. Таким образом, отправитель не знает, куда отправлен его файл, а получатель не знает, откуда он получен.

Загрузить дистрибутив клиента для сети ANts P2P (рис. 13.1) можно по адресу sourceforge.net/projects/antsp2p/, а руководство по работе с программой вы найдете на сайте tinyurl.com/eezq4.

ВИРТУАЛЬНАЯ МАШИНА JAVA

Для работы клиента ANts P2P необходимо установить виртуальную машину Java, дистрибутив которой доступен по ссылке java.com/ru/download/.

Загрузив и распаковав архив с дистрибутивом, запустите из папки клиента файл ANtsP2P.jar. Инсталлированное приложение ANts P2P подключается посредством глобальной сети к другим клиентам, установленным на компьютерах совершенно незнакомых пользователей, в результате чего выстраивается анонимная сеть, с помощью которой пользователи могут безопасно передавать различные файлы и информацию через виртуальные асимметрично зашифрованные туннели между узлами. Имеется в этом приложении и встроенный клиент IRC для обмена сообщениями в реальном времени.

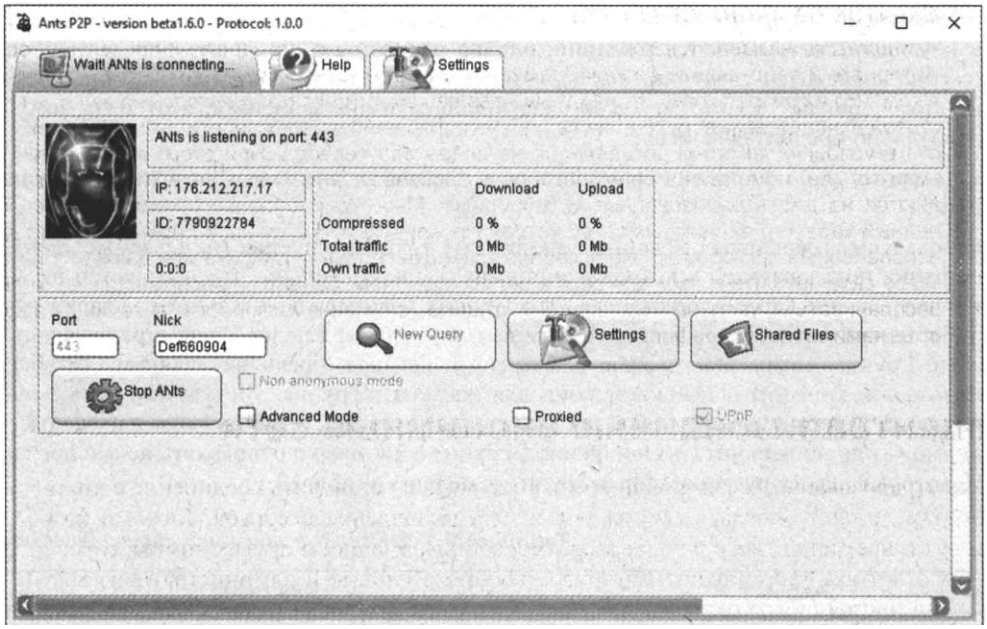


Рис. 13.1. Интерфейс]ava-клиента для сети ANts P2P

Зашифрованные пакеты, которые проходят через промежуточные узлы сети, не могут быть перехвачены на этих узлах. А для обмена ключами шифрования служит алгоритм, позволяющий двум сторонам получить общий закрытый ключ на основе использования незащищенного от прослушивания, но защищенного от подмены, канала связи.

Bitmessage

Bitmessage — криптографическая система обмена электронными сообщениями с открытым исходным кодом, позволяющая пользователям отправлять зашифрованные сообщения другим пользователям системы. В этом смысле Bitmessage может быть использована в качестве альтернативы электронной почте. Анонимность при работе через Bitmessage обеспечивается следующим:

- отправляемые сообщения рассылаются на компьютеры *всех* других доступных участников сети, при этом осуществляется перемешивание зашифрованных исходящих сообщений каждого пользователя с зашифрованными исходящими сообщениями всех других пользователей сети;
- используются длинные адреса вида вм-биКЬКОЬ0А5ЬАЬЕбР1Х&копЬ«1АиХАс1dQ, которые могут создаваться пользователем в неограниченном количестве;
- используются алгоритмы шифрования с открытым ключом — соответственно, только назначенный получатель может расшифровать сообщение. Даже сам отправитель сообщения не сможет расшифровать свое собственное сообщение, поскольку ключ, используемый для шифрования, отличается от ключа, служащего для расшифровки;
- отправляемое сообщение не содержит адреса получателя, поэтому каждый участник сети пытается расшифровать абсолютно все приходящие из сети сообщения, в том числе ему и не предназначенные, однако из всего объема полученных в зашифрованном виде сообщений он способен расшифровать только предназначенные лично ему;

- отправитель сообщения может узнать, доставлено ли сообщение получателю или нет с помощью системы подтверждений, однако отправитель не может определить, какой именно компьютер-участник сети является истинным получателем сообщения, поскольку это сообщение хранится у всех участников сети вне зависимости от того, кому оно изначально предназначалось;
- зашифрованные сообщения хранятся в сети два дня, после чего удаляются участниками сети;
- используются децентрализованные анонимные группы общения (называемые *chan),* сообщения пользователей в которых анонимны в такой степени, что неизвестен ни адрес получателя, ни адрес отправителя. Эти группы невозможно отключить, удалив какой-либо центральный сервер или группу серверов, благодаря полной децентрализованности сети. Группы также невозм пользовать криптографические ключи для доступа к группе, достаточно знать лишь ее название. Таким образом, любой пользователь Bitmessage, знающий имя и адрес рассылки, может анонимно читать сообщения в группе и анонимно отправлять новые послания. Некоторые адреса русскоязычных групп приведены в табл. 13.1.

Таблица 13.1. *Список русскоязычных групп* Bitmessage

Имя	Адрес	Описание
	BM-207\Л/074MiiuyxAC8n3(2M371AMt<00eP№	Русскоязычный канал
sharereactor.ru	BM-20Apзi^66P\Л/(28I^Ta2HiiM3yЬnE\ЛЛ/иН8	Обмен файлами
coputerra	BM-2cX\Л/8Xi85l_\nM/д4а4уе87иоCiclET52иасip8	Журнал «Компьютерра»
ги.lipux	BM-2c119д\№1-3arCo2и20]B9oyaHPMc1eC!2]\Л/рЫ	Линуксоводы
ги.Їйитог	BM-2сип<УА9к4иННка\Л/Хл/ка7liC!I-pclиl-yiKто	Юмор
ги.чгеЬгг^егэ	BM-2c\ЛiyxC9ia7Hi89r33Pl-и P O ^ p A в е 18\nM/	Общение веб-мастеров
C E ^ P A I.	BM-2c\Л/Ь2Ш3pTliT2т124c^1У5РВРУдТРТхи	Общий канал

habrahabr.ru

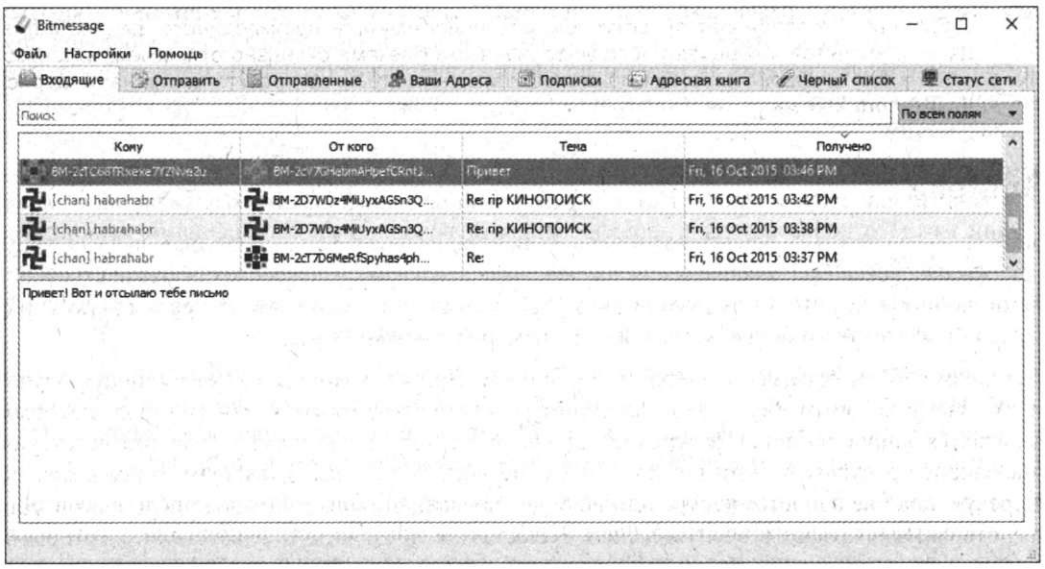


Рис. 13.2. Интерфейс клиента для сети Bitmessage

Официальный клиент Bitmessage (рис. 13.2) доступен для загрузки на сайте tinyurl.com/Ьр86с36 и поддерживается на платформах Windows, OS X и Linux.

Помимо официального клиента, вы можете отправлять/получать сообщения Bitmessage в практически любой обычной программе электронной почты — например, в Mozilla Thunderbird или Почте Windows.

Freenet

Freenet — это децентрализованная и строго анонимная одноранговая сеть, работающая поверх Интернета, включающая большое количество равноправных компьютеров и позволяющая публиковать любые материалы без возможности определить отправителя. Конфиденциальность данных гарантируется строгой криптографией — чтобы получить файл, в запросе требуется сообщить ассоциированный с ним ключ.

Создание Freenet является попыткой устранить цензуру средств коммуникаций пользователей. По существу, основной концепцией Freenet является убеждение, что никому не позволено решать, что приемлемо, а что — нет. В сети поощряется терпимость к ценностям других, а, в случае отсутствия последней, пользователей просят закрыть глаза на контент, который противоречит их взглядам.

Подробнее про сеть Freenet вы узнаете из *главы 14.*

PERFECT DARK

Perfect Dark — разработанный в Японии и находящийся в настоящее время на стадии открытого тестирования клиент для анонимной одноименной файлообменной сети, основанной на модификации протокола Kademlia. В целом структура сети Perfect Dark напоминает новейшие версии Freenet, но только с более интенсивным использованием распределенных хеш-таблиц. Анонимность сети Perfect Dark базируется на отказе от использования прямых соединений между конечными клиентами, сокрытии IP-адресов и полном шифровании всех передаваемых данных, причем направление движения трафика подчиняется известной вероятности, а распределенное файловое хранилище не имеет определенной структуры, что осложняет попытки доказать нелегальность производимого файлообмена. Данные хранятся и передаются зашифрованными блоками отдельно от ключей, использованных для шифрования этих блоков. Официальная страница проекта доступна по адресу tinyurl.com/2tyewa.

Gnutella

Gnutella — полностью децентрализованная файлообменная сеть, созданная в 1999 году. Сеть формируется при подключении одного пира к другому и позволяет обмениваться любыми данными. В результате полной децентрализации сеть практически невозможно уничтожить, т. к. для этого потребуется вывести из строя каждый ее узел.

Механизм работы сети заключается в следующем. При подключении к сети клиент получает от узла, с которым ему удалось соединиться, список из пяти активных узлов, которым отсылается запрос на поиск ресурса по ключевому слову. Узлы ищут у себя соответствующие запросу ресурсы и, если не находят их, пересылают запрос активным узлам вверх по «дереву», пока не найдется ресурс или не будет превышено максимальное число шагов. Для предотвращения отказа в обслуживании существуют правила, в соответствии с которыми запросы могут пересылать вверх по «дереву» только выделенные пиры, а остальным разрешено лишь делать запросы. Действует также система кэширующих узлов. Запросы в сети

Gnutella пересылаются по протоколу TCP или UDP, а копирование файлов осуществляется через протокол HTTP.

В 2002 году был разработан принципиально новый протокол Gnutella2 и первые его клиенты, обладающие обратной совместимостью с клиентами Gnutella. В соответствии с протоколом Gnutella2 часть узлов становятся концентраторами (хабами), остальные остаются обычными узлами. Каждый обычный узел имеет соединение с одним-двумя концентраторами, которые связаны с сотнями обычных узлов и десятками других концентраторов. Каждый узел периодически пересылает концентратору список идентификаторов ключевых слов, по которым можно найти публикуемые этим узлом ресурсы. Идентификаторы сохраняются в общей таблице на концентраторе. Когда узлу нужно найти ресурс, он посылает запрос по ключевому слову своему концентратору, который либо находит ресурс в своей таблице и возвращает идентификатор узла, обладающего ресурсом, либо возвращает список других концентраторов, которые узел вновь запрашивает по очереди случайным образом. Такой поиск называется *методом обхода сети.* Примечательной особенностью сети Gnutella2 является возможность размножения информации о файле в сети без копирования самого файла, что очень полезно с точки зрения отслеживания вирусов.

Для передаваемых пакетов в сети разработан собственный формат, гибко реализующий возможность наращивания функциональности сети путем добавления дополнительной служебной информации. Запросы и списки ключевых слов пересылаются на концентраторы по протоколу UDP. Протокол Gnutella2, по сути, не является более новой версией протокола Gnutella, а представляет его ответвление. В целом, две сети похожи между собой, отличаясь форматами пакетов и методом поиска.

Существует несколько клиентов, поддерживающих как одну только сеть Gnutella, так и мультисетевые, работающие в обеих версиях протокола Gnutella (табл. 13.2). На рис. 13.3 показан интерфейс программы Shareaza — мультисетевого клиента, поддерживающего обе версии протокола Gnutella.

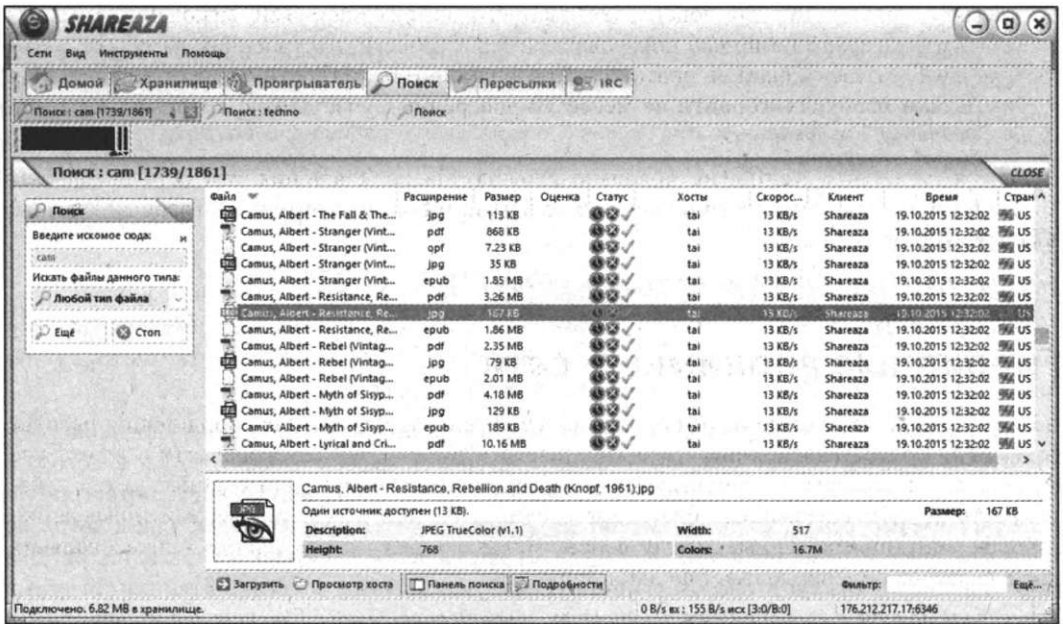


Рис. 13.3. Интерфейс клиента Shareaza

Таблица 13.2. Список популярных клиентов сети Gnutella

Название	Ссылка	Протокол	Операционная система
Gtk-Gnutelia	tinyurl.com/q4xcxvx	Gnutella	Windows, OS X, Linux
LimeWire	freelimewiredownload.net	Gnutella	Windows
PeerProject	peerproject.org	Gnutella, Gnute!la2	Windows
Phex	phex.org	Gnutella	Windows, OS X, Linux
Shareaza	shareaza.sourceforge.net	Gnutella, Gnutella2	Windows

I2P

Аббревиатура I2P расшифровывается как Invisible Internet Project, проект «Невидимый Интернет», и скрывает под собой ответвление ранее описанного проекта Freenet. Суть проекта I2P, созданного в 2003 году, — организовать свободно доступную сверхустойчивую, анонимную, оверлейную (т. е. создаваемую поверх другой сети), зашифрованную сеть и программное обеспечение, применимое для веб-серфинга, анонимного хостинга (создания анонимных сайтов, форумов и чатов, файлообменных серверов и т. д.), систем обмена мгновенными сообщениями, ведения блогов, а также для файлообмена (в том числе пирингового), электронной почты, VoIP и многого другого.

Подробнее про сеть I2P вы узнаете из *главы 15.*

RetroShare

RetroShare — платформа для децентрализованного обмена письмами, мгновенными сообщениями и файлами с помощью шифрованной F2F/P2P-сеta, построенной на основе алгоритмов GNU Privacy Guard и протокола совершенной секретности с упреждением. Для работы в сети необходимо найти не менее 10 доверенных участников, которые более или менее регулярно входят в сеть.

Несмотря на то, что RetroShare довольно сложна для подключения, эта сеть предлагает практически безграничные возможности к общению и обмену контентом, главный признак которых — безопасность.

Подробнее про сеть RetroShare вы узнаете из *главы 16.*

Гибридные анонимные сети

В гибридных сетях, в отличие от полностью децентрализованных, для координации работы, поиска или предоставления информации о существующих компьютерах в сети и их статусе используются серверы. Гибридные сети сочетают скорость централизованных сетей и надежность децентрализованных благодаря схемам с независимыми серверами индексации, синхронизирующими данные между собой. При выходе из строя одного или нескольких таких серверов сеть продолжает функционировать.

Далее рассмотрен ряд основных гибридных анонимных сетей, а с самой популярной из них — сетью Tor — вы познакомитесь детальнее в *главе 17.*

Cjdns

Cjdns представляет собой сетевой протокол, с помощью которого создаются гибридные защищенные децентрализованные сети. Протокол Cjdns может работать через обычный Интернет, создавая оверлейные сети, или напрямую — между роутерами (маршрутизаторами), образуя *ячеистую сеть* (рис. 13.4). Таковой является, например, сеть НурегЬопа.

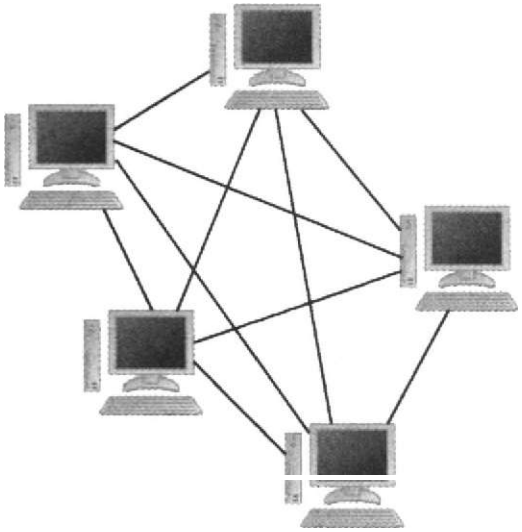


Рис. 13.4. Топология ячеистой сети

Работа сетевого протокола Cjdns осуществляется через сетевой туннель. Программы могут работать в этой сети при условии, что они поддерживают протокол IPv6. После установки нужного программного обеспечения трафик автоматически перенаправляется в эту сеть, что позволяет избежать дополнительной настройки программ. В сети на основе протокола Cjdns для пользователя генерируется IPv6-адрес, который относится к приватной части IPv6-адресов, а это означает, что коллизии между настоящим IPv6-адресом и присвоенным пользователю приватным предотвращаться не будут.

При подключении через Интернет пользователю нужно найти уже существующий узел сети и узнать его адрес и ключ. При подключении маршрутизатор-маршрутизатор — все это осуществляется автоматически. Маршрутизация трафика обеспечивается с помощью системы, аналогичной Kademlia DHT, — точнее говоря, каталог маршрутов постоянно обновляется из-за того, что конфигурация сети может поменяться. Таким образом сеть поддерживает оптимальную нагрузку через все узлы и выбирает самый короткий путь для трафика.

Трафик в этой приватной сети не может быть расшифрован никем, кроме узла, которому он должен быть доставлен. Однако сама сеть не анонимная — с помощью трассировки можно узнать цепочку узлов и выяснить реальный IPv4-адрес отправителя, впрочем, при подключении маршрутизатор-маршрутизатор эта проблема отпадает, и сеть также становится анонимной.

В данный момент протокол Cjdns находится в состоянии разработки и доступен для большинства UNIX-подобных систем, таких как Linux, OS X, FreeBSD и Illumos. Подробную информацию о сети и протоколе можно найти по адресу cjdroute.net.

Psiphon

Psiphon — канадский проект, созданный с целью обеспечения граждан стран, где осуществляется цензура Интернета, доступом к интернет-ресурсам, заблокированным сетевой цензурой. В сети Psiphon жители стран со свободным доступом к Интернету предоставляют свои компьютеры для хостинга прокси-серверов с зашифрованным соединением, используемых гражданами стран с интернет-цензурой. Доступ их к интернет-ресурсам осуществляется через доверенных участников проекта, подключенных к главному серверу Psiphon.

Для соединения с прокси-сервером через протокол SSH, SSH+ или VPN используются выдаваемые пользователю администратором прокси-сервера уникальные веб-адрес, логин и пароль без внесения каких-либо изменений в настройки браузера. Такая процедура может осуществляться только доверенными лицами, и поскольку администратор прокси-сервера владеет документированной информацией об активности своего пользователя, полная защита данных этого пользователя не обеспечивается. При этом программа предупреждает администратора об изменениях в его собственной сети, чтобы он мог предоставить пользователям новые веб-адреса.

Сеть Psiphon поддерживает анонимный веб-серфинг и ведение блогов, но не подходит для чатов и VoIP. Одна из отличительных особенностей Psiphon —- это отсутствие необходимости загружать большие программы для ее установки. Требуются лишь небольшой по размеру клиент и доступ к онлайн-службам, что является значительным преимуществом для пользователей, обеспокоенных тем, что их компьютеры могут проверить на предмет наличия на них запрещенных программ.

Каждая новая версия Psiphon упрощается, и текущая третья версия — одна из самых маленьких по размеру и незаметных программ. Загрузить приложение Psiphon можно по адресу tinyurl.com/n9avc6e.

Psiphon работает следующим образом: пользователь загружает небольшой исполняемый файл приложения, не требующий установки: либо на компьютер, либо на карту памяти, которую можно носить с собой. После запуска программы приложение Psiphon автоматически соединится с одним из серверов по зашифрованному каналу, и на экране откроется окно Psiphon (рис. 13.5).

В раскрывающемся списке в нижней части окна программы вы можете выбрать страну — местонахождение сервера. В случае, если установить соединение не получается, попробуйте перезапустить программу с правами администратора.

> ***BITMASK — ФУНКЦИОНАЛЬНЫЙ АНАЛОГ PSIPHON***
>
> **По ссылке bitmask.net/ru можно загрузить приложение Bitmask с аналогичным функционалом.**

Сеть Psiphon разрабатывалась только для работы в среде Windows и Android, поэтому пользователи OS X, iOS и других операционных систем не имеют к ней доступа. Второй недостаток Psiphon — в отличие от таких инструментов анонимности, как Tor, — в том, что она не гарантирует защиту ваших личных данных. Кроме того, некоторые блокировки Psiphon обойти не в состоянии — это зависит от вашего провайдера.

> ***ОПРЕДЕЛИТЕЛЬ ТИПА БЛОКИРОВКИ***
>
> **На страницах habrahabr.ru/post/229377/ и habrahabr.ru/post/228305/ вы найдете описание типов блокировки сайтов и инструмент для их анализа.**

Несмотря на то, что трафик внутри сети Psiphon шифруется, информацию о том, что ваш компьютер подключен к серверам Psiphon, получить можно. Защиты от анализа трафика

в сети Psiphon посторонними лицами также нет — хотя список серверов Psiphon и постоянно меняется. Это означает, что при наличии соответствующих инструментов можно определить личность пользователя Psiphon и содержание его трафика.

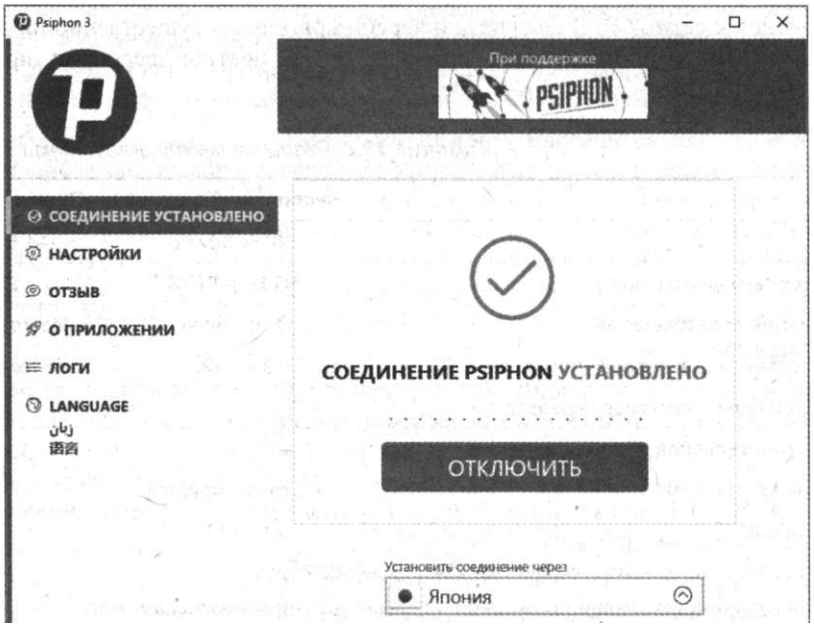


Рис. 13.5. Окно приложения Psiphon

Tor

Tor — это бесплатное программное обеспечение, служащее для организации сети, предназначенной для защиты от перехвата трафика и скрытия реального IP-адреса подключенных к ней компьютеров пользователей. Достигается это за счет передачи данных от клиентского компьютера до веб-сервера по цепочке из нескольких, случайно выбранных, узлов сети. Данные, передаваемые по такой цепочке, неоднократно шифруются, а на выходе из сети вместо адреса клиентского компьютера подставляется адрес последнего компьютера в цепочке. Такая технология называется *луковой маршрутизацией.*

Луковая маршрутизация и приемы работы в сети Tor описаны в *главе 17.*

Java Anonymous Proxy

Сеть JAP, также называемая AN.ON и JonDonym, выпадает из категорий децентрализованных и гибридных анонимных сетей и предназначена для обеспечения анонимности исключительно веб-трафика. Аббревиатура JAP расшифровывается как Java Anonymous Proxy — анонимный прокси на [языке] Java. Эта прокси-сеть позволяет, наподобие Tor, просматривать веб-контент анонимно. Пересылка трафика производится в зашифрованном виде через фиксированную группу микс-прокси-серверов, причем пользователь не может составить произвольную цепочку серверов. В результате гарантируется высокая степень анонимности, а также высокая скорость передачи данных. Компрометация анонимности клиента JAP не-

возможна без перехвата всего входящего и исходящего трафика всех узлов каскада и их содействия с целью расшифровывания пакетов. Сеть JAP также умеет использовать маршрутизаторы Tor в качестве каскада для обеспечения анонимности HTTP-трафика.

Существуют как бесплатная, так и платная (премиум) версии программного обеспечения для подключения к сети JAP. В бесплатной версии программы существенно ниже скорость подключения. Прочие различия между бесплатной и платной версиями приведены в табл. 13.3.

***Таблица** 13.3. Различия между аккаунтами в сети JAP*

Параметры	Бесплатный аккаунт	Премиум-аккаунт
Скорость	30-50 кбит/с	1-1,5 Мбит/с'
Доступные порты подключения	HTTP/HTTPS	Все**
Макс, количество пользователей	Ограничено	Неограниченно
Макс, размер файла для передачи по сети (HTTP)	2 Мбайт	Неограничен
Количество доступных регионов серверов	2	2-3
Количество микс-серверов (прокси-серверов)	2	3
Доступность подключения	Не гарантируется	99%
Поддержка S0CKS5	Нет	Да
* Указана средняя скорость, но гарантируется не менее 600 Кбит/с. ** БМТР-порт 25 блокируется всеми каскадами с целью предотвращения спам-атак.		

Стоимость премиум-подписки зависит от выбранного плана (с абонентской платой или нет) и объема оплачиваемого трафика (см. tinyurl.com/qf948pz).

Рассмотрим процесс бесплатного подключения к сети JAP:

1. **Перейдите на страницу tinyurl.com/j4ce и скачайте файл japsetup.exe — это компактная версия установщика, требующая подключения к Интернету. Можно скачать и вариант Complete setup program — полную версию установщика вместе с библиотекой Java (требуется для работы программы), которая может быть использована для установки на компьютере, не подключенном к Интернету.**

   СРЕДА ВЫПОЛНЕНИЯ JAVA

   Для работы в сети JAP необходим установленный пакет Oracle Java Runtime Environment, дистрибутив которого можно загрузить по ссылке java.com/ru/download/.

2. **После завершения установки и запуска программы вы увидите окно программы и диалоговое окно Installation assistant (Ассистент установки), показанное на рис. 13.6.**
3. **Не изменяя настроек, нажимайте кнопку Next (Далее), чтобы пропустить окно выбора языка интерфейса и окно ввода кода премиум-подписки.**

   ПРЕМИУМ-ПОДПИСКА JAP БЕСПЛАТНО

   В демонстрационных целях вы можете получить код премиум-подписки бесплатно, указав свой адрес электронной почты на сайте tinyurl.com/6n8t8ku.

4. **На следующем этапе потребуется перейти по адресу ip-check.info и, щелкнув мышью на ссылке Start test!, провести тестирование браузера на предмет подключения к JAP.**

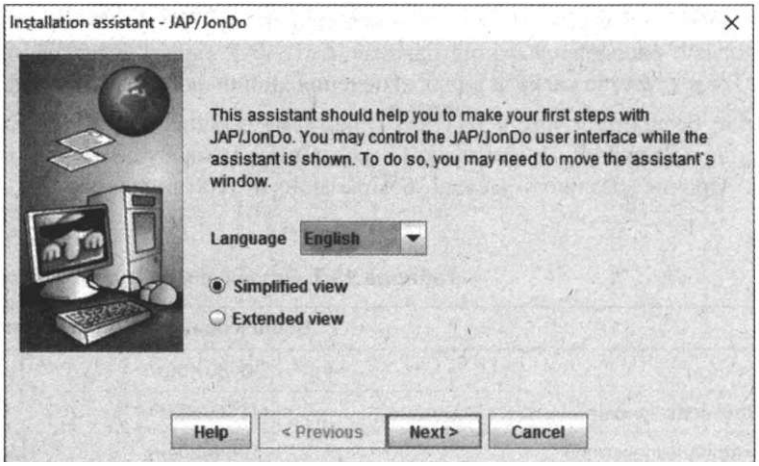


Рис. 13.6. Диалоговое окно Installation assistant

5. Получив результаты тестирования, выберите один из вариантов и нажмите кнопку Next (Далее):
   - Some data of the test site a colored in red (Некоторые результаты тестирования окрашены в красный цвет);
   - All data are either colored in green or orange (Все результаты тестирования окрашены или в зеленый, или в оранжевый цвет);
   - The test website is not shown in the browser (Страница тестирования не отобразилась в браузере);
   - I don't have a clue what to do (Я не понял, что нужно сделать).
6. В зависимости от выбранного варианта, ассистент установки может предложить вам скачать специальный профиль JonDoFox для браузера Firefox или указать IP-адрес и порт Jap в настройках браузера (рис. 13.7).

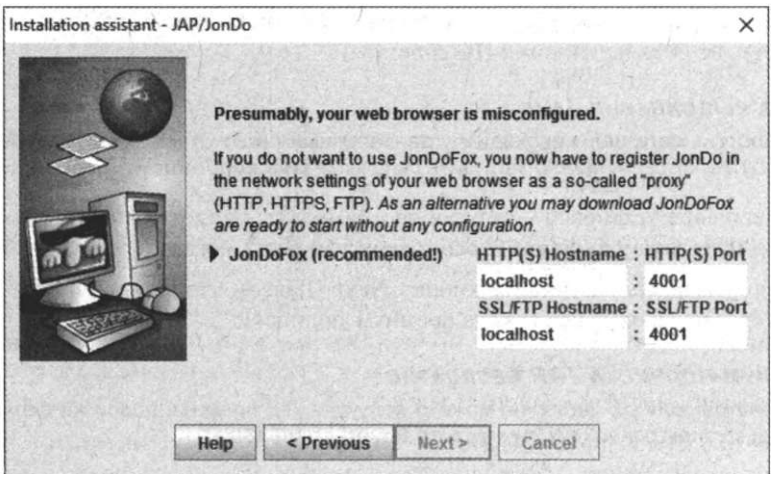


Рис. 13.7. Предупреждение о необходимости настройки браузера

1. Выполните предписанные рекомендации, не закрывая диалоговое окно ассистента установки. При этом:
   - если вы решите вместо скачивания профиля выполнить настройки браузера указанием адреса и порта для протоколов, обратитесь к *разд. «Настройка браузеров для работы с I2P» главы 15* — настройка для JAP производится аналогично, за исключением того, что IP-адрес (`localhost` на рис. 13.7) и номер порта (`4001` на рис. 13.7) нужно брать из диалогового окна **Installation assistant** (Ассистент установки);
   - в случае, если вы выберете вариант создания профиля JonDoFox (скачивается по ссылке **tinyurl.com/96mob94)** для браузера Firefox, помимо вашего профиля вы сможете каждый раз при запуске программы выбрать и специализированный (рис. 13.8). Тогда для работы через сеть JAP нужно будет выбрать профиль **JonDoFox** и нажать кнопку **Запуск Firefox** (Run Firefox).

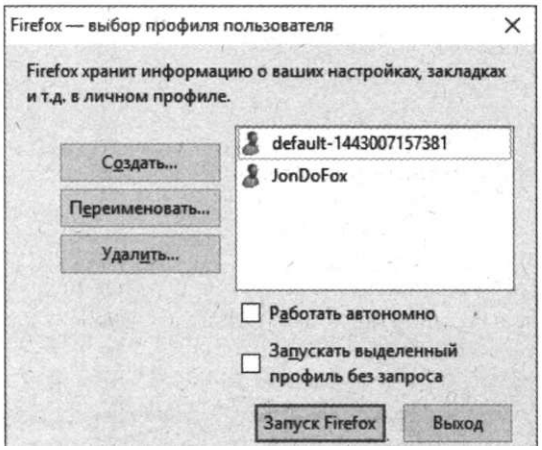


Рис. 13.8. Диалоговое окно выбора профиля браузера

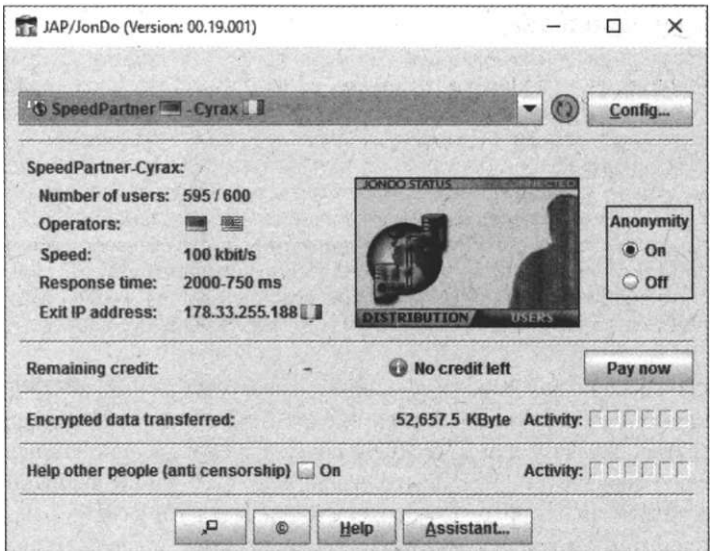


Рис. 13.9. Главное окно программы JAP

8. **Нажмите кнопку Previous (Назад) в диалоговом окне Installation assistant (Ассистент установки) и вновь пройдите тестирование. Если вы закрыли диалоговое окно Installation assistant (Ассистент установки), то можете открыть его снова, нажав кнопку Assistant (Ассистент) в главном окне программы (рис. 13.9).**

В раскрывающемся списке в верхней части окна программы можно выбрать цепочку серверов, через которую следует передавать/получать интернет-трафик (большинство цепочек доступны только при наличии платной премиум-подписки). Ниже отображается информация о выбранной цепочке серверов: количество подключенных пользователей, местонахождение серверов, скорость, время отклика и IP-адрес. Переключатель Anonymity (Анонимность) в правой части окна программы позволяет отключить (Off) или включить (On) подключение через сеть JAP.

ГЛАВА 14

Freenet: концепция свободной сети

Принцип работы

Установка и настройка клиента

Просмотр фрисайтов

Freenet — это децентрализованная и строго анонимная одноранговая сеть, работающая поверх Интернета, включающая большое количество равноправных компьютеров и позволяющая публиковать любые материалы без возможности определить отправителя.
Она представляет собой попытку устранить цензуру средств коммуникации пользователей. По существу, в основе Freenet лежит уверенность в том, что никому не позволено решать, что приемлемо. В сети поощряется терпимость к ценностям других, а в случае отсутствия последней пользователей просят закрыть глаза на контент, который противоречит их взглядам.

Принцип работы

Сеть Freenet построена на базе объединения в общий пул предоставленных ее участниками своей полосы пропускания и дискового пространства своих компьютеров для публикации в сети или получения из нее разного рода данных. Freenet использует разновидность маршрутизации по ключам, похожей на распределенную хеш-таблицу, необходимую для определения местонахождения пользовательских данных. Сеть хранит данные и позволяет извлекать их при помощи связанного с ними ключа, аналогично подобной схеме в протоколе HTTP.

Конфиденциальность данных гарантируется строгой криптографией — чтобы получить файл, в запросе требуется сообщить ассоциированный с ним ключ. Роль такого ключа выполняет хеш-код файла, или DSA-ключ, что образует также механизм проверки целостности.

Сеть обеспечивает высокую работоспособность при полной анонимности и децентрализации всех внутренних процессов. Она не имеет центральных серверов и не находится под контролем каких-либо персон или организаций. Даже создатели Freenet не имеют никакого контроля над всей сетью, кроме того, что они обновляют код. Переданная в сеть информация шифруется и распространяется по всему миру через многочисленные анонимные компьютеры сети, постоянно обменивающиеся этой информацией. Теоретически весьма слож-

но определить, какой участник хранит тот или иной файл, т. к. содержимое каждого файла зашифровано и может быть разбито на части, которые распределяются между множеством различных компьютеров.

Сеть разрабатывается с 2000 года, и хотя ее клиент статуса релиза еще не достиг, существующие версии 0.x достаточно стабильны для выполнения своих функций. При первом включении в сеть передача данных происходит существенно медленнее аналогов, но по мере работы в сети скорость возрастает.

Установка и настройка клиента

Клиент сети Freenet для операционной системы Windows, OS X или Linux можно загрузить на странице по адресу: freenetproject.org/downIoad.htmI. После установки клиента необходимо открыть в браузере страницу с адресом http://127.0.0.1:8888/.

> ***БРАУЗЕРЫ И FREENET***
>
> **Для большей безопасности при работе в сети Freenet следует задействовать для Freenet отдельный браузер, предпочтительно в режиме конфиденциальности. Следует отметить, что браузер Internet Explorer недостаточно стабильно работает с Freenet, поэтому лучше использовать Chrome, Firefox или Opera.**

В случае успешной установки и запуска клиента вы увидите страницу, показанную на рис. 14.1.

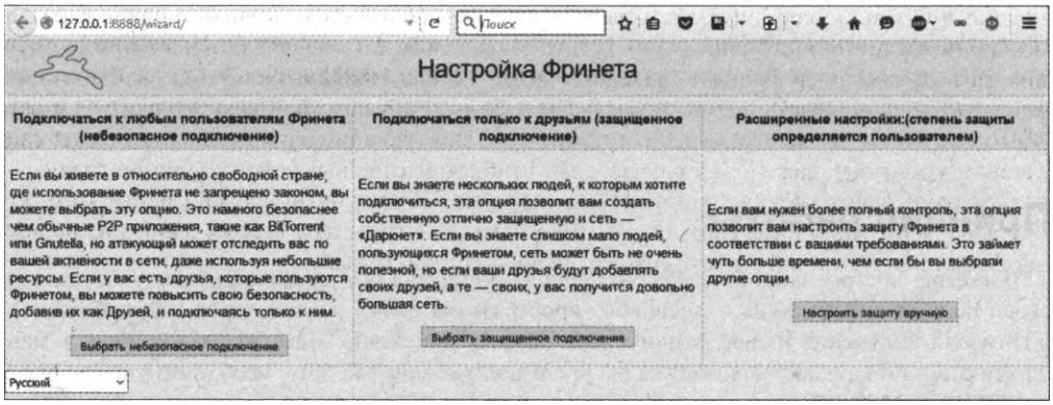


Рис. 14.1. Интерфейс мастера настройки подключения к сети Freenet

На этом этапе вы можете выбрать способ подключения: открытый — к любым пользователям сети, закрытый — к друзьям, уже пользующимся Freenet, или же вручную настроить степень защиты. Как правило, новые пользователи начинают с небезопасного способа подключения и при добавлении десяти или более друзей переходят на безопасный режим. В процессе настройки вам будет предложено воспользоваться приватным режимом браузера (которые мы рассматривали в *главе 1),* выбрать размер хранилища в диапазоне от 0,5 до 500 Гбайт (чем больше, тем выше скорость обмена данными), указать скорость подключения (выбрать определенное значение установкой переключателя или ввести свое — например: юо **мів) и т. д**. Позднее вы сможете изменить эти настройки в соответствующем разделе страницы http://127.0.0.1:8888**/seclevels/.** После завершения настроек по адресу http://127.0.0.1:8888/ будет доступна панель управления сетью, показанная на рис. 14.2.

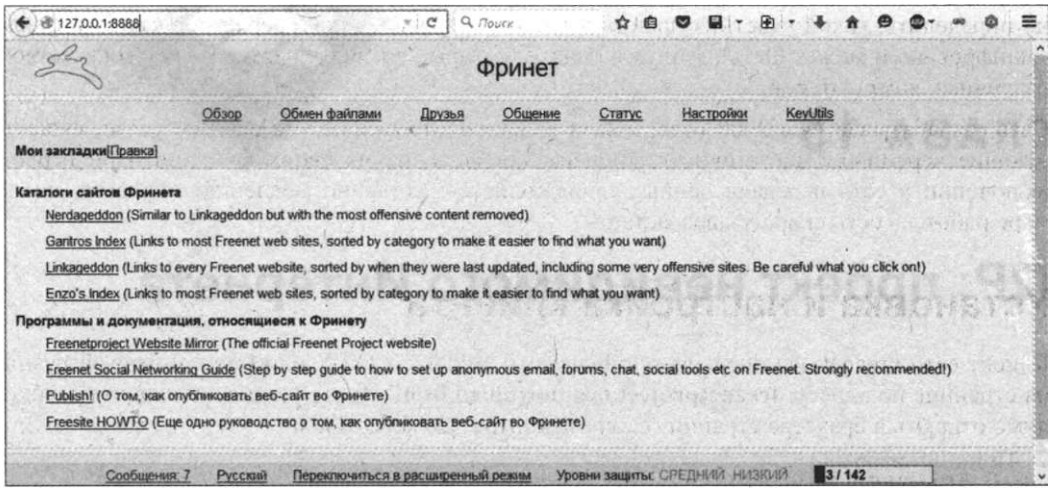


Рис. 14.2. Панель управления сетью Freenet

Просмотр фрисайтов

В разделе **Обзор** (Browse) по адресу **http://127.0.0.1:8888/** вы можете просмотреть каталог сайтов Freenet, выполнить поиск по ключевым словам (важно отметить, что согласно концепции и названию сети, публикуемый контент не фильтруется, поэтому может оказаться оскорбительным или незаконным, — будьте осторожны), а также создать и анонимно опубликовать собственный фрисайт (по адресу **http://127.0.0.1:8888/msertsite/** вы найдете соответствующее руководство). После выгрузки публикации ваш сайт будет находиться в сети настолько долго, насколько окажется популярен. При этом опубликованный в Freenet сайт останется доступен даже в том случае, если ваш компьютер выключен. И, самое важное — если уровни защиты Freenet установлены правильно, будет очень сложно найти того, кто опубликовал тот или иной сайт. На рис. 14.3 показана страница в Freenet одного из пользователей сети, на которой он опубликовал свою любимую музыку.

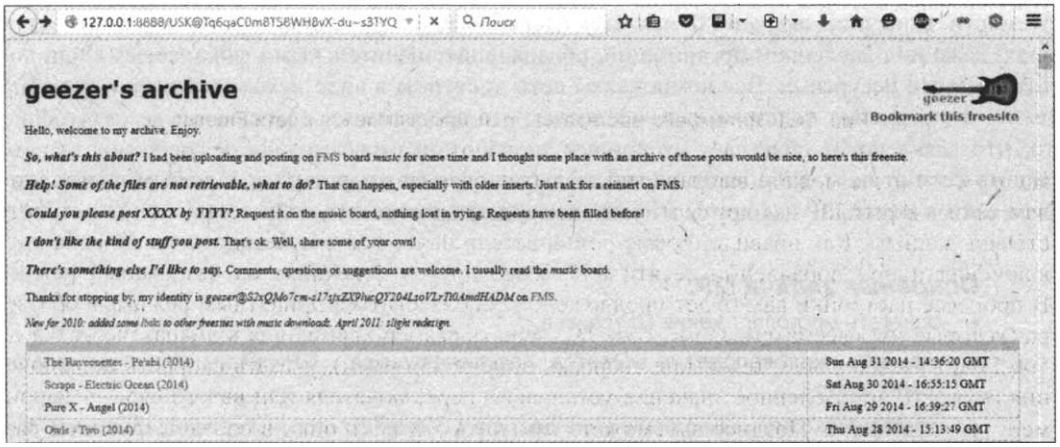


Рис. 14.3. Страница в сети Freenet

ГЛАВА 15

I2P: проект невидимого Интернета

Принцип работы

Чесночная маршрутизация

Установка программного обеспечения

Настройка браузеров для работы с I2P

Проверка работоспособности I2P

Сеть I2P (Invisible Internet Project, проект «Невидимый Интернет») представляет собой ответвление ранее описанной сети Freenet (см. *главу 14).* **Суть проекта I2P, созданного в 2003 году, — организовать свободную и доступную, сверхустойчивую, анонимную, оверлейную (т. е. создаваемую поверх другой сети), зашифрованную сеть и программное обеспечение, обеспечивающее веб-серфинг, анонимный хостинг (создание анонимных сайтов, форумов и чатов, файлообменных серверов и т. п.), работу систем обмена мгновенными сообщениями и ведения блогов, а также файлообмен (в том числе пиринговый), электронную почту, VoIP и многое другое.**

Основу I2P составляет защищенная децентрализованная анонимная компьютерная сеть с малым временем отклика и свойствами автономности, отказоустойчивости и масштабируемости. Конечной задачей I2P является способность ее функционировать в жестких условиях, даже под давлением организаций, обладающих значительными финансовыми или политическими ресурсами. Все компоненты сети доступны в виде исходного кода и бесплатны — это позволяет пользователям убедиться, что программное обеспечение делает именно то, что заявлено, и облегчает сторонним разработчикам возможность совершенствовать защиту сети от чьих-либо настойчивых попыток ограничить в ней свободное общение. Адреса сайтов в сети I2P находятся в псевдодоменном пространстве .i2p.

Основные задачи I2P:

- скрывать местоположение I2P-сайтов;
- скрывать местоположение клиентов, подключающихся к I2P-сайтам, в том числе и от самих сайтов;
- сделать невозможным ограничение доступа к сайтам со стороны провайдеров и/или магистральных узлов.

Принцип работы

Чтобы понимать, как работает сеть I2P, важно усвоить несколько ключевых понятий:

- во-первых, I2P строго разделяет программное обеспечение, участвующее в сети, — маршрутизаторы и анонимные концы (цели), связанные с отдельными приложениями. Конечные пользователи, как правило, имеют несколько локальных адресов на маршрутизаторе: например, один прокси для IRC-серверов, другой — для поддержки пользовательского анонимного веб-сервера (I2P-сайта, eepsite), еще один — для торрентов и т. д. При этом, когда используется I2P, информация о действиях пользователя, а также о том, что пользователь подключен к определенному маршрутизатору, скрывается;
- во-вторых, следует понять концепцию *туннеля.* Туннель — это ориентированный путь через явно выбранный список маршрутизаторов. Поскольку в сети I2P используется многоуровневое шифрование, каждый из маршрутизаторов может расшифровать только один слой. Расшифрованная информация слоя содержит IP-адрес следующего маршрутизатора, а также зашифрованную информацию, которая перенаправляется далее. Каждый туннель имеет начальную точку (первый маршрутизатор, также известный как *шлюз*) и конечную точку. Однако сообщения по туннелю могут быть отправлены только в одну сторону — чтобы получить обратное сообщение, требуется создать еще один туннель.

  Соответственно, для работы сети создаются туннели двух типов: *исходящий,* который отправляет сообщение от создателя туннеля, и *входящий,* который передает сообщение обратно создателю туннеля. Процесс передачи данных в сети I2P проиллюстрирован на рис. 15.1, где отправитель **(Катерина)** создает исходящий туннель, а принимающая сторона **(Михаил)** устанавливает входящий туннель. Входящий шлюз принимающей стороны позволяет получать сообщения от других пользователей и пересылать их до конечной точки (в данном случае, это **Михаил).** При передаче сообщения исходящая конечная точка (на рис. 15.1 обозначена как **Исходящая точка)** должна отправить сообщение на входящий шлюз принимающей стороны. Для этого отправитель **(Катерина)** добавляет в зашифрованное сообщение соответствующие инструкции. Как только исходящая конечная точка расшифрует сообщение, она получит инструкцию по пересылке сообщения на правильный входящий шлюз;

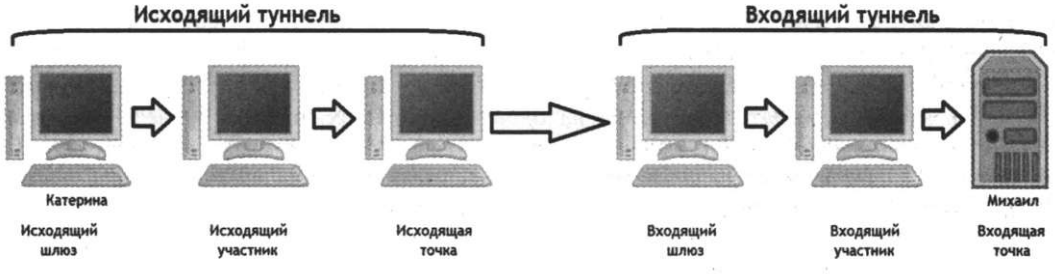


Рис. 15.1. Процесс передачи данных в сети I2P

- в-третьих, следует упомянуть сетевую базу данных NetDB. Существует два типа метаданных, хранящихся в `router.info` и `leaseSet`. Метаданные `router.info` содержат информацию о маршрутизаторах, необходимых для обмена данными (их открытые ключи, адреса и т. д.), а leaseSet предоставляет маршрутизаторам информацию, необходимую для связи конкретных точек и создания из шлюзов туннеля, который позволяет ДОС-

тичь получателя. Маршрутизаторы пересылают свои данные `router.info` в NetDB напрямую, а данные leaseSet направляются через исходящий туннель для обеспечения анонимности, чтобы избежать корреляции маршрутизатора с его leaseSet .

Для создания собственных входящих и исходящих туннелей Катерина производит в поиск для сбора данных router.info и составляет списки пиров, которые может использовать в качестве транзитных участков в своих туннелях (рис. 15.2, *а).* Затем она отправляет сообщение в первый транзитный участок с запросом на создание туннеля и перенаправление запроса далее. Процедура выполняется до тех пор, пока туннель не будет построен (рис. 15.2, б).

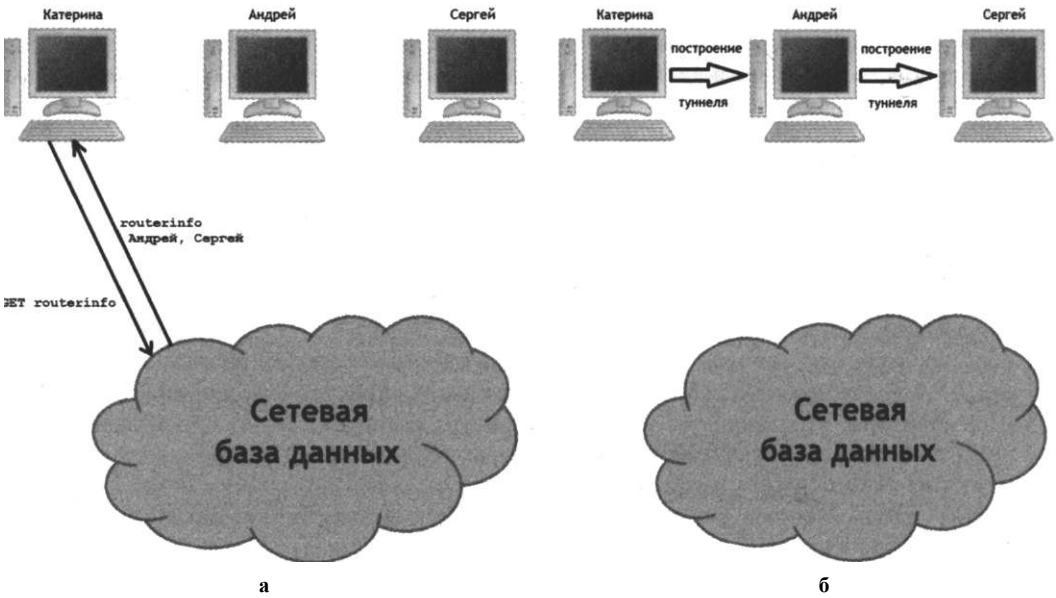


Рис: 15.2. Запрос данных в сетевой БД (а) и построение туннеля (б)

Таким образом, если Катерина хочет послать сообщение Михаилу, она сначала выполняет поиск в NetDB, чтобы найти значение leaseSet Михаила и получить информацию о текущих входящих туннелях Михаила. Затем она выбирает один из своих исходящих туннелей и отправляет сообщение по нему с инструкциями для исходящей конечной точки, чтобы переслать сообщение на один из входящих шлюзов туннеля Михаила. Когда в исходящем туннеле конечная точка получает эти инструкции, она передает сообщение с запросом, и когда входящий шлюз туннеля Михаила получает запрос, он направляется вниз по туннелю к маршрутизатору Михаила (рис. 15.3).

Если Катерина хочет, чтобы Михаил ответил на сообщение, она должна передать инструкцию явно, как часть самого сообщения. Это может быть сделано путем создания более высокого слоя, осуществляемого в потоковой библиотеке. Опционально, Катерина может также сократить время отклика, вкладывая свое последнее значение leaseSet в сообщение, так что Михаилу, к
в NetDB для обращения к Катерине.

Несмотря на то, что сами туннели при помощи многослойного шифрования защищены от несанкционированного доступа к участникам внутри сети («транспортный слой» зашифро-

ван сам по себе), чтобы скрыть сообщение отправителя на пути от исходящей до конечной точки туннеля и входящего шлюза, необходимо добавить дополнительный слой шифрования. Это обеспечивается так называемым *чесночным* шифрованием, которое позволяет маршрутизатору Катерины обернуть несколько сообщений в одно «чесночное», зашифрованное открытым ключом, что не даст промежуточному участнику определить количество сообщений и их содержимое. Так, для установки связи между Катериной и Михаилом сообщение будет зашифровано открытым ключом, опубликованным в leaseset Михаила, что позволит ему прочитать зашифрованное сообщение на маршрутизаторе Михаила.

В целом, такая технология называется *чесночной маршрутизацией.*

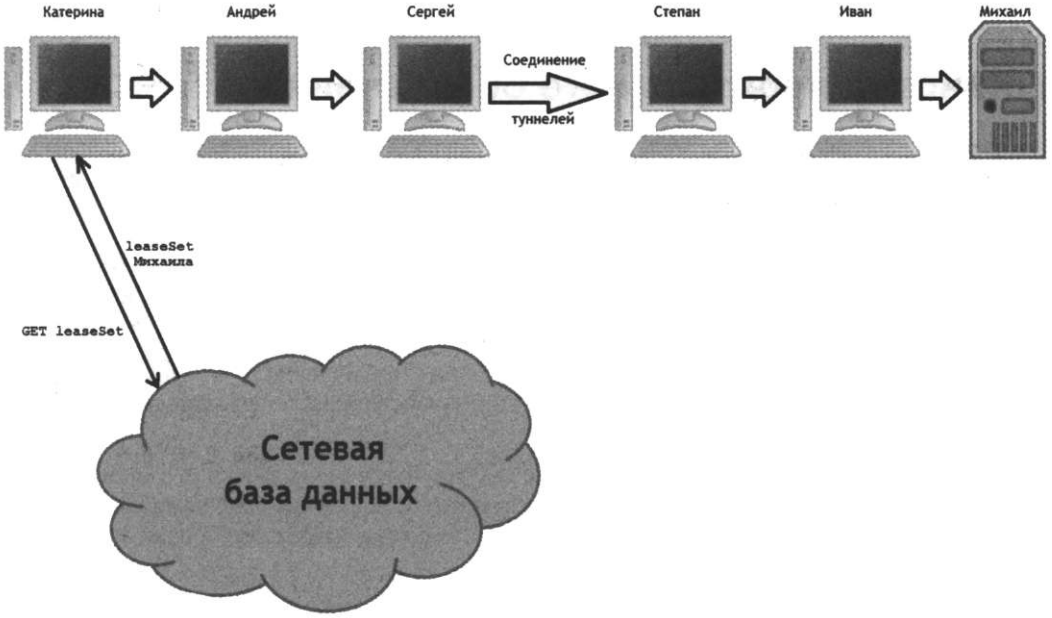


Рис. 15.3. Процесс построения туннеля в сети I2P

Чесночная маршрутизация

Чесночная маршрутизация — это технология анонимного зашифрованного обмена информацией через компьютерную сеть, используемая в анонимной сети I2P и являющаяся расширением *луковой маршрутизации,* на которой основан проект Tor (см. *главу 17).*

Суть этой технологии в том, что при использовании многослойного шифрования единственное сообщение (так называемый *чеснок)* может содержать в себе множество *зубчиков* — полностью сформированных сообщений вместе с инструкциями по их доставке. В один «чеснок» в момент его формирования перед отправкой закладываются множество «зубчиков», являющихся зашифрованными сообщениями как нашего узла, так и чужими — транзитными. Является ли тот или иной «зубчик» в «чесноке» нашим сообщением или это чужое транзитное сообщение, которое просто проходит через нас, знает только создатель «чеснока», — никто иной узнать эту информацию не может. Чесночная технология применяется тогда, когда нужно отправить, зашифрованное сообщение через промежуточные узлы, у которых не должно быть доступа к этой информации.

Например, если некоторый маршрутизатор просит другой маршрутизатор поучаствовать в общем туннеле, он помещает этот запрос в «чеснок», шифрует его открытым алгоритмом и передает через туннель. Если же клиент хочет отправить сообщение в точку назначения, маршрутизатор отправителя обернет данные этого сообщения (вместе с другими сообщениями) в «чеснок», зашифрует этот «чеснок» открытым алгоритмом, опубликованным в leaseSet получателя, и передаст его через соответствующие туннели.

Инструкции, присоединенные к каждому «зубчику» внутри зашифрованного слоя, включают возможность запроса, чтобы «зубчик» был отправлен локально к удаленному маршрутизатору или к удаленному туннелю на удаленном маршрутизаторе. В этих инструкциях есть поля, позволяющие промежуточному узлу запрашивать задержку отправки в определенный промежуток времени или условия встречи.

Установка программного обеспечения

Рассмотрев вкратце принципы функционирования сети I2P, обратимся к практической части и познакомимся с официальным программным обеспечением, доступным на сайте по адресу: geti2p.net/ru/.

> ***СРЕДА ВЫПОЛНЕНИЯ JAVA***
>
> Для работы в сети I2P необходим установленный пакет Oracle Java Runtime Environment, дистрибутив которого можно загрузить по ссылке java.com/ru/download/.

Загрузив установочный пакет I2P со страницы geti2p.net/ru/, запустите его исполняемый файл двойным щелчком мыши, после чего, следуя указаниям мастера установки, инсталлируйте приложение.

В процессе установки или при первом запуске программы (в зависимости от указанных при установке настроек) может потребоваться разрешить соединения для компонентов Java Runtime Environment в брандмауэре Windows, а также указать типы сетей, в которых разрешены такие соединения.

Установив программу и настроив брандмауэр, можно приступить к настройке I2P и браузера. Управление программой осуществляется через консоль — специальную веб-страницу, открываемую в браузере после запуска программы.

На начальном этапе следует убедиться в работоспособности программы. Для этого запустите программу I2P с помощью ярлыка Start I2P (no window). Если в браузере откроется веб-страница с консолью I2P (рис. 15.4), установка прошла успешно. В дальнейшем открыть консоль I2P можно будет двойным щелчком на ярлыке I2P router console.

В операционной системе OS X при установке программного обеспечения I2P могут возникнуть сложности из-за необходимости пакета Java 6. Поэтому сначала установите в этой ОС пакет Java 6, доступный по ссылке tinyurl.com/ozgkufe. Дело в том, что для работы I2P здесь требуется именно устаревшая версия Java 6, несмотря на то, что новая версия Java 8 уже может быть в OS X установлена ранее.

1. Итак, в операционной системе OS X загрузите JAR-дистрибутив пакета I2P с сайта geti2p.net/ru/ и установите его.
2. Запустите службу I2P щелчком мыши на файле Start I2P Router. Если запуск произойдет успешно, вы увидите консоль управления I2P, показанную на рис. 15.4.

   В противном случае, понадобится использовать файл скрипта runplain.sh, доступный в той же папке /Applications/i2p, что и файл Start I2P Router. Самый простой способ вы-

полнить скрипт — это запустить приложение Терминал (Terminal) и перетащить файл скрипта runplain.sh в окно терминала, как показано на рис. 15.5. После выполнения сценария откроется окно браузера, и вы увидите консоль управления I2P (см. рис. 15.4).

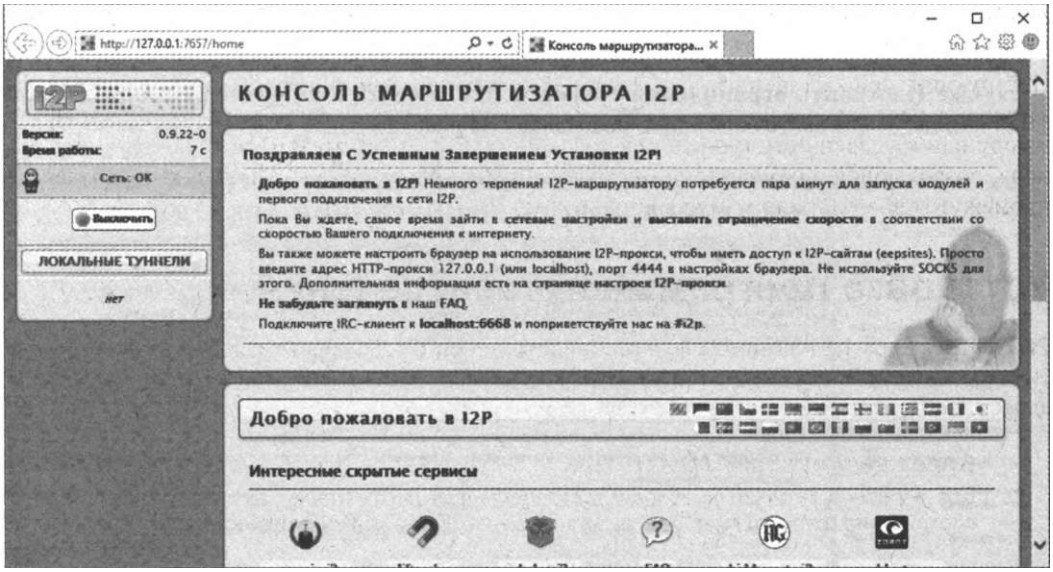


Рис. 15.4. Консоль управления I2P

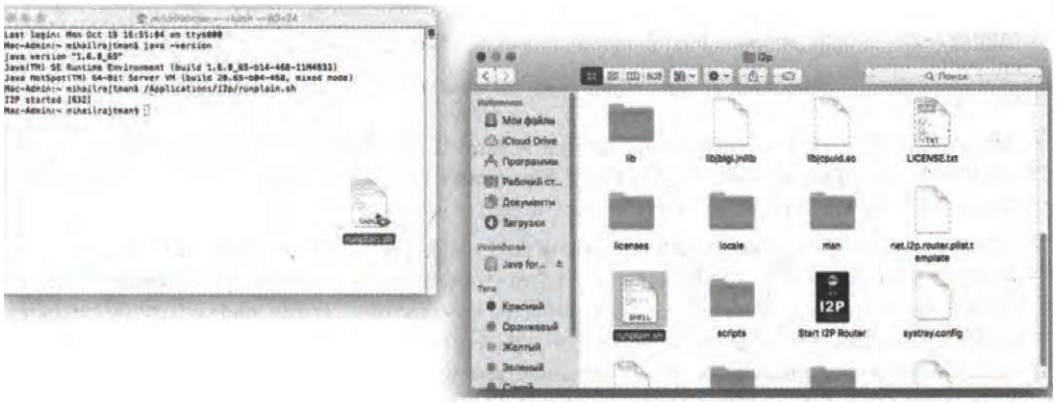


Рис. 15.5. Использование скрипта runplain.sh

В окне консоли отображаются элементы управления, ссылки на разделы настроек и справочной информации, а также данные о текущем состоянии подключения. Сразу после запуска программы в правой части страницы консоли открывается стартовая страница с кратким описанием возможностей сети и ссылками на различные внешние ресурсы, а также проверяется доступность подключения к Интернету и сети I2P.

Проверить состояние подключения к I2P можно в строке Сеть (Network) в левой части страницы консоли. Как правило, если статус проверки сети не содержит слова ОШИБКА (ERR), то программа находится в рабочем состоянии, однако желательно настроить саму

программу и брандмауэр таким образом, чтобы статус был OK. В этом случае программа будет работать наиболее эффективно.

Далее следует установить ограничение скорости и определить долю транзитного трафика — потока данных, которые будут проходить через ваш компьютер от одного участника сети к другому.

1. Для настройки ограничения скорости и доли транзитного трафика щелкните мышью на ссылке Настроить ограничения скорости (I2P Network Configuration) в нижней части страницы — откроется страница, показанная на рис. 15.6.

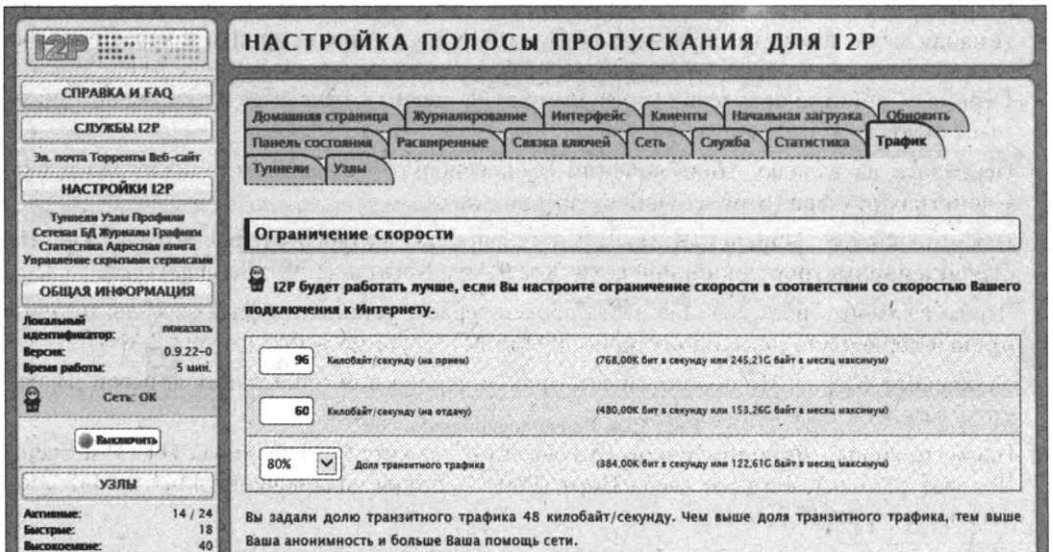


Рис. 15.6. Раздел **Настройка полосы пропускания для I2P**

2. В подразделе Ограничение скорости (Bandwidth Limiter) введите в поля Килобайт/секунду (на прием) (KBps In) и Килобайт/секунду (на отдачу) (KBps Out) скорость подключения к Интернету, которую вы хотите выделить для работы с сетью I2P.
3. В раскрывающемся списке Доля транзитного трафика (Share) выберите долю пропускной способности, которую вы готовы предоставить программе для передачи данных между другими участниками сети через ваш компьютер. Этому параметру не рекомендуется присваивать значение менее пятидесяти процентов, поскольку чем выше доля транзитного трафика у пользователей сети, тем быстрее будет работать сеть и тем выше анонимность каждого пользователя.
4. Для сохранения настроек нажмите кнопку Сохранить настройки (Save changes) в нижней части страницы.

Это единственная настройка, на которую следует обратить внимание при первом подключении к сети.

Завершив настройку программы, следует на работу с сетью I2P настроить браузер. При этом, для работы в сети I2P лучше выделить отдельный браузер. Доступ к I2P, как и к сети Tor (см. *главу 17),* осуществляется через внутренний прокси-сервер. В текущей версии по умолчанию задействованы только HTTP- и HTTPS-соединения, для которых назначается адрес 127.0.0.1 и порты 4444 и 4445 соответственно. Эти настройки используются как для

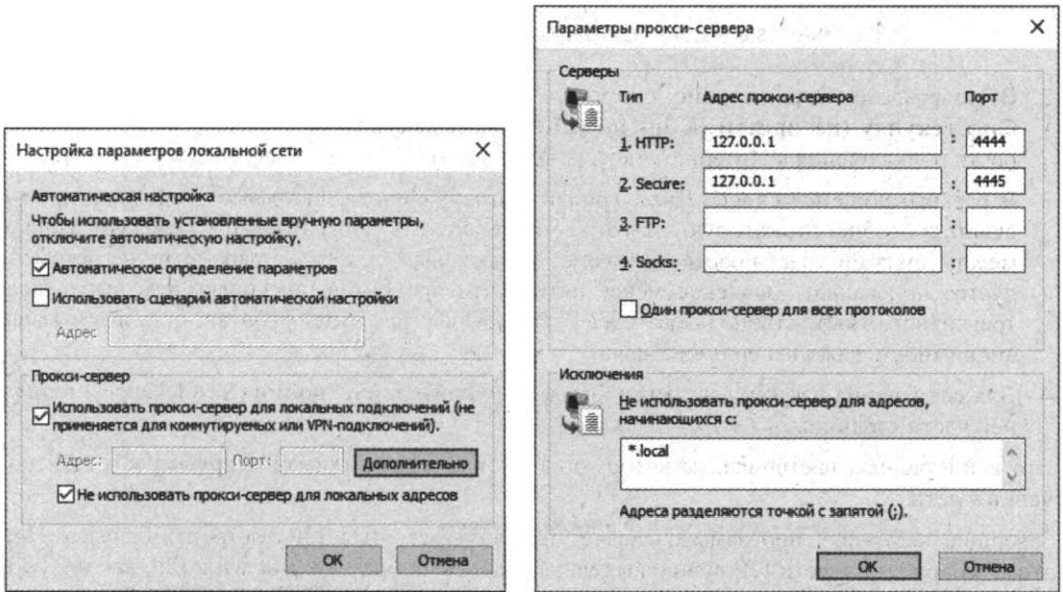
доступа к внутренним анонимным сайтам сети (их адрес заканчивается на .12p), так и для анонимного серфинга в Интернете.

Настройка браузеров для работы с I2P

Браузер Internet Explorer

Для начала настроим самый распространенный браузер — Internet Explorer. Выполните следующие действия:

1. В правом верхнем углу окна программы Internet Explorer нажмите кнопку и выберите команду меню Свойства браузера (Browser Options). Можно пройти и через основное меню: нажмите клавишу <Alt>, а затем выберите в появившейся строке меню команду Сервис | Свойства браузера (Tools | Browser Options), — откроется одноименное диалоговое окно.
2. Перейдите на вкладку Подключения (Connections) — содержимое диалогового окна Свойства браузера (Browser Options) изменится.
3. Нажмите кнопку Настройка сети (LAN Settings)— откроется диалоговое окно Настройка параметров локальной сети (Local Area Network (LAN) Settings) (рис. 15.7, а).
4. Чтобы назначить подключение через прокси-сервер, установите флажок Использовать прокси-сервер для локальных подключений (Use a proxy server for your LAN).
5. Установите флажок Не использовать прокси-сервер для локальных адресов (Bypass proxy server for local addresses).
6. Нажмите кнопку Дополнительно (Advanced) и укажите в полях ввода HTTP и Secure IP-адрес 127.0.0.1, а в поле ввода Порт (Port) — порты подключения 4444 и 4445 соответственно (рис. 15.7, *б*).



а б

Рис. 15.7. Настройка параметров прокси-сервера в браузере Internet Explorer

В целях обеспечения анонимности вы можете установить для FTP-прокси те же параметры, что и для HTTP-прокси (127.0.0.1:4444).

> ***ПРИМЕЧАНИЕ для ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ***
>
> Если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения, указанные шаги недоступны. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке **Подключения** (Connections) диалогового окна **Свойства браузера** (Browser Options), и нажать кнопку **Настройка** (Settings).

7. Нажмите соответствующие кнопки OK, чтобы закрыть открытые диалоговые окна.

Браузер Mozilla Firefox

В браузере Firefox настройка I2P осуществляется следующим образом:

1. В правом верхнем углу окна программы Firefox нажмите кнопку и выберите команду меню **Настройки** (Settings). Или же, нажав клавишу <Alt>, выберите команду меню **Инструменты | Настройки** (Tools | Options). В любом случае откроется страница **Настройки** (Options).
2. Перейдите на вкладку **Дополнительные** (Advanced).
3. Выберите дополнительную вкладку **Сеть** (Network) и нажмите кнопку **Настроить** (Setup). Открывшееся после этого диалоговое окно **Параметры соединения** (Connection settings) предназначено для указания данных прокси-сервера (рис. 15.8).

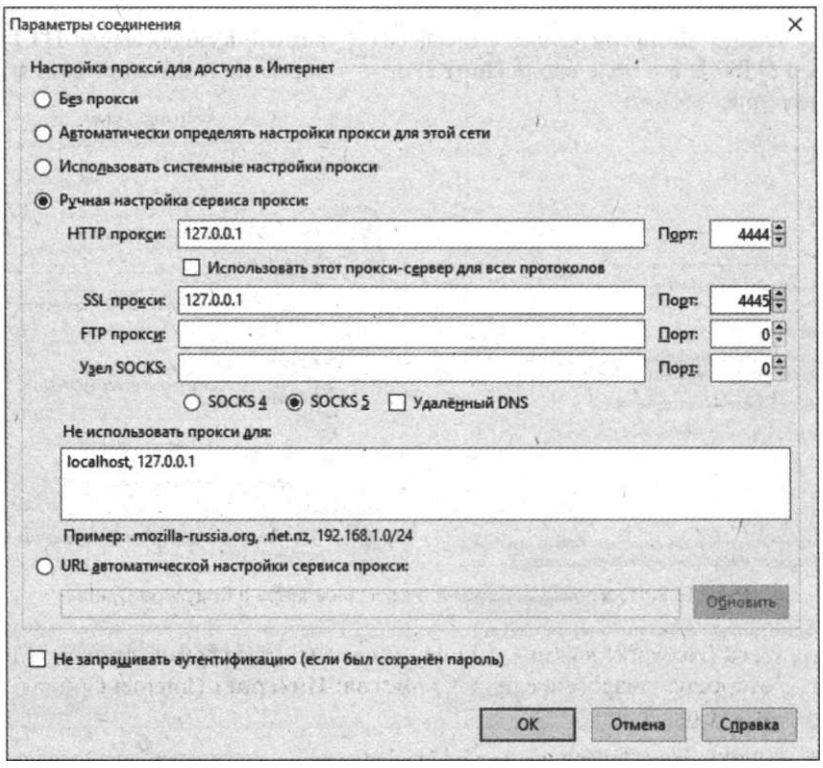


Рис. 15.8. Настройка параметров прокси-сервера в браузере Mozilla Firefox

4. Чтобы назначить подключение через прокси-сервер, установите переключатель в положение Ручная настройка сервиса прокси (Manual proxy configuration), а затем укажите в полях ввода HTTP прокси (HTTP Proxy) и SSL прокси (SSL Proxy) IP-адрес 127.0.0.1, а в поле ввода Порт (Port) — порты подключения 4444 и 4445 соответственно.

   В целях обеспечения анонимности вы можете установить для FTP-прокси те же параметры, что и для HTTP-прокси (127.0.0.1:4444).

5. Закройте открытые диалоговое окно и страницу настроек.

В операционной системе OS X настройка осуществляется аналогичным образом, только доступ к пункту Настройки (Options) осуществляется из меню Firefox.

Браузер Opera

Настройки в операционной системе Windows осуществляются следующим образом:

1. Выберите команду меню Opera | Настройки (Opera | Preferences) — откроется вкладка Настройки (Preferences) (рис. 15.9, *слева).*

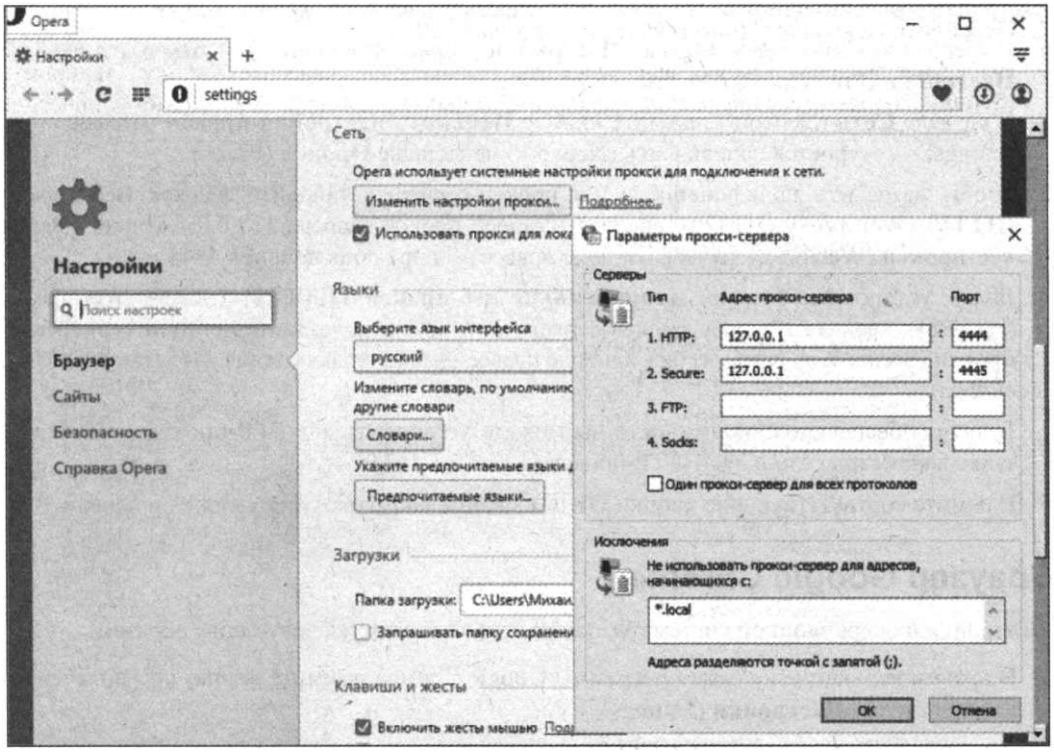


Рис. 15.9. Настройка параметров прокси-сервера в браузере Opera

2. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси (Change proxy settings) — откроется диалоговое окно Свойства: Интернет (Internet Options) на вкладке Подключения (Connections).
3. Нажмите кнопку Настройка сети (LAN Settings) — откроется диалоговое окно Настройка параметров локальной сети (Local Area Network (LAN) Settings).

4. Чтобы назначить подключение через прокси-сервер, установите флажок **Использовать прокси-сервер для локальных подключений** (Use a proxy server for your LAN).
5. Установите флажок Не **использовать прокси-сервер для локальных адресов** (Bypass proxy server for local addresses).
6. Нажмите кнопку **Дополнительно** (Advanced) и укажите в полях ввода **HTTP** и **Secure** IP-адрес 127.0.0.1, а в поле ввода **Порт** (Port) — порты подключения 4444 и 4445 соответственно (рис. 15.9, *справа).*

   В целях обеспечения анонимности вы можете установить для FTP-прокси те же параметры, что и для HTTP-прокси (127.0.0.1:4444).

   ПРИМЕЧАНИЕ для ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ

   Если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения, указанные шаги недоступны. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке **Подключения** (Connections) диалогового окна **Свойства браузера** (Browser Options), и нажать кнопку **Настройка** (Settings).

7. Нажмите соответствующие кнопки OK, чтобы закрыть открытые диалоговые окна.

Настройки в операционной системе OS X осуществляются следующим образом:

1. Выберите команду меню **Opera | Настройки** (Opera | Preferences) — откроется вкладка **Настройки** (Preferences) (см. рис. 15.9, *слева).*
2. **В** разделе **Сеть** (Network) нажмите кнопку **Изменить настройки прокси** (Change proxy settings) — откроется панель **Сеть** (Network) на вкладке **Прокси** (Proxy).
3. Чтобы назначить подключение через прокси-сервер, установите флажок **Веб-прокси (HTTP)** (Web proxy (HTTP)), введите IP-адрес прокси-сервера 127.0.0.1 в поле **Сервер веб-прокси** (Web proxy server), а в поле правее — порт подключения 4444.
4. Далее установите флажок **Защищенный веб-прокси (HTTPS)** (Secure Web proxy (HTTPS)), введите IP-адрес прокси-сервера 127.0.0.1 в поле **Защищенный сервер веб-прокси** (Secure Web proxy server), а в поле правее — порт подключения 4445 (см. рис. 15.11, *справа).*

   В целях обеспечения анонимности вы можете установить для **FTP-прокси** (FTP Proxy) те же параметры, что и для HTTP-прокси (127.0.0.1:4444).
5. Нажмите соответствующие кнопки OK и чтобы закрыть открытые окна и панели.

Браузер Google Chrome

Настройки в операционной системе Windows осуществляются следующим образом:

1. В правом верхнем углу окна программы Google Chrome нажмите кнопку и выберите команду меню **Настройки** (Settings).
2. Щелкните мышью по ссылке **Показать дополнительные настройки** (Show advanced settings) — вид диалогового окна изменится (рис. 15.10, *слева).*
3. В разделе **Сеть** (Network) нажмите кнопку **Изменить настройки прокси-сервера** (Change proxy settings) — откроется диалоговое окно **Свойства: Интернет** (Internet Options) на вкладке **Подключения** (Connections).
4. Нажмите кнопку **Настройка сети** (LAN Settings) — откроется диалоговое окно **Настройка параметров локальной сети** (Local Area Network (LAN) Settings).

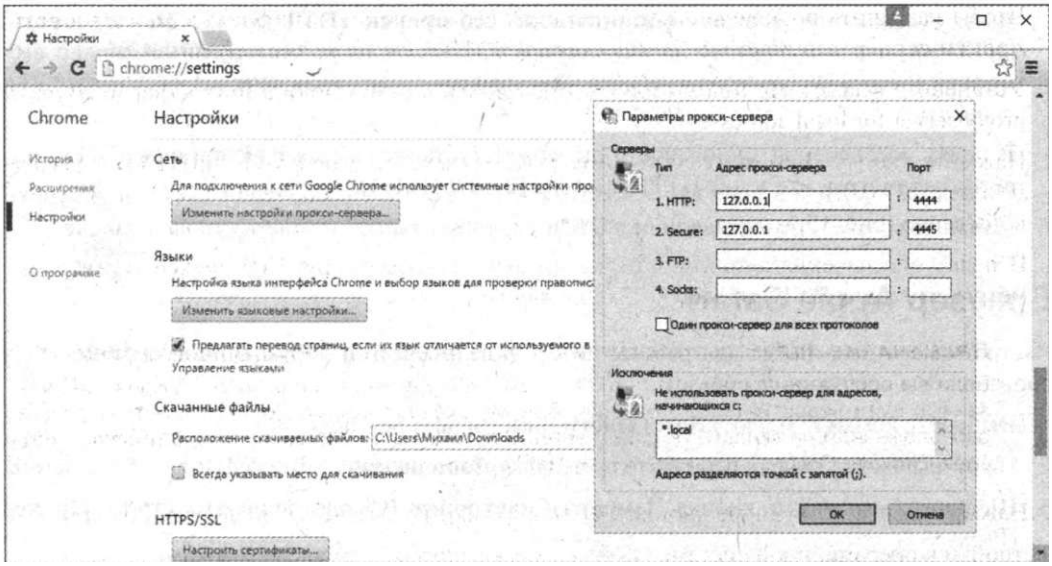


Рис. 15.10. Настройка параметров прокси-сервера в браузере Google Chrome

5. Чтобы назначить подключение через прокси-сервер, установите флажок Использовать прокси-сервер для локальных подключений (Use a proxy server for your LAN).
6. Установите флажок Не использовать прокси-сервер для локальных адресов (Bypass proxy server for local addresses).
7. Нажмите кнопку Дополнительно (Advanced), а затем укажите в полях ввода HTTP и Secure IP-адрес 127.0.0.1, а в поле ввода Порт (Port) — порты подключения 4444 и 4445 соответственно (рис. 15.10, *справа).*

   В целях обеспечения анонимности вы можете установить для FTP-прокси те же параметры, что и для HTTP-прокси (127.0.0.1:4444).

> ***ПРИМЕЧАНИЕ для ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ***
>
> **Если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения, указанные шаги недоступны. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке Подключения (Connections) диалогового окна Свойства браузера (Browser Options), и нажать кнопку Настройка (Settings).**

8. Нажмите кнопку OK, чтобы закрыть диалоговое окно, и закройте вкладку Настройки (Preferences) щелчком мыши по значку X.

Настройки в среде OS X выполняются следующим образом:

1. Выберите команду меню Chrome | Настройки (Chrome | Preferences) — откроется вкладка Настройки (Preferences) (см. рис. 15.10, *слева).*
2. Щелкните мышью по ссылке Показать дополнительные настройки (Show advanced settings) — вид диалогового окна изменится.
3. В разделе Сеть (Network) нажмите кнопку Изменить настройки прокси-сервера (Change proxy settings) — откроется панель Сеть (Network) на вкладке Прокси (Proxy).
4. Чтобы назначить подключение через прокси-сервер, установите флажок Веб-прокси (HTTP) (Web proxy (HTTP)), введите IP-адрес прокси-сервера 127.0.0.1 в поле Сервер веб-прокси (Web proxy server), а в поле правее — порт подключения 4444.

5. Далее установите флажок **Защищенный веб-прокси (HTTPS)** (Secure Web proxy (HTTPS)), введите IP-адрес прокси-сервера 127.0.0.1 в поле **Защищенный сервер веб-прокси** (Secure Web proxy server), а в поле правее — порт подключения 4445 (рис. 15.11, *справа).*

   В целях обеспечения анонимности вы можете установить для **FTP-прокси** (FTP Proxy) те же параметры, что и для HTTP-прокси (127.0.0.1:4444).

6. Нажмите соответствующие кнопки OK и x, чтобы закрыть открытые окна и панели.

Браузер Apple Safari

Настройка браузера Safari для работы через прокси-сервер в операционной системе OS X производится следующим образом:

1. Выберите команду меню **Safari | Настройки** (Safari | Settings).
2. На открывшейся панели перейдите на вкладку **Дополнения** (Advanced) (рис. 15.11, *слева).*
3. Щелкните мышью на кнопке **Изменить настройки** (Change settings) в строке **Прокси** (Proxy).
4. Чтобы назначить подключение через прокси-сервер, установите флажок **Веб-прокси (HTTP)** (Web proxy (HTTP)), введите IP-адрес прокси-сервера 127.0.0.1 в поле **Сервер веб-прокси** (Web proxy server), а в поле правее — порт подключения 4444.
5. Далее установите флажок **Защищенный веб-прокси (HTTPS)** (Secure Web proxy (HTTPS)), введите IP-адрес прокси-сервера 127.0.0.1 в поле **Защищенный сервер веб-прокси** (Secure Web proxy server), а в поле правее — порт подключения 4445 (рис. 15.11, *справа).*

   В целях обеспечения анонимности вы можете установить для **FTP-прокси** (FTP Proxy) те же параметры, что и для HTTP-прокси (127.0.0.1:4444).

6. Нажмите соответствующие кнопки OK и x, чтобы закрыть открытые окна и панели.

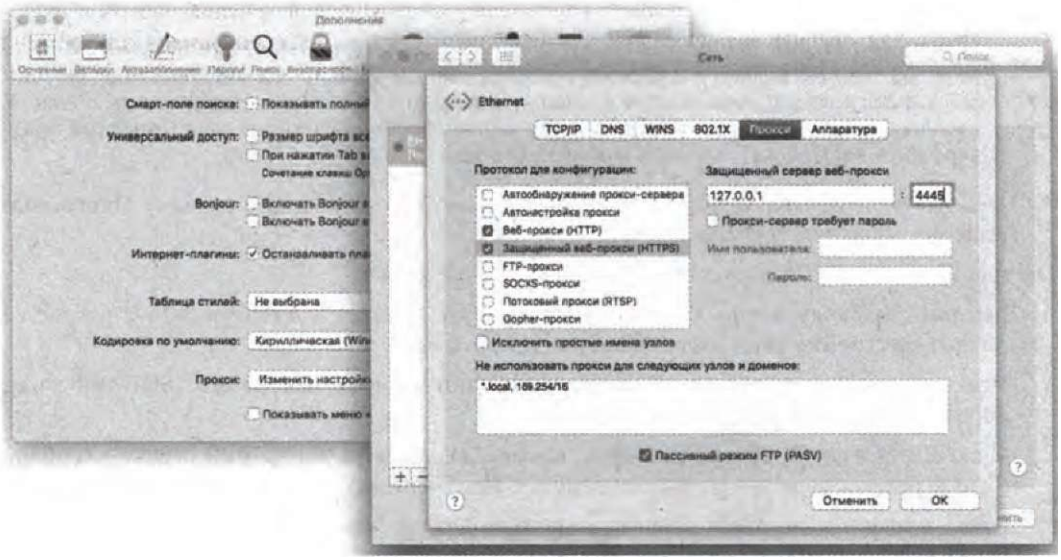


Рис. 15.11. Настройка параметров прокси-сервера в браузере Safari

Проверка работоспособности I2P

Выполнив указанные настройки, попробуйте зайти на любой внутренний сайт сети — например, на **i2p-projekt.i2p** (рис. 15.12). В некоторых случаях, особенно после первого запуска, программе может потребоваться время для создания списка адресов участников и построения туннелей для доступа к сайтам.

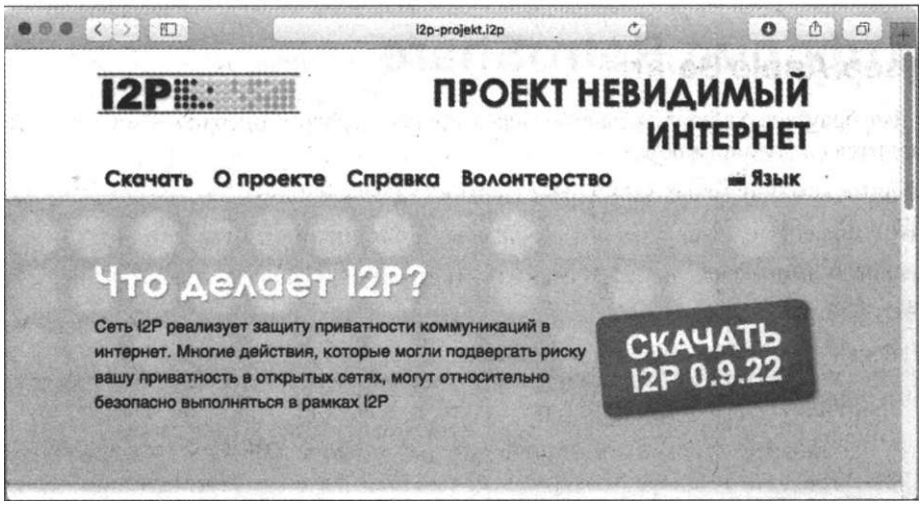


Рис. 15.12. Сайт с **доменом I2P**

Помимо доступа к внутренним сайтам сети и анонимному серфингу, вы можете воспользоваться и внутренним чатом, для чего можно подключить любой IRC-клиент. Кроме того, в программу в виде плагинов интегрированы торрент-клиент I2P8nark и почтовый клиент с веб-интерфейсом Susimail. Доступ к обеим этим программам можно получить из консоли I2P. Помимо указанных сервисов, имеются так же платформа для ведения блогов и форумов, клиент для обмена мгновенными сообщениями внутри I2P, программы для обмена файлами и другие программы и сервисы. Узнать о них можно из справочной информации в консоли управления и на официальном сайте сети.

ГЛАВА 16

Платформа RetroShare

Принцип работы

Общение в RetroShare

Обмен файлами в RetroShare

Установка и настройка клиента RetroShare

Поиск пиров

Регистрация в чате

RetroShare — платформа для децентрализованного обмена письмами, мгновенными сообщениями и файлами с помощью шифрованной F2F[1]/P2P-сети, построенной на основе алгоритмов GNU Privacy Guard и протокола совершенной секретности с упреждением.

Принцип работы

Топология RetroShare подразумевает осуществление соединений и обмен данными лишь с доверенными участниками сети и исключает как внешние контакты, так и непосредственные контакты с другими участниками, не являющимися доверенными. IP-адреса участников сети RetroShare недоступны друг другу, за исключением ограниченного круга доверенных участников — так называемых *друзей.* Все соединения с пирами, не являющимися друзьями, осуществляются посредством одной или нескольких независимых цепочек анонимных туннелей, прокладываемых между узлами сети с взаимным доверием. Взаимное доверие между участниками устанавливается на основе обмена сертификатами, содержащими открытый ключ. Подобная топология сети вместе с сильным шифрованием обеспечивает децентрализацию и анонимизацию обмена данными между участниками.

Устанавливая соединение, пользователь выбирает существующую или генерирует новую пару GPG-ключей. После проверки их подлинности и обмена асимметричными ключами соединение устанавливается по протоколу SSH, а для шифрования передаваемых сообщений служит протокол OpenSSL. Друзья друзей по умолчанию не могут соединяться, но могут видеть друг друга, если пользователи разрешили им такую возможность.

[1] **Friend 2 Friend — тип пиринговой сети, в которой участники устанавливают соединения только с теми пользователями, которым доверяют. Для аутентификации могут использоваться цифровые подписи или пароли.**

Выбранным или сразу всем друзьям можно открывать доступ к папкам своего компьютера для скачивания контента. При этом для каждой папки доступ настраивается отдельно. Можно также включить и анонимный доступ к файлам в папке — в этом случае файлы могут быть найдены только через поиск, а скачивающий не будет знать, с какого компьютера качает файл. Передача файлов происходит по сегментам через несколько транзитных участков. В целом данные передаются только между друзьями, но путь от отправителя до конечного получателя конкретного сегмента может идти через несколько друзей.

Общение в RetroShare

Все входящие/исходящие сообщения в RetroShare шифруются, и несанкционированный доступ к ним максимально затруднен. Для общения используются *чаты* **нескольких типов:**

- **в том случае, если с участником сети произведен обмен сертификатами и установлено прямое соединение, с ним возможен** *прямой приватный чат*
- *широковещательный чат* **со всеми подключенными друзьями обеспечивает простой доступ к рассылке сообщений. Сообщения, посылаемые в сеть, при этом являются широковещательными, т. е. их получат все подключенные друзья, но друзья друзей или другие пользователи RetroShare их увидеть и прочитать не смогут;**
- **доступен также** *удаленный приватный чат* **с одним из пользователей сети, позволяющий приватно связаться с лицом из** *ближнего круга,* **не являющимся в настоящее время доверенным.**

  Ближний круг — это друзья и друзья друзей с включенным полным взаимным доверием. Такой чат полезен в случае, если требуется наладить временный приватный контакт с человеком или произвести обмен сертификатами, когда передача сертификатов через публичные чат-комнаты (о них см. далее) нежелательна. Удаленный контакт реализуется через систему анонимных туннелей и возможен лишь в том случае, когда оба участника подключены к RetroShare;
- *публичные чат-комнаты* **— это самый простой и широко используемый способ общения в сети RetroShare, предоставляющий анонимность, динамичность, быстроту соединения и не требующий заметных познаний в топологии и особенностях работы платформы. Для вхождения в публичные чаты достаточно обменяться сертификатом с роботом, выбрав один из сайтов по адресу retroshare.rocks.**

  Важно отметить, что обмен сертификатами с роботом лишь позволяет быстро загрузить основные публичные чаты и не дает возможности пользоваться ресурсами сети. Для поиска и просмотра контента в RetroShare нужно найти как минимум одного участника сети, готового осуществить взаимный обмен сертификатами. В целях безопасности роботы сайтов, выбранных по указанному ранее адресу, деактивируют доверие к сертификату пользователя через 30 суток после подписания. Предполагается, что за это время потенциальный участник сети обменялся сертификатами с несколькими действительными участниками, тем самым установив взаимное доверие и осуществив подключение к RetroShare. Как только пользователь подключился к сети, необходимость подключения к чат-серверам роботов отпадает, и весь обмен данными ведется децентрализованно.

  Публичные чаты не модерируются и не цензурируются. Это значит, что там отсутствует администрирование в какой-либо форме, а также возможность наложения запрета на доступ к чат-комнате — так называемого *бана.* **Для защиты от спама имеется возможность на уровне клиента установить для нарушителей так называемый** *немой режим —*

в результате клиент будет игнорировать сообщения от одного или нескольких пользователей чата, занимающихся рассылкой спама. Для установления подлинной анонимности в публичных чат-комнатах желательно, чтобы псевдоним в чате отличался от псевдонима, указанного в GPG-сертификате пользователя. В этом случае недоброжелатель будет неспособен сопоставить псевдоним, используемый в чате, с сертификатом конкретного пользователя;

- *приватные чат-комнаты* аналогичны по своему замыслу публичным чатам за исключением того, что заходить в приватную чат-комнату можно лишь тем пользователям, которые получили приглашение от одного действительного участника этого чата, а имена приватных чат-комнат невидимы никому, за исключением их участников. Приватные чаты полезны при обсуждении каких-либо важных тем со строго ограниченным кругом лиц.

Кроме чатов для общения используется и *почтовая служба* RetroShare — наиболее мощный и ценный сервис платформы, функционал которого аналогичен широко известным службам электронной почты в открытых сетях. Однако имеются и существенные различия:

- отсутствует сервер — вся исходящая и входящая почта хранится только на локальных компьютерах участников обмена и только в шифрованном виде;
- промежуточные серверы-хранилища не используются, если получатель сообщения в сети отсутствует, — сообщение будет доставлено тогда, когда получатель подключится к сети;
- псевдонимный сервис — IP-адрес источника получателю неизвестен, отображается лишь идентификатор и псевдоним, а передача данных ведется посредством анонимных туннелей. Это означает, что третьему лицу за обозримое время невозможно не только раскрыть содержимое передаваемой информации, но и связать источник письма с его получателем;
- спам исключается, т. к. отсылка почтовых сообщений возможна лишь друзьям, либо ближнему кругу друзей;
- отсутствуют ограничения на размер вложений.

Для *голосовой связи* между двумя участниками платформы RetroShare служит VoIP-коммуникатор, реализованный в виде отдельного плагина.

Реализована в сети RetroShare и *система форумов,* разрешающая как анонимные, так и авторизованные сообщения. С ее помощью также можно обмениваться сообщениями с друзьями.

Обмен файлами в RetroShare

В сети RetroShare используется система каналов объявлений, которая позволяет автоматически загружать файлы, размещенные на конкретном канале, каждому подписчику. Реализация, сущность, цели и задачи каналов RetroShare аналогичны торрент-трекерам, однако ключевое отличие их состоит в том, что участник RetroShare является владельцем собственного канала, и по умолчанию публикации в нем разрешены только создателю канала. При этом создатель канала может передавать права на публикацию контента неограниченному числу доверенных участников. Публикации на каналах объявлений всегда анонимны — извлечение информации о псевдониме пользователя, владеющего каналом, в программе не предусмотрено. Каналы могут быть как публичными, так и приватными.

В случае публикации контента, содержащего большое количество файлов, RetroShare позволяет создавать так называемые *коллекции* — XML-файлы, содержащие структуру папок, имена файлов и их хеш-данные. С их помощью при скачивании коллекции пользователь может выбрать все или только определенные файлы.

Установка и настройка клиента RetroShare

Процедуру подключения к сети RetroShare мы рассмотрим на примере операционной системы Windows. Процедура эта предполагает три базовых этапа:

- **скачивание и установка клиентской программы;**
- **создание личного сертификата;**
- **поиск доверенных пиров.**

Несмотря на кажущуюся сложность двух последних этапов, никаких принципиальных сложностей при подключении к сети RetroShare нет. Итак:

1. **Перейдите на сайт ru.retroshare.net и скачайте дистрибутив RetroShare для своей операционной системы (поддерживаются операционные системы Windows, OS X и различные версии Linux).**
2. **Распакуйте инсталлятор из архива и запустите его.**
3. **Следуя указаниям мастера, установите программу. Во время подготовки к установке будет предложено выбрать тип установки: стандартный (с записью ключей в реестр) и портативный.**

   Для системы Windows настоятельно рекомендуется выбирать портативную установку, при которой все файлы программы будут находиться в одной папке и не будут привязаны к файловой структуре операционной системы. Такая установка впоследствии позволит осуществить перенос программы на другой компьютер простым копированием папки с установленной программой.

При первом запуске клиент RetroShare выводит на экран окно мастера, помогающего пользователю создать личный сертификат (рис. 16.1):

1. **В поле Имя (Name) укажите псевдоним пользователя.**
2. **В поле Пароль (Password) укажите желаемый пароль и подтвердите его ввод в поле ниже. Пароль может быть произвольным, но в целях безопасности лучше, чтобы его длина составляла не менее 8 символов и чтобы он содержал как буквы, так и цифры и прочие символы.**

   Пароль обеспечивает доступ к закрытому ключу и личному сертификату, содержащему открытый ключ, которые позволяют шифровать в RetroShare весь контент, начиная с сетевых транзакций и заканчивая локальными файлами.
3. **Заполните поле Узел сети (Location). Оно может сыграть существенную роль, если вы хотите пользоваться сгенерированной парой ключей на разных компьютерах — например, на двух ноутбуках дома и на компьютере в офисе. В этом случае в каждом экземпляре программы будет использоваться одни и те же закрытый и открытый ключи с различным местоположением: `home1`, `home2`, `work` — и вам не потребуется просить друзей добавить ваш сертификат несколько раз. Если же у вас один-единственный компьютер и большего их количества в обозримом будущем не предвидится, то в качестве местоположения можете указывать что угодно.**

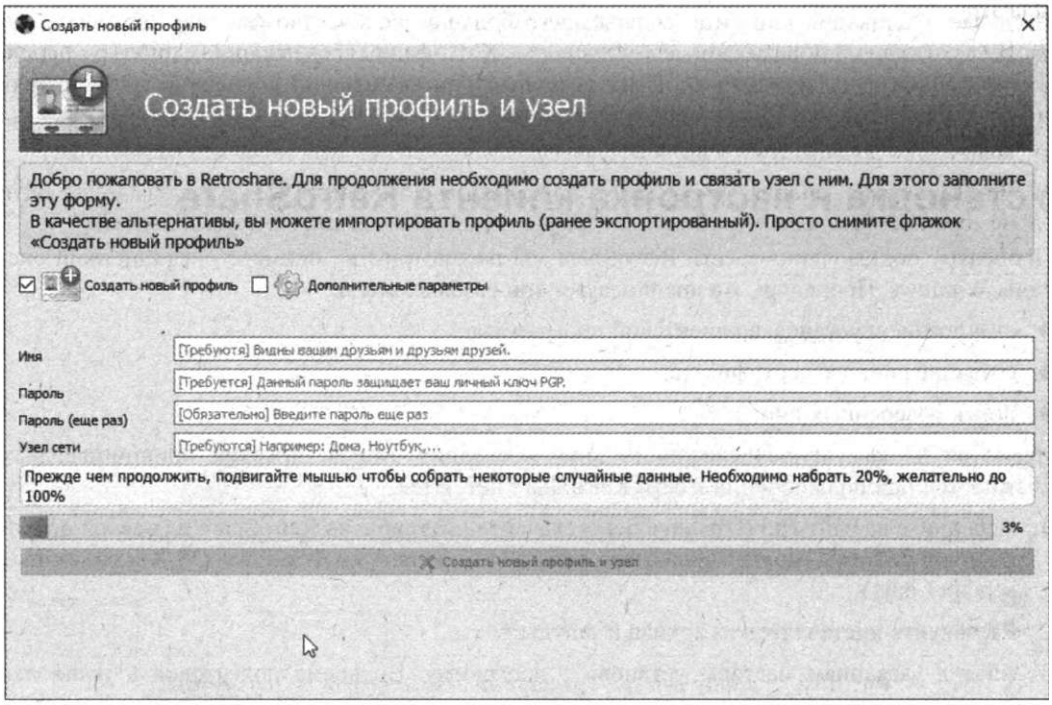


Рис. 16.1. Мастер создания профиля пользователя RetroShare

4. При генерации сертификата активно перемещайте указатель мыши по экрану и, по возможности, начните копирование любых файлов с/на жесткий диск. Так генерируемые ключи станут «более случайными».
5. При заполнении индикатора процесса до 100% нажмите кнопку Создать новый профиль и узел (Generate new profile) и авторизуйтесь в программе, введя пароль к сертификату.

ПРЕДУПРЕЖДЕНИЕ О НАЛИЧИИ ПЛАГИНОВ

При первой загрузке программы могут появиться запросы на регистрацию обнаруженных плагинов (*FeedReader.dll* и *VOIP.dll*) — в этом случае подтвердите их регистрацию, нажав кнопку Да (Yes).

ПРЕДУПРЕЖДЕНИЕ БРАНДМАУЭРА

При первой загрузке программы может появиться предупреждение об ограничении брандмауэром некоторых возможностей программы. В этом случае разрешите их использование, установив соответствующие флажки и нажав кнопку Разрешить доступ (Allow access). Таким образом вы разрешите пропускать трафик RetroShare как в домашней сети, так и в общественных сетях. В сети RetroShare шифруется весь трафик, поэтому бояться нечего — передается лишь «цифровой шум», извлечь информацию из которого смогут только адресаты.

Прежде чем начинать погружение в сеть RetroShare, следует изменить некоторые настройки клиента RetroShare, установленные по умолчанию: расширить канал обмена служебными данными и увеличить количество туннелей, предоставляемых вами другим участникам сети.

Для этого:

1. В главном окне приложения RetroShare нажмите кнопку Параметры (Options) и перейдите на вкладку Транслятор (Relay).
2. В соответствующих полях группы элементов управления Количество (Amount) укажите количество друзей, друзей друзей и прочих пользователей (как показано на рис. 16.2).

   Чем выше эти значения, тем более вы полезны для сети RetroShare, т. к. к вам будет идти не только собственный трафик, но и транзитный трафик от других пользователей.

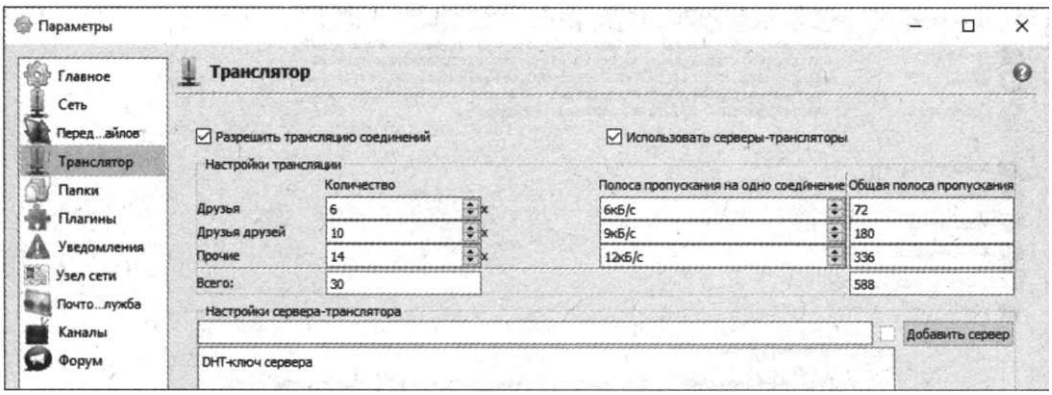


Рис. 16.2. Фрагмент вкладки Транслятор диалогового окна Параметры

3. Установите флажок Использовать серверы-трансляторы (Use translator servers), если у вас непрозрачный маршрутизатор или межсетевой экран. Такая настройка упростит вхождение в сеть. Если вы не имеете понятия о состоянии своего маршрутизатора или межсетевого экрана, то этот флажок соединение не ухудшит.
4. В соответствующих полях группы элементов управления Полоса пропускания на одно соединение (One connection bandwidth) определите значения максимально допустимой скорости на одно соединение для друзей, друзей друзей и прочих пользователей (см. рис. 16.2). Указанные здесь значения установлены для сети со скоростью подключения 10 Мбит/с и их следует увеличить во столько раз, во сколько скорость вашего соединения выше 10 Мбит/с.
5. Перейдите на вкладку Папки (Folders) и в поле Входящая папка (Input Folder) укажите целевую папку для скачиваемых файлов.
6. Закройте диалоговое окно Параметры (Options), нажав кнопку ОК.

Поиск пиров

Следующий этап предполагает поиск доверенных пиров и обмен сертификатами с ними. Предполагается, что на этом этапе у вас нет друзей, пользующихся RetroShare. Доверенных пиров можно найти в чате сети RetroShare, к которому можно подключиться, обменявшись сертификатом с одним или несколькими роботами, выбрав один из сайтов по адресу retroshare.rocks. Рассмотрим процесс по шагам:

1. В главном окне приложения RetroShare нажмите кнопку Параметры (Options) и перейдите на вкладку Узел сети (Node). Затем откройте дополнительную вкладку Сертификат (Certificate) — на ней указан ваш сертификат (рис. 16.3).

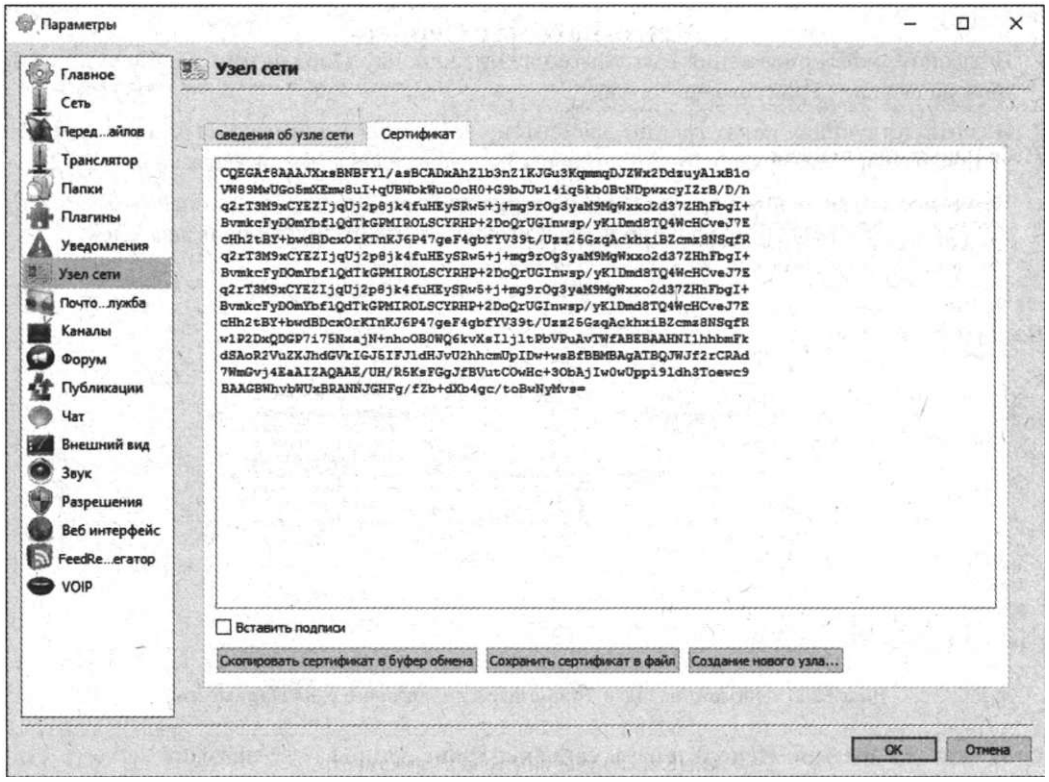


Рис. 16.3. Вкладка Узел сети диалогового окна Параметры

2. Выделите все содержимое текстового поля (с помощью комбинации клавиш <Ctrl>+<A>) и скопируйте его в буфер обмена (комбинацией клавиш <Ctrl>+<C>).

3. Перейдите по ссылке **retroshare.rocks** и, выбрав один из серверов, доступных онлайн, вставьте комбинацией клавиш <Ctrl>+<V> в соответствующее поле скопированный сертификат (рис. 16.4).

4. Введите CAPTCHA-код и нажмите кнопку **Validate** (Проверить) — через пару секунд вы увидите страницу с ключом для входа в чат.

5. Выделите код полностью, нажав кнопку **Выбрать все,** и скопируйте его в буфер обмена.

6. Перейдите к программе RetroShare и нажмите кнопку **Добавить** (Add) на панели инструментов в окне программы — вы увидите диалоговое окно мастера добавления друга (рис. 16.5).

7. Установите переключатель в положение **Ввести сертификат вручную** (Manually input certificate) и нажмите кнопку **Далее** (Next).

8. На следующей странице диалогового окна в нижнее поле вставьте скопированный с сайта **retroshare.rocks** ключ и нажмите кнопку **Далее** (Next).

9. На следующей странице (рис. 16.6) установите флажок **Аутентификация друга (Введите ключ PGP)** (Authenticate friend (sign PGP key)) и нажмите кнопку **Завершить** (Finish).

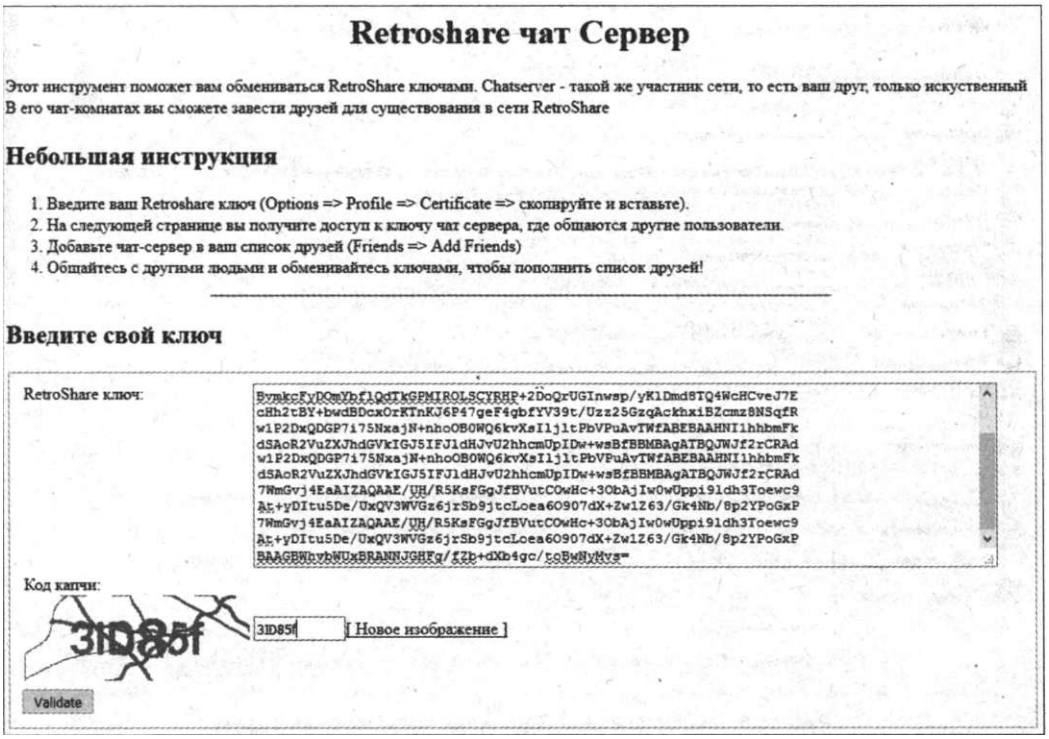


Рис. 16.4, Получение ключа к чат-комнате

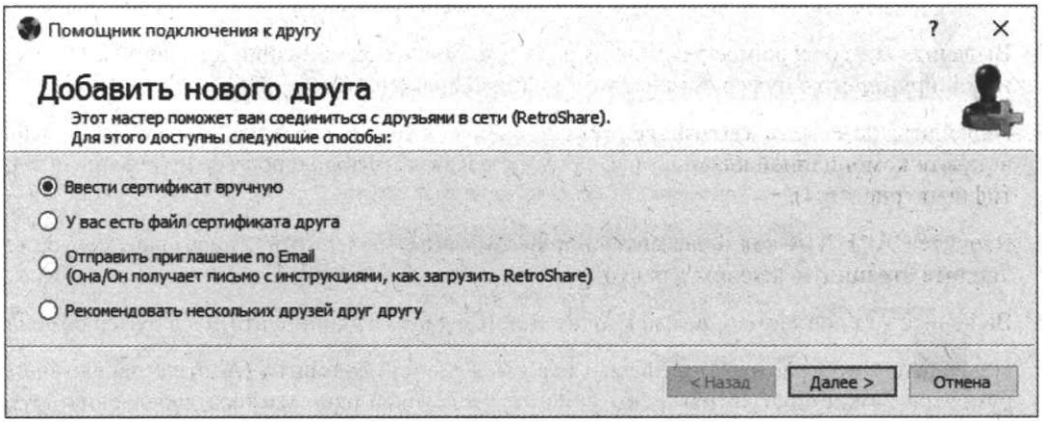


Рис. 16.5. Диалоговое окно Помощник подключения к другу (фрагмент)

10. Введите пароль к своему сертификату, созданному ранее при регистрации профиля, — отобразится окно процесса подключения (рис. 16.7, *слева).* Здесь можно нажать кнопку **ОК** — подключение к пиру будет проходить в фоновом режиме.
11. Через какое-то время появится всплывающее окно (рис. 16.7, *справа*), сообщающее о том, что мы подключились к роботу (при условии, что он в данный момент в сети). Если появилось сообщение, что друга найти невозможно, попробуйте выбрать другой чат на сайте ге1го$Ьаге.госк$ и повторить добавление друга.

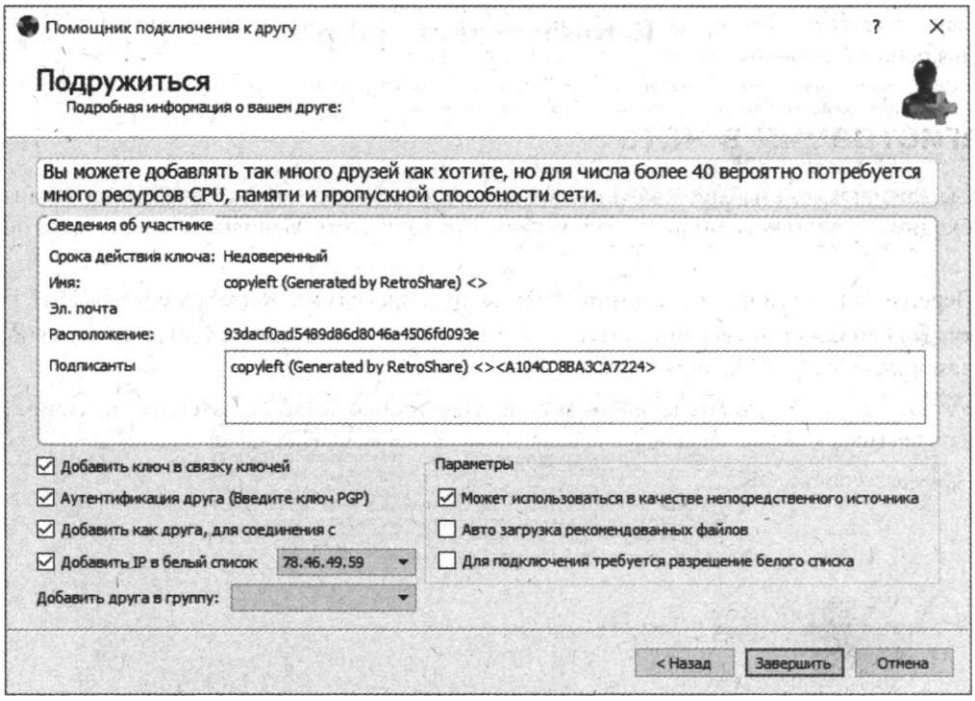


Рис. 16.6. Диалоговое окно Помощник подключения к другу

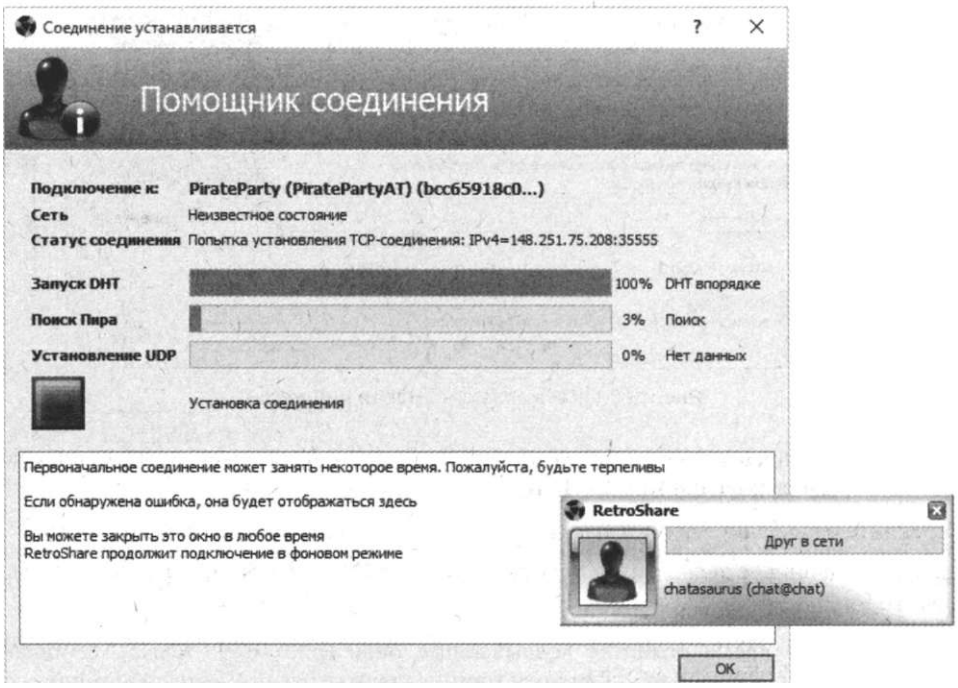


Рис. 16.7. Информация о процессе соединения (слева) и всплывающее сообщение о статусе друга (*справа)*

В результате всей этой процедуры у вас появится один (или более, если вы добавили в друзья роботов нескольких чатов) доверенный пир.

Регистрация в чате

Чтобы заходить в чаты, публиковать записи в форумах или делать объявления в каналах, необходимо создать как минимум одну личность. Для этого выполните следующие дейст-

1. Перейдите на вкладку **Участники** (People) окна программы RetroShare и нажмите кнопку **Создать новую личность** (Create new identity) — откроется диалоговое окно **Новая личность** (New identity) (рис. **16.8).**
2. Установите переключатель в положение **Псевдоним** (Nick) и введите желаемое имя в поле **Ник** (Nick).
3. Нажмите кнопку ОК.

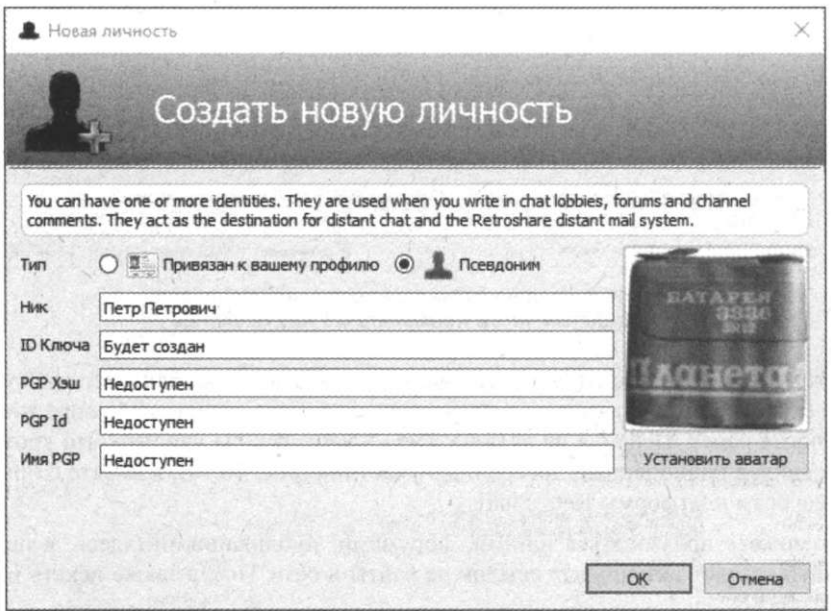


Рис. 16.8. Диалоговое окно **Новая личность**

Теперь можно подписываться на чат-комнаты. На этапе поиска доверенных узлов главный для вас чат — **Retroshare 0.6 Key Exchange.**

1. Перейдите на вкладку **Чаты** (Chat Lobbies) — вы увидите список доступных чатов.
2. Щелкните двойным щелчком по чату **Retroshare 0.6 Key Exchange,** чтобы войти в него (рис. **16.9).**

   В этом чате находятся пользователи, которые будут рады помочь вам подключиться к анонимной платформе RetroShare.
3. Щелкните правой кнопкой мыши по нижнему полю и выберите команду меню **Вставить ссылку на мой сертификат** (Link to my certificate) в контекстном меню — в поле сооб-

щения появится ссылка вида **RetroShare Certificate (nick (Generated by RetroShare), @homel).**

4. Нажмите кнопку Послать (Send), чтобы отправить сообщение. Подождите, пока кто-нибудь не ответит на ваш запрос и не опубликует ссылку (см. рис. 16.9).

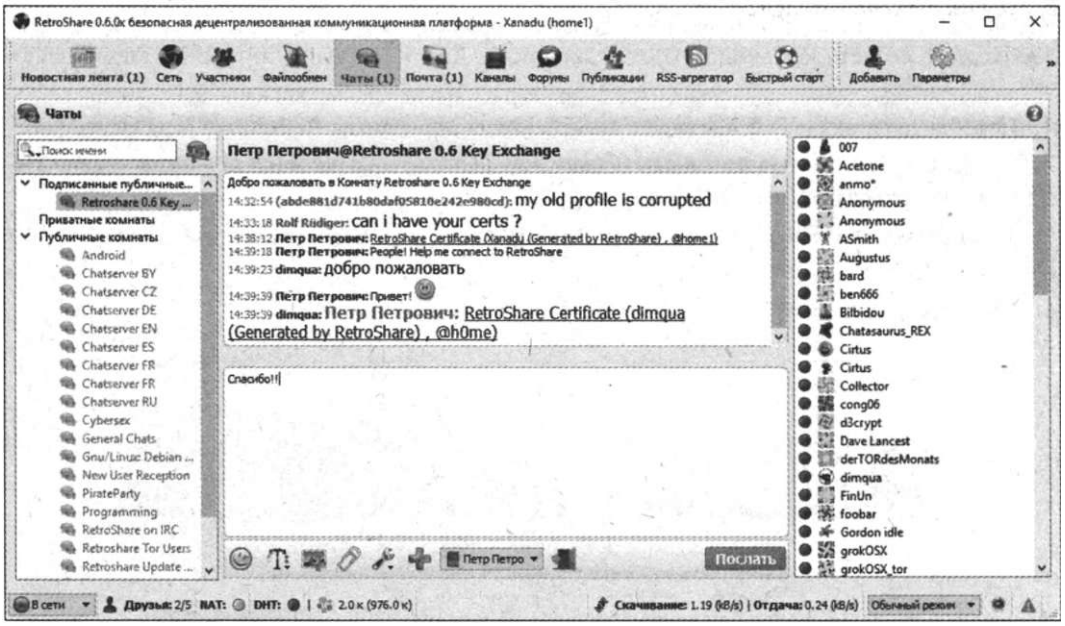


Рис. 16.9. Вкладка **Чаты** окна программы RetroShare с открытым чатом **Retroshare 0.6 Key Exchange**

5. После того, как кто-либо откликнется на вашу просьбу и опубликует ссылку на собственный сертификат, щелкните по ней мышью и добавьте доверенного пира точно так же, как и робота ранее. Перейдя на вкладку Сеть (Network), вы увидите, что кроме роботов у вас появился полноценный доверенный участник (рис. 16.10), а вместе с ним — и доступ к ресурсам платформы RetroShare.

Теперь вы можете пользоваться чатами, форумами, публикациями (здесь, к примеру, вы можете найти каталог актуальных ссылок на сайты в сети Tor), а также искать и скачивать файлы (рис. 16.11).

> ***RETROSHARE и TOR***
>
> **На странице tinyurl.com/no54zq5 вы найдете руководство по настройке работы сети RetroShare через Tor.**

Следует отметить, что на начальном этапе подключения к сети RetroShare загружаются лишь списки контента, но не сам контент. Для того чтобы каналы или форумы отображали контент, на них следует подписаться, щелкнув правой кнопкой мыши и выбрав пункт Подписаться (Subscribe).

Вы в сети — теперь остается найти не менее десяти доверенных участников, которые более или менее регулярно входят в сеть. Наиболее верная во всех смыслах стратегия вхождения в сеть RetroShare — это время. Согласно этой стратегии следует в течение двух-трех недель понаблюдать, кто есть в чатах, о чем ведется разговор, какие у кого интересы, наконец, раз-

говориться с кем-либо в публичном или приватном чате и только потом предложить тому или иному участнику обменяться сертификатами.

Несмотря на то, что RetroShare довольно сложна для подключения, эта сеть предлагает практически безграничные возможности общения и обмена контентом, главный признак которых — безопасность. Дополнительную информацию о сети RetroShare вы найдете по адресу tinyurl.com/oxedg42.

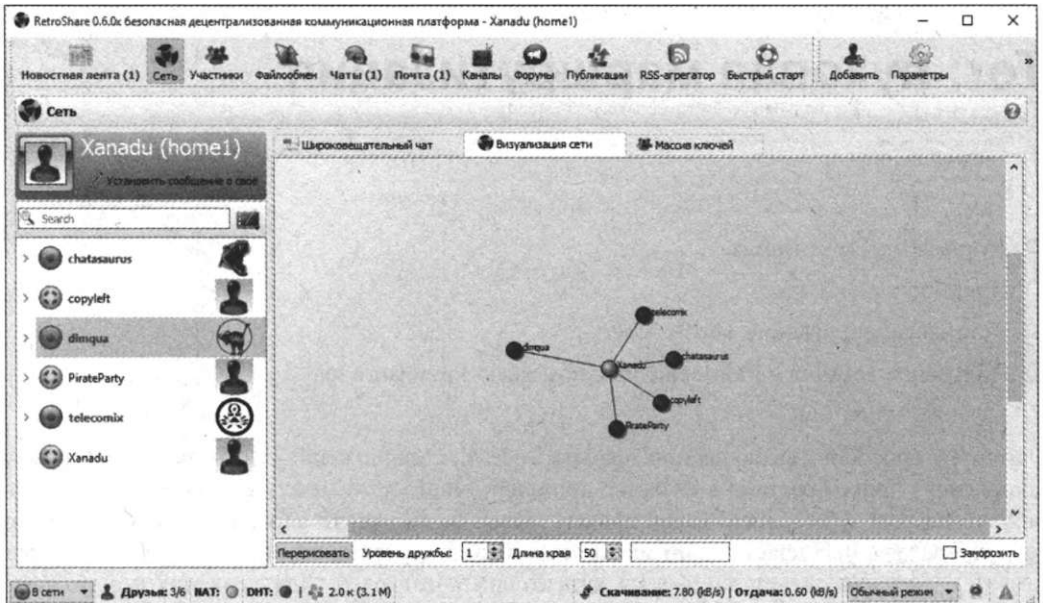


Рис. 16.10. Вкладка Сеть окна программы RetroShare с визуализацией окружения пользователя

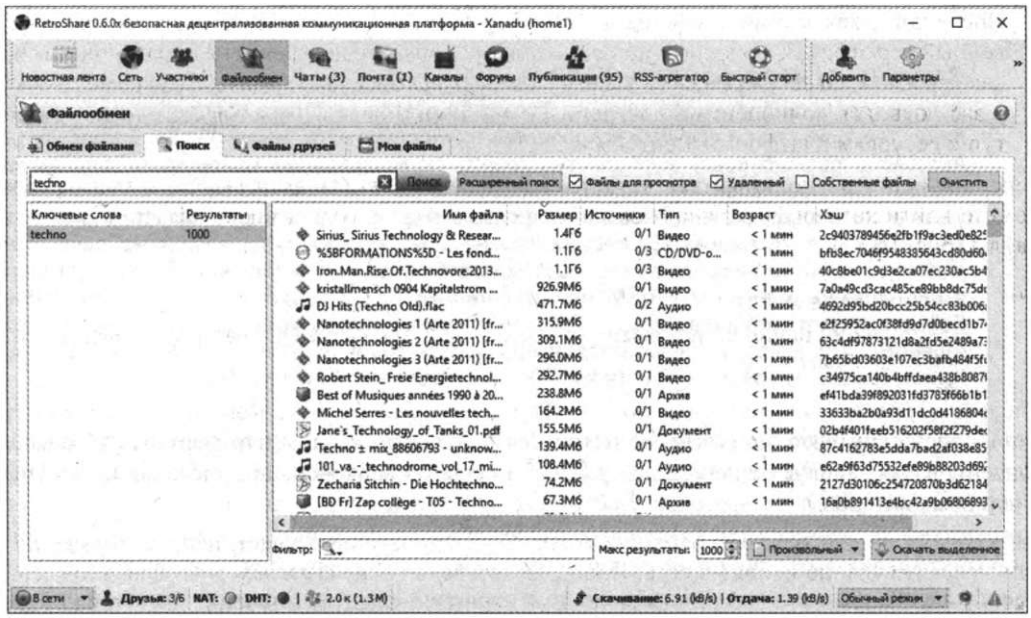


Рис. 16.11. Вкладка Файлообмен окна программы RetroShare

ГЛАВА 17

Tor: луковая маршрутизация

Луковая маршрутизация

Принцип работы Tor

Установка приложения Tor Browser

Получение доступа к Pandora.com с помощью PirateBrowser

Одним из способов, позволяющих скрыть свое местоположение, является использование анонимного прокси-сервера в качестве промежуточного узла между клиентским компьютером и сервером веб-сервиса. Такой прокси-сервер подменяет IP-адрес клиентского компьютера в передаваемых пакетах данных на свой, а при получении ответа от сервера исправляет замену и перенаправляет данные на клиентский компьютер. Для усиления безопасности можно использовать цепочки из прокси-серверов, а в качестве защиты от прослушивания — применять шифрование передаваемых данных. Пример такой технологии представляет система Tor.

ЗАКОННО ЛИ ИСПОЛЬЗОВАТЬ TOR?

Вопреки пропагандируемому мнению, Tor используется не только преступниками, педофилами, террористами и прочими нехорошими личностями. Это, мягко говоря, далеко не так. Активисты разного рода, журналисты, просто люди, любящие приватность, составляют портрет пользователей Tor. Позиция разработчиков Tor, отвечающих на вопрос «а что, у вас есть, что скрывать?», обозначена фразой: «Нет, это не секрет, — просто это не ваше дело». Вы можете заниматься своими делами дома, но вам будет неприятно, если сосед следит за вами, заглядывая в окно. То же касается и таких скандальных программ разведки в виртуальном мире, как PRISM (tinyurl.com/njz47be), X-Keyscore (tinyurl.com/ph9df6k), Echelon (tinyurl.com/p8sauhj) или Tempora (tinyurl.com/nrqnypc). К тому же, нет никаких гарантий, что никто не попытается использовать ваши данные в грязных и корыстных целях. Далеко не все люди кристально чисты, а проблемы будут ваши.

Tor — это бесплатное программное обеспечение, служащее для организации сети, предназначенной для защиты от перехвата трафика и скрытия реального IP-адреса подключенных к ней компьютеров пользователей. Достигается это за счет передачи данных от клиентского компьютера до веб-сервера по цепочке из нескольких, случайно выбранных, узлов сети. Данные, передаваемые по такой цепочке, неоднократно шифруются, а на выходе из сети вместо адреса клиентского компьютера подставляется адрес последнего компьютера в цепочке. Такая технология называется *луковой маршрутизацией.*

Луковая маршрутизация

Луковая маршрутизация — это технология, которая обеспечивает анонимный обмен информацией через компьютерную сеть. Пакеты данных, передаваемые в Интернете, состоят из двух частей: полезной нагрузки и заголовка, используемого для маршрутизации. Полезная нагрузка — это сами данные, будь то сообщение электронной почты, веб-страница или аудиофайл. В заголовке же указывается различная техническая информация, в том числе адрес отправителя и получателя.

В луковой маршрутизации данные неоднократно шифруются и в виде пакетов отсылаются через несколько сетевых узлов, называемых *луковыми маршрутизаторами.* Каждый маршрутизатор удаляет верхний слой шифрования, чтобы открыть предназначенные ему трассировочные инструкции и отослать пакеты данных на следующий маршрутизатор, где все повторяется. Таким образом, промежуточные узлы не знают источник, пункт назначения и содержание полезной нагрузки.

На рис. 17.1 показано, что зашифрованный пакет исходных данных попадает к луковому маршрутизатору (роутеру) А, который удаляет один слой шифрования и узнает, откуда получен пакет (хотя он и не знает, от отправителя или предшествующего лукового маршрутизатора) и куда направить его дальше — к маршрутизатору Б. Маршрутизатор Б получает пакет от маршрутизатора А и удаляет еще один слой шифрования, чтобы узнать, куда переслать пакет далее. Узнав это, маршрутизатор Б отправляет пакет маршрутизатору В, который удаляет последний слой шифрования и передает исходные незашифрованные данные получателю.

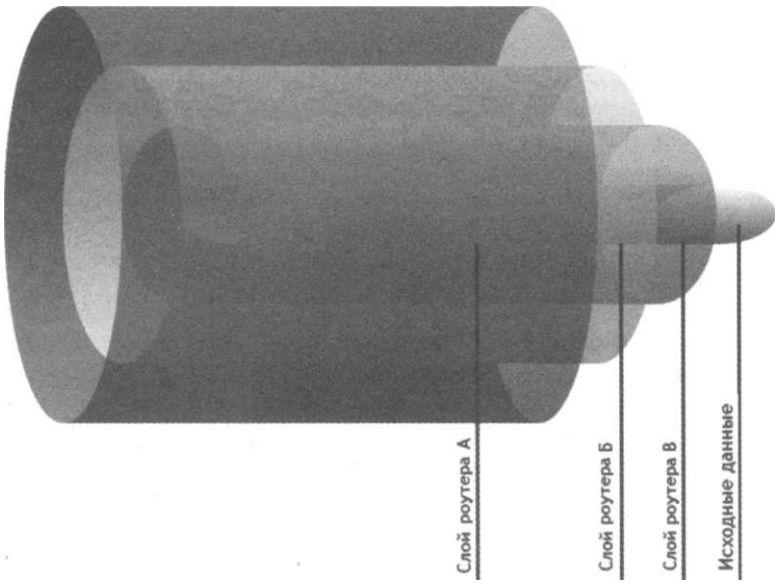


Рис. 17.1. Структура пакета данных в сети Tor

Получатель запроса может отправить ответ по той же цепочке без ущерба для анонимности каждой из сторон. При этом слои шифрования, наоборот, «наращиваются» на каждом маршрутизаторе, пока ответ не достигнет отправителя запроса. Отправитель владеет всеми ключами сессии, используемыми в цепочке, и поэтому сможет расшифровать все слои: от

внешнего, зашифрованного ближайшим к отправителю маршрутизатором в цепочке, до внутреннего, зашифрованного маршрутизатором, ближайшим к получателю запроса.

Идея луковой маршрутизации состоит в том, чтобы сохранить анонимность отправителя и получателя данных и обеспечить защиту полезной нагрузки во время ее передачи по сети. При луковой маршрутизации пакеты данных передаются из источника к месту назначения через последовательность прокси-серверов (луковых маршрутизаторов), которые перенаправляют пакеты данных в непредсказуемом направлении. Чтобы избежать «прослушивания» данных злоумышленником, между маршрутизаторами они передаются в зашифрованном виде. Преимущество луковой маршрутизации (и смешанных соединений в целом) состоит в том, что отпадает необходимость доверия каждому участвующему маршрутизатору. Даже если один или несколько из них окажутся взломанными, анонимное соединение все равно сможет быть установлено. Это достигается за счет того, что каждый маршрутизатор в такой сети принимает пакеты данных, шифрует их заново и передает их на другой луковый маршрутизатор.

Злоумышленник, имеющий возможность проводить мониторинг *всех* луковых маршрутизаторов в сети, теоретически может проследить путь пакетов данных через сеть, но задача его сильно усложняется, если он имеет доступ лишь к одному или даже нескольким маршрутизаторам на пути пакетов данных. Тем не менее, луковая маршрутизация не предоставляет гарантированную анонимность для отправителя или получателя от всех потенциальных прослушиваний — при локальном прослушивании можно просмотреть весь трафик, переданный с того или иного компьютера. Она обеспечивает лишь высокую степень несвязности, затрудняя определять отправителей и получателей.

Принцип работы Tor

Самый распространенный способ реализации луковой маршрутизации — это проект Tor (от англ. The Onion Router, луковый маршрутизатор), созданный в 2004 году. Проект представляет собой средство организации системы прокси-серверов, позволяющей устанавливать анонимное сетевое соединение, защищенное от прослушивания. Система эта реализуется в виде анонимной сети виртуальных туннелей, предоставляющей возможность передачи данных в зашифрованном виде.

С помощью Tor пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика осуществляется за счет использования распределенной сети серверов — луковых маршрутизаторов. Технология Tor также обеспечивает защиту от инструментов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых переговоров и тайну связи в целом. Tor оперирует сетевыми уровнями луковых маршрутизаторов, позволяя создавать анонимные исходящие соединения и анонимные скрытые службы.

Снижения рисков перехвата и анализа трафика Tor добивается, настраивая ваши сеансы связи через каналы, проходящие через несколько компьютеров в Интернете. Вместо построения прямого пути от источника до пункта назначения, пакеты данных в сети Tor пересылаются по случайным маршрутам через несколько серверов. При этом ни один из серверов не знает полного пути пакета данных — только от какого сервера пришли данные и куда следует их передать. Для каждого транзитного участка между серверами на маршруте генерируется отдельный набор ключей шифрования.

Допустим, у нас имеется достаточно большая компьютерная сеть. На некоторых компьютерах этой сети установлено специальное программное обеспечение, позволяющее шифровать данные и передавать его друг другу (на рис. 17.2 эти компьютеры обозначены знаком X и, по сути, представляют собой луковые маршрутизаторы). Пусть Катерина хочет загрузить данные с сайта, расположенного на веб-сервере А (на рисунке отмечен как Сайт А), и при этом не выдать в запросе свой IP-адрес. Соединение происходит в два этапа: на *первом этапе* клиентская программа Tor компьютера Катерины запрашивает на сервере Tor данные об узлах Tor, их местоположении и характеристиках, а на *втором этапе* по имеющимся данным строится случайная цепочка из трех или более узлов Tor, по которой будет происходить обмен данными с сервером А.

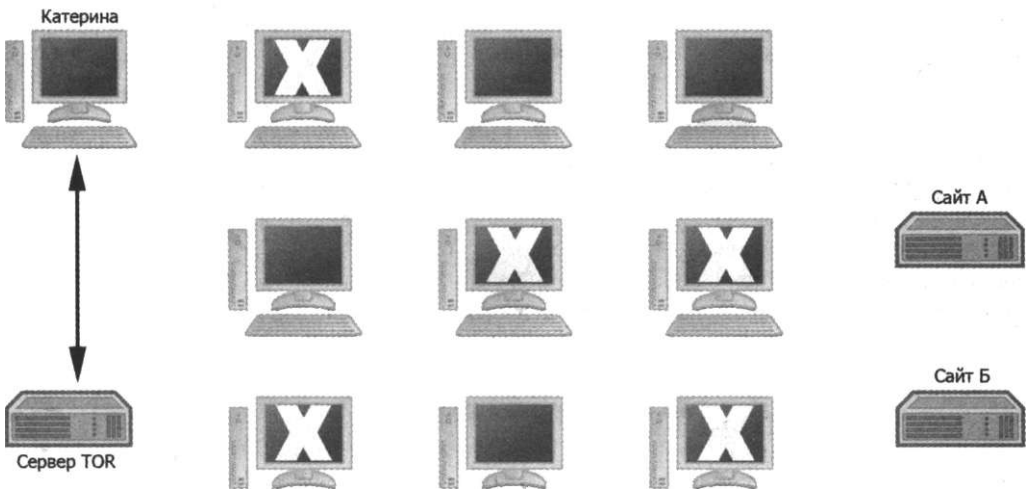


Рис. 17.2. Запрос к серверу Tor о количестве и расположении узлов

Проще всего представить эту схему на примере цепочки в три узла. Итак, компьютер Катерины шифрует данные и адрес места назначения, передаваемые на сервер А ключом последнего, третьего компьютера в цепочке. Затем к этому зашифрованному пакету добавляется адрес последнего узла в цепочке, и данные вновь шифруются, на этот раз ключом второго узла. А потом дважды зашифрованный пакет шифруется ключом первого узла цепочки. В получившемся пакете данные защищены тройным шифрованием разными ключами, как слоями. Такой «слоеный» пакет отправляется первому узлу цепочки (рис. 17.3).

Первый узел, получив зашифрованный пакет данных, расшифровывает его своим ключом и, получив из него адрес второго узла цепочки, отправляет расшифрованный пакет ему. Второй узел так же расшифровывает полученный пакет и отправляет его третьему узлу. Проходя по цепочке, данные расшифровывается слой за слоем, пока не достигнут последнего узла цепочки. Последний узел — в нашем случае это третий — окончательно расшифровав пакет, отправляет незашифрованные данные на сервер А. Сервер А отправляет ответ обратно на третий узел цепочки, где они вновь шифруются и передаются назад по цепочке на компьютер Катерины.

Таким образом, каждый узел в сети знает только адреса двух своих соседей по цепочке, при этом первый узел знает адрес клиентского компьютера, но не знает адреса сервера и изначального содержимого пакета данных, а последний узел знает адрес сервера и содержимое

пакета данных, но не знает адреса получателя. Промежуточные узлы не знают ни адреса сервера, ни адреса отправителя, ни содержимого передаваемых пакетов.

Для повышения эффективности уровня безопасности примерно раз в десять минут создается новая цепочка для передачи данных. Так, если через несколько минут Катерина запросит загрузку контента с сайта Б, цепочка будет иной (рис. 17.4).

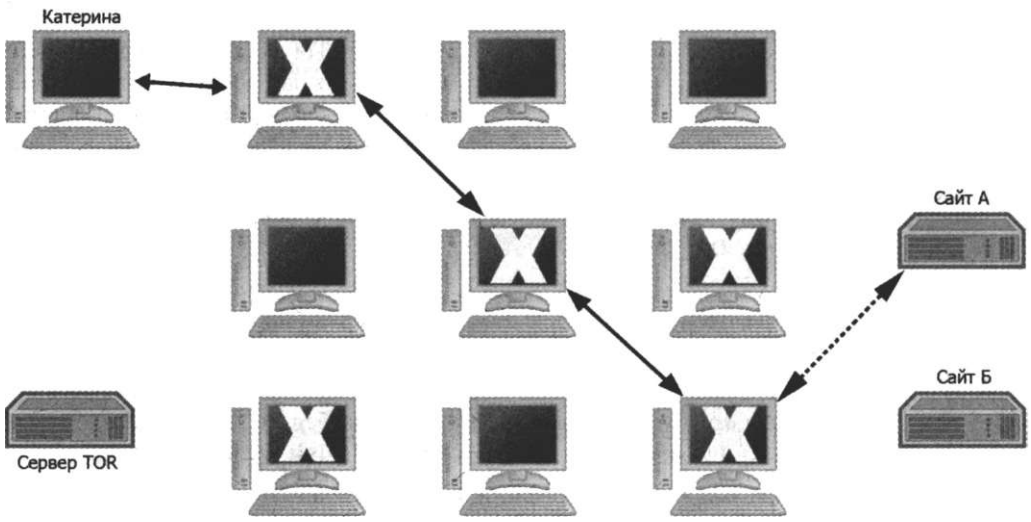


Рис. 17.3. Передача запроса через Tor

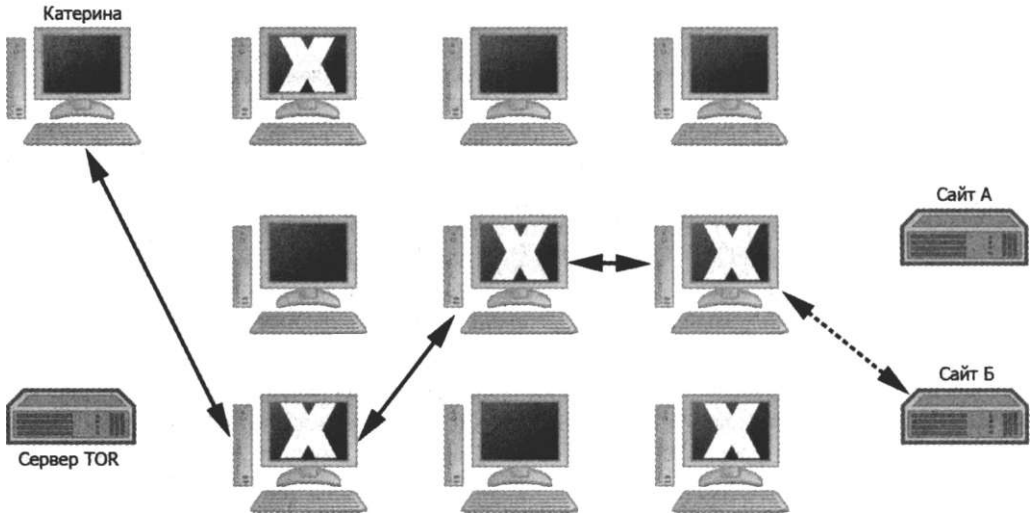


Рис. 17.4. Передача ответа через Tor

Разумеется, Tor не может полностью анонимизировать вашу личность в Интернете. Для усиления защиты своих данных не следует использовать реальную персональную информацию: имя, фамилию, дату рождения, банковские реквизиты, адреса электронной почты

и т. п. Необходимо также использовать специальное программное обеспечение — Tor Browser, при работе в котором тоже не следует расслабляться, — опасность представляют скрипты, например, JavaScript, поэтому выполнение сценариев в браузере следует отключать, а при необходимости использования — быть крайне осторожным.

Установка приложения Tor Browser

Для работы в сети Tor удобно воспользоваться браузером Tor Browser, представляющим собой специальную версию программы Firefox, настроенную на работу в конфиденциальном режиме с использованием Tor. Tor Browser организован как портативное (portable) приложение и может быть установлен на Flash-накопитель. Официальную русскую версию браузера Tor Browser можно загрузить по ссылке tinyurl.com/3ty5dkk. Итак:

1. Перейдите на сайт tinyurl.com/3ty5dkk и, выбрав в раскрывающемся списке пункт Русский, нажмите кнопку Download Tor Browser.
2. Загрузите установочный пакет Tor Browser и запустите его двойным щелчком мыши. Если система выведет предупреждение о попытке установки программы от неизвестного издателя, разрешите установку. Может также потребоваться запустить программу установки от имени администратора.
3. В открывшемся диалоговом окне мастера установки выберите папку распаковки программы, нажав кнопку Browse (Обзор), а затем кнопку Install (Установить).
4. По окончании установки перейдите в папку с установленной программой и запустите браузер, щелкнув мышью по ярлыку Start Tor Browser — откроется диалоговое окно Сетевые настройки Tor (Tor Network Settings), предназначенное для предварительной настройки подключения к сети Tor (рис. 17.5).

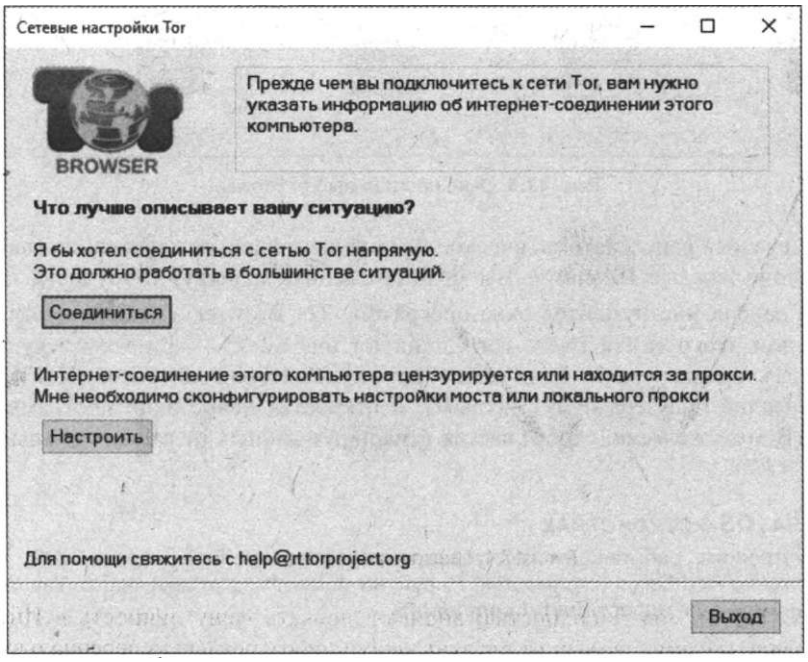


Рис. 17.5. Диалоговое окно Сетевые настройки Tor

5. В зависимости от преследуемых целей, нажмите одну из кнопок:
   - **Соединиться** (Connect) — чтобы соединиться с сетью Tor напрямую, без прокси-сервера. Как правило, в большинстве случаев этот вариант срабатывает;
   - **Настроить** (Configure) — следует нажать, если доступ к Интернету на используемом компьютере ограничивается, и требуется доступ через прокси-сервер.
6. Пусть мы нажали кнопку **Соединиться** (Connect) — откроется окно программы Tor Browser и отобразится страница с сообщением об успешном подключении к сети Tor (рис. 17.6). Вы можете проверить соединение через сеть Tor, посетив один из сайтов определения IP-адреса компьютера.

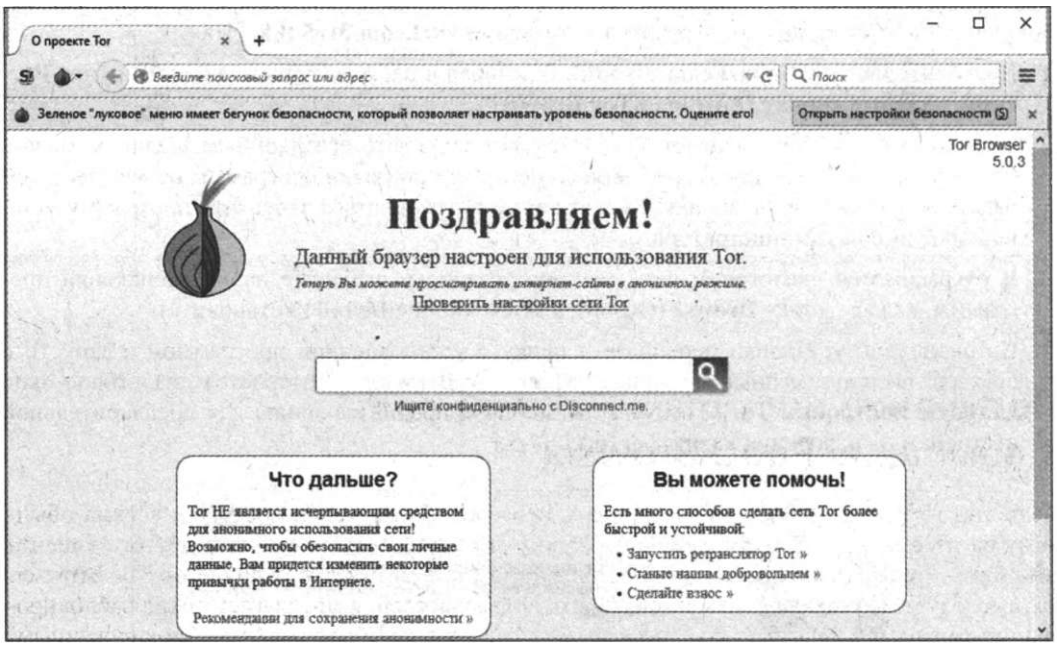


Рис. 17.6. Окно программы Tor Browser

Как уже отмечалось ранее, автоматическое изменение маршрута следования пакетов происходит примерно каждые 10 минут. Вы можете сменить маршрут и вручную, нажав кнопку на панели инструментов окна программы Tor Browser и выбрав пункт **Новая цепочка Tor для этого сайта** (New Tor Circuit for this Site), — при этом текущая вкладка браузера будет перезагружена. Если же выбрать пункт **Новая личность** (New Identity), все открытые вкладки браузера будут закрыты, и откроется новое окно программы с новым IP-адресом. В этом же меню отображается и маршрут данных от вашего компьютера в Интернет (рис. 17.7).

> ***TOR НА IOS-УСТРОЙСТВАХ***
>
> **Для устройств, работающих под управлением операционной системы iOS, разработано приложение Red Onion (стоимостью 75 руб. на момент подготовки книги). Узнать о нем подробнее можно по адресу tinyurl.com/jgsbj5j.**

С помощью Tor Browser можно посещать ресурсы в псевдодомене **.onion,** созданном для обеспечения доступа к анонимным или псевдоанонимным адресам сети Tor. Подобные

адреса не являются полноценными записями DNS, и информация о них не хранится в корневых серверах DNS, но при установке дополнительного программного обеспечения, необходимого для выхода в сеть Tor (кроме Tor Browser это может быть, к примеру, Orbot — для устройств под управлением операционной системы Android или плагин Torbutton — для браузера Firefox), программы, работающие с Интернетом, получают доступ к сайтам в доменной зоне .onion, посылая запрос через группу луковых маршрутизаторов сети Tor. Onion-сайты, как и I2P-сайты (eepsite), — представители Даркнет-ресурсов, темной стороны Интернета, о которой мы поговорим позднее.

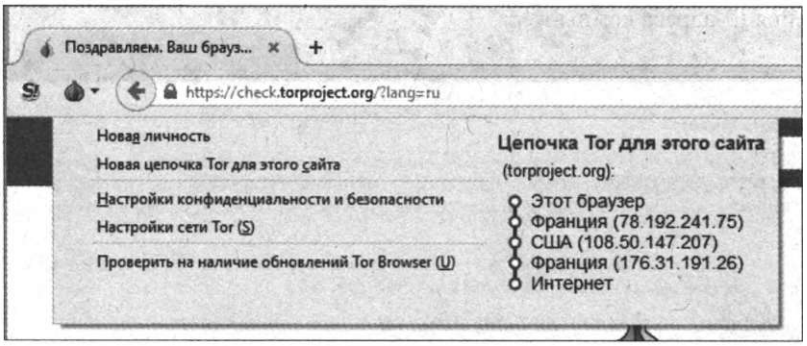


Рис. 17.7. Меню и цепочка Tor для текущего сайта

Получение доступа к *Pandora.com* с помощью PirateBrowser

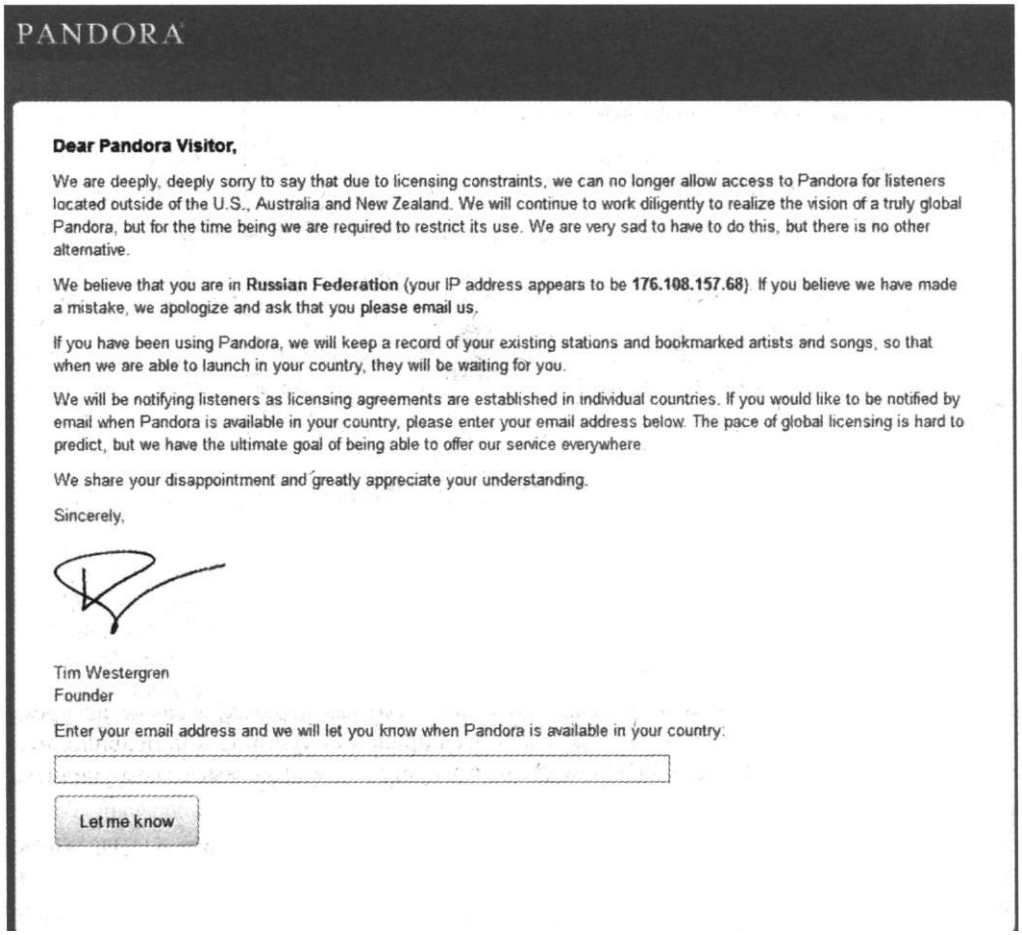
Цель этого раздела — продемонстрировать вам способ получения доступа к весьма обычному на первый взгляд сайту интернет-радио — Pandora.com с помощью другого клиента сети Tor — программы PirateBrowser. Программа PirateBrowser, в отличие от Tor Browser, не преследует цели обеспечить анонимность пользователей, а предлагает обход заблокированных сайтов и одновременный комфортный серфинг по обычным (не заблокированным) сайтам. Другими словами, если используется Tor Browser, то все сайты в нем открываются через сеть Tor. А в PirateBrowser, благодаря дополнению FoxyProxy, можно создавать свои собственные «белые» списки сайтов, для доступа к которым будет использован Tor (или другие прокси-серверы). Все же прочие сайты, которые не присутствуют в этих списках, станут открываться обычным способом. Тем самым веб-серфинг становится наиболее комфортным.

Вернемся к сайту Pandora.com. Принцип работы этого радио следующий: композиции, отмеченные слушателем как понравившиеся и похожие на них, воспроизводятся на радио чаще. Те же, что слушателю не понравились, не воспроизводятся, а похожие на них играются существенно реже. На сайте Pandora.com используется уникальная схема определения «похожести» композиций, именуемая The Music Genome Project, суть которой в том, что каждая композиция имеет свой «геном» — набор нескольких сотен описывающих музыку параметров, которые фиксируются музыкальными аналитиками. Поэтому на радиостанции Pandora.com вы слушаете те композиции, которые с очень большой вероятностью вам понравятся.

Несколько лет назад очередная больная фантазия американских защитников авторских прав была воплощена в реальность, и радиостанция перестала вещать за пределами Соединенных

Штатов. С тех пор любой посетитель сайта с неамериканским IP-адресом получает страницу с извинениями (рис. 17.8).

Возможно, вы уже получили доступ к этому сайту другими путями, но, тем не менее, я предложу здесь довольно простой способ, отталкиваясь от которого, вы сможете посещать и другие сайты, недоступные по каким-либо причинам, в том числе просматривать ролики на сервисе YouTube и получать доступ к контенту на других ресурсах, так или иначе заблокированных в вашей стране.


PANDORA

Dear Pandora Visitor,

We are deeply, deeply sorry to say that due to licensing constraints, we can no longer allow access to Pandora for listeners located outside of the U.S., Australia and New Zealand. We will continue to work diligently to realize the vision of a truly global Pandora, but for the time being we are required to restrict its use. We are very sad to have to do this, but there is no other alternative.

We believe that you are in **Russian Federation** (your IP address appears to be **176.108.157.68**). If you believe we have made a mistake, we apologize and ask that you please email us.

If you have been using Pandora, we will keep a record of your existing stations and bookmarked artists and songs, so that when we are able to launch in your country, they will be waiting for you.

We will be notifying listeners as licensing agreements are established in individual countries. If you would like to be notified by email when Pandora is available in your country, please enter your email address below. The pace of global licensing is hard to predict, but we have the ultimate goal of being able to offer our service everywhere.

We share your disappointment and greatly appreciate your understanding.

Sincerely,

Tim Westergren
Founder

Enter your email address and we will let you know when Pandora is available in your country:

Let me know

Рис. 17.8. Глубочайшие извинения интернет-радиостанции Pandora за то, что вы живете в России

Прежде всего, для обхода установленного ограничения понадобится браузер PirateBrowser. Это отдельная программа, разработанная создателями скандального ресурса Pirate Bay и представляющая собой сборку из портативной версии браузера Firefox с предустановленными расширением FoxyProxy и клиентом для доступа к сети Tor.

В описании PirateBrowser сообщается, что программа позволяет обходить интернет-цензуру в Иране, Северной Корее, Великобритании, Бельгии и других странах. При этом подчеркивается, что приложение предназначено только для обхода ограничений и, несмотря на использование Tor, не обеспечивает анонимности во Всемирной паутине.

Итак, приступим:

1. Загрузите с адреса piratebrowser.ru и установите браузер PirateBrowser.
2. Запустите приложение PirateBrowser, щелкнув двойным щелчком на ярлыке Start PirateBrowser, — вы увидите диалоговое окно, информирующее о процессе подключения к сети Tor (рис. 17.9), а через несколько секунд — главное окно «пиратского» браузера.

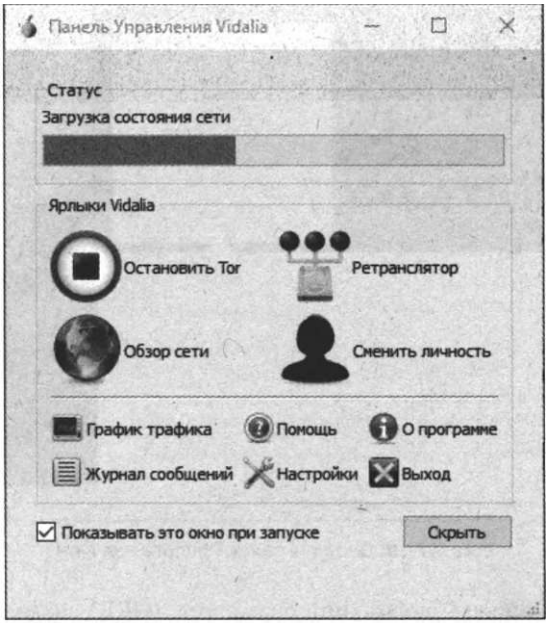


Рис. 17.9. Процесс подключения к сети Tor

Связь с определенными веб-сайтами, блокируемыми в разных странах, а также ресурсами .onion осуществляется через прокси с помощью расширения FoxyProxy. Как правило, никаких дополнительных настроек в него вносить не требуется — в этом мы можем убедиться, перейдя на сайт pandora.com (рис. 17.10).

При необходимости вы можете получить доступ к настройкам, нажав клавишу <Alt> (чтобы отобразить строку меню в браузере), а затем выбрав команду меню Tools | FoxyProxy Standard | Use proxy "TOR" for all URLs (Инструменты | FoxyProxy, стандартная версия | Использовать прокси "TOR" для всех адресов).

Если же у вас возникнет необходимость покопаться в настройках прокси поглубже, осуществить это можно следующим образом:

1. Нажмите клавишу <Alt> (чтобы отобразить строку меню в браузере) и выберите команду меню Tools | FoxyProxy Standard | Options (Инструменты | FoxyProxy, стандартная версия I Настройки) — откроется диалоговое окно FoxyProxy Standard (FoxyProxy, стандартная версия).
2. Выделите пункт TOR и нажмите кнопку Edit selection (Изменить) в правой части диалогового окна FoxyProxy Standard (FoxyProxy, стандартная версия) — откроется диалоговое окно Proxy Settings (Параметры прокси) (рис. 17.11, *слева).*

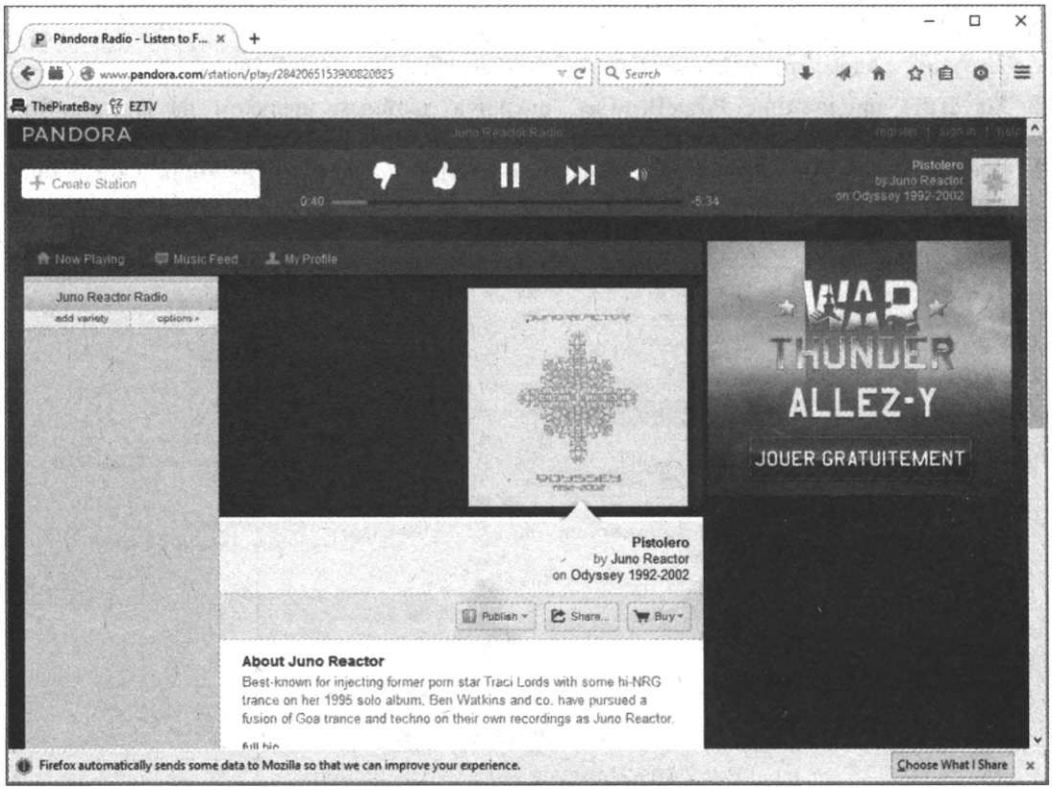


Рис. 17.10. Доступ к сайту Pandora получен

3. Чтобы добавить в список любой интернет-адрес (URL), нажмите кнопку Add New Pattern (Добавить новый шаблон) — откроется диалоговое окно Add/Edit Pattern (Добавить/Изменить шаблон) (рис. 17.11, *справа).*
4. Для создания шаблона в этом окне следует задать несколько правил, согласно которым будет осуществляться подключение добавляемого ресурса через прокси:
   - в поле Pattern Name (Имя шаблона) укажите название шаблона— к примеру, `Pandora;`
   - в поле URL pattern (Адрес шаблона) введите маску **`URL`** — например, **`*.pandora.*.`** Символ * здесь обозначает, что под действие шаблона попадают любые сайты на домене pandora: music.pandora.com, pandora.us и т. п.;
   - установите переключатель URL Inclusion/Exclusion (Адрес включен/исключен) в соответствующее положение: Whitelist (Белый список) или Blacklist (Черный список). Разумеется, в белый список попадают адреса, которые соответствуют заданному шаблону, а в черный — которые не соответствуют;
   - установите переключатель Pattern Contains (Шаблон содержит) в положение Wildcards (Метасимволы) или Regular Expression (Регулярное выражение).
5. Нажмите кнопку OK, чтобы добавить новый шаблон.
6. Закройте открытые диалоговые окна.

Аналогичным образом вы можете добавлять в программу любые другие шаблоны.

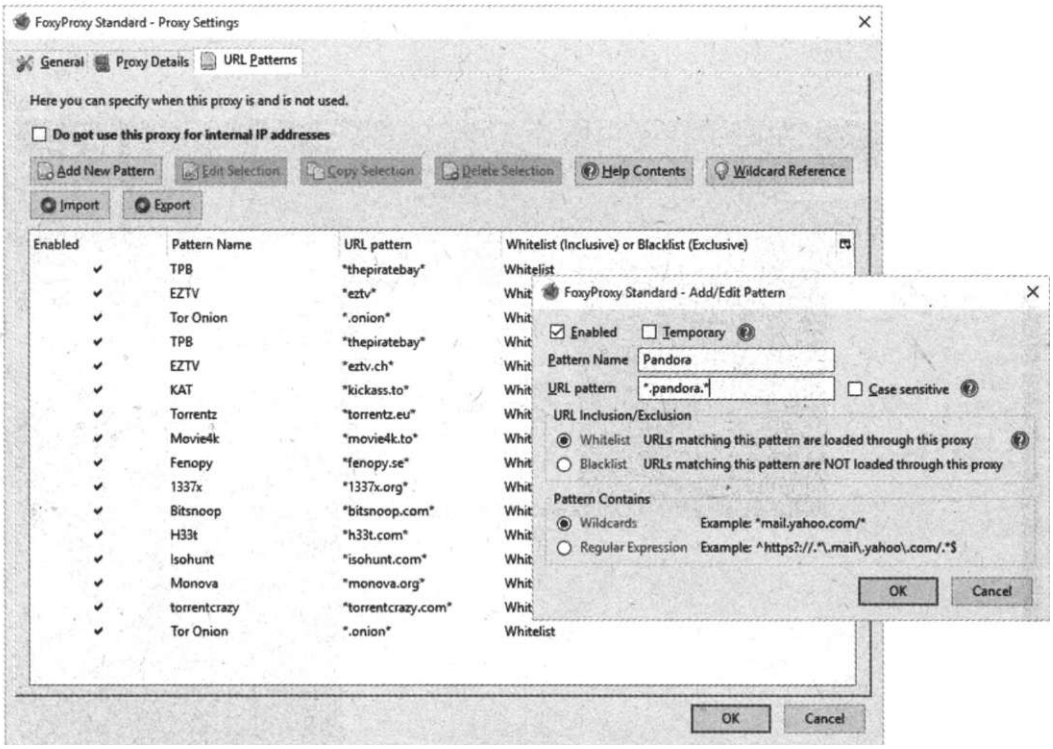


Рис. 17.11. Диалоговое окно Proxy Settings

В том случае, если в процессе работы сайта возникают задержки или иные неполадки, одним из способов решения может стать перезапуск подключения к сети Tor. Для этого щелкните на значке Tor в области уведомлений (он выглядит как зеленая луковица) правой кнопкой мыши и выберите пункт Новая Личность (New Identity) (рис. 17.12).

После закрытия окна программы PirateBrowser клиент для подключения к сети Tor автоматически завершает работу.

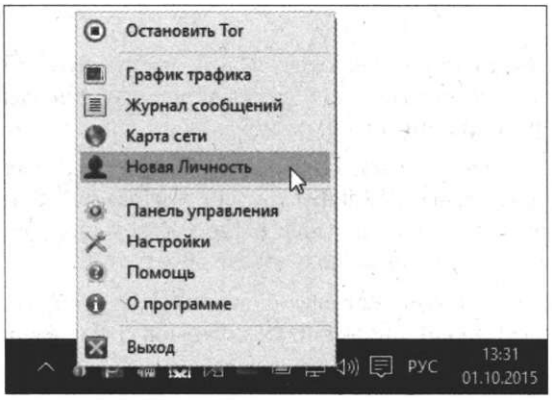


Рис. 17.12. Выбор команды переподключения к сети Tor

ЧАСТЬ IV

Обеспечение максимального уровня анонимности и безопасности с помощью Tails

Глава 18.	**Основы операционной системы Tails**
Глава 19.	**Установка и первый запуск Tails**
Глава 20.	**Анонимное подключение к Интернету**
Глава 21.	**Шифрование и конфиденциальность**
Глава 22.	**Работа с файлами в Tails**
Глава 23.	**Дополнительные возможности работы с Tails**

Вот вы и добрались до главного раздела всей книги, ради которого она и задумывалась, — руководства по операционной системе Tails. Освоив ее, вы сможете пользоваться этой защищенной системой на любом компьютере, оснащенном USB-интерфейсом или приводом оптических дисков.

Операционная система Tails использовалась Эдвардом Сноуденом для разоблачения американских спецслужб. Сноуден — американский технический специалист, бывший сотрудник ЦРУ и Агентства национальной безопасности (АНБ) США. В начале июня 2013 года он передал газетам The Guardian и The Washington Post секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру при помощи информационных сетей и сетей связи, включая сведения о проектах PRISM, X-Keyscore и Tempora. По данным закрытого доклада Пентагона, Сноуден похитил 1,7 млн секретных файлов, большинство документов касается «жизненно важных операций американской армии, флота, морской пехоты и военно-воздушных сил». Сноуден получил политическое убежище и в настоящее время проживает в России, но его точное местонахождение не разглашается по соображениям безопасности. Теперь очередь освоить Tails за вами! :-)

ГЛАВА 18

Основы операционной системы Tails

Введение в Tails

Программное обеспечение в составе Tails

Проблемы безопасности при работе в Tails

Обеспечение защиты пользователя Tails

Сокрытие факта использования Tails

Tails — это не анонимная сеть вовсе, хотя и является инструментом, точнее, комплексом инструментальных средств для обеспечения анонимности и приватности. Аббревиатура Tails расшифровывается как The Amnesic Incognito Live System — наличие слова Amnesic (амнезия) подчеркивает, что после каждой перезагрузки система забывает все предыдущие действия пользователя и таким образом не позволяет установить, чем он занимался.

Введение в Tails

Tails представляет собой дистрибутив Linux на основе Debian (и обновляемый через несколько месяцев после каждого релиза Delian), созданный для обеспечения приватности и анонимности. Все исходящие соединения в этой системе передаются через анонимную сеть Tor (см. *главу 17),* а все неанонимные блокируются. Tails предназначена для загрузки с DVD, SD-карты или Flash-накопителя в качестве операционной системы в режиме Live и не оставляет следов на компьютере, где использовалась (поскольку запускается отдельно от операционной системы, на нем установленной). Проект разрабатывался пять лет и в виде финального релиза увидел свет весной 2014 года.

Основная задача Tails — это обеспечение пользователя при работе на компьютере и в Сети максимально возможным уровнем анонимности при сохранении простоты использования операционной системы. Система работает практически на любом современном компьютере (кроме PowerPC и ARM), оборудованном двумя гигабайтами оперативной памяти. Количество оперативной памяти может быть и меньше, но в таком случае система будет работать заметно медленнее, и не исключены сбои. По умолчанию Tails не задействует для хранения файлов либо других временных данных жесткий диск компьютера и даже носитель, на котором записана вся информация, хранится в оперативной памяти. Это сделано для того, чтобы после завершения рабочей сессии нельзя было определить, чем пользователь занимался на компьютере, даже получив доступ к носителю с Tails. Впрочем, при необходимо-

сти в системе можно создавать постоянные разделы для сохранения личных файлов, настроек операционной системы и пр. Эти данные шифруются и прочитать их, не зная ключа, невозможно.

Tails является свободным программным обеспечением и распространяется совершенно бесплатно.

Программное обеспечение в составе Tails

Операционная система Tails основана на платформе Delian (debian.org), содержит удобную и интуитивно понятную среду рабочего стола GNOME и включает следующее программное обеспечение:

- среда рабочего стола GNOME;
- сетевые инструменты:
  - подключение к сети Ток, запускаемое в изолированном режиме (песочнице) с поддержкой сетевых мостов, включая обфусцированные (т. е. с запутанным кодом), и установленным приложением Vidalia;
  - инструмент управления проводными и беспроводными сетями;
  - программу Tor Browser — веб-браузер, представляющий собой модифицированную версию браузера Mozilla Firefox. В нем для обеспечения анонимности:
    - все cookie-файлы сохраняются только на время сеанса;
    - установлено расширение Torbutton — обеспечивающее анонимность и защиту от выполнения вредоносного кода JavaScript;
    - установлено расширение HTTPS Everywhere, с помощью которого подключения к поддерживающимся сайтам осуществляются с SSL-шифрованием;
    - установлено расширение NoScript, настраивающее выполнение или полностью отключающее сценарии JavaScript;
    - установлено расширение AdBlock Plus, предназначенное для блокировки рекламных баннеров;
  - клиент мгновенного обмена сообщениями Pidgin с настроенным криптографическим протоколом OTR для безопасной переписки;
  - клиент электронной почты Icedove (Thunderbird) с дополнением Enigmail, предназначенным для шифрования информации и создания электронных цифровых подписей;
  - новостной агрегатор Liferea — для сбора сообщений из RSS-лент;
  - текстовый редактор Gobby — для совместной работы над документами;
  - набор программ Aircrack-ng, предназначенных для обнаружения беспроводных сетей, аудита (проверки стойкости) ключей шифрования WEP и WPA/WPA2-PSK, в том числе тестирования беспроводных сетей на подверженность атакам на оборудование и атакам на алгоритмы шифрования;
  - клиент I2P — для доступа к одноименной анонимной сети;
  - приложение Electrum, предназначенное для управления денежными средствами в пиринговой платежной системе «Биткоин»;

- мультимедийные-приложения:
  - пакет программ LibreOffice:
    - Writer — текстовый редактор;
    - Cale — программа для создания электронных таблиц;
    - Impress — программа для создания презентаций;
    - Draw — графический редактор;
    - Math — редактор формул;
  - программы GIMP и Inkscape — для обработки изображений;
  - программа предпечатной подготовки Scribus — для верстки документов;
  - редактор Audacity — для записи и обработки аудиофайлов;
  - нелинейный аудио/видеоредактор PiTiVi — для монтажа мультимедийных материалов;
  - Poedit — бесплатный и открытый кроссплатформенный редактор каталогов локализации;
  - утилиты Simple Scan и SANE — для сканирования документов и фотографий;
  - приложение Brasero — для записи CD/DVD;
  - граббер Sound Juicer — для копирования компакт-дисков аудио в цифровой формат;
  - программа Traverso — для записи и обработки многоканальных аудиофайлов;
- инструменты шифрования и обеспечения приватности:
  - спецификация шифрования дисков LUKS и приложение GNOME Disks — для установки и шифрования устройств хранения данных (например, Flash-накопителей);
  - GnuPG — программа для шифрования данных и электронной почты с помощью OpenPGP и создания электронных цифровых подписей;
  - инструмент Monkeysign, предназначенный для подписи и обмена ключами OpenPGP;
  - генератор паролей PWGen;
  - криптографическая схема разделения секрета Шамира, используемая в реализациях gfshare и ssss;
  - виртуальная клавиатура Florence, обеспечивающая защиту от кейлогеров;
  - инструментарий MAT — для анонимизации метаданных в файлах;
  - менеджер паролей KeePassX;
  - инструмент GtkHash — для вычисления контрольных сумм;
  - криптографическая утилита командной строки Keyringer с системой управления версиями Git;
  - утилита командной строки Paperkey, предназначенная для распечатки ключей OpenPGP на бумаге.

Дистрибутив операционной системы Tails обладает следующими дополнительными возможностями:

- механизмом автоматического апгрейда до новой версии дистрибутива, записанного на Flash-диск или SD-карту;

- возможностью запуска в виртуальной операционной среде таких программ, как VirtualBox;
- настраиваемостью — помимо предустановленного программного обеспечения, в операционную систему Tails допускается инсталлировать любое другое, предназначенное для Debian. Таким образом, вы быстро можете создать собственную сборку Tails;
- ядром с поддержкой режима PAE, а также атрибута NX-бит и симметричного мультипроцессирования, — на соответствующем аппаратном обеспечении;
- поддержкой основных специальных опций для людей с ограниченными возможностями;
- возможностью использования упреждающей защиты со многими приложениями — благодаря инструменту AppArmor, который определяет, к каким системным ресурсам и с какими привилегиями может получить доступ то или иное приложение;
- механизмом стирания содержимого памяти при выключении компьютера и при физическом извлечении носителя — для защиты от атак методом холодной перезагрузки и анализа дампов памяти.

Проблемы безопасности при работе в Tails

Используя Tails, обеспечивающую максимально возможный уровень анонимности и безопасности, не считайте, тем не менее, эту операционную систему «волшебной», — в любом программном обеспечении могут присутствовать недостатки. Поэтому при работе в Tails рекомендуется учитывать следующие моменты.

Скомпрометированное аппаратное обеспечение

Если компьютер был скомпрометирован злоумышленником, имеющим к нему физический доступ и установившим постороннее аппаратное обеспечение (например, кейлогер или модифицированный BIOS), использовать Tails может быть небезопасно.

Установка и подключение к недоверенным системам

Запускаемая на вашем компьютере Tails не может быть скомпрометирована вирусом, поразившим операционную систему, установленную на компьютере, но:

- установочный дистрибутив системы Tails должен быть скачан из доверенных источников. В противном случае он может оказаться измененным злоумышленником и не обеспечить должного уровня безопасности;
- подключение к компьютеру со скомпрометированной операционной системой USB- или SD-носителя, предназначенного для установки Tails, может повлечь нежелательное изменение устанавливаемой копии Tails и снизить уровень безопасности, — используйте только свой доверенный компьютер для создания носителя с Tails.

Модификации BIOS и другого встроенного ПО

Операционная система Tails не защищает от вредоносных действий, осуществляемых злоумышленником путем модификации BIOS или другого встроенного программного обеспечения (прошивок) компьютера. Этим программным обеспечением невозможно напрямую управлять из операционной системы, поэтому ни одна операционная система в мире не защищает от вредоносных действий такого рода (см. пример на сайте tinyurl.com/nc3c75x).

Перехват трафика с выходных узлов Tor

Сеть Tor фокусируется на сокрытии вашего местонахождения, а не на шифровании трафика. Как вы уже знаете, в сети Tor трафик передается через группу случайных узлов (маршрутизаторов), скрывающих ваши следы, — это не дает возможности определить, откуда данные поступили и куда направляются. Соединение обычно осуществляется через цепочку из трех маршрутизаторов, последний из которых осуществляет подключение непосредственно к устройству назначения. Этот последний узел называется *выходным* и передает данные на сервер назначения в незашифрованном виде. Стало быть, злоумышленник на этом участке пути может перехватить любой трафик.

Чтобы предотвратить перехват трафика с выходных узлов Tor, вы для передачи конфиденциальных данных через Интернет всегда должны использовать технологии сквозного шифрования, — например, криптографический протокол SSL.

Операционная система Tails содержит несколько инструментов для надежного шифрования трафика, которые следует изучить и использовать при веб-серфинге и коммуникациях с другими людьми.

Обнаружение использования Tor и Tails

Интернет-провайдер или администратор локальной сети может увидеть, что вы подключились к узлу в сети Tor, а не к обычному веб-серверу. Скрыть тот факт, что вы используете Tor, позволяет применение мостов Tor (ретрансляторов). Кроме того, доступ к сети Tor может быть заблокирован, и использование мостов Tor позволяет решить также и эту проблему. Настроить Tor для доступа через ретранслятор довольно легко — полный русскоязычный мануал вы найдете на сайте bridges.torproject.org.

Сервер, к которому вы обращаетесь, проанализировав публичный список выходных узлов, также может зафиксировать, что обращение к нему происходит от одного из выходных узлов Tor.

Атаки посредника

Атака посредника (MitM, Man-in-the-Middle attack) представляет собой одну из форм активной прослушки, при которой злоумышленник создает независимый канал связи между жертвами и ретранслирует сообщения, передаваемые между ними. Таким образом, у жертв создается видимость, что они обмениваются данными непосредственно друг с другом, не догадываясь о присутствии посторонних, хотя на самом деле вся линия связи контролируется злоумышленником (рис. 18.1).

При работе в сети Tor атака посредника вполне допустима на этапе связи от выходного узла до сервера назначения. Кроме того, сам выходной узел может оказаться под контролем злоумышленника, проводящего атаку посредника.

И вновь, чтобы защитить свои данные от подобных атак, необходимо использовать сквозное шифрование и соблюдать особую осторожность при проверке аутентичности сервера.

Как правило, это происходит автоматически с использованием специальных цифровых подписей веб-сайтов — SSL-сертификатов, выдаваемых центрами сертификации и проверяемых браузером. Если в браузере отображается уведомление о нарушении безопасности, наподобие показанного на рис. 18.2, ваш компьютер может стать жертвой атаки посредника. Не следует игнорировать это предупреждение, если у вас нет другого способа проверки подписи сертификата.

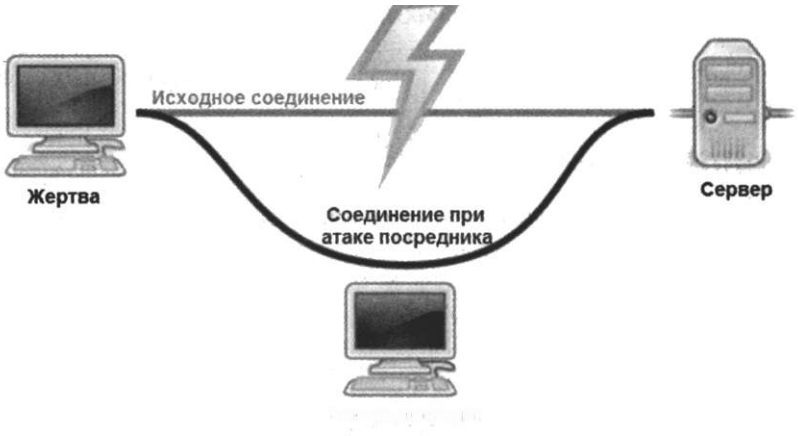


Рис. 18.1. Схема атаки посредника

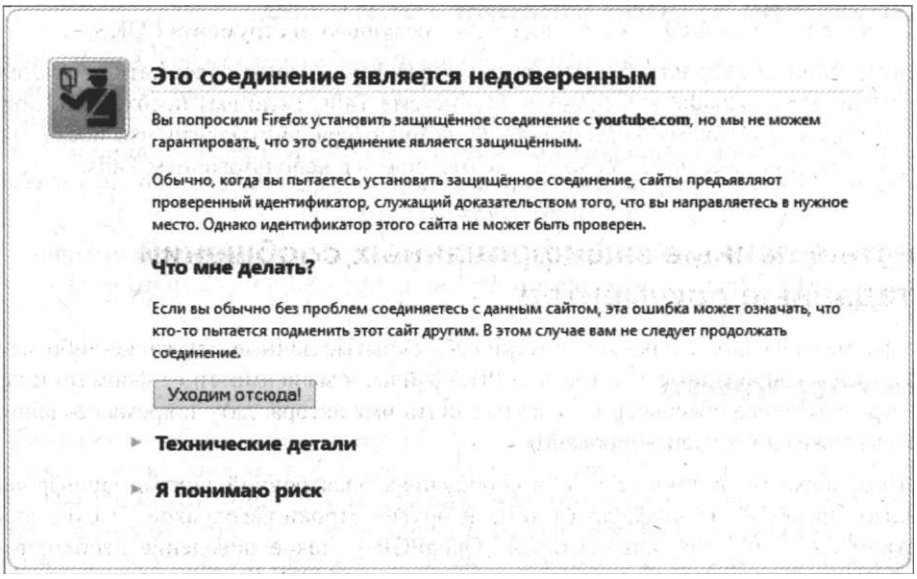


Рис. 18.2. Уведомление о недоверенном соединении

Возможность атаки посредника нельзя исключать даже при использовании защищенного соединения по протоколу HTTPS. При таком виде соединения для шифрования запросов используются протоколы TLS или SSL, что, на первый взгляд, защищает канал от сниффинга и атак посредника. Однако злоумышленник может для каждого TCP-соединения создать две независимые SSL-сессии: клиент устанавливает SSL-соединение со злоумышленником, а тот, в свою очередь, создает соединение с сервером. Браузер в таких случаях обычно предупреждает, что сертификат не подписан доверенным центром сертификации, но рядовые пользователи устаревших браузеров легко обходят это предупреждение. К тому же, у злоумышленника может оказаться сертификат, подписанный корневым центром сертификации и не создающий предупреждений.

Таким образом, предоставляя механизм анонимности, Tor с одной стороны — снижает вероятность атаки посредника на конкретного пользователя, а с другой — упрощает проведение крупномасштабных атак посредника на выходных узлах или конкретных серверах.

Атаки на опознание трафика

Конфигурация сети Tor не обеспечивает защиту от перехвата трафика, поступающего в сеть Tor и исходящего из нее: оба потока трафика сети могут быть проанализированы, и выполнена корреляция входного и выходного трафиков. Такое возможно в случае, если, к примеру, ваш провайдер (администратор локальной сети) и провайдер сервера назначения (или администратор сервера назначения) сотрудничают в попытке перехвата трафика.

Следы шифрования документов

Документы в операционной системе Tails по умолчанию не шифруются, если только вы не организовали для постоянного хранения файлов специальный зашифрованный раздел. Но вы можете шифровать документы вручную, используя такие инструменты для защиты файлов, как GnuPG, или шифруя весь носитель с помощью инструмента LUKS.

Существует, впрочем, вероятность, что те или иные файлы могут содержать доказательства того, что они были созданы в операционной системе Tails. Если вам необходимо получить из Tails доступ к локальному жесткому диску компьютера, учитывайте, что после этого на нем могут быть обнаружены следы вашей деятельности с использованием Tails.

Открытые данные зашифрованных сообщений и метаданные документов

Многие форматы файлов сохраняют внутри себя скрытые данные или какие-либо метаданные. Так, отредактированные текстовые и PDF-файлы, в зависимости от формата и используемого программного обеспечения, могут хранить имя автора, дату и время создания файла, а иногда даже сводку рецензирования.

Кроме того, обратите внимание, что в сообщениях электронной почты, зашифрованных с помощью OpenPGP, не шифруются тема и другие строки заголовков. Это не является недостатком системы Tails или протокола OpenPGP — такое поведение необходимо для обратной совместимости с оригинальным протоколом SMTP. К сожалению, возможности зашифровать строку темы сообщения в настоящее время не существует.

Графические файлы формата TIFF или JPEG и им подобные хранят колоссальный объем скрытых данных. Такие файлы, созданные с помощью цифровых камер или смартфонов, содержат метаданные в формате EXIF, включающие дату и время, а иногда и координаты съемки, модель и серийный номер фотокамеры (смартфона), а также миниатюру исходного изображения. Оставляют, как правило, эти метаданные в обрабатываемых файлах и графические редакторы. Во Всемирной паутине размещено огромное количество кадрированных или размытых изображений, в которых метаданные EXIF содержат миниатюры исходных снимков.

Операционная система Tails не удаляет метаданные из файлов автоматически, но содержит инструмент MAT (mat.boum.org), позволяющий сделать это.

Системы глобальной слежки

Крупные системы глобальной слежки могут отслеживать трафик между всеми компьютерами в сети одновременно. Анализируя в ней параметры коммуникаций, такие системы способны идентифицировать цепочки Tor и сопоставлять пользователей и серверы назначения.

На компромисс, позволяющий такую слежку, создателям Tor пришлось пойти для создания службы с малым временем отклика, достаточным для комфортного веб-серфинга, общения и SSH-подключений.

Двойная жизнь

Как правило, не следует использовать один и тот же сеанс работы в Tails для выполнения двух различных задач или выдачи себя за двух разных личностей, связь между которыми вы хотите скрыть. К примеру, скрыть факт проверки электронного почтового ящика от имени одного пользователя и факт анонимной публикации документа от имени другого.

Во-первых, Tor имеет тенденцию в пределах сеанса повторно использовать одни и те же цепочки узлов. Поскольку выходной узел в цепочке знает как адрес сервера назначения (и, возможно, содержимое сообщения, если оно не зашифровано), так и адрес предыдущего узла, от которого поступили данные, может быть выполнена корреляция нескольких запросов в пределах цепочки и определено, что они выполнены одним и тем же пользователем. Если ваши данные потенциально могут отслеживаться с помощью глобальной системы, как описано ранее, вероятность сопоставления запросов весьма высока.

Во-вторых, в случае уязвимости в системе безопасности или ошибочном использовании Tails или одного из приложений в ее составе, может произойти утечка информации о сеансе, после чего будет несложно доказать, что за различные действия, совершенные во время сеанса работы, ответственен один и тот же человек.

Способ избежать обеих угроз заключается в перезагрузке операционной системы Tails каждый раз, когда вы хотите выдать себя за другого человека.

Как поясняется в *главе 20,* возможность смены личности в программе Tor Browser не является идеальным решением для сокрытия следов и связи между вашими вымышленными персоналиями, — только *завершение работы и перезагрузка операционной системы Tails!*

Слабые пароли

Сеть Tor позволяет сохранить анонимность в Интернете, а операционная система Tails позволяет не оставлять следов на компьютере, который вы используете. Но, опять же, оба этих инструмента не могут выполнить за вас работу по соблюдению элементарной компьютерной безопасности в плане использования надежных паролей.

Слабые пароли могут быть взломаны методом полного перебора. Чтобы узнать, являются ли ваши пароли слабыми и как создавать более надежные пароли, обратитесь к *главе 2*.

Эволюция Tails

Операционная система Tails, как и программное обеспечение, которое она включает, постоянно дорабатывается и обновляется, и может содержать программные ошибки или уязвимости в сфере безопасности. Своевременно обновляйте свою копию операционной системы Tails, как описано в *главе 19*.

В этой книге описана версия Tails 2.0, однако на момент чтения книги может быть уже доступна более новая версия операционной системы, которая включает новые и более совершенные инструменты обеспечения анонимной и защищенной работы.

Обеспечение защиты пользователя Tails

Операционная система Tails сохраняет в тайне действия пользователя благодаря тому, что по умолчанию не записывает данные никуда, кроме оперативной памяти. При необходимости пользователь в любой момент может нажать кнопку выключения на корпусе компьютера, и все данные сеанса будут удалены, а вместе с ними и возможность установить выполненные на этом компьютере действия. Вызвать немедленную перезагрузку или выключение компьютера можно также из меню, вызываемого кнопкой , расположенной в правом верхнем углу экрана (рис. 18.3).

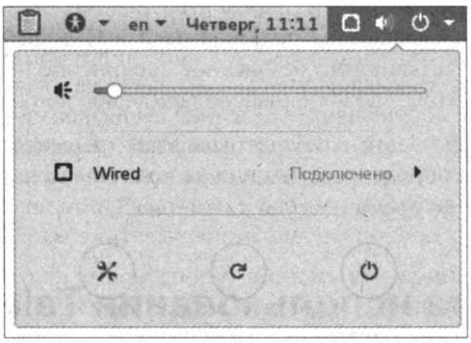


Рис. 18.3. Команды незамедлительного завершения работы в Tails

После вызова любой из этих команд отменить выключение компьютера и получить доступ к файлам в системе будет уже невозможно. Нельзя также, не имея ключа, получить доступ и к документам, хранящимся в зашифрованном разделе носителя с Tails.

В плане защиты анонимности пользователя в Интернете Tails также предоставляет много возможностей. Так, абсолютно все соединения устанавливаются через анонимную сеть Tor. Если же какое-то приложение попробует обратиться в сеть напрямую, то оно будет блокировано. Вместо Tor можно использовать и сеть I2P, нажав на начальном экране клавишу <TaЬ> и введя команду `i2p`.

В роли браузера в системе Tails выступает Tor Browser, рассмотренный в *главе 17. К* числу его положительных качеств можно отнести и то, что Tor Browser использует расширение HTTPS Everywhere, обеспечивающее зашифрованный обмен данными с сайтами, поддерживающими протокол HTTPS. Кроме того, в этом браузере установлено расширение NoScript, предназначенное для настройки блокирования сценариев JavaScript и Java на различных сайтах. Несмотря на потенциальную опасность сценариев на языке JavaScript, по умолчанию в Tor Browser они не отключены. Это связано с тем, что система и без того достаточно хорошо защищена от известных уязвимостей, а большинство сайтов некорректно работают без JavaScript. Стоит также отметить, что большая часть пользователей сети Tor использует JavaScript, и его отключение может выделить ваш компьютер на их фоне, а значит, и повысить вероятность его отслеживания. А вот плагин Adobe Flash, в связи с наличием в нем большого количества уязвимостей, в Tor Browser не предустановлен. Установка

дополнительных расширений в браузере не запрещена, однако надо иметь в виду, что бесконтрольное их использование может привести к нарушению анонимности пользователя.

Работа с электронной почтой в Tails обеспечивается приложением Icedove (Thunderbird) с дополнением Enigmail, поддерживающим стандарт шифрования OpenPGP. С помощью OpenPGP можно кодировать сообщения со своим ключом безопасности, без которого их чтение невозможно.

Общение в системе организовано через клиент мгновенного обмена сообщениями Pidgin с настроенным криптографическим протоколом OTR, обеспечивающим безопасный обмен сообщениями между пользователями (см. *главу* 7).

Некоторые механизмы для защиты пользователя встроены непосредственно и в саму операционную систему — к примеру, Tails шифрует содержимое буфера обмена, а на панели инструментов доступна кнопка вызова виртуальной клавиатуры, использование которой предотвращает перехват нажатий клавиш кейлогерами. Центр предупреждений Tails выводит важные сообщения, которые могут оповещать о возможном нарушении анонимности. Например, если пользователь попытается подключиться к Интернету сразу после включения Tails и до того, как будет установлено безопасное соединение через сеть Tor, система предупредит пользователя об этом, заблокировав подключение до получения подтверждения.

На сегодняшний день, Tails — это наиболее известная из имеющихся в открытом доступе анонимная операционная система, рекомендуемая всем пользователям, заботящимся о своей анонимности, особенно во время доступа в Интернет.

Сокрытие факта использования Tails

Как говорилось ранее, злоумышленник может узнать, что вы пользуетесь сетью Tor. Но операционная система Tails старается максимально скрыть факт использования Tails пользователями в сети Tor, особенно на фоне всех остальных пользователей программы Tor Browser.

Важные замечания касательно посещаемых сайтов

Сайты, которые вы посещаете, могут извлекать весьма много информации о вашем браузере: название и номер версии браузера, размер окна, список доступных расширений, часовой пояс, доступные шрифты и т. д. Чтобы скрыть факт использования Tails, программа Tor Browser, включенная в эту операционную систему, предоставляет те же данные, что и в других операционных системах.

Однако некоторые из дополнений в программе Tor Browser, включенной в состав Tails, специфичны для этой системы. Некоторые злоумышленники могут учитывать этот факт, чтобы выявить пользователей операционной системы Tails. К примеру, операционная система Tails содержит блокировщик рекламы Adblock Plus. И если злоумышленник сможет определить, что рекламные объявления, включенные в веб-страницу, не скачиваются на вашем компьютере, он может идентифицировать вас как пользователя Tails.

Вы также должны учитывать, что при использовании программы Unsafe Browser никаких специальных мер обеспечения безопасности не предпринимается.

Важные замечания касательно провайдеров и сетевых администраторов

- Мосты в сети Tor в большинстве случаев — прекрасный способ скрыть тот факт, что вы подключаетесь к этой сети (см. *главу 19).*
- Не только система Tails генерирует трафик через сеть Tor. Как правило, пользователи Tor Browser в других операционных системах также создают связанную с Tor сетевую активность. И если вы используете интернет-подключение совместно с другими пользователями Tor Browser, которые не работают в системе Tails, то вашему провайдеру будет гораздо сложнее выяснить, используется ли система Tails теми или иными пользователями, генерирующими Tor-трафик.
- Система Tails *не* применяет механизм защиты входа, используемый в сети Tor. С помощью этого механизма пользователь сети Tor всегда использует одни и те же определенные узлы для построения первого транзитного участка. А поскольку система Tails не сохраняет никаких данных о сети Tor между отдельными сеансами работы, то она тем более не хранит информацию и об упомянутом механизме защиты входа. Таким образом, при каждом входе пользователя Tails в сеть Tor выбирается случайный первый узел, до которого происходит построение первого транзитного участка.
- При запуске система Tails синхронизирует системные часы, чтобы убедиться в точности времени. Если при этом обнаруживается, что дата существенно отличается в одну из сторон, Tor Browser прекращает работу и перезапускается. Такое поведение может быть использовано для выявления пользователей системы Tails, главным образом потому, что синхронизация происходит при каждом запуске системы Tails.

ГЛАВА 19

Установка и первый запуск Tails

Загрузка и проверка образа Tails
Выбор типа носителя
Запись Tails на носитель
Обновление Tails
Запуск операционной системы Tails
Обзор рабочего стола Tails
Зашифрованное хранилище
Решение проблем запуска
Завершение работы Tails
Безопасное стирание Tails

Настало время приступить к практической работе в операционной системе Tails. Для начала я расскажу вам, как скачать образ, проверить его на достоверность и установить, а затем мы осуществим первый запуск с последующей настройкой.

Загрузка и проверка образа Tails

Дистрибутив операционной системы Tails вы можете скачать в виде ISO-образа — единого файла, который затем можно легко записать на DVD или установить на Flash-накопитель или SD-карту. Загрузить дистрибутив можно как по прямой ссылке, так и в виде torrent-файла, а затем использовать программу наподобие mTorrent для скачивания Tails (рис. 19.1).

Файл цифровой подписи для проверки ISO-образа можно скачать отдельно по ссылке **Tails signature** (он также включен в состав торрента). Дополнительно, по ссылке **signature of the Torrent file,** вы можете скачать файл цифровой подписи для проверки самого торрента перед скачиванием дистрибутива.

Подключение к сайту осуществляется через протокол HTTPS, а достоверность сайта обеспечивается соответствующим сертификатом, подтверждающим, что вы можете доверять его контенту. Впрочем, на этом сайте, как и на любом другом во Всемирной паутине, вы уязвимы при проведении атаки посредника, поэтому крайне важно выполнить проверку достоверности скачанного ISO-образа, который, в случае атаки посредника, может быть модифицирован злоумышленником.

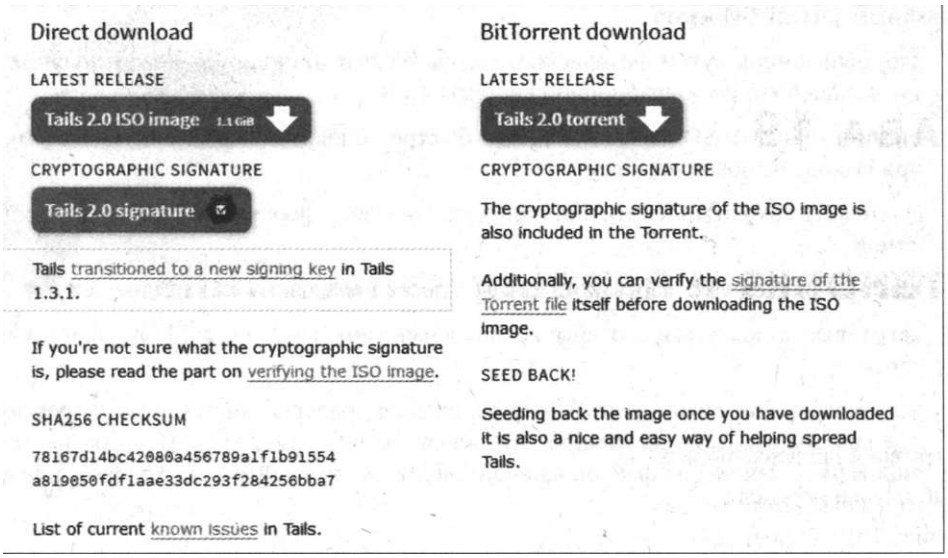


Рис. 19.1. Страница со ссылками для скачивания дистрибутива Tails

Поскольку каждый ISO-образ операционной системы Tails подписан с помощью ключа OpenPGP (надеюсь, вы помните, что OpenPGP — это стандарт шифрования данных, обеспечивающий криптографическую защиту и аутентификацию с помощью собственных ключей пользователей), то проверку этой подписи и следует провести. Пошаговые инструкции по проверке целостности ISO-образа приведены на странице tinyurl.com/71ms3d6.

Крайне важно поддерживать операционную систему Tails в актуальном состоянии, своевременно скачивая и устанавливая обновления, которые могут закрывать потенциальные уязвимости в системе ее безопасности. Кроме того, на сайте проекта вы можете подписаться на рассылку уведомлений о выходе новых версий Tails.

Далее я расскажу вам, как установить Tails на Flash-накопитель или SD-карту и записать на DVD.

Выбор типа носителя

При выборе типа носителя (DVD, Flash-накопитель или SD-карта), на который вы планируете записать (развернуть) образ операционной системы Tails, следует руководствоваться следующими особенностями каждого из них:

- DVD:
  - содержимое DVD предназначено только для чтения, поэтому запущенная с такого диска копия Tails не подвержена вирусам или атакам;
  - DVD дешевы, но вам придется записывать новый диск каждый раз при выходе новой версии операционной системы Tails;
  - можно использовать и перезаписываемые диски DVD-RW, но такие носители теряют преимущества режима «только для чтения»;
  - некоторые компактные ноутбуки и подобные устройства могут не иметь встроенного привода оптических дисков;

- Flash-**накопители**/SD-**Карта:**
  - злоумышленник путем физического вмешательства или вируса может получить доступ к вашей копии операционной системы Tails;
  - Flash-**накопители**/SD-**Карты** позволяют быстро обновить операционную систему Tails при выходе ее новой версии;
  - вы можете сохранять настройки и документы в зашифрованном разделе на самом носителе;
  - Flash-**накопители**/SD-**Карты** компактны и легко помещаются в карман одежды;
  - некоторые старые компьютеры не поддерживают загрузку с **накопители**/SD-**Карты**;
  - некоторые **накопители**/SD-**Картыі** или кардридеры оборудованы переключателем режима «только для чтения», что вроде бы позволяет предотвратить несанкционированное изменение файлов на носителе, но не полагайтесь на эту функцию на ненадежных компьютерах.

Запись Tails на носитель

Прежде чем приступать к записи (развертыванию) образа диска на какой-либо носитель, загрузите актуальную версию дистрибутива Tails с официального сайта проекта по адресу tinyurl.com/7nlfa31. Затем выполните следующие действия — в зависимости от типа носителя и используемой операционной системы.

Запись Tails на DVD

Windows 7/8/10

1. Вставьте чистый DVD в привод оптических дисков компьютера.
2. Щелкните правой кнопкой мыши по скачанному файлу с именем вида tails-i386-x.x.iso и выберите из контекстного меню команду Записать образ диска (Burn Disc Image) — вы увидите окно программы Средство записи образов дисков Windows (Windows Disc Image Burner) (рис. 19.2).
3. Нажмите кнопку Записать (Burn). Если установить флажок Проверить диск после записи (Verify disc after burning), то после окончания процесса диск будет протестирован на отсутствие ошибок записи.

Если в вашей версии Windows отсутствует инструмент Средство записи образов дисков Windows (Windows Disc Image Burner), обратитесь к следующему разделу, описывающему способ записи образа диска с помощью программ сторонних производителей.

> ***ЗАПИСЬ ISO-ОБРАЗОВ В WINDOWS VISTA***
>
> **В операционной системе Windows Vista для записи ISO-образов также используется встроенная утилита, носящая название Записать диск (Burn Disc). Процесс записи схож с более поздними версиями Windows за исключением необходимости выбора режима записи — этот переключатель необходимо установить в положение Mastered (ISO).**

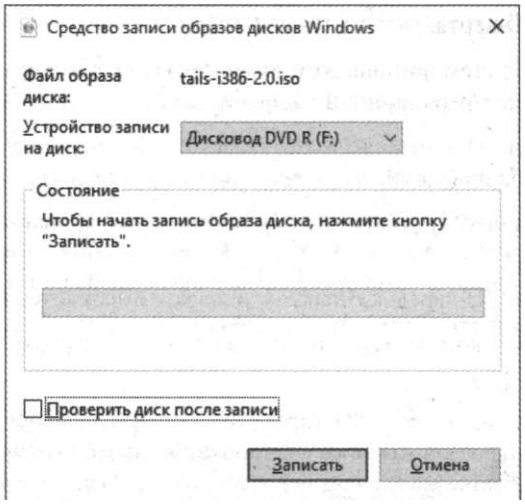


Рис. 19.2. Окно программы Средство записи образов дисков Windows

Windows 2000 и более ранние версии

Прежде чем записывать ISO-образ, необходимо загрузить и установить программное обеспечение для записи дисков, — например, Infra Recorder (infrarecorder.org) или ISO Recorder (isorecorder.alexfeinman.com). Запись (развертывание) ISO-образа в программе ISO Recorder осуществляется следующим образом:

1. Вставьте чистый DVD в привод оптических дисков компьютера.
2. Щелкните правой кнопкой мыши по скачанному файлу с именем вида tails-i386-x.x.iso и выберите из контекстного меню команду Скопировать образ в CD/DVD (Burn Disc Image to CD/DVD) — вы увидите окно программы ISO Recorder (рис. 19.3).
3. Нажмите кнопку След. (Next), чтобы записать диск.

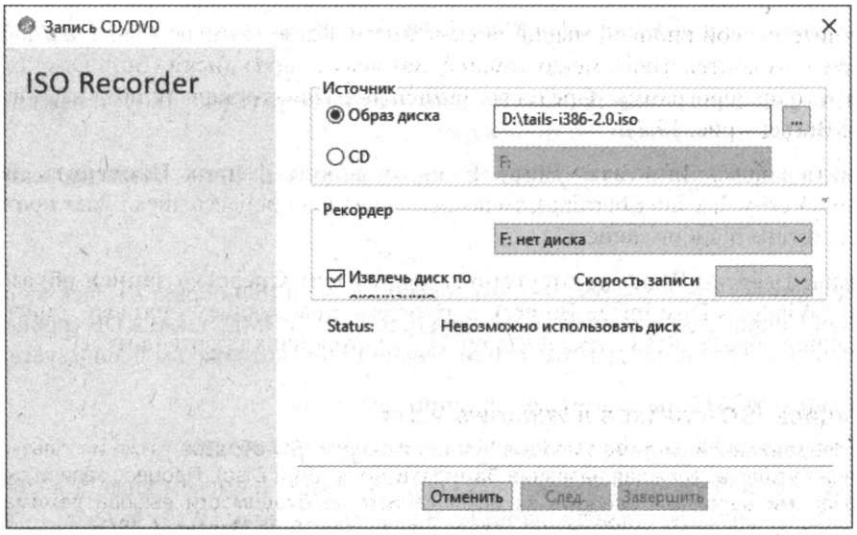


Рис. 19.3. Окно программы ISO Recorder

OS X El Capitan и более поздние версии

Для записи ISO-образов в операционной системе OS X El Capitan используется приложение Запись диска (Burn Disc). С его помощью развертывание ISO-образа на диск осуществляется так:

1. Вставьте чистый DVD в привод оптических дисков компьютера.
2. Щелкните правой кнопкой мыши по скачанному файлу с именем вида tails-i386-x.x.iso и выберите из контекстного меню команду **Записать образ диска на диск** (Burn Disc Image on disc) — вы увидите окно программы Запись диска (Burn Disc) (рис. 19.4).
3. Нажмите кнопку **Записать** (Burn), чтобы записать диск.

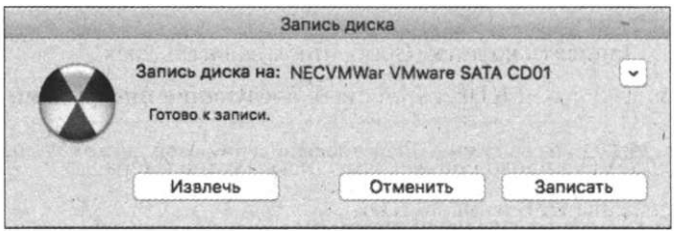


Рис. 19.4. Окно программы Запись диска

OS X Yosemite и более ранние версии

Для записи ISO-образов в операционной системе OS X Yosemite и более ранних версиях используется приложение Дисковая утилита (Disk Utility). С его помощью развертывание ISO-образа на диск осуществляется так:

1. Запустите приложение Дисковая утилита (Disk Utility) — значок программы доступен в папке **Программы | Утилиты** (Applications | Utilities).
2. Вставьте чистый DVD в привод оптических дисков компьютера.
3. Перетащите скачанный ISO-файл в левую часть окна программы Дисковая утилита (Disk Utility).
4. Выберите ISO-файл в окне программы Дисковая утилита (Disk Utility) и нажмите кнопку **Записать** (Burn) на панели инструментов.
5. На появившейся панели также нажмите кнопку **Записать** (Burn), чтобы записать диск.

Linux

В качестве примера здесь мы рассмотрим способы записи ISO-образа на диск в операционной системе Ubuntu с окружением рабочего стола как GNOME, так и KDE (процесс может незначительно отличаться в зависимости от версии Linux, которую вы используете).

В окружении GNOME выполните следующие действия:

1. Вставьте чистый DVD в привод оптических дисков компьютера.
2. Щелкните правой кнопкой мыши по скачанному файлу с именем вида tails-i386-x.x.iso и выберите из контекстного меню команду **Записать на диск** (Write to Disc) — вы увидите окно **Записать на диск** (Burn Disc) (рис. 19.5).

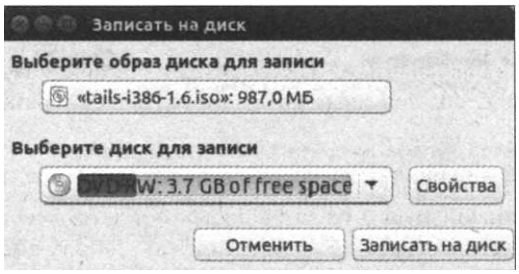


Рис. 19.5. Окно программы Запись на диск

3. В раскрывающемся списке Выберите диск для записи (Select a disc to write to) выберите чистый диск.
4. Нажмите кнопку Записать на диск (Burn), чтобы записать диск.

В окружении рабочего стола KDE выполните следующие инструкции по записи ISO-образа на диск:

1. Вставьте чистый DVD в привод оптических дисков компьютера.
2. Запустите приложение K3B из меню KDE.
3. В нижней части открывшегося окна программы нажмите кнопку Дополнительные действия (More actions) и выберите пункт Записать образ (Burn Image).
4. Запишите диск с установками по умолчанию.

Установка Tails на Flash-накопитель или SD-карту

ФУНКЦИЯ ЗАШИФРОВАННОГО ХРАНИЛИЩА TAILS

Описанные далее способы установки Tails на Flash-нэкопитель или SD-карту не позволяют задействовать функцию зашифрованного хранилища для постоянного хранения файлов и настроек. Чтобы воспользоваться этой возможностью, необходимо запустить операционную систему Tails, например, в виртуальной машине, и уже в ней создать накопитель с помощью инструмента Tails Installer.

Windows

Установка Tails на Flash-накопитель или SD-карту в Windows осуществляется с помощью приложения Universal USB Installer, которое можно загрузить по адресу tinyurl.com/y87u7aq. Обратите внимание, что вам понадобится его версия 1.9.5.4 или более поздняя. Итак:

1. Подключите к компьютеру Flash-накопитель или SD-карту объемом не менее 2 Гбайт.
2. Запустите приложение Universal USB Installer и подтвердите лицензионное соглашение, нажав кнопку I Agree (Я согласен) — откроется окно программы (рис. 19.6).
3. Выберите пункт Tails в верхнем раскрывающемся списке.
4. Нажмите кнопку Browse (Обзор) и выберите скачанный образ операционной системы Tails — файл с именем вида tails-i386-x.x.iso.
5. В нижнем раскрывающемся списке выберите подключенный к компьютеру накопитель.
6. Установите флажок We will Format (Отформатировать), чтобы стереть все имеющиеся данные с подключенного накопителя.

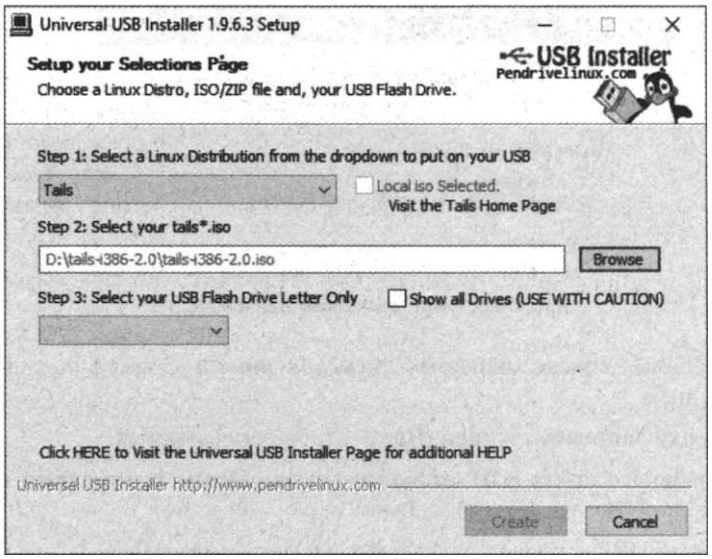


Рис. 19.6. Окно программы Universal USB Installer

7. Нажмите кнопку Create (Создать), чтобы начать процесс создания загрузочного накопителя Tails.
8. После нажатия кнопки Да (Yes) в диалоговом окне с запросом на проведение операции, вы увидите окно процесса создания загрузочного накопителя.
9. По завершении операции безопасно извлеките накопитель из разъема на компьютере.

OS X

В операционной системе OS X создание загрузочного накопителя Tails выполняется при помощи приложения Терминал (Terminal). Но прежде чем начать запись, нужно определить имя накопителя в системе (обычно имена накопителей имеют вид `/dev/disk8`, `/dev/disk9` и т. д.). Для этого:

1. Не подключая Flash-накопитель или SD-карту к компьютеру, запустите приложение Терминал (Terminal) (доступно в папке Программы | Утилиты (Applications | Utilities)) и введите следующую команду:

   ```
   diskutil list
   ```

   Вы увидите результат выполнения команды со списком доступных устройств хранения данных, например:

   ```
   $ diskutil list
   /dev/diskO
    #:  TYPE NAME                    SIZE           IDENTIFIER
    0:  GUID_partition_scheme        *500.1 GB      diskO
    1:  EFI                          209.7 MB       diskOsl
    2:  Apple_HFS MacDrive           250.0 GB       disk0s2
   ```

2. Подключите Flash-накопитель или SD-карту к компьютеру и вновь выполните в приложении Терминал (Terminal) команду:

   ```
   diskutil list
   ```

Вы увидите результат выполнения команды со списком доступных устройств хранения данных, в том числе и подключенный накопитель для операционной системы Tails, например:

```
$ diskutil list
/dev/diskO
#: TYPE NAME                    SIZE           IDENTIFIER
0: GUID_partition_scheme        *500.1 GB      diskO
1: EFI                          209.7 MB       diskOsl
2: Apple_HFS MacDrive           250.0 GB       disk0s2
/dev/diskl
#: TYPE NAME                    SIZE           IDENTIFIER
0: FDisk_jpartition_scheme      *4.0 GB        diskl
1: Apple_HFS Untitled 1         4.0 GB         disklsl
```

В моем примере, подключенный накопитель объемом 4,0 Гбайт имеет имя `/dev/diskl`. В вашем случае имя может быть иным.

> ***ТОЧНО ОПРЕДЕЛИТЕ ИМЯ НАКОПИТЕЛЯ!***
>
> **Если вы не смогли определить точное имя накопителя, прекратите процесс создания загрузочного устройства Tails, иначе вы рискуете стереть данные на системном диске и потерять файлы.**

3. Выполните следующую команду, заменив в ней имя **/dev/diskl** тем, которое узнали на своем компьютере на шаге 2.

```
diskutil unmountDisk /dev/diskl
```

4. Выполните следующую команду, заменив текст **taiis-i386-2.**o**.iso** путем к ISO-файлу образа Tails на своем компьютере, а текст **/dev/diskl** — именем накопителя, которое узнали на своем компьютере на шаге 2. Перед именем накопителя следует добавить букву г для ускорения процесса создания загрузочного накопителя.

```
dd if=tails-i386-2.0.iso of=/dev/rdiskl bs=16m && sync
```

> ***ТОЧНЫЙ ПУТЬ К ISO-ФАЙЛУ***
>
> **Если вы не знаете путь к ISO-файлу образа Tails на своем компьютере или получаете ошибку о невозможности обнаружения файла (папки), сначала введите команду** `dd if=`**, а затем перетащите ISO-файл в окно программы Терминал (Terminal) — вы увидите точный путь к ISO-файлу.**

Если все команды выполнены успешно, начнется процесс создания загрузочного накопителя Tails. Он займет несколько минут.

> ***PERMISSION DENIED***
>
> **При возникновении ошибки прав доступа выполните указанную ранее команду со словом** `sudo`**:**
>
> ```
> sudo dd if=fails-i386-2.0.iso of=/dev/rdiskl bs=16m && sync
> ```

По завершении процесса создания загрузочного накопителя Tails вы увидите соответствующее уведомление.

Linux

В операционной системе Linux создание загрузочного накопителя Tails выполняется, как и в OS X, при помощи приложения Терминал (Terminal). Но сначала нужно определить имя накопителя в системе (обычно имена накопителей имеют вид `/dev/sdb`, `/dev/sdc` и т. д.).

1. Подключив Flash-накопитель или SD-карту к компьютеру, запустите приложение Диски (Disks).
2. Выберите накопитель в левой части окна программы Диски (Disks) — в правой нижней части окна, в строке Устройство (Device), вы увидите имя накопителя (рис. 19.7).

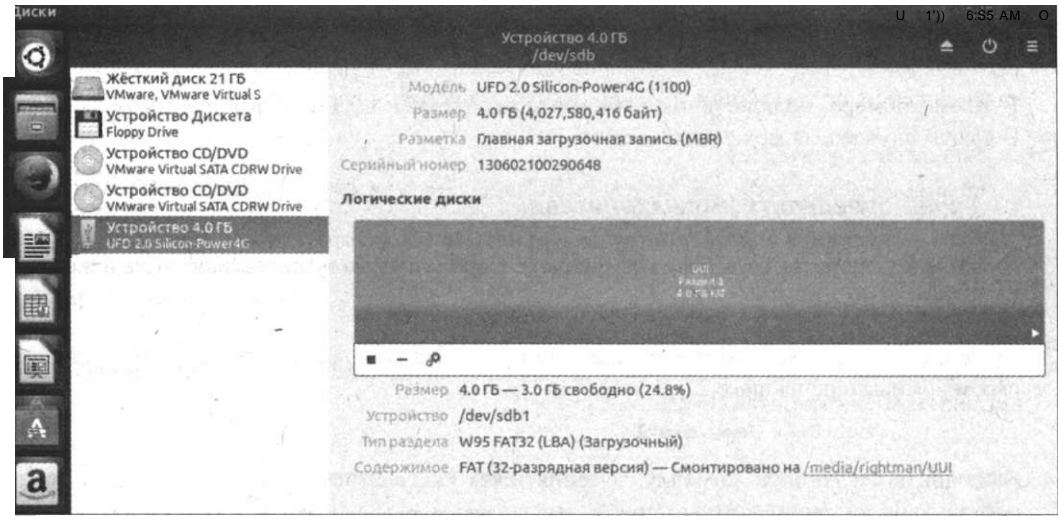


Рис. 19.7. Определение имени накопителя в операционной системе Ubuntu

В моем примере, подключенный накопитель объемом 4,0 Гбайт имеет имя `/dev/sdbi`. В вашем случае имя может быть иным.

3. Запустите приложение Терминал (Terminal) и введите следующую команду, заменив текст `/hame/rightman/Desktop/tails-i386-2.0.iso` путем к ISO-файлу образа Tails на своем компьютере, а текст `/deiv/sdbi` — именем накопителя, которое узнали на своем компьютере на шаге 2.

```
dd if=' /home/rightman/Desktop/tails-i386-2.0.iso' of=/deiv/sdc bs=16M ss sync
```

ПРИМЕЧАНИЕ

Если вы не знаете путь к ISO-файлу образа Tails на своем компьютере или получаете ошибку о невозможности обнаружения файла (папки), сначала введите команду `dd`, нажмите клавишу <Пробел>, а затем перетащите ISO-файл в окно программы Терминал (Terminal) — вы увидите точный путь к ISO-файлу.

Если все команды выполнены успешно, начнется процесс создания загрузочного накопителя Tails. Он займет несколько минут.

Установка Tails с помощью Tails Installer

Описанный здесь способ установки Tails на Flash-накопитель или SD-карту, в отличие от предыдущего, позволяет задействовать функцию зашифрованного хранилища для постоянного хранения файлов и настроек.

С помощью утилиты Tails Installer установка операционной системы Tails возможна только на Flash-накопитель или SD-карту объемом не менее 4 Гбайт. При этом используется вся память накопителя, поэтому установка на него второй операционной системы или создание на нем дополнительного раздела невозможны. В настоящее время приложение Tails Installer доступно для запуска только в операционной системе Tails.

Итак:

1. Запустите операционную систему Tails с DVD или с USB-накопителя/SD-**Карты.** Обратите внимание: система будет устанавливаться не на текущий носитель, поэтому для дальнейшей работы вам понадобится второй — пустой — накопитель.

   КАК ЗАПУСТИТЬ TAILS?

   Если вы еще не знаете, как запустить операционную систему Tails, прочитайте соответствующий раздел главы, а затем вернитесь к этому.

2. На рабочем столе операционной системы Tails выберите команду меню Приложения | Tails I Tails Installer (Applications | Tails | Tails Installer) — откроется окно программы Tails Installer (рис. 19.8).
3. Для установки операционной системы Tails на новый накопитель нажмите кнопку Клонировать & Установить (Install by cloning).



Рис. 19.8. Интерфейс программы Tails Installer

4. Подключите Flash-накопитель (SD-карту), предназначенный для установки операционной системы Tails, — название, объем и имя накопителя появятся в раскрывающемся списке Целевое устройство (Target Device) (рис. 19.9).
5. Выберите в этом раскрывающемся списке целевой накопитель.

   Обратите внимание, что все данные с целевого накопителя будут удалены. Учтите также, что эта операция не обеспечивает конфиденциального удаления имеющихся на целе-

вом накопителе данных. А если на клонируемом накопителе имеется зашифрованный раздел, постоянные файлы и настройки из него на целевой скопированы не будут.

6. Для начала установки нажмите кнопку Установить Tails (Install Tails) и подтвердите свое решение в открывшемся диалоговом окне — начнется процесс установки (см. рис. 19.9).
7. После завершения установки безопасно извлеките накопитель.



Рис. 19.9. Процесс установки операционной системы Tails

Теперь вам доступны возможности использования зашифрованного раздела для постоянного безопасного хранения файлов и данных, а также возможность апгрейда установленной версии Tails до новой при релизе обновления. В последнем случае вы увидите уведомление о выходе обновления и сможете его установить, нажав кнопку Обновить из ISO (Upgrade).

Обновление Tails

Tails включает механизм автоматического обновления операционной системы до новой версии, если она установлена на Flash-накопитель или SD-карту (обновление системы на DVD невозможно). В случаях, если автоматическое обновление осуществить не удается, вы можете вручную выполнить апгрейд системы, — в этом разделе описаны оба способа.

Важно отметить, что обновления операционной системы Tails с каждым выпуском закрывают найденные уязвимости в области безопасности, поэтому выполнять своевременный апгрейд системы очень важно.

Оба способа реализуемы, только если обновляемая операционная система на Flash-накопителе или SD-карте установлена с помощью приложения Tails Installer. При этом *файлы в защищенном хранилище в процессе обновления будут сохранены!*

Если же вы пользуетесь системой Tails, записанной на DVD или установленной вручную, без помощи приложения Tails Installer, то обновление выполнить невозможно, — понадобится скачать и установить новую версию операционной системы из ISO-образа.

Автоматическое обновление с помощью Tails Upgrader

После запуска Tails и подключения компьютера к сети Ток инструмент Tails Upgrader автоматически проверит наличие обновлений на сервере и предложит обновить систему, если состоялся релиз новой версии. Обновления запрашиваются и скачиваются через сеть Ток. Автоматическое обновление имеет ряд преимуществ:

- требуется только одно устройство с установленной операционной системой Tails, а само обновление выполняется на лету в запущенной системе Tails. После завершения процесса обновления понадобится перезагрузить систему, чтобы воспользоваться новыми возможностями;
- пакет обновлений, как правило, по размеру меньше, чем полный ISO-образ системы;
- механизм обновления автоматически выполняет верификацию скачиваемых файлов, а вот при выполнении обновления из ISO-образа вы можете забыть проверить файл на целостность.

Для выполнения автоматического обновления требуется соблюдение следующих двух условий:

- наличие Flash-накопителя или SD-карты с установленной посредством Tails Installer системой Tails;
- активное подключение к Интернету.

Если доступно обновление системы Tails, вы будете оповещены об этом с помощью диалогового окна, показанного на рис. 19.10.

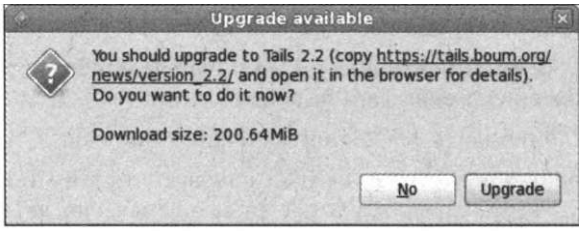


Рис. 19.10. Сообщение о наличии обновления операционной системы Tails

Обратите внимание, что:

- перед выполнением обновления рекомендуется завершить работу всех приложений;
- продолжительность загрузки обновления зависит от его размера и скорости подключения к Интернету и может занять от нескольких минут до нескольких часов;
- подключение к сети будет прервано после завершения загрузки обновления.

Если вы готовы выполнить обновление, нажмите кнопку Обновить (Upgrade) и дождитесь окончания процесса обновления.

В том случае, если вы пропустили один или несколько пакетов обновления, нужно поочередно установить каждый из них. К примеру, если у вас установлена версия 1.8 и текущий релиз отмечен версией 1.8.2, вам понадобится обновить систему до версии 1.8.1, перезагрузиться, а затем выполнить обновление до версии 1.8.2.

Обновление вручную с помощью Tails Installer

УСТАНОВКА НА DVD И ИЗ-ПОД OS X

Если вы используете систему Tails, записанную на DVD, для обновления до новой версии вам понадобится записать новый диск. Если Flash-накопитель с Tails был записан в операционной системе OS X с использованием командной строки, то для обновления систему нужно будет переустановить, действуя по инструкции, приведенной на странице tinyurl.com/hg3q797.

Обновление системы Tails на Flash-накопителе или SD-карте до новой версии вручную следует проводить в случаях, если:

- пакет обновления для используемой версии системы недоступен на веб-сайте Tails;
- автоматическое обновление недоступно по техническим причинам (недостаточно памяти, недостаточно свободного пространства на устройстве и т. п.);
- обновление нужно выполнить с другого устройства, на котором установлена более новая версия Tails. Например, в случае, если отсутствует соединение с Интернетом;
- автоматическое обновление завершилось неудачей, и требуется восстановить устройство с Tails.

Далее рассмотрено два способа обновления системы: через клонирование и из ISO-образа с новым выпуском операционной системы Tails.

Обновление через клонирование

Как и в случае чистой установки, для обновления через клонирование вам понадобится запустить приложение Tails Installer в уже обновленной системе Tails на устройстве, отличном от того, которое вы планируете обновить.

1. Запустите систему Tails с DVD, Flash-накопителя или SD-карты на устройстве, с которого будет выполняться клонирование.
2. Выберите команду меню Приложения | Tails | Tails Installer (Applications | Tails | Tails Installer) для запуска приложения Tails Installer.
3. Выберите пункт Клонировать & Обновить (Upgrade by cloning).
4. Подключите устройство, на котором следует обновить систему Tails, — название Flash-накопителя или SD-карты появится в раскрывающемся списке Целевое устройство (Target Device). Выберите его в этом списке при необходимости.
5. Для запуска процесса обновления нажмите кнопку Установить Tails (Install Tails), а затем щелкните мышью по кнопке Да (Yes) для подтверждения, — начнется процесс обновления.

Обновление из ISO-образа

1. Запустите систему Tails с DVD, Flash-накопителя или SD-карты на устройстве, отличном от того, система на котором предназначена для обновления.
2. Выберите команду меню Приложения | Tails | Tails Installer (Applications | Tails | Tails Installer) для запуска приложения Tails Installer.
3. Выберите пункт Обновить из ISO (Upgrade from ISO).
4. Подключите устройство, на котором следует обновить систему Tails, — название Flash-накопителя или SD-карты появится в раскрывающемся списке Целевое устройство (Target Device). Выберите его в этом списке при необходимости.

5. Нажмите кнопку **Обзор** (Browse) и выберите файл ISO-образа.

   Если ISO-образ сохранен в зашифрованном хранилище, понадобится ввести пароль для доступа к нему.

6. Для запуска процесса обновления нажмите кнопку **Установить Tails** (Install Tails), а затем щелкните мышью по кнопке Да (Yes) для подтверждения, — начнется процесс обновления.

Запуск операционной системы Tails

Для запуска операционной системы Tails необходимо подключить к компьютеру носитель с установленной системой (установить диск в дисковод или вставить Flash-накопитель/SD-карту в соответствующий слот) и, перезагрузив компьютер, запустить его с DVD или подключенного Flash-накопителя/SD-карты.

Вероятно, что для запуска компьютера с носителя, отличного от жесткого диска, потребуется внести изменения в настройки BIOS компьютера. Пошагово процесс выглядит так:

1. Вставьте DVD в привод оптических дисков, Flash-накопитель — в USB-разъем или SD-карту в разъем кардридера, а затем перезагрузите компьютер.

   Если компьютер настроен на приоритетную загрузку с оптического диска или портативного накопителя, вы увидите окно операционной системы Tails. В противном случае загрузится ваша обычная операционная система, к примеру, Windows или OS X.

2. Если сразу загрузиться в Tails не удалось, для выбора режима загрузки с портативного носителя, снова перезагрузите компьютер и при появлении приглашения вида **Press ... to enter SETUP** (текст может быть иной, но клавиша вместо символов... будет обозначена) сразу же нажмите указанную клавишу для входа в настройки BIOS (на рис. 19.11 эта надпись расположена в левом нижнем углу экрана).

   ЗАГРУЗКА С FLASH-ДИСКА НА КОМПЬЮТЕРЕ MAC

   Процесс загрузки на компьютере Mae выглядит так: выключите компьютер, подключите носитель с Tails, включите компьютер и сразу же нажмите и удерживайте клавишу <Option>, пока не появится меню загрузки. В меню загрузки выберите пункт с текстом вида **EFI Boot** и с изображением портативного накопителя — После этого операционная система Tails должна загрузиться. В противном случае вам потребуется загрузить и установить утилиту rEFInd — менеджер загрузки EFI **(tinyurl.com/blemexk).**

   КЛАВИША ВХОДА В НАСТРОЙКИ BIOS

   Для IBM-совместимых компьютеров обычно это клавиша <F1>, <F2>, <Del>, <Esc> или <F10>. Уточнить клавишу вы можете в руководстве пользователя к своему ноутбуку или материнской плате (если это стационарный компьютер).

3. Если вы успели нажать клавишу входа в настройки BIOS до ее исчезновения с экрана, вы увидите экран настроек BIOS (который имеет множество версий и вариантов интерфейса: названий пунктов, их расположения и т. п.), и в нем вам нужно найти список очередности загрузки устройств. В BIOS Setup, показанном на рис. 19.12, этот список расположен на вкладке **Boot.**

   Перемещаться между вкладками можно с помощью клавиш со стрелками, а выбирать пункты/подпункты — клавишей <Enter>. Точные клавиши и связанные с ними действия указываются в нижней части экрана и уточнены в правой.

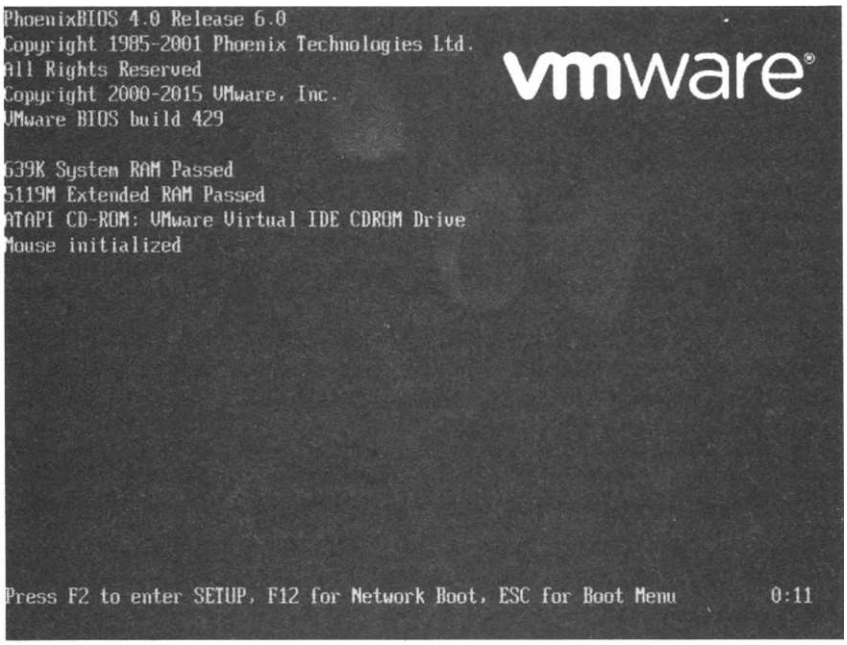


Рис. **19.11. В этом случае для входа в настройки BIOS следует нажать клавишу <F2>. Обратите также внимание, что нажатие клавиши <Esc> сразу же откроет меню загрузки** (Boot Menu), **в котором вы сможете выбрать загрузочный носитель и загрузиться с него, не прибегая к манипуляциям с настройками BIOS**

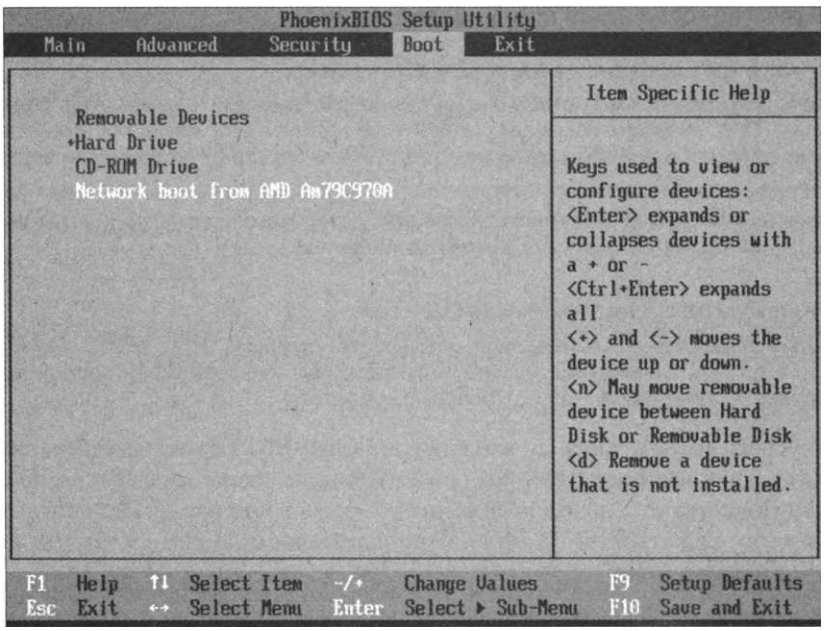


Рис. 19.12. **Интерфейс программы BIOS со списком очередности загрузки устройств**

4. Измените порядок позиций в списке так, чтобы подключенный носитель с установленной операционной системой Tails оказался в самом верху списка (обычно это осуществляется выбором пункта и нажатием клавиши <+> или <Page Up>, однако на вашем компьютере управление может выполняться иным образом). Пункт подключенного носителя может носить название Flash-lbcrf/SD-Карты, а также Removable Devices (см. рис. 19.12), removable drive, USB media или подобное, — это зависит от версии BIOS.
5. Нажмите клавишу <F10> для сохранения настроек и подтвердите свое решение нажатием клавиши <Y> — после автоматической перезагрузки вы должны увидеть экран, показанный на рис. 19.13.



Рис. 19.13. Экран загрузки операционной системы Tails

ПРИ ВОЗНИКНОВЕНИИ ОШИБОК ЗАГРУЗКИ TAILS

Отключите настройки Fast boot и Secure boot, если они присутствуют в вашей версии BIOS. Если есть такая возможность, попробуйте загрузить компьютер с помощью интерфейса UEFI вместо BIOS (или же наоборот отключите UEFI, чтобы запустить компьютер с интерфейсом BIOS). Включите настройки Legacy mode и CSM boot, если они присутствуют в вашей версии BIOS. Запоминайте все вносимые изменения, т. к., возможно, вам придется вернуть их, чтобы запустить вашу обычную операционную систему. Вы также можете обратиться к руководствам во Всемирной паутине, например, доступным по адресу tinyurl.com/o6tf8ov.

6. Для запуска операционной системы Tails выберите пункт Live и нажмите клавишу <Enter>.

   Режим Live (failsafe) отключает некоторые функции ядра операционной системы и может повысить качество работы и производительность Tails на некоторых компьютерах. Если вы считаете, что возникающие ошибки связаны с аппаратным обеспечением используемого компьютера, попробуйте запустить операционную систему Tails в режиме Live (failsafe).

7. В раскрывающемся списке в нижней части экрана приветствия выберите пункт Русский (рис. 19.14).
8. Далее выберите, следует ли выполнить начальную настройку операционной системы Tails. Если согласны — нажмите кнопку Yes (Да), если нет — нажмите кнопку No (Нет), а затем кнопку Login (Войти).

   Дополнительные параметры настройки включают в себя установку пароля администратора, активацию режима спуфинга MAC-адресов (позволяет скрыть серийные номера используемого сетевого оборудования и затрудняет определение вашей геопозиции), а также настройку сетевого моста, брандмауэра и прокси (если подключение к Интернету блокируется).
9. Нажмите кнопку Login (Войти) — если вы отказались от начальной настройки системы, то увидите рабочий стол операционной системы Tails (см. далее).

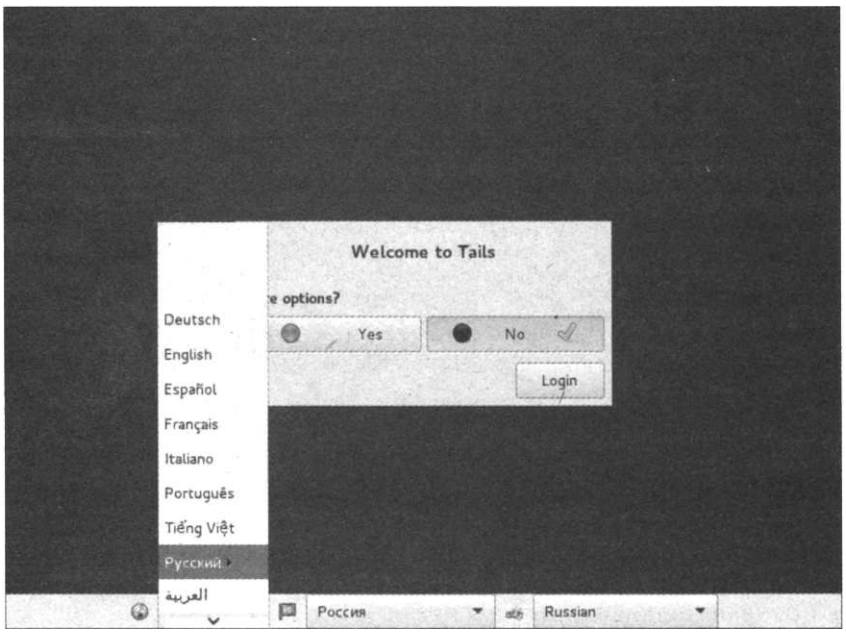


Рис. 19.14. Экран приветствия операционной системы Tails

Параметры загрузки

При загрузке Tails вы можете указать дополнительные параметры, изменяющие обычный режим работы этой операционной системы. Доступно два инструмента: меню загрузки и окна Tails Greeter.

Меню загрузки

Меню загрузки — это первый экран, который отображается во время загрузки операционной системы Tails.

1. Для добавления параметра загрузки нажмите клавишу <TaЬ> на экране загрузки (см. рис. 19.13) — в нижней части экрана вы увидите список доступных параметров.

2. Нажмите клавишу <Пробел>, а затем введите параметр, который следует использовать.

   На момент подготовки книги поддерживался только один параметр загрузки: **i2p,** активирующий поддержку сети I2P (рис. 19.15).



Рис. 19.15. Экран загрузки с параметром i2p

3. Если требуется указать более одного параметра загрузки, их следует вводить друг за другом, разделяя пробелом.
4. Нажмите клавишу <Enter> для запуска Tails.

Окна Tails Greeter

Tails Greeter — это группа окон, появляющаяся после экрана загрузки, но перед открытием рабочего стола GNOME. На рис. 19.14 показано первое окно Tails Greeter, позволяющее выполнить следующие задачи:

- запустить Tails без начальной настройки — выбрав пункт No (Нет) и нажав кнопку Login (Войти) или клавишу <Enter>;
- запустить Tails с интерфейсом на языке, отличном от английского — выбрав нужный язык в раскрывающемся списке в нижней части экрана. Здесь также можно выбрать страну и раскладку клавиатуры;
- для первичной настройки системы выберите пункт Yes (Да), а затем нажмите кнопку Forward (Вперед) — вы увидите второе окно Tails Greeter (рис. 19.16).

Далее описаны первичные настройки, доступные в этом окне.

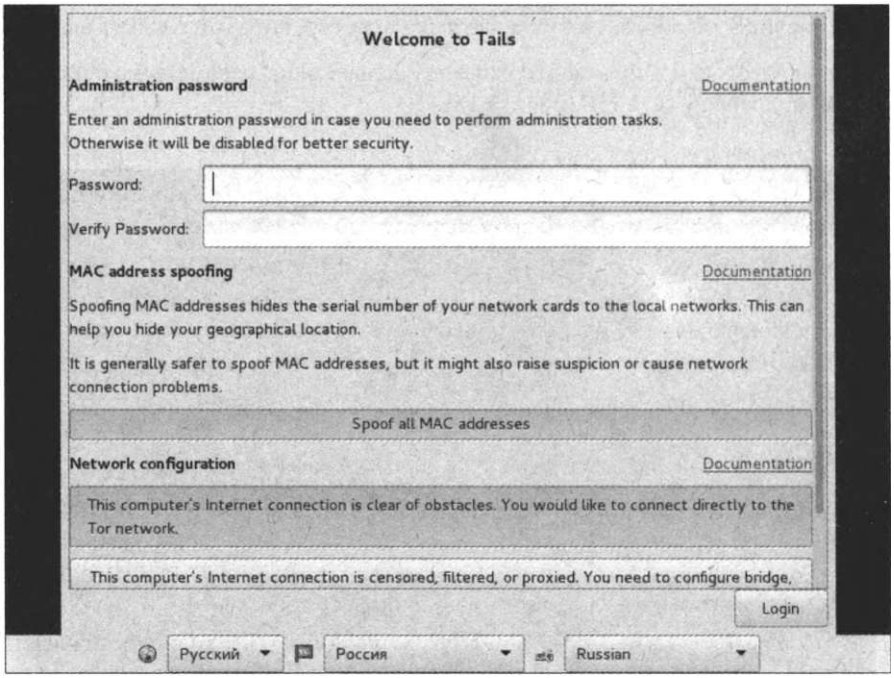


Рис. 19.16. Экран первичной настройки Tails

Пароль администратора

В системе Tails пароль администратора требуется для подтверждения выполнения системных задач, например:

- установки дополнительных программ;
- доступа к внутреннему жесткому диску компьютера;
- выполнения команд в программе для системного администрирования `sudo`.

Для обеспечения дополнительной защиты по умолчанию пароль администратора отключен. Тем самым предотвращается физический или удаленный доступ злоумышленника к запущенной системе Tails с целью получения административных привилегий и выполнения соответствующих задач без вашего ведома.

Однако, чтобы получить возможность выполнения в Tails необходимых административных команд, можно, используя Tails Greeter, задать пароль администратора:

1. В первом окне Tails Greeter (см. рис. 19.14) выберите пункт Yes (Да), а затем нажмите кнопку **Forward** (Вперед).
2. В группе элементов управления **Administration password** (Пароль администратора) второго окна Tails Greeter (см. рис. 19.16) укажите желаемый пароль в полях ввода Password (Пароль) и Verify Password (Проверка пароля).

Спуфинг MAC-адресов

Любой сетевой интерфейс — проводной или Wi-Fi — имеет уникальный MAC-адрес (серийный номер), присваиваемый производителем каждому устройству. MAC-адреса исполь-

зуются в локальных сетях с целью идентификации сетевых интерфейсов для успешной передачи данных.

Как IP-адрес идентифицирует ваш компьютер в Интернете, так и MAC-адрес позволяет определить, какое именно конкретное устройство вы используете в локальной сети. MAC-адреса задействованы только в локальных сетях и не передаются через Интернет.

Тем не менее, наличие подобного уникального идентификатора может угрожать вашей безопасности и в локальной сети — например, в следующих случаях:

- если вы подключаетесь с ноутбука к различным сетям Wi-Fi, MAC-адрес вашего беспроводного интерфейса фиксируется во всех этих локальных сетях. Злоумышленник может проанализировать их и, обнаружив ваш MAC-адрес, *отследить ваше географическое местоположение;*
- злоумышленник может проанализировать трафик, исходящий с вашего компьютера в локальную сеть, и понять, что вы, вероятно, используете Tails. В этом случае ваш MAC-адрес будет *идентифицировать вас как пользователя системы Tails.*

Система Tails позволяет временно менять MAC-адреса ваших сетевых интерфейсов, генерируя для них на время сеанса работы случайные значения. Эта процедура называется *спуфингом MAC-адресов* и позволяет в Tails скрывать серийные номера используемых сетевых интерфейсов и, что важно, анонимизировать вас в локальной сети.

Спуфинг MAC-адресов в Tails используется по умолчанию, т. к. это очень важная процедура. Но в некоторых случаях она может. повлечь проблемы с соединением с сетью или представить вашу сетевую активность подозрительной. Далее вы узнаете, следует ли использовать спуфинг MAC-адресов или нет, в зависимости от ситуации.

Необходимость в смене MAC-адреса

Спуфинг MAC-адресов в Tails включен по умолчанию для всех сетевых интерфейсов. В большинстве случаев это полезно, даже если вы не нуждаетесь в сокрытии своего географического местоположения, — например, когда:

- *вы подключаете свой компьютер к открытой сети Wi-Fi,* к примеру, в метро или в ресторане, — там, где не нужно регистрироваться в ней для подтверждения своей личности. При этом смена MAC-адреса позволит скрыть тот факт, что ваш компьютер подключен к этой сети;
- *вы часто подключаете компьютер к определенной сети,* к примеру, в гостях, на рабочем месте, в университете и т. д. Смена MAC-адреса скроет тот факт, что ваш компьютер подключается к этой сети в определенное время. Также будет скрыт факт, что именно вы пользовались подключением к этой сети из системы Tails.

Прекращение смены MAC-адреса

Однако в некоторых случаях спуфинг MAC-адресов может стать источником проблем, и тогда эту возможность следует отключить.

Обратите внимание, что даже если спуфинг MAC-адресов отключен, защита ваших данных в Интернете обеспечивается:

- злоумышленник может увидеть только зашифрованный поток данных в/из сеть Tor;
- используемый вами MAC-адрес не передается через Интернет на веб-сайты, которые вы посещаете.

Разумеется, отключение спуфинга MAC-адресов позволит отслеживать в локальной сети ваше географическое местоположение. Если это представляет для вас угрозу, используйте другое сетевое устройство или сеть.

Далее представлено несколько примеров ситуаций, когда спуфинг MAC-адресов лучше отключить:

- *вы используете публичный компьютер* — к примеру, в интернет-кафе или в библиотеке. Этим компьютером регулярно пользуются в этой локальной сети разные посетители, и его MAC-адрес не ассоциируется с вами. На таких компьютерах смена MAC-адреса может привести к потере соединения с сетью. К тому же, появление неизвестных MAC-адресов вызовет подозрения у сотрудников, администрирующих эту сеть;
- на некоторых сетевых интерфейсах *спуфинг MAC-адресов невозможен* из-за аппаратных или программных ограничений. Операционная система Tails временно отключает такие интерфейсы, но вы можете отключить спуфинг MAC-адресов, чтобы их использовать;
- некоторые сети *поддерживают подключение устройств только с определенными (внесенными в настройки) MAC-адресами.* И если вы ранее подключались к такой сети, смена MAC-адреса может препятствовать подключению;
- *вы используете свой компьютер в домашней сети* — в таком случае вы и MAC-адрес сетевого интерфейса вашего компьютера ассоциируются с вашей домашней сетью, поэтому смена MAC-адреса бесполезна. Опять же, если доступ к вашей сети организуется согласно определенным MAC-адресам, его смена может препятствовать подключению.

Отключить функцию спуфинга MAC-адресов можно в окне Tails Greeter:

1. В первом окне Tails Greeter (см. рис. 19.14) выберите пункт Yes (Да), а затем нажмите кнопку Forward (Вперед).
2. В группе элементов управления MAC address spoofing (Спуфинг MAC-адресов) второго окна Tails Greeter (см. рис. 19.16) установите в выключенное состояние кнопку Spoof all MAC addresses (Спуфинг всех MAC-адресов).

Дополнительные сведения

Ваше географическое местоположение могут выявить и другие средства слежения: видеонаблюдение, прослушивание телефонов, отслеживание транзакций банковских карт и пр. Кроме того:

- при использовании сети Wi-Fi любой человек в зоне действия беспроводной сети может просмотреть ваш MAC-адрес — даже без необходимости подключения к той же точке доступа Wi-Fi;
- некоторые сетевые сервисы могут передавать MAC-адреса через Интернет на серверы аутентификации, однако это не должно повлиять на ваше решение использовать функцию спуфинга MAC-адресов. Если вы решите отключить функцию спуфинга MAC-адресов, ваш компьютер может быть идентифицирован вашим же провайдером;
- при использовании сетей передачи данных в мобильном телефоне — таких как 3G\4G или GSM, идентификатор вашей SIM-карты (IMSI) и серийный номер телефона (IMEI) всегда доступны оператору сотовой связи.

Настройка сети

В зависимости от используемого подключения к Интернету, вам может понадобиться настроить соединение с сетью Tor.

Такая необходимость может возникнуть, если:

- вам необходимо использовать для доступа к Интернету прокси-сервер;
- установленный на вашем компьютере брандмауэр допускает подключение только через определенные порты;
- вы хотите использовать мосты Tor, поскольку ваше подключение к Интернету ограничивается, или вы намереваетесь скрыть факт использования подключения к сети Tor.

В таких случаях во втором окне Tails Greeter (см. рис. 19.16) нажмите кнопку This computer's Internet connection is censored, filtered, or proxied. You need to configure bridge, firewall, or proxy settings — после загрузки рабочего стола и подключения к Интернету мастер настройки поможет вам сконфигурировать подключение к сети Tor.

Мосты Tor

Когда сеть Tor используется в системе Tails с настройками по умолчанию, каждый, кто способен анализировать трафик, исходящий с вашего компьютера (к примеру, провайдер или злоумышленник), может быть осведомлен о том, что вы подключены к сети Tor.

Это может стать проблемой в следующих ситуациях:

- *использование сети Tor запрещено по цензурным соображениям* — поскольку все соединения с Интернетом осуществляются через сеть Tor, система Tails становится бесполезна, разве что для автономной работы с документами и т. д.;
- *использование сети Tor представляет опасность или может вызвать подозрения* — в этом случае использование системы Tails с настройками по умолчанию может навлечь серьезные неприятности.

Мосты Tor, также называемые *ретрансляторами Tor*, представляют собой альтернативные непубличные точки входа в сеть Tor. Их использование затруднит, хотя и не сведет к нулю, вероятность обнаружения того, что вы используете Tor.

Если вам близка одна из ситуаций из числа здесь упомянутых, в системе Tails рекомендуется использовать мосты Tor.

Чтобы осуществить подключение к сети Tor через мост, необходимо знать адрес по крайней мере одного моста. Вы можете узнать адреса мостов несколькими способами — например, найти их на сайте tinyurl.com/oubb31w или получить по электронной почте.

Мосты менее надежны в, плане безопасности и, как правило, менее производительны по сравнению с другими узлами сети Tor.

Использование сетевых мостов в Tails

Чтобы работать в Tails с использованием мостов Tor, вы должны иметь под рукой адрес, по крайней мере, одного такого моста. Например, вы можете записать его на листе бумаги или хранить в защищенном разделе.

В системе Tails можно использовать мосты следующих типов:

- `bridge`
- `obfs2`
- `obfs3`
- `obfs4`
- `ScrambleSuit`

Для подключения к сети Tor через мост нажмите кнопку This computer's Internet connection is censored, filtered, or proxied. You need to configure bridge, firewall, or proxy settings во втором окне Tails Greeter (см. рис. 19.16) — после запуска системы Tails вы сможете настроить мосты с помощью мастера и просмотреть цепочку ретрансляторов на карте сети в программе Vidalia.

Использование Tor в странах с цензурой

Мосты Tor — важный инструмент, способный помочь во многих случаях, но они не предоставляют абсолютную защиту от всех действий злоумышленника, пытающегося связать вашу деятельность с сетью Tor.

В основном, мосты Tor предназначены для пользователей стран, где доступ к сети Tor ограничивает цензура. Если использование Tor может привести к негативным последствиям, следуйте некоторым дополнительным правилам, чтобы предотвратить идентификацию себя как пользователя сети Tor:

- всегда запускайте систему Tails в режиме мостов Tor;
- используйте только обфусцированные мосты (obfs3, ScrambleSuit и obfs4), т. к. их гораздо сложнее определить, чем другие;
- чем меньше известны мосты, тем лучше. К сожалению, адреса некоторых мостов могут быть доступны на сайте Tor или по электронной почте, и злоумышленник также может узнать их. Предпринимаются некоторые способы противодействия этому, но они далеки от совершенства.

Идеальным вариантом будет, если вы можете найти надежного человека или организацию другой страны, который или которая смогут запустить для вас приватный обфусцированный мост. В этом случае приватность означает, что мост должен быть настроен с применением опции `PublishServerDescriptor 0`. Без нее в сети Tor станет известно о вашем мосте, и его адрес будет предоставлен другим пользователям (и, как следствие, окажется в руках злоумышленника).

Отключение от сети (автономный режим)

Если вы хотите работать полностью в автономном режиме, то можете перед запуском Tails отключить все сетевые подключения. Это может быть полезно для реализации дополнительной степени защиты при работе с конфиденциальными документами.

Для перехода в автономный режим выполните следующие действия:

1. В первом окне Tails Greeter (см. рис. 19.14) выберите пункт Yes (Да), а затем нажмите кнопку Forward (Вперед).
2. В группе элементов управления Network configuration (Конфигурация сети) второго окна Tails Greeter (см. рис. 19.16) нажмите кнопку Disable all networking (Отключить все сетевые подключения).

Обзор рабочего стола Tails

Пространство рабочего стола, используемое в Tails, называется GNOME. Среда GNOME применяется во многих UNIX-подобных системах. Далее вы познакомитесь с основными элементами рабочего стола в операционной системе Tails.

Верхняя навигационная панель

В верхней части экрана находится верхняя навигационная панель. В ее левой части доступны два меню: **Приложения** (Applications) и **Места** (Places). Меню **Приложения** (Applications) обеспечивает доступ к установленным приложениям и конфигурационным инструментам среды GNOME (рис. 19.17).

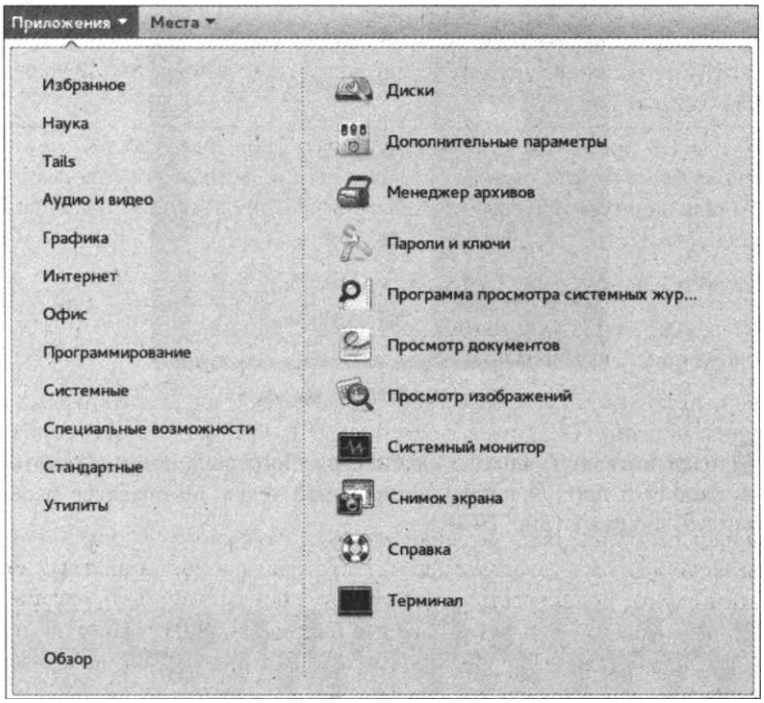


Рис. 19.17. Меню Приложения

СИСТЕМНЫЕ НАСТРОЙКИ

Вы можете изменить различные системные настройки, например, свойства клавиатуры или разрешение монитора, выбрав в меню **Приложения** (Applications) пункт **Системные | Параметры** (System Tools | Settings). По умолчанию все произведенные в системе настройки сбрасываются при каждом перезапуске Tails. Для сохранения настроек нужно использовать зашифрованное хранилище (см. соответствующий раздел).

В меню **Приложения | Избранное** (Applications | Favorites) расположены ярлыки наиболее часто используемых приложений: веб-браузер Tor Browser, клиент электронной почты Icedove, IM-мессенджер Pidgin, менеджер паролей KeePassX и инструмент командной строки Terminal.

Меню **Места** (Places) предоставляет быстрый доступ к различным каталогам и носителям (рис. 19.18).

В правой части верхней навигационной панели расположены следующие элементы управления:

- кнопка открывает окно программы Vidalia — консоли сети Tor с графическим интерфейсом;

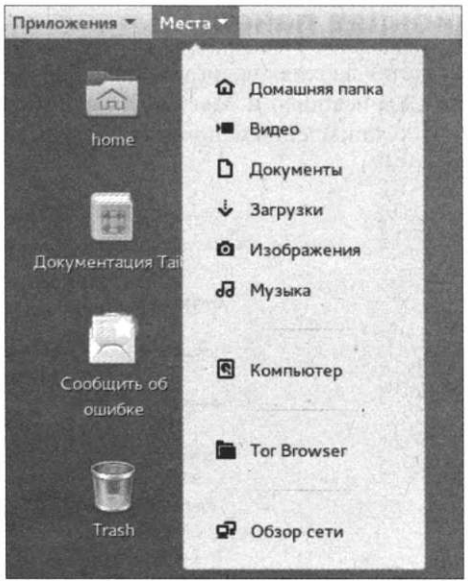


Рис. 19.18. Меню Места

- кнопка |Щ открывает виртуальную клавиатуру Florence, с помощью которой вы можете набирать пароли и прочий конфиденциальный текст, не опасаясь перехвата данных аппаратными кейлогерами (рис. 19.19);



Рис. 19.19. Виртуальная клавиатура

- кнопка позволяет получить доступ к апплету OpenPGP, предназначенному для шифрования/расшифровки содержимого буфера обмена;
- кнопка скрывает под собой меню специальных возможностей, позволяющих увеличивать экранный текст, отображать визуальные предупреждения, управлять контрастностью изображения и т. п. (рис. 19.20);
- следом расположено меню раскладок клавиатуры, позволяющее переключать ввод на разные языки;
- кнопка с текущим днем недели и временем позволяет отобразить панель календаря;
- в правом верхнем углу экрана расположена кнопка со значками сетевого подключения, уровня громкости и включения, открывающая доступ к настройкам системы и управлению компьютером (рис. 19.21).

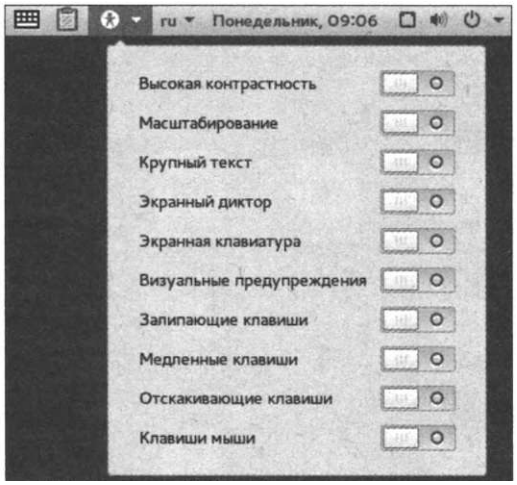


Рис. 19.20. Меню специальных возможностей

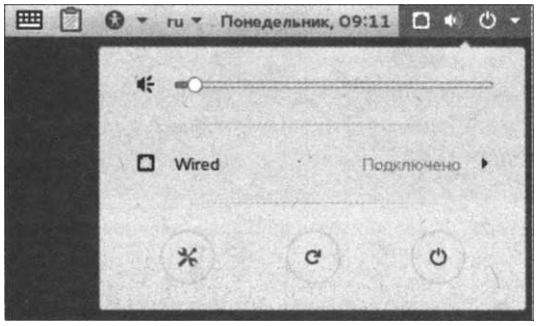


Рис. 19.21. Вид меню управления компьютером

С помощью меню этой кнопки вы можете отрегулировать уровень громкости, отключить/настроить соединение с Интернетом, а также открыть окно системных настроек и перезагрузить или выключить компьютер.

Обзор приложений

Чтобы просмотреть все установленные приложения, а также выполнить их поиск, произведите следующие действия:

1. Выберите команду меню **Приложения | Обзор** (Applications | Overview) или нажмите клавишу на клавиатуре — вы увидите экран со списком избранных приложений слева и панелью рабочих столов справа.
2. Нажмите кнопку , расположенную в левой части экрана, — вы увидите экран, похожий на изображенный на рис. 19.22.

Здесь можно просмотреть список всех или только популярных (см. вкладки в нижней части экрана) приложений, прокручивая его колесиком мыши или нажатиями круглых кнопок в правой части экрана. Введя запрос в поле в верхней части экрана, вы сможете произвести поиск среди установленных приложений, папок и файлов.

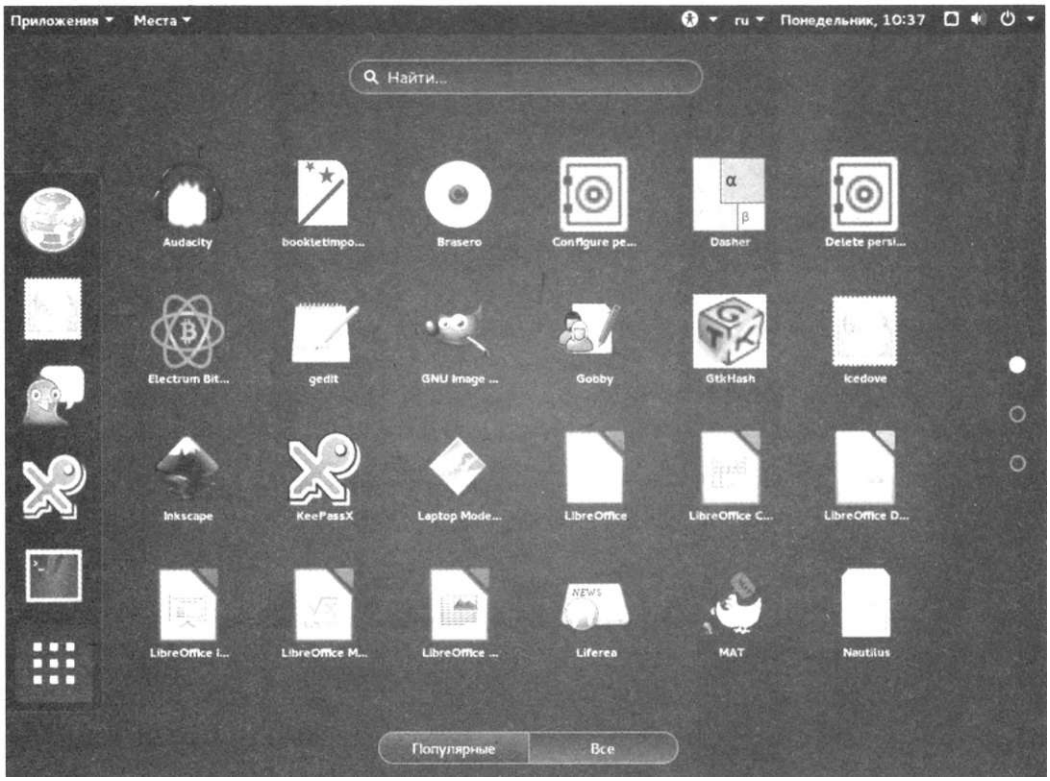


Рис. 19.22. Обзор приложений в операционной системе Tails

Запуск терминала суперпользователя

Для запуска терминала суперпользователя в системе Tails выполните следующие действия:

1. Выберите команду меню **Приложения | Системные | Терминал суперпользователя** (Applications | Accessories | Root Terminal).
2. Выполните в терминале команду `sudo -i`.

Рабочий стол

На рабочем столе системы Tails по умолчанию расположены следующие ярлыки:

- — открывает домашнюю папку пользователя в файловом менеджере Nautilus (рис. 19.23);
- — открывает хранилище удаленных файлов и папок;
- — открывает локальную копию справочной системы Tails;
- — открывает раздел поддержки локальной копии сайта Tails для решения проблем в процессе эксплуатации системы.

Как можно видеть, в качестве файлового менеджера в Tails используется приложение Nautilus, служащее в среде GNOME для управления файлами/папками, передачи данных по протоколу FTP/SFTP и т. п. Управление файлами и папками осуществляется с помощью

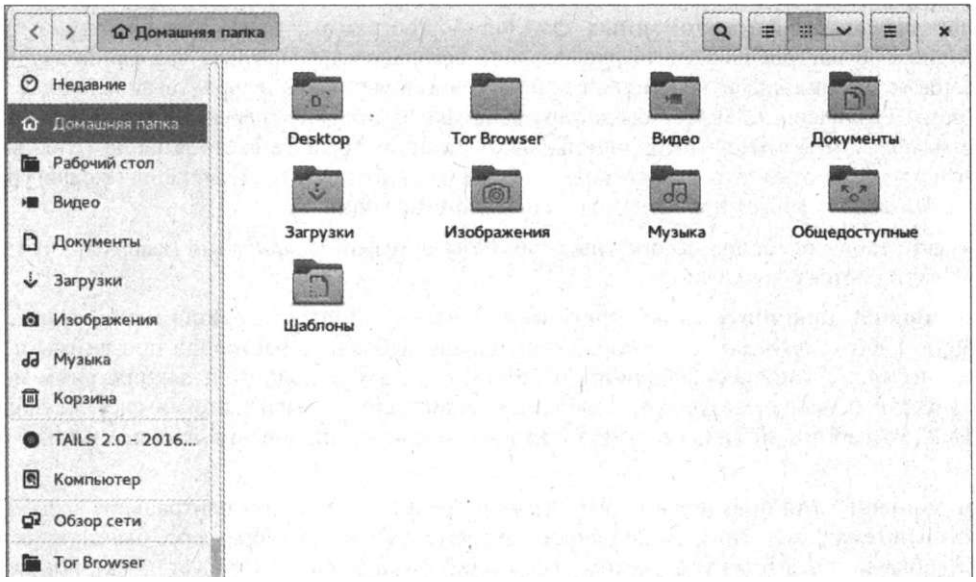


Рис. 19.23. Окно файлового менеджера Nautilus

мыши, клавиатуры и контекстных меню аналогично тому, как это делается в других операционных системах.

Для подключения к серверу используется команда **Nautilus | Подключиться к серверу** (Nautilus | Connect to Server).

Зашифрованное хранилище

Если операционная система Tails установлена на Flash-накопитель или SD-карту с помощью инструмента Tails Installer, то в свободном пространстве на таком носителе можно создать зашифрованное хранилище. Файлы в этом хранилище шифруются и остаются доступны после перезагрузки или повторного запуска системы Tails.

В зашифрованном хранилище могут быть сохранены данные следующих типов:

- персональные документы и файлы;
- программные пакеты, загруженные и установленные в Tails;
- конфигурационные файлы используемых программ;
- персональные ключи шифрования.

Содержимое хранилища шифруется с помощью пароля. Создав зашифрованное хранилище, вы можете выбирать, задействовать ли его при каждом запуске Tails.

Меры безопасности

При работе с зашифрованным хранилищем следует соблюдать следующие меры безопасности:

* **хранение конфиденциальных документов** — зашифрованное хранилище не скрывается. Злоумышленник, завладев устройством, может узнать о наличии на нем зашифрованного хранилища и силой или обманом выпытать у вас пароль для доступа к нему;

перезапись конфигурационных файлов — программы, предустановленные в Tails, тщательно настроены с учетом требований безопасности. При использовании зашифрованного хранилища и перезаписи конфигурационных файлов предустановленных программ безопасность может быть нарушена или программы перестанут работать должным образом. Учтите, что принципы анонимизации Tor и Tails строятся на усложнении возможности отличить одного пользователя Tails от другого. Изменение конфигурационных файлов может привести к вашей деанонимизации.

Будьте также особенно осторожны с так называемыми *дотфайлами* (файлами, чьи имена начинаются с точки);

- **установка дополнительных программ** — чтобы обеспечить анонимность и бесследность работы пользователя, разработчики Tails выбрали и настроили программы с учетом их совместной беспроблемной работы. Установка дополнительных программ может привести к непредсказуемым проблемам и появлению уязвимостей в системе защиты Tails. Разработчики Tails не смогут помочь вам при возникновении проблем в таком случае;
- дополнения для **браузеров** — веб-браузер представляет собой центральное звено в таких системах, как Tails. Дополнения, предустановленные в браузере, были тщательно подобраны и настроены с учетом требований безопасности. При установке новых или изменении настроек существующих дополнений вы можете нарушить свою анонимность;
- **использование при исключительной необходимости** — используйте зашифрованное хранилище только в случае исключительной необходимости и по минимуму. По возможности, всегда запускайте систему Tails без поддержки зашифрованного хранилища. Все возможности зашифрованного хранилища опциональны и должны активироваться явно. Только указанные вами файлы и папки будут в нем сохраняться;
- **открытие зашифрованного хранилища из других операционных систем** — получить доступ к зашифрованному хранилищу возможно также и из-под других операционных систем, но это может угрожать безопасности ваших данных. Другие операционные системы могут сохранять информацию об обработке конфиденциальных данных.

Создание зашифрованного хранилища

Еще раз хочу вас предупредить: использование зашифрованного хранилища в системе, которая предназначена для обеспечения анонимности и сокрытия следов вашей работы на компьютере и в сети, может снизить уровень защиты (см. *разд. «Меры безопасности»* ранее в этой главе).

Запуск мастера создания зашифрованного хранилища

Чтобы запустить мастер создания зашифрованного хранилища, выберите команду меню **Приложения | Tails | Configure persistent volume** (Applications | Tails | Configure persistent volume), — вы увидите окно, показанное на рис. 19.24.

Если появится сообщение об ошибке: **Error, Persistence partition is not unlocked,** — значит, функция ранее созданного зашифрованного хранилища не задействована в окне Tails Greeter, и вы не сможете получить доступ к его настройкам, но при необходимости можете удалить существующее и создать.

При первом запуске (или после удаления ранее созданного зашифрованного хранилища) мастер поможет создать на устройстве, с которого запущена операционная система Tails, новое зашифрованное хранилище.

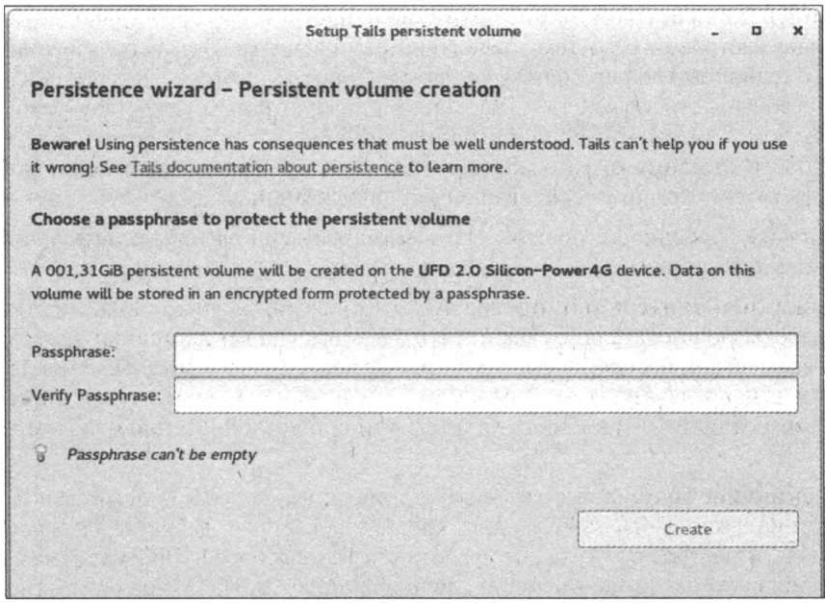


Рис. 19.24. Окно мастера создания зашифрованного хранилища

Итак:

1. Зашифрованное хранилище защищается с помощью пароля — укажите пароль в полях **Passphrase** (Кодовая фраза) и **Verify Passphrase** (Повторите кодовую фразу) (см. рие. 19.24).
2. Нажмите кнопку **Create** (Создать).
3. Дождитесь окончания процесса создания хранилища.

Если процесс создания будет прерван, вы больше не сможете запустить операционную систему Tails с этого устройства. Это может случиться, если в процессе создания хранилища вы закроете окно мастера или отключите Flash-накопитель или SD-карту от компьютера. Для решения проблемы переустановите систему Tails на устройстве.

Настройки хранилища

После создания хранилища в окне мастера настройки вы увидите список доступных параметров (рис. 19.25). Каждый пункт списка определяет набор файлов, которые будут сохранены в зашифрованном хранилище. Вы можете открыть окно настройки зашифрованного хранилища в любой момент, выбрав команду меню **Приложения | Tails | Configure persistent volume** (Applications | Tails | Configure persistent volume).

На постоянной основе могут быть сохранены только указанные в окне настройки функции. В будущих выпусках операционной системы Tails предполагается реализовать и некоторые другие возможности: браузерные дополнения, обои рабочего стола, RSS-каналы, настройки звуковой карты, мыши, сенсорной панели и пр.

Чтобы применить изменения, внесенные в окне настройки зашифрованного хранилища, Tails следует перезапустить.

Если сбросить тот или иной флажок, соответствующая функция после перезапуска Tails будет отключена, но связанные с ней файлы останутся в зашифрованном хранилище.

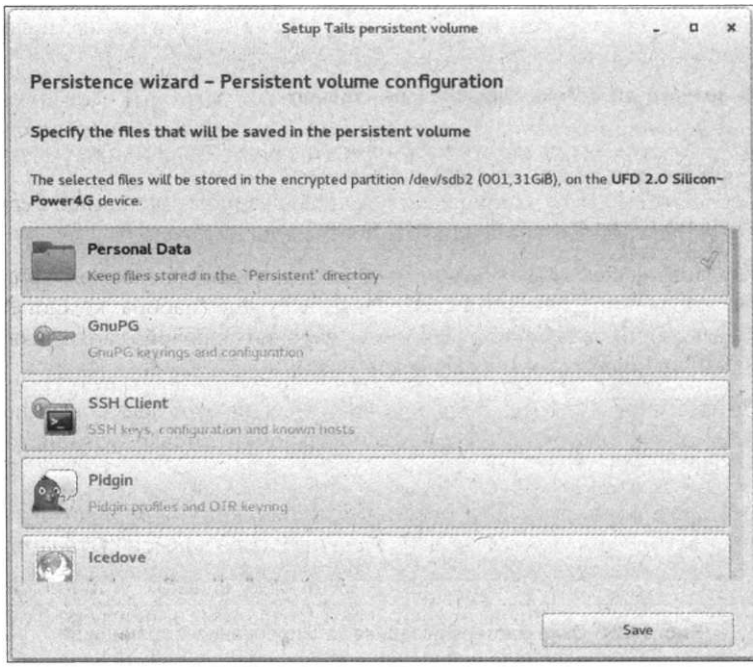


Рис. 19.25. Окно настройки зашифрованного хранилища

Как можно видеть, окно настроек предлагает следующий набор параметров:

- **Personal Data** (Персональные данные) — если этот флажок установлен, вы можете сохранять свои персональные файлы и рабочие документы в папку **Persistent.** Для доступа к ней выберите команду меню **Места | Persistent** (Places | Persistent);
- **GnuPG** — если этот флажок установлен, создаваемые и импортируемые OpenPGP-ключи будут сохраняться в зашифрованном хранилище. Если вы вручную отредактируете или перезапишете конфигурационный файл ~/.gnupg/gpg.conf, уровень анонимности может быть нарушен, степень шифрования GnuPG будет ослаблена или вовсе станет неработоспособной;
- **SSH Client** — если этот флажок установлен, в зашифрованном хранилище будут сохраняться все файлы, относящиеся к SSH-клиенту:
  - создаваемые и импортируемые SSH-ключи;
  - открытые ключи хостов, к которым вы подключаетесь;
  - конфигурационный файл ~/.ssh/config.

  Если вы вручную отредактируете конфигурационный файл ~/.ssh/config, убедитесь, что не перезаписана конфигурация по умолчанию в файле /etc/ssh/ssh_config. В противном случае степень шифрования наряду с работой SSH-клиента могут быть нарушены;
- **Pidgin** — если этот флажок установлен, в зашифрованном хранилище будут сохраняться все конфигурационные файлы IM-мессенджера Pidgin, а также:
  - настройки ваших аккаунтов, собеседников и чатов;
  - ваши криптографические ключи OTR;
  - содержимое бесед, если в программе Pidgin активирована соответствующая настройка.

Все настройки Pidgin доступны из графической оболочки программы, и вам нет необходимости вручную редактировать конфигурационные файлы.

Обратите внимание, что программа Pidgin не сможет загрузить ваш аккаунт, если зашифрованное хранилище используется в режиме «только для чтения», — т. е. когда в окне Tails Greeter установлен флажок **Read-only** (Только для чтения);

- **Icedove** — если этот флажок установлен, в зашифрованном хранилище будут сохраняться настройки и электронные сообщения из программы Icedove;
- **GNOME Keyring** — если этот флажок установлен, в зашифрованном хранилище будут сохраняться данные инструментария GNOME Keyring (набора компонейтов в среде GNOME, отвечающих за хранение секретов, паролей, ключей, сертификатов и прочих данных для защищенной работы с приложениями);
- **Network Connections** (Сетевые подключения) — если этот флажок установлен, в зашифрованном хранилище будут сохраняться настройки сетевых уртройств и подключений.

  Для сохранения сетевых паролей — обеспечивающих, к примеру, доступ к защищенным беспроводным сетям, — флажок **GNOME Keyring** также должен быть установлен;
- **Browser bookmarks** (Закладки браузера) — если этот флажок установлен, в зашифрованном хранилище будут сохраняться закладки, созданные в браузере Tor Browser. Эта опция не касается небезопасного браузера;
- **Printers** (Принтеры) — если этот флажок установлен, в зашифрованном хранилище будут сохраняться настройки принтеров;
- **Bitcoin Client** (Биткоин-клиент) — если этот флажок установлен, в зашифрованном хранилище будут сохраняться счета и настройки биткоин-клиента Electrum;
- **APT Packages** (APT-пакеты) — если этот флажок установлен, в зашифрованном хранилище будут сохраняться пакеты, которые вы устанавливаете с помощью менеджера пакетов Synaptic или команды `apt-get`. Эта опция разрешает скачивать и переустанавливать дополнительное программное обеспечение в любых рабочих сеансах, даже автономных.

  Если вы активировали функцию **APT Packages** (APT-пакеты), рекомендуется также установить флажок описанной далее функции **APT Lists** (APT-списки);
- для автоматической переустановки установленных пакетов при перезапуске Tails используйте описанную далее функцию **Additional software packages** (Дополнительные программные пакеты);
- **APT Lists** (APT-списки) — если этот флажок установлен, в зашифрованном хранилище будут сохраняться списки всех программных пакетов, доступных для установки. APT-списки необходимы для установки дополнительных программ и просмотра доступных программных пакетов и индексируют файлы, загружаемые с помощью менеджера пакетов Synaptic или команды `apt-get update`. Эта функция доступна для использования в любых рабочих сеансах, даже автономных;
- Dotfiles (Дотфайлы)— если этот флажок установлен, все файлы в каталоге /live/ рег51з1епсеЯаПзОа1а_ип1ос1^Мо1А1ез связываются с домашней папкой. Файлы в подкаталогах также связываются с помощью соответствующих подпапок домашнего каталога.

  Эту опцию лучше пояснить на примере. Пусть в папке /Нуе/регз151епсеЯаП50а1а_ unlocked/dotfiles расположены следующие файлы:

```
/live/persistence/Tail3Data_imlocked/dotfiles
I— файл_а
I— папка
I    I— файл_С
I    '— подпапка
I         '— файл_в
'— пустаяпапка
```

Тогда включение опции Dotfiles приведет в папке /home/amnesia к следующему результату:

```
/home/amnesia
|— файл_а    /live/persistence/TailsData_unlocked/dotfile3/файл_а
'— папка
    |— файл_в    /live/per3istence/TailsData_unlocked/dotfiles/nanKa^aitn_е
    '— подпапка
        '— файл_в -> /live/persistence/TailsData_unlocked/dotfileз/папка/подпапка/файл_в
```

Эта опция полезна, если вы хотите перманентно сохранить какие-либо файлы, но не папки, в которых они расположены. Прекрасным примером являются так называемые дотфайлы (отсюда и название этой функции)— скрытые конфигурационные файлы в корне вашего домашнего каталога, например: *-/.gitconfig* и *-/.bashrc*.

Как можно видеть из примера, пустые папки игнорируются, т. е. функция Dotfiles связывает в домашней папке только файлы, но не каталоги из зашифрованного хранилища;

- Additional software packages (Дополнительные программные пакеты) — это экспериментальная функция, которая не представлена в окне настройки зашифрованного хранилища.

  Если она включена, список дополнительного выбранного вами программного обеспечения автоматически устанавливается в начале каждого сеанса работы с Tails. Соответствующие программные пакеты хранятся в зашифрованном хранилище и автоматически обновляются для обеспечения безопасности после установки подключения к Интернету.

  Чтобы использовать эту функцию, в окне настройки зашифрованного хранилища необходимо установить флажки APT Packages (APT-пакеты) и APT Lists (APT-списки).

Если дополнительные программные пакеты при работе в автономном режиме не устанавливаются, причина может заключаться в устаревших APT-списках. Проблема будет решена при следующем запуске Tails с активной функцией хранилища и подключением к Интернету.

Чтобы составить список дополнительного программного обеспечения, запустите Tails с паролем администратора и отредактируйте (от имени администратора) файл /live/persistence/ TailsDatajjnlockedrtive-additional-software.conf. В каждой строке этого файла укажите имя пакета Debian, который должен быть установлен в качестве дополнительного.

Например, для автоматической установки редактора диаграмм dia и менеджера шрифтов Fontmatrix добавьте в файл live-additionai-software.conf следующие строки:

```
dia
fontmatrix
```

Чтобы узнать о программных пакетах, доступных в Debian, посетите ресурс packages. debian.org/stable/.

Учтите также, что установка дополнительного программного обеспечения осуществляется на ваш страх и риск. Многие программы требуют дополнительной настройки сетевого подключения через Tor и в противном случае не будут функционировать. Некоторые программы могут снижать уровень безопасности Tails, к примеру, внося собственные правила в брандмауэр. Программное обеспечение, не включенное официально в Tails, не тестируется на безопасность.

Использование зашифрованного хранилища

При загрузке операционной системы Tails вам будет предложено использовать или нет зашифрованное хранилище. Нажав кнопку **Yes** (Да) в группе **Use persistence?** (Использовать хранилище?) окна Tails Greeter (рис. 19.26) вы активируете зашифрованное хранилище для текущего сеанса работы. После этого вам понадобится ввести пароль в расположенное ниже текстовое поле.

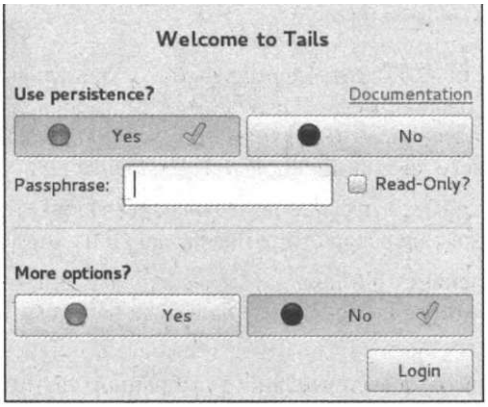


Рис. 19.26. Активация защищенного хранилища в окне Tails Greeter

Если установить флажок **Read-Only** (Только для чтения), содержимое зашифрованного хранилища будет доступно, в том числе и для изменения, но все изменения не будут сохранены.

Для доступа к папке Persistent, содержащей ваши персональные файлы и рабочие документы, выберите команду меню **Места | Persistent** (Places | Persistent).

Продвинутые пользователи могут получить доступ к содержимому зашифрованного хранилища, выбрав команду меню **Места | Компьютер** (Places | Computer), а затем перейдя к каталогу live/persistence/TailsData_unlocked.

Изменение пароля доступа к зашифрованному хранилищу

Для изменения пароля доступа к зашифрованному хранилищу:

1. Запустите систему Tails, установив пароль администратора (см. *разд. «Пароль администратора»* ранее в этой главе).
2. Выберите команду меню **Приложения | Утилиты | Диски** (Applications | Utilities | Disks).

В приложении Диски (Disks) все текущие устройства хранения данных показаны в левой части окна. Если выбрать одно из устройств, подробная информация о нем: разделы, название, объем и т. п. — отобразится в правой его части.

3. Найдите, какое из устройств хранения данных содержит защищенное хранилище. Разделы на нем должны иметь метки **Tails** и **TailsData** — последний раздел как раз и является защищенным хранилищем.
4. В правой части окна выберите раздел с меткой **TailsData** (рис. **19.27).**

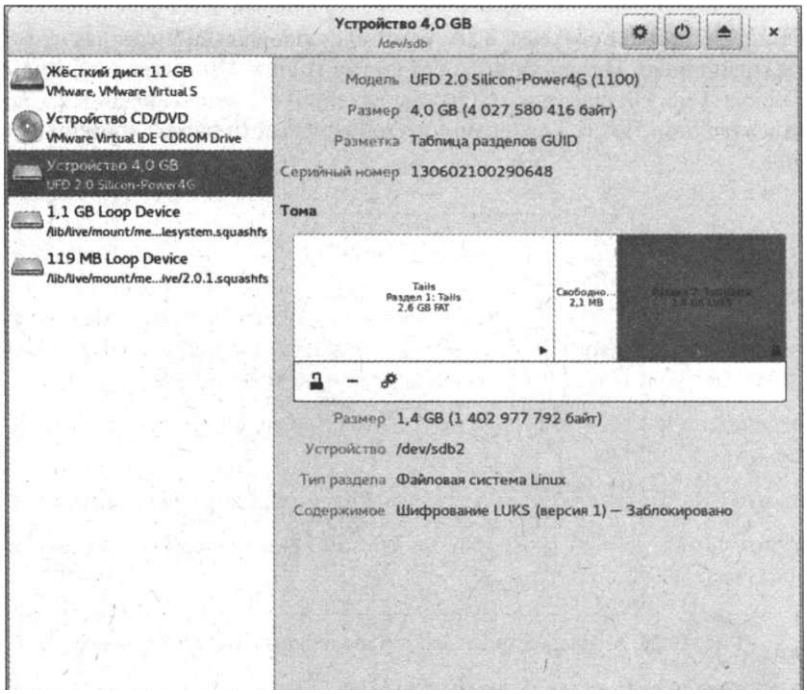


Рис. 19.27. Выбор раздела с защищенным хранилищем в окне программы Диски (Disks)

5. Нажмите кнопку и в меню выберите пункт **Изменить пароль** (Change Passphrase) — вы увидите окно, предназначенное для смены пароля доступа к защищенному хранилищу (рис. 19.28).

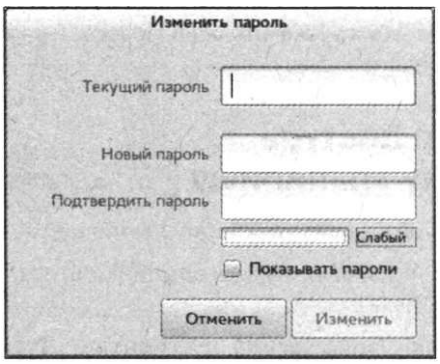


Рис. 19.28. Окно смены пароля для доступа к защищенному хранилищу

6. Введите текущий пароль и дважды новый пароль, а затем нажмите кнопку **Изменить** (Change).
7. В открывшемся окне с подтверждением введите свой пароль администратора и нажмите кнопку **Подтвердить** (Authenticate).

Теперь вы можете перезапустить операционную систему Tails и получить доступ к защищенному хранилищу через новый пароль.

Копирование зашифрованного хранилища на новый носитель

Приведенные далее инструкции научат вас копировать содержимое защищенного хранилища на новый носитель. Следуйте им, если у вас есть основания полагать, что настройки вашего хранилища повреждены или если вы хотите быть очень предусмотрительным.

Создание носителя

1. Установите последнюю версию операционной системы Tails на новое устройство, используя инструкции, приведенные в этой главе ранее. Не используйте устройство с поврежденной версией системы Tails для создания нового носителя.
2. Создайте защищенное хранилище на новом устройстве. Используйте другой пароль для защиты нового хранилища.
3. Настройте нужные характеристики созданного защищенного хранилища.
4. Перезагрузите новое устройство, активируйте защищенное хранилище и установите пароль администратора.

Копирование документов с другого зашифрованного хранилища

Монтирование текущего хранилища

1. Подключите устройство с Tails, с которого нужно скопировать данные.
2. Выберите команду меню **Приложения | Утилиты | Диски** (Applications | Utilities | Disks), чтобы открыть приложение Диски (Disks).
3. В левой части окна выберите устройство с Tails, с которого нужно скопировать данные.
4. В правой части окна щелкните мышью на разделе с шифрованием LUKS (рис. 19.27) — раздел должен иметь метку **TailsData.**
5. Нажмите кнопку для разблокировки старого зашифрованного хранилища. Введите пароль в открывшемся окне и нажмите кнопку **Разблокировать** (Unlock).
6. Щелкните мышью на разделе **TailsData** с файловой системой Ext4, появившемся ниже раздела с шифрованием LUKS (рис. 19.29).
7. Нажмите кнопку — старое хранилище будет подмонтировано по адресу /media/amnesia/TailsData.

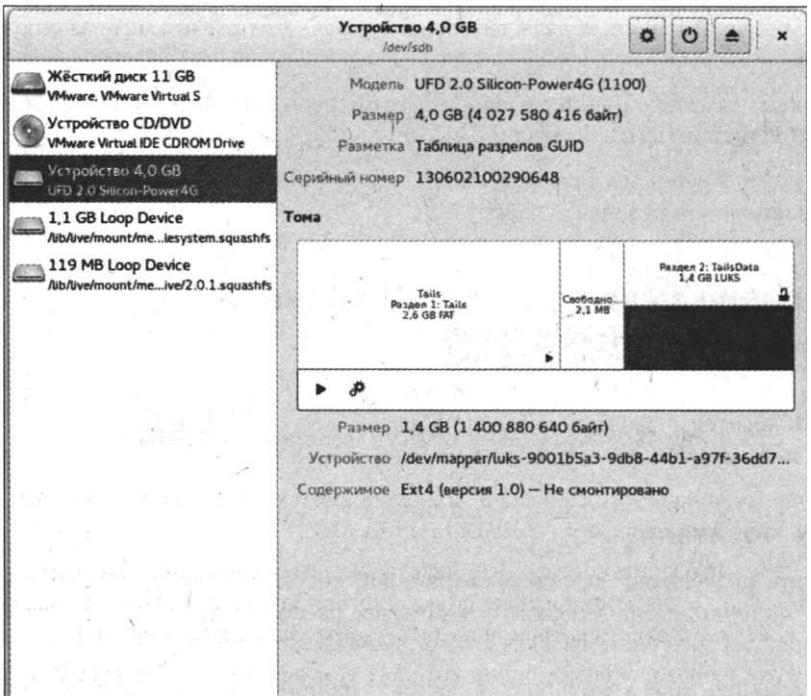


Рис. 19.29. Выбор раздела TailsData с файловой системой Ext4 в окне программы Диски

Копирование файлов в новое хранилище

1. Выберите команду меню **Приложения | Системные | Терминал суперпользователя** (Applications | Accessories | Root Terminal) для открытия окна командной строки с привилегиями администратора и подтвердите запрос вводом пароля администратора.
2. Выполните команду `nautilus` для открытия окна файлового менеджера с правами администратора (рис. 19.30).

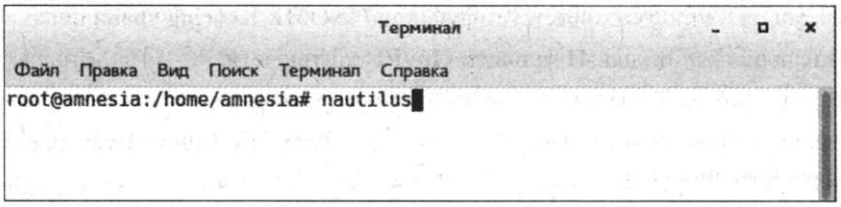


Рис. 19.30. Ввод команды `nautilus` в окне программы Терминал суперпользователя

3. В окне файлового менеджера перейдите в каталог /tecIia/атпезіаЯаiIзОаIа, чтобы открыть старое хранилище (рис. 19.31).
4. На панели заголовка файлового менеджера нажмите кнопку____, выберите пункт **Создать вкладку** (New Tab) и перейдите в каталог /live/persistenc^TailsData_unlocked на новой вкладке.
5. Перейдите на вкладку **TailsData.**

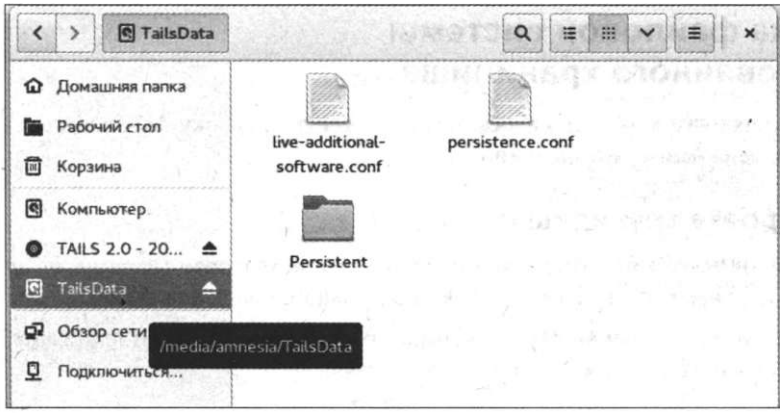


Рис. 19.31. Содержимое каталога /media/amnesia/TailsData

6. Для копирования папки, содержащей данные старого хранилища, в новое, перетащите ее с вкладки TailsData на вкладку TailsData_unlocked.

   В процессе копирования подтвердите действие для всех файлов и нажмите кнопку Совместить (Merge) для копирования подкаталогов. Затем, возможно, понадобится подтвердить действие для всех файлов и нажать кнопку Заменить (Replace).

   Не копируйте папки, предназначение которых вам неизвестно. На всякий случай далее приведено краткое описание папок хранилища:

   - папка apt содержит данные функций APT Packages (APT-пакеты) и APT Lists (APT-списки) хранилища. Обратите внимание, что эта папка не содержит персональных данных;
   - папка bookmarks хранит данные функции Browser bookmarks (Закладки браузера) хранилища;
   - папка cups-configuration хранит данные функции Printers (Принтеры) хранилища;
   - папка dotfiles соответствует функции Dotfiles (Дотфайлы) хранилища;
   - папка electrum хранит данные функции Bitcoin Client (Биткоин-клиент) хранилища;
   - папка gnome-keyring соответствует функции GNOME Keyring хранилища;
   - папка gnupg хранит данные функции GnuPG хранилища;
   - папка icedove хранит данные функции Icedove хранилища;
   - папка nm-connections соответствует функции Network Connections (Сетевые подключения) хранилища;
   - папка openssh-client содержит данные функции SSH Client хранилища;
   - папка Persistent соответствует функции Personal Data (Персональные данные) хранилища;
   - папка pidgin хранит данные функции Pidgin хранилища.

7. После завершения процесса копирования закройте файловый менеджер.
8. В окне терминала выполните следующую команду для восстановления прав ваших персональных файлов:

```
find /live/persistence/TailsData_unlocked/ -uid 1000 -exec chown -R 1000:1000 '{}'
```

Проверка файловой системы зашифрованного хранилища

В редких случаях вам может понадобиться выполнить проверку файловой системы зашифрованного раздела на отсутствие ошибок.

Разблокировка хранилища

1. Запустите систему Tails, установив пароль администратора (см. *разд. «Пароль администратора»* ранее в этой главе) и отключив (!) защищенное хранилище.
2. Выберите команду меню **Приложения | Утилиты | Диски** (Applications | Utilities | Disks), чтобы открыть приложение Диски (Disks).
3. В левой части окна выберите устройство с Tails.
4. В правой части окна щелкните мышью на разделе с шифрованием LUKS (см. рис. 19.27) — раздел должен иметь метку **TailsData.**
5. Нажмите кнопку для разблокировки старого зашифрованного хранилища. Введите пароль в открывшемся окне и нажмите кнопку **Разблокировать** (Unlock).
6. Подтвердите действие вводом пароля администратора.
7. Щелкните мышью на разделе **TailsData** с файловой системой Ext4, появившемся ниже раздела с шифрованием LUKS (см. рис. 19.29).
8. Ниже вы увидите идентификатор устройства вашего защищенного хранилища. Он выглядит как уникальная последовательность символов **/dev/mapper/luks-xxxxxxxx.** Трижды щелкните на этой строке мышью и нажмите сочетание клавиш **<Ctrl**>+<0 для копирования идентификатора в буфер обмена.

Проверка файловой системы

1. Выберите команду меню **Приложения! Системные! Терминал суперпользователя** (Applications | Accessories | Root Terminal) для открытия окна командной строки с привилегиями администратора и подтвердите запрос вводом пароля администратора.
2. В окне терминала выполните следующую команду, заменив в ней слово *устройство* идентификатором вашего устройства, скопированным в предыдущем разделе:

   `fsck -y` *устройство*

   Другими словами, введя команду fsck -y, нажмите сочетание клавиш <Shift>+ +<Ctrl>+<V> для вставки идентификатора устройства из буфера обмена.
3. Нажмите клавишу <Enter> — если в файловой системе ошибок не обнаружено, вы увидите строку с текстом **TailsData: clean** (рис. 19.32).

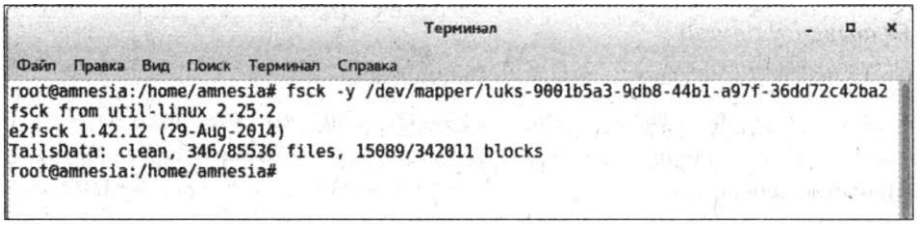


Рис. 19.32. Результат проверки файловой системы

Если ошибки будут обнаружены, утилита `fsck` исправит их автоматически. После этого вы можете повторить описанную команду, чтобы убедиться, что все ошибки исправлены.

Удаление зашифрованного хранилища

Для удаления зашифрованного хранилища на устройстве с системой Tails выполните следующие действия:

1. Запустите систему Tails, установив пароль администратора (см. *разд. «Пароль администратора»* ранее в этой главе) и отключив (!) защищенное хранилище.
2. Выберите команду меню **Приложения | Tails | Delete persistent volume** (Applications | ails I Delete persistent volume), а затем нажмите кнопку **Delete** (Удалить).

Способ подойдет для быстрого удаления всех файлов, сохраненных в зашифрованном хранилище. После этого вы можете создать новое зашифрованное хранилище без необходимости переустановки системы Tails.

Безопасное стирание зашифрованного хранилища

Описанный в предыдущем разделе способ не защищает от попыток злоумышленника восстановить файлы из зашифрованного хранилища. Для безопасного стирания зашифрованного хранилища запустите другую копию системы Tails и выполните следующие шаги:

1. Отформатируйте устройство со стираемым хранилищем и создайте один зашифрованный раздел — так вы удалите и Tails, и зашифрованное хранилище.
2. Затрите свободное пространство на созданном зашифрованном разделе (см. *разд. «Затирание свободного места» главы 21).*
3. Установите Tails на этот носитель.
4. Запустите установленную систему Tails и создайте новое зашифрованное хранилище.

Решение проблем запуска

Если операционная система Tails не запускается должным образом, возможно, причина неработоспособности в вашем случае уже рассматривалась на странице **tinyurl.com/qgxoqyf,** поскольку некоторые проблемы могут быть одинаковы для разных моделей компьютеров.

Вы также можете отправить письмо (на английском языке) на адрес электронной почта **tails-support-private@boum.org** согласно инструкциям на странице **tinyurl.com/hvn4kwm.** В письме следует указать:

1. Как версия системы Tails используется?
2. Выполнена ли проверка ISO-образа на целостность?
3. Марка и модель компьютера.
4. Что происходит при запуске? Укажите сообщение об ошибке, если оно появляется.
5. С какого устройства запускается Tails: DVD, Flash-накопителя с установкой Tails вручную, Flash-накопителя с установкой посредством Tails Installer, SD-карты? Обратите внимание, что если использовался метод установки, не указанный на официальном сайте (в этой книге), служба поддержки вам не поможет.
6. Запускалась ли успешно система Tails на этом компьютере ранее: с другого носителя или другая версия Tails?

7. Запускается ли Tails с этого носителя на других компьютерах?
8. Запускается ли Tails успешно на этом компьютере, если установка выполнена другими методами? К примеру, запускается с DVD и не запускается с Flash-накопителя.
9. Какой метод установки использовался для настройки Tails?

Далее мы рассмотрим случай, если при загрузке Tails отображается меню загрузки, а окно Tails Greeter не появляется.

1. На экране меню загрузки (см. рис. 19.13) нажмите клавишу <TaЬ>.
2. Удалите опцию **quiet** из командной строки загрузки.
3. Добавьте опции **debug** и **nosplash.**
4. Эта процедура позволит отображать системные сообщения при загрузке операционной системы Tails. Вы можете включить их в отчет и сообщить об ошибке одним из способом:
   - с помощью ярлыка **Сообщить об ошибке** (WhisperBack), если есть возможность запустить Tails с другого носителя;
   - отправив письмо на адрес электронной почты **tails-support-private@boum.org.**
5. Если появляется следующее сообщение об ошибке: **/bin/sh: can't acc&s tty; job control turned off следует за (initramfs),** попробуйте удалить опцию **üve-media=removabie.**

Если после удаления вами этой опции злоумышленник установит поддельную версию Tails на внутренний жесткий диск компьютера, вы по ошибке можете начать работу именно в ней вместо подлинной системы, а это чревато утечкой конфиденциальных данных. Если удаление опции **1 ive-medi a=removable** приводит к успешному запуску системы Tails, сообщите об этом разработчикам одним из указанных ранее способов. В этом случае вы должны установить Tails на другой, поддерживающийся Flash-накопитель.

Завершение работы Tails

Существует несколько способов завершения работы операционной системы Tails:

- щелчком мыши по кнопке со значками сетевого подключения, уровня громкости и включения в правом верхнем углу экрана и нажатием кнопки **Выключить немедленно** (Shutdown Immediately) или **Перезагрузить немедленно** (Reboot Immediately) в появившемся меню (см. рис. 19.21);
- нажатием кнопки питания на корпусе компьютера;
- извлечением устройства с Tails из USB-порта или кардридера или открытием привода оптических дисков.

  В редких случаях последний способ может нарушить файловую систему зашифрованного хранилища — *поэтому используйте его в самом крайнем случае!* Предотвратить возникновение этой проблемы позволяет использование зашифрованного хранилища в режиме «только для чтения».

  Если после применения этого способа отключения хранилище перестало функционировать, следует попробовать проверить файловую систему зашифрованного хранилища, как описано в *разд. «Проверка файловой системы зашифрованного хранилища»* ранее.

В процессе выключения все данные, находящиеся в оперативной памяти, для предупреждения атак методом холодной перезагрузки стираются.

Безопасное стирание Tails

Для удаления Tails с Flash-накопителя или SD-карты выполните приведенные далее инструкции.

> ***ЗАТРИТЕ СВОБОДНОЕ МЕСТО***
>
> **Содержимое носителя в процессе его форматирования будет удалено, но злоумышленник может воспользоваться средствами восстановления данных для доступа к удаленной информации из вашего защищенного хранилища Tails. Для предотвращения такой ситуации воспользуйтесь методом затирания свободного места, описанным в *главе 21*.**

Linux

Эта инструкция предназначена для версий Linux со средой GNOME: Ubuntu, Debian, Tails и др.

Использование дисковой утилиты

Будьте внимательны, т. к. вы можете стереть данные с внутреннего жесткого диска компьютера. Если вы не уверены, что выбрали правильный носитель для стирания, прекратите операцию.

1. Отключите от компьютера Flash-накопитель или SD-карту, данные с которых нужно стереть.
2. Запустив операционную систему, установленную на компьютере, запустите приложение Диски (Disks).

   В левой части окна приложения вы увидите список всех носителей данных, подключенных к компьютеру.
3. Подключите к компьютеру Flash-накопитель или SD-карту, данные с которых нужно стереть — новое устройство появится в списке. Щелкните по нему мышью.
4. Убедитесь, что данные устройства, отображаемые в правой части окна, соответствуют устройству с Tails: модель, размер и т. п.
5. Чтобы стереть данные с выбранного устройства, нажмите кнопку и выберите команду **Форматировать** (Format), как показано на рис. 19.33.
6. В открывшемся окне **Форматировать диск** (Format Disk) выполните следующие действия (рис. 19.34):
   - чтобы надежно стереть все данные, выберите пункт **Перезаписывать существующие данные нулями (медленно)** (Overwrite existing data with zeroes) в раскрывающемся списке **Очистить** (Erase);
   - выберите пункт **Совместимо со всеми системами и устройствами (MBR/DOS)** (Compatible with all systems and devices (MBR/DOS)) в раскрывающемся списке **Разметка** (Partitioning).
7. Нажмите кнопку **Форматировать** (Format), а затем нажмите одноименную кнопку в окне подтверждения.
8. После завершения процесса форматирования нажмите кнопку в окне программы Диски (Disks).

Система Tails будет удалена.

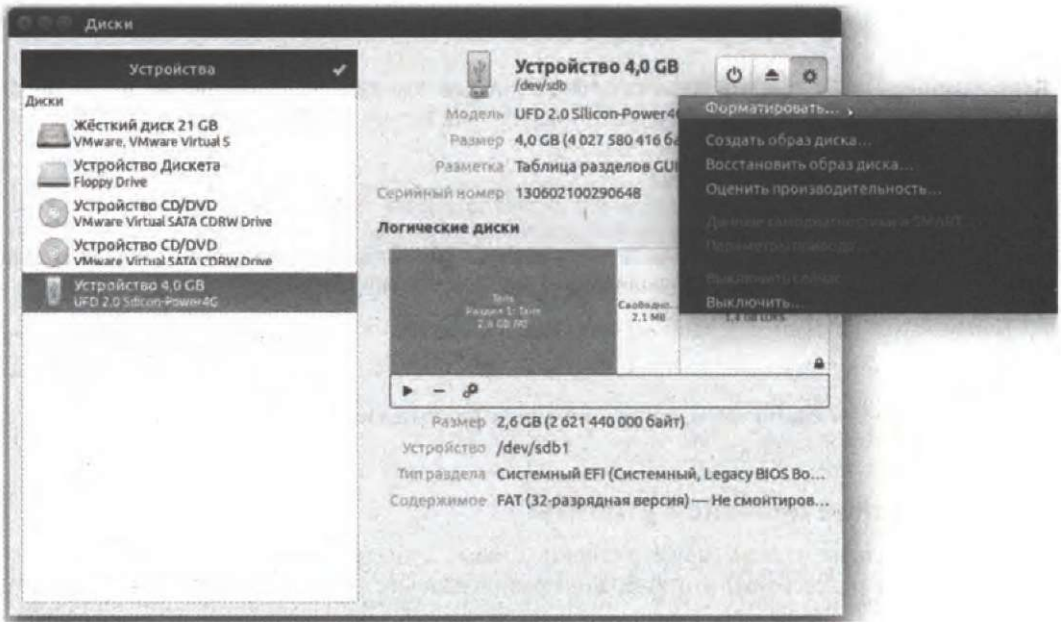


Рис. 19.33. Выбор команды форматирования устройства в окне программы Диски

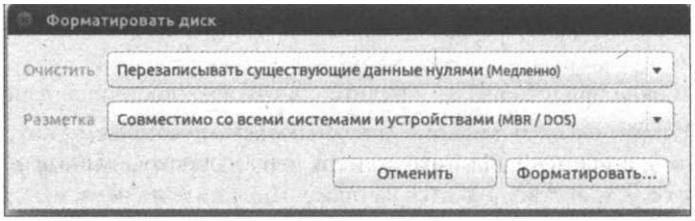


Рис. 19.34. Вид окна Форматировать диск

Сброс носителя с Tails

Если Tails — единственная используемая вами система Linux, вы можете стереть Flash-накопитель или SD-карту прямо из-под запущенной операционной системы Tails.

1. При запуске Tails добавьте опцию `toram` в меню загрузки (см. *разд. «Меню загрузки»* ранее в этой главе).
2. Если система Tails запустится успешно, следуйте инструкциям по форматированию накопителя в программе Диски (Disks), как описано в предыдущем разделе.

Если запуск системы не удастся, это означает, что на компьютере установлен недостаточный объем оперативной памяти для выполнения такой операции. В этом случае необходимо найти другой компьютер или другой носитель с Tails, чтобы отформатировать текущий.

Windows: использование утилиты Diskpart

Эта инструкция применима в любых версиях Windows, кроме Windows XP (версия утилиты Diskpart в операционной системе Windows XP не поддерживает портативные носители). Для

получения справочной информации об утилите Diskpart обратитесь к странице по адресу **tinyurl.com/zsaa856.**

Будьте внимательны, т. к. вы можете стереть данные с внутреннего жесткого диска компьютера. Если вы не уверены, что выбрали правильный номер носителя для стирания, прекратите операцию.

1. Отключите от компьютера Flash-накопитель или SD-карту, данные с которых нужно стереть.
2. Откройте окно командной строки любым способом — например, нажав сочетание клавиш <Win>+<R>, указав значение cmd в поле ввода и нажав клавишу <Enter>.
3. В окне командной строки введите команду `diskpart`, чтобы запустить утилиту Diskpart.
4. Выполните команду `list disk` для отображения всех носителей данных, подключенных к компьютеру. Например:

```
DISKPART> list disk
    Диск ###  Состояние      Размер   Свободно Дин  GPT

    Диск 0    В сети           60    Gбайт    0 байт
```

5. Подключите к компьютеру Flash-накопитель или SD-карту, данные с которых нужно стереть. Выполните команду `list disk` повторно — новый диск, соответствующий подключенному устройству, появится в списке. Например:

```
DISKPART> list disk
    Диск ###  Состояние      Размер   Свободно Дин  GPT

    Диск 0    В сети           60    Gбайт    0 байт
    Диск 1    В сети         3841 Мбайт   3008 Кбайт       *
```

   Убедитесь, что размер появившегося диска соответствует объему накопителя, который вы собираетесь стереть. Запомните номер диска, присвоенный программой Diskpart устройству с Tails.

6. Выберите устройство с Tails, выполнив команду `select disk=`*`номер`*. Замените в этой команде слово *номер* номером диска (устройства), который вы собираетесь стереть. Например:

```
DISKPART> select disk=1
Выбран диск 1.
```

7. Выполните команду `clean`, чтобы удалить с накопителя таблицу разделов.
8. Выполните команду `convert mbr`, чтобы создать на накопителе новую таблицу разделов.
9. Выполните команду `create partition primary`, чтобы создать на накопителе новый первичный раздел.

Система Tails будет удалена.

OS X: использование приложения Дисковая утилита

Эты инструкция предназначена для операционной системы OS X (пример приведен для версии El Capitan).

Будьте внимательны, т. к. вы можете стереть данные с внутреннего жесткого диска компьютера. Если вы не уверены, что выбрали правильный носитель для стирания, прекратите операцию.

1. Отключите от компьютера Flash-накопитель или SD-карту, данные с которых нужно стереть.
2. Запустите приложение Дисковая утилита (Disk Utility).
3. В левой части окна утилиты вы увидите список всех носителей данных, подключенных к компьютеру.
4. Подключите к компьютеру Flash-накопитель или SD-карту, данные с которых нужно стереть, — новое устройство появится в списке. Щелкните по нему мышью.
5. Убедитесь, что данные устройства, отображаемые в правой части окна, соответствуют устройству с Tails: модель, размер и т. п.
6. Чтобы стереть содержимое устройства, нажмите кнопку Стереть (Erase) в верхней части окна.
7. Нажмите кнопку Стереть (Erase) для подтверждения (рис. 19.35).

Система Tails будет удалена.



Рис. 19.35. Вид окна программы Дисковая утилита

ГЛАВА 20

Анонимное подключение к Интернету

Подключение к сети

Управление Tor с помощью Vidalia

Безопасный веб-серфинг в Tor Browser

Анонимное общение в мессенджере Pidgin

Защищенная электронная почта Icedove (Thunderbird)

Обмен биткоинов в Electrum

Использование сети I2P

Причины низкой скорости передачи данных в Tor

В этой главе описаны способы работы в операционной системе Tails с сетевыми ресурсами, причем, помимо сети Tor рассматривается возможность подключения к сети I2P. Вы также научитесь общаться в чатах Pidgin и управлять электронной почтой в клиенте Icedove (Thunderbird).

Подключение к сети

Общие положения

Подключиться к сети вы можете с помощью проводного или Wi-Fi-соединения, а также через сотовые сети передачи данных:

- если обнаружено проводное соединение, система Tails подключится к нему автоматически;
- для подключения к сети Wi-Fi:
  - откройте системное меню, щелкнув на кнопке в правом верхнем углу экрана (рис. 20.1);
  - выберите пункт **Wi-Fi,** а затем нужную беспроводную сеть. Введите пароль для доступа к сети при необходимости;
- для подключения к сотовой сети передачи данных:
  - откройте системное меню, щелкнув на кнопке в правом верхнем углу экрана;
  - выберите пункт **Мобильные** (Mobile Broadband).



Рис. 20.1. Системное меню в операционной системе Tails

Для подключения к сети Tor через мост или настройки прокси для доступа к Интернету, вам нужно настроить конфигурацию Tor при запуске Tails (см. *разд. «Настройка сети» главы 19).*

После успешной установки сетевого подключения:

- вы получите доступ к Интернету, при этом связь с сетью Tor будет установлена автоматически, а приложение Vidalia запущено;
- если для подтверждения доступа к Интернету требуется регистрация, см. далее *разд. «Регистрация на порталах перехвата».*

Для изменения сетевых настроек — к примеру, отключения режима автоматического подключения к сетям Wi-Fi, выполните следующие действия:

1. Откройте системное меню, щелкнув на кнопке в правом верхнем углу экрана (см. рис. 20.1).
2. Нажмите кнопку (#) для открытия окна системных настроек.
3. Щелкните мышью на пункте Сеть (Network).

Если вы планируете многократно использовать собственные настройки сети или хотите сохранить пароли к защищенным беспроводным сетям для использования в будущих сеансах, то можете активировать функцию Network connections (Сетевые подключения) защищенного хранилища (см. *разд. «Настройки хранилища» главы 19).*

Если вы беспокоитесь о том, чтобы вас в сети не идентифицировали как пользователя Tails, обратитесь к *разд. «Сокрытие факта использования Tails» главы 18.*

Регистрация на порталах перехвата

Многие общедоступные (обычно через беспроводные сети передачи данных) интернет-соединения требуют от своих пользователей для получения доступа к Интернету регистрации и авторизации. Такие сети организуются в общественном транспорте, интернет-кафе, библиотеках, аэропортах, гостиницах, университетах и т. п. При попытке войти в подобную сеть так называемый *портал перехвата* перехватывает пользовательский запрос веб-страницы и перенаправляет браузер на страницу авторизации. Но когда используется сеть Tor, эта система не работает, поскольку ей требуется браузер с неограниченным сетевым доступом. На такой случай в операционной системе Tails предусмотрена программа Небезопасный браузер (Unsafe Browser), которая может быть запущена из меню Приложения | Интернет (Applications | Internet) (рис. 20.2).



Рис. 20.2. Небезопасный браузер в операционной системе Tails

Интерфейс программы Небезопасный браузер (Unsafe Browser) окрашен в красный цвет, чтобы отличить его от Tor Browser и предупредить о небезопасности его использования.

Небезопасный браузер не обеспечивает анонимности при работе в сети! Используйте его только для авторизации на порталах перехвата или просмотра ресурсов в локальной сети. К файлам, загруженным с помощью программы Небезопасный браузер (Unsafe Browser), невозможно получить доступ за пределами самого небезопасного браузера.

В целях безопасности не запускайте одновременно программы Небезопасный браузер (Unsafe Browser) и Tor Browser. Очень легко ошибиться, перепутав браузеры (значки их идентичны), что может привести к катастрофическим последствиям.

Управление Tor с помощью Vidalia

Приложение Vidalia при установке соединения с Интернетом запускается автоматически и позволяет осуществлять некоторый контроль над подключением к сети Tor. Об успешном запуске Vidalia сообщит значок в виде зеленой луковицы ^ на верхней навигационной панели. Этот значок может менять свой вид в зависимости от состояния подключения к Tor:

- значок в виде зеленой луковицы означает успешное подключение к сети Tor;
- желтый цвет значка свидетельствует, что подключение к сети Tor осуществляется, но еще не установлено.

  В некоторых случаях желтый цвет значка остается, даже если подключение к сети Tor уже установлено. Об этом свидетельствуют появление уведомления Tor готов или успешное открытие веб-страниц в программе Tor Browser.

  Операционная система Tails имеет некоторые средства защиты, которые будут препятствовать подключениям к Интернету, минующим сеть Tor;

- перечеркнутый значок луковицы означает, что подключение к сети Tor прервано. В этом случае все соединения с Интернетом по умолчанию блокируются.

Для доступа к дополнительным возможностям приложения Vidalia щелкните правой кнопкой мыши на значке луковицы на верхней навигационной панели.

Карта сети

Функция **Карта сети** (Network Map) отображает информацию о доступных узлах (ретрансляторах) Tor и текущих цепочке и подключении (рис. 20.3):

- на панели в левой части окна **Карта сети Tor** (Network Map) отображается список всех открытых ретрансляторов Tor;
- на панели в нижней части окна указан список из цепочек соединений, установленных в сети Tor. При подключениит к серверу назначения его адрес отобразится вложенным в соответствующую цепочку Tor.

  В приведенном на рис. 20.3 примере подключение к серверу **tails.boum.org** выполняется через цепочку ретрансляторов **redjohn, HostplanetME2** и выходной узел **cavefelem2;**
- на панели в верхней части окна отображается приблизительная карта расположения каждого ретранслятора из цепочки.

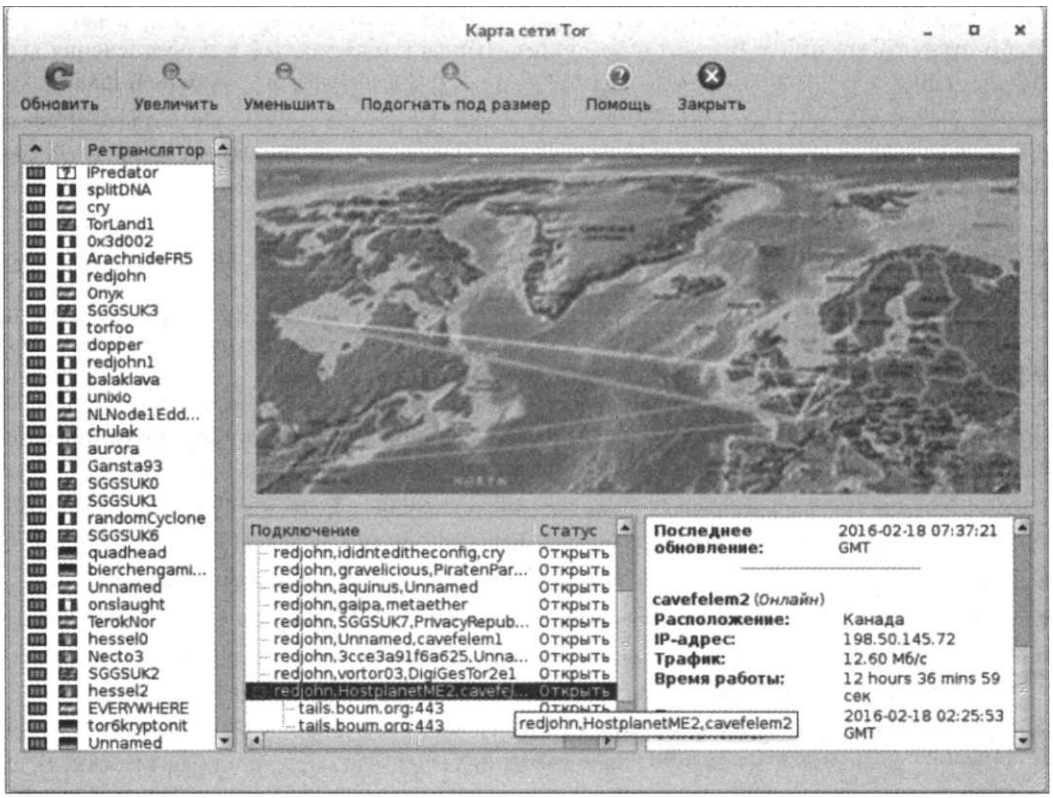


Рис. 20.3. Карта сети Tor в окне программы Vidalia

В приведенном на рис. 20.3 примере ретрансляторы **redjohn** и **HostplanetME2** находятся во Франции, **a cavefelem2** — в Канаде;

- если щелкнуть мышью на цепочке, в правой части окна отобразятся технические характеристики каждого ретранслятора, используемого в ней.

Смена личности в Vidalia

Функция **Новая личность** (New Identity) в программе Vidalia составляет новую цепочку ретрансляторов Tor, но только для новых подключений (к новым серверам).

Эта функция не обеспечивает полного удаления следов для прекращения отождествления пользователей друг с другом до и после смены личности:

- существующие подключения остаются открыты;
- другие источники информации могут выявить ваши прошлые действия — например, cookie-файлы, хранящиеся в Tor Browser, или сгенерированный логин в Pidgin.

Для максимальной конспирации рекомендуется перезагрузить Tails.

Чтобы настроить мосты, брандмауэр или прокси, следует выбрать соответствующую настройку в окне Tails Greeter (см. *разд. «Настройка сети» главы 19).*

Безопасный веб-серфинг в Tor Browser

Tor Browser — это веб-браузер Mozilla Firefox, сконфигурированный для обеспечения анонимной работы в Интернете. Учитывая популярность Firefox, вы могли использовать этот браузер ранее, поэтому пользовательский интерфейс Tor Browser может быть вам знаком.

Чтобы научиться просматривать в браузере локальные ресурсы, обратитесь к *разд. «Ресурсы в локальной сети» главы 23.*

Упреждающая защита с помощью AppArmor

В Tor Browser в операционной системе Tails внедрен инструмент AppArmor для защиты системы и ваших данных от некоторых типов атак, направленных против Tor Browser. Он представляет собой программный инструмент упреждающей защиты, основанный на политиках безопасности, которые определяют, к каким системным ресурсам и с какими привилегиями может получить доступ то или иное приложение. Как следствие, Tor Browser может считывать и записывать данные в ограниченном числе папок.

Именно поэтому вы можете столкнуться с ошибкой запрета доступа, например, если попытаетесь загрузить файлы в домашнюю папку.

- Вы можете сохранять файлы из Tor Browser в одноименную папку, расположенную в домашнем каталоге. Содержимое этой папки удаляется при завершении работы Tails.
- Если вам необходимо опубликовать файлы во Всемирной паутине с помощью Tor Browser, сначала скопируйте их в эту папку.
- Если вы установите флажок **Personal Data** (Персональные данные) в настройках защищенного хранилища, вы сможете использовать также папку Persistent/Tor Browser. В таком случае содержимое этой папки будет сохраняться и оставаться доступным во всех сеансах работы (при условии активации хранилища при запуске Tails).

Чтобы иметь возможность скачивать файлы размером более объема доступной оперативной памяти, необходимо активировать функцию Personal Data (Персональные данные) в настройках защищенного хранилища.

Шифрование передачи данных с помощью HTTPS

Использование протокола HTTPS вместо HTTP помогает шифровать коммуникации в Интернете. При этом все данные, передаваемые между браузером и сервером (сайтом), который вы посещаете, передаются в зашифрованном виде. Таким образом, от перехвата защищаются данные, передаваемые с выходных узлов в сети Tor (см. ***разд. «Перехват трафика с выходных узлов Tor» главы 18).***

К примеру, вот как выглядит браузер, когда вы собираетесь авторизоваться с учетной записью электронной почты на сайте Mail.ru, используя веб-интерфейс (рис. 20.4).

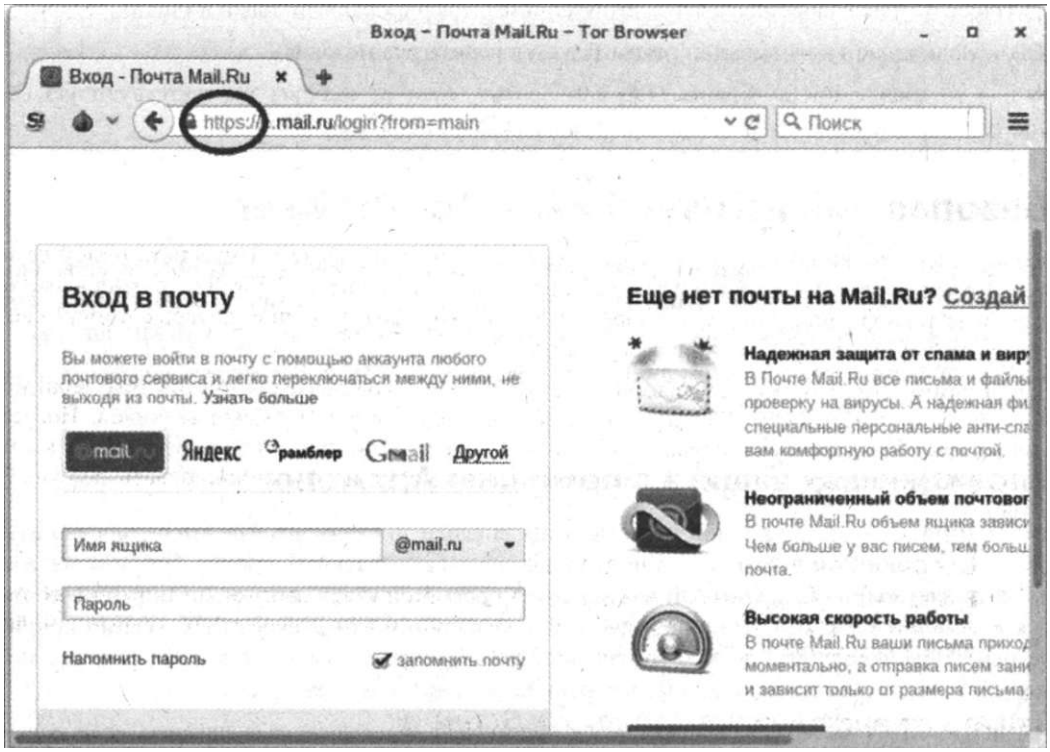


Рис. 20.4. Страница авторизации на сайте Mail.ru

Обратите внимание на значок в левой части адресной строки и адрес, начинающийся с https:// (вместо http:///). Это информирует о том, что для связи с сервером Mail.ru используется шифрованное соединение по протоколу HTTPS.

При отправке/передаче конфиденциальной информации (например, паролей), следует использовать только те серверы, которые поддерживают передачу данных по протоколу HTTPS. В противном случае, передаваемые данные очень легко может перехватить злоумышленник или изменить контент страницы, отображаемой в вашем браузере.

Протокол HTTPS также включает механизмы для проверки подлинности посещаемого сервера (но они не лишены недостатков — см. *разд. «Атаки посредника» главы 18).*

Дополнение HTTPS Everywhere

Как уже говорилось в *главе 1,* HTTPS Everywhere — это дополнение для браузеров, обеспечивающее использование протокола HTTPS на сайтах, которые его поддерживают (но по умолчанию не используют).

Многие сайты во Всемирной паутине также поддерживают зашифрованное подключение по протоколу HTTPS лишь ограниченно. Например, на них по умолчанию может использоваться протокол HTTP или зашифрованные страницы могут ссылаться на незашифрованные.

В операционной системе Tails HTTPS Everywhere установлено как Firefox-дополнение для программы Tor Browser и шифрует соединения с большинством сайтов, решая указанные проблемы путем изменения всех запросов на такие сайты с использованием протокола HTTPS.

Чтобы больше узнать о дополнении HTTPS Everywhere, вы можете:

- посетить веб-сайт **tinyurl**.com/38sqvb9;
- обратиться к *разд. «Использование протокола HTTPS» главы 1.*

Torbutton

Для обеспечения анонимности и конфиденциальности при работе в Интернете одной сети Tor недостаточно. Все современные веб-браузеры, в том числе и Firefox, поддерживают уязвимые технологии JavaScript, Adobe Flash, cookie-файлы и прочие, которые смогут свести на нет анонимность, обеспечиваемую сетью Tor.

В программе Tor Browser все подобные технологии обрабатываются внутри браузера дополнением под названием Torbutton, предотвращающим атаки злоумышленников. Но эта защита имеет свою цену — ограничение использования указанных технологий ведет к отключению некоторых функций, а некоторые сайты могут не функционировать должным образом.

> ***ЦЕПОЧКИ TOR В TAILS***
>
> **В операционной системе Tails возможность просмотра узлов цепочки Tor Browser (как это показано на рис. 17.7) отключена, т. к. нет уверенности в ее безопасности. Цепочки Tor вы можете просмотреть в окне программы Vidalia.**

Защита от вредоносного кода JavaScript

Если JavaScript отключить по умолчанию, многие безопасные и, возможно, полезные сценарии JavaScript работать перестанут, что приведет к ошибкам отображения многих веб-сайтов. Поэтому в Tor Browser поддержка сценариев JavaScript по умолчанию включена, но на Torbutton возлагаются надежды по отключению потенциально опасного кода JavaScript.

Это необходимый компромисс между безопасностью и удобством использования, и на сегодняшний день неизвестны какие-либо JavaScript-сценарии, способные поставить под угрозу анонимность работы в Tails[1].

[1] **См. tinyurl.com/zf8n5d3.**

Чтобы разобраться в поведении Tor Browser, в частности, в отношении JavaScript и cookie-файлов, вы можете обратиться к спецификации программы Tor Browser, доступной по адресу **tinyurl.com/bq7mx4a.**

Изменение уровня безопасности

Вы можете использовать ползунковый регулятор **Уровень безопасности** (Security level), предоставляемый дополнением Torbutton и в зависимости от его положения ограничивающий функции браузера с целью поиска компромисса между безопасностью и удобством использования (юзабилити). Например, установив высокий уровень безопасности, вы полностью заблокируете исполнение JavaScript-сценариев и многие другие функции, влияющие на безопасность.

Ползунковый регулятор **Уровень безопасности** (Security level) по умолчанию установлен в положение **Низкий** (Low) — это положение обеспечивает уровень защиты по умолчанию и наиболее удобный веб-серфинг.

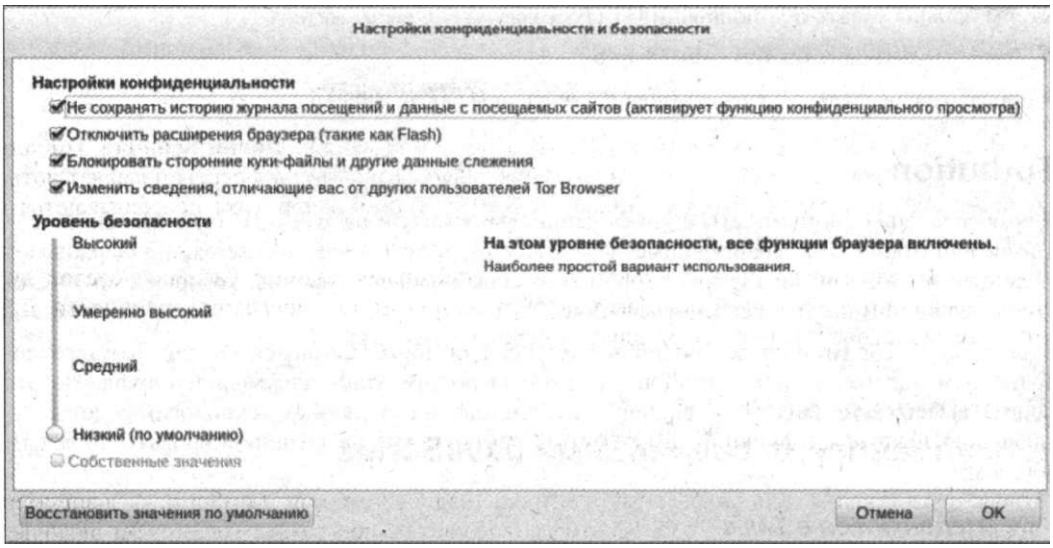


Рис. 20.5. Окно Настройки конфиденциальности и безопасности

Для изменения положения ползункового регулятора **Уровень безопасности** (Security level) в окне программы Tor Browser нажмите кнопку и выберите пункт **Настройки конфиденциальности и безопасности** (Privacy and Security Settings) (рис. 20.5).

Смена личности в Tor

Функция **Новая личность** (New Identity) в программе Tor Browser выполняет следующее:

- закрывает все открытые вкладки;
- удаляет данные сеанса работы, включая кэш, историю посещений и cookie-файлы;
- прерывает текущее соединение и составляет новую цепочку Tor;
- стирает содержимое буфера обмена.

НОВАЯ ЛИЧНОСТЬ В VIDALIA

Аналогичная функция в Vidalia лишь прерывает текущее соединение и составляет новую цепочку Tor.

Чтобы использовать эту функцию, в окне программы Tor Browser нажмите кнопку и выберите пункт Новая личность (New Identity) (рис. 20.6).

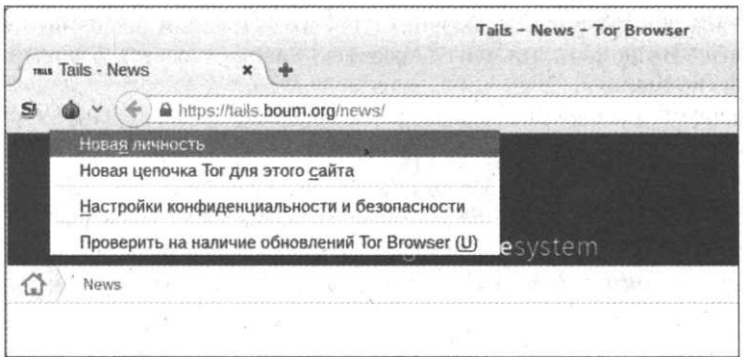


Рис. 20.6. Выбор пункта Новая личность

Не путайте команду Новая личность (New Identity) с командой Новая цепочка Tor для этого сайта (New Tor Circuit for this Site). Последняя команда только перенаправляет поток данных через цепочку других случайных узлов Tor. Вкладки при этом не закрываются и данные сеанса не удаляются.

Функция Новая личность (New Identity) не обеспечивает полного удаления следов для прекращения отождествления пользователей друг с другом до и после смены личности. Для максимальной конспирации рекомендуется перезагрузить Tails.

Дополнение NoScript для управления сценариями JavaScript

Чтобы предоставить дополнительный контроль над сценариями JavaScript — например, чтобы полностью отключить их на некоторых веб-сайтах, программа Tor Browser включает в себя дополнение NoScript.

По умолчанию NoScript отключен, и потенциально безопасные сценарии JavaScript допускаются к выполнению дополнением Torbutton, как описано ранее в *разд. «Защита от вредоносного кода JavaScript* этой главы.

Дополнительную информацию на этот счет вы можете найти на сайте по адресу tinyurl.com/hdevbxv.

Анонимное общение в мессенджере Pidgin

Для бесед в чатах и обмена мгновенными сообщениями, в операционную систему Tails включен мессенджер Pidgin. Чтобы запустить его, выберите команду меню **Приложения | Интернет | Клиент обмена мгновенными сообщениями Pidgin** (Applications | Internet | Pidgin Instant Messenger).

Описание приемов работы в программе Pidgin вы найдете в *разд. «Pidgin» главы 7.*

Предустановленные учетные записи

По умолчанию в программе Pidgin настроены две учетные записи:

- `irc.oftc.net` — подключает к IRC-серверу OFTC (сообщества открытых и свободных технологий) и к чатам `#tails`.
- `127.0.0.1` — подключает к IRC-серверу I2P.

При запуске Tails эти аккаунты неактивны. Для их активации выполните команду меню **Учетные записи | Включить аккаунт** (Accounts | Enable Account), а затем выберите нужные аккаунты из подменю.

Протокол шифрования OTR

Как уже обсуждалось в *главе* 7, протокол Off-the-Record позволяет вести конфиденциальные беседы через системы обмена мгновенными сообщениями, обеспечивая:

- **шифрование** — никто, кроме вас и вашего собеседника, не может читать ваши сообщения;
- **аутентификацию** — вы удостоверяетесь, что ваш собеседник является именно тем человеком, за которого себя выдает;
- **отрицание** — отсылаемые сообщения не имеют цифровых подписей, связывающих их с вами, и *после* разговора подделать ваши сообщения может кто угодно. Тем не менее, во время беседы вы и ваш собеседник убеждены, что видите подлинные сообщения;
- **обратную безопасность** — ранее проведенные беседы не могут быть скомпрометированы, даже если утеряны открытые ключи.

По умолчанию протокол OTR отключен, поэтому ваши коммуникации без его использования не приватны.

Надо также учитывать, что *OTR шифрует только сообщения* — передаваемые файлы с помощью OTR не шифруются. Кроме того, в процессе приватной беседы в IRC *сообщения, отправленные с опцией /me, не шифруются,* и получатель об этом уведомляется.

Чтобы ключи и настройки Pidgin сохранялись для использования в будущих сеансах работы, вы должны активировать функцию **Pidgin** в настройках защищенного хранилища.

Блокировка Tor IRC-серверами

Некоторые IRC-серверы блокируют соединения, исходящие из сети Tor, поскольку Tor может использоваться злоумышленниками для рассылки спама. Список ресурсов, блокирующих соединения из сети Tor, публикуется на сайте tinyurl.com/cdqpo8s.

Генерация имени пользователя

Каждый раз при запуске Tails для всех учетных записей Pidgin генерируется случайное имя пользователя, что обеспечивает уникальность вашего имени в каждом сеансе и сокрытие факта использования вами системы Tails. Генерируемые имена основаны на списке распространенных англоязычных имен (используется алгоритм Кристофера Фунта, tinyurl.com/7kyeelh).

Если вы хотите использовать одно и то же имя пользователя во всех сеансах работы, то должны активировать функцию **Pidgin** в настройках защищенного хранилища.

Поддержка других протоколов

Для обеспечения безопасности в программе Pidgin в операционной системе Tails поддерживаются только протоколы IRC и XMPP.

Защищенная электронная почта Icedove (Thunderbird)

Чтение и отправка электронной почты в операционной системе Tails осуществляется с помощью программы Icedove. Исходя из маркетинговых соображений, псевдоним Icedove присвоен в системе Tails программе Mozilla Thunderbird, но это одна и та же программа.

Для запуска Icedove выберите команду меню **Приложения | Интернет | Icedove** (Applications I Internet | Icedove).

Если вы хотите сохранять сообщения электронной почты и настройки Icedove для использования в будущих сеансах работы, то должны активировать функцию **Icedove** в настройках защищенного хранилища.

Описание приемов работы в программе Mozilla Thunderbird вы найдете в ***разд. «Практическое руководство по PGP-шифрованию» главы 6.***

Настройка учетной записи

1. При первом запуске программы Icedove вы увидите окно мастера настройки конфигурации вашей учетной записи электронной почты.

   Если в будущем вам вновь понадобится открыть окно мастера настройки, в окне программы Icedove нажмите кнопку и выберите команду меню **Настройки | Параметры учетной записи** (Preferences | Account Settings). Затем, в открывшемся одноименном диалоговом окне в раскрывающемся списке **Действия для учетной записи** (Account Actions) выберите пункт **Добавить учетную запись почты** (Add Mail Account).

2. Введите свое имя, адрес электронной почты и пароль к почтовому ящику в соответствующие поля (рис. 20.7).

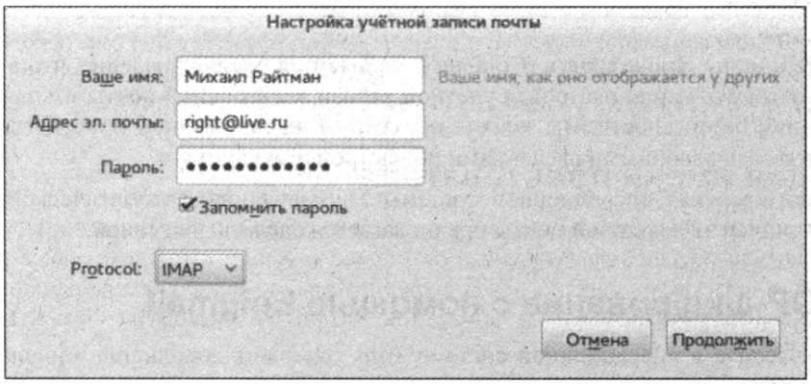


Рис. 20.7. Настройка учетной записи **в** программе Icedove

3. Укажите протокол, используемый для подключения к вашему провайдеру электронной почты. Программа Icedove позволяет подключаться к провайдеру электронной почты как по протоколу IMAP, так и по протоколу POP (сравнение протоколов POP и IMAP приведено в табл. 20.1):
   - при использовании протокола IMAP программа Icedove постоянно синхронизируется с сервером и отображает сообщения электронной почты и папки с ними, которые хранятся на сервере. Протокол IMAP рекомендуется, если вы осуществляете доступ к электронной почте из разных операционных систем;
   - при использовании протокола POP программа Icedove скачивает письма, которые поступают в почтовый ящик на сервере и, опционально, удаляет их с сервера. Протокол POP рекомендуется, если вы осуществляете доступ к электронной почте только из операционной системы Tails и храните их в защищенном хранилище.

Таблица 20.1. *Основные различия протоколов POP и IMAP*

	POP	1MAP
Хранение	Ваш компьютер — если используется протокол POP, обычно все сообщения скачиваются на компьютер пользователя и при соответствующей настройке удаляются с сервера	Сервер — если используется протокол IMAP, все сообщения остаются на сервере. Проще говоря, протокол IMAP превращает клиент электронной почты в браузер данных, хранящихся на почтовом сервере
Мобильность	Низкая — при использовании протокола POP нужно вручную (или через определенные промежутки времени с помощью программы) проверять наличие новых сообщений	Высокая — протокол IMAP позволяет постоянно синхронизировать данные о наличии новых сообщений
Скорость	Высокая — новые сообщения скачиваются сразу все	Низкая — т. к. почтовый клиент обращается к серверу периодически
Квота	Неограниченная — если настроен режим удаления скачанных писем с сервера, вам не нужно беспокоиться о наличии свободного места в хранилище на сервере	Ограниченная — как правило, пользователям выделяется ограниченное место в хранилище на сервере
Безопасность	Высокая — ваши сообщения не хранятся на сервере (при соответствующей настройке)	Низкая — вы доверяете провайдеру электронной почты хранение сообщений

4. Нажмите кнопку Продолжить (Continue) — появится предупреждение, что в программе Icedove автоматическая настройка учетной записи электронной почты отключена по соображениям безопасности. Вы можете обратиться на сайт вашего провайдера электронной почты за справочными сведениями по настройке аккаунта.

   В будущих версиях операционной системы Tails функцию автоматической настройки учетной записи электронной почты предполагается сделать доступной.

OpenPGP-шифрование с помощью Enigmail

Программа Icedove в операционной системе Tails содержит дополнение Enigmail, предназначенное для шифрования и аутентификации электронных писем с помощью OpenPGP. Настроить Enigmail для используемой учетной записи электронной почты вы можете, за-

пустив мастер установки Enigmail, нажав кнопку **a** и выбрав команду меню **Enigmail | Мастер установки** (Enigmail | Setup Wizard). В процессе настройки можно будет создать ключ OpenPGP, связанный с вашим адресом электронной почты.

Описание приемов работы с дополнением Enigmail в программе Mozilla Thunderbird вы найдете в *разд. «Практическое руководство по PGP-шифрованию» главы 6.*

Обеспечение дополнительной защиты с помощью TorBirdy

Программа Icedove в операционной системе Tails содержит также дополнение TorBirdy, обеспечивающее дополнительный уровень конфиденциальности и анонимности и предназначенное для работы Icedove через сеть Tor.

Обратите внимание, что это дополнение блокирует передачу сообщений электронной почты в формате HTML. Соответственно, письма, полученные в формате HTML, отображаются в виде обычного текста, что может усложнить их читабельность.

Обмен биткоинов в Electrum

Биткоин-клиент Electrum прекрасно вписывается в контекст операционной системы Tails, т. к.:

- вы можете использовать свой кошелек с различных устройств и избежать потери биткоинов в случае ошибки резервной копии или сбоя компьютера;
- клиент Electrum не скачивает всю цепочку блоков, поэтому отсутствует задержка при запуске;
- вы можете подписывать транзакции в автономном режиме для обеспечения дополнительной безопасности.

Чтобы запустить программу Electrum, выберите команду меню **Приложения | Интернет | Electrum Bitcoin Wallet** (Applications | Internet | Electrum Bitcoin Wallet). Руководство по работе с программой вы найдете по адресу **tinyurl.com/j73tbsk.**

Использование сети I2P

I2P — это альтернативная Tor анонимная сеть, позволяющая в безопасном режиме совершать наиболее распространенные в Интернете действия — такие как просмотр веб-страниц, чтение/отправку электронной почты, обмен файлами и т. п. В отличие от сети Tor, которая сфокусирована на получении доступа к обычным сайтам Всемирной паутины, I2P более ориентирована на скрытые Даркнет-ресурсы. Любой пользователь в сети I2P может запустить анонимный сервер, создав так называемый *I2P-сайт* (eepsite), который доступен только в пределах сети **I2P** и характеризуется доменом верхнего уровня **.i2p** (по аналогии с **.onion** для скрытых ресурсов в сети Tor). Например, главная страница проекта I2P также доступна в сети **I2P** по адресу **http://i2p-projekt.i2p.**

I2P и TOR

I2P и Tor — это разные сети, поэтому нельзя получить доступ из одной в другую.

Сеть I2P не подключается по умолчанию при запуске операционной системы Tails. Чтобы получить доступ к сети I2P, следует добавить опцию i2p в меню загрузки (для получения подробных инструкций обратитесь к *разд. «Меню загрузки» главы 19).*

После добавления опции в меню загрузки Tails опции `i2p` подключение к сети I2P будет выполнено автоматически при появлении рабочего стола Tails и выполнении синхронизации времени.

Консоль маршрутизатора I2P можно запустить с помощью команды **Приложения | Интернет | Браузер L2P** (Applications | Internet | I2P Browser). Эта консоль отображает текущее состояние подключения к сети I2P, популярные I2P-сайты (форумы, сервисы электронной почты, файлообменные хостинги и т. д.) и предоставляет возможность перезапуска и отключения сети I2P (рис. 20.8).

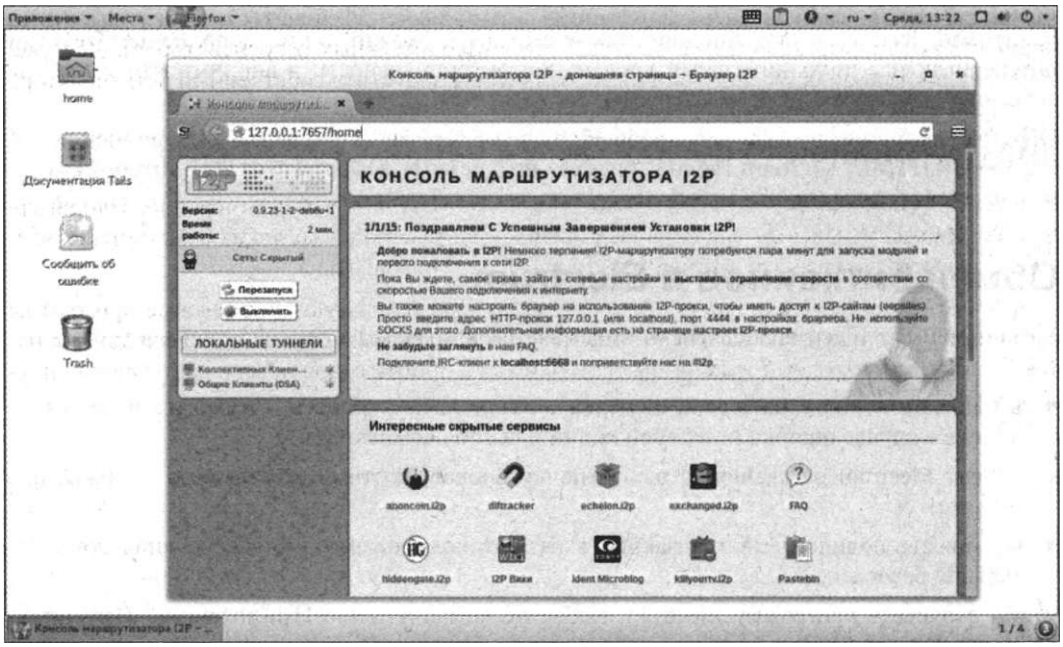


Рис. 20.8. Консоль маршрутизатора I2P в операционной системе Tails

Адреса в доменной зоне **.i2p** могут быть открыты только в программе Браузер I2P (I2P Browser). Обычные веб-сайты в этом браузере не открываются.

Более подробно сеть I2P рассматривается в *главе 15.*

Причины низкой скорости передачи данных в Tor

Вы часто будете сталкиваться с тем, что сеть Tor работает медленно. Здесь описаны некоторые причины, по которым снижается производительность этой сети.

Сложные схемы передачи данных

Сеть Tor обеспечивает анонимность благодаря построению цепочки из трех узлов (ретрансляторов). Таким образом, вместо непосредственного подключения к нужному серверу назначения, соединение устанавливается между каждым узлом цепочки, а это занимает больше времени.

Кроме того, Tor выстраивает цепочки с ретрансляторами в разных странах (к примеру, соединение компьютера пользователя и сервера из Москвы может проходить через Индию, Китай и США), из-за чего расстояние увеличивается, а скорость передачи данных снижается.

Качество ретрансляторов

Ретрансляторы в сети Tor запускаются добровольцами на децентрализованной основе, поэтому все они имеют различные характеристики производительности и скорости передачи данных. В целом, скорость передачи данных в сети может увеличиться, если повысить ее мощность (увеличить количество быстрых и производительных ретрансляторов). Для увеличения пропускной способности сети Tor вы можете запустить собственный ретранслятор.

Злоупотребление сетью Tor

Некоторые пользователи злоупотребляют сетью Tor, случайно или намеренно. Например, сеть Tor иногда используется для проведения DDoS-атак. Во время таких атак ретрансляторы Tor испытывают перегрузки, зачастую большие, чем цели атаки.

Некоторые пользователи, подключаясь через сеть Tor, используют пиринговые программы (к примеру, скачивают торренты), что также негативно сказывается на ее производительности. Если вам необходимо использовать пиринговое программное обеспечение, рекомендуется обратиться для этой цели к сети I2P.

ГЛАВА 21

Шифрование и конфиденциальность

Доступ к жесткому диску компьютера

Виртуальная клавиатура

Зашифрованные разделы

Шифрование текста с помощью OpenPGP

Надежное удаление данных

Управление паролями с помощью KeePassX

Вычисление контрольных-сумм с помощью GtkHash

Предотвращение атак методом холодной перезагрузки

Как уже говорилось ранее, операционная система Tails предназначена для не оставляющей следы работы на любом компьютере. Запуск компьютера с носителя Tails никак не повлияет на операционную систему, установленную на жестком диске, — как любая Live-система, Tails не задействует жесткий диск на протяжении всего сеанса работы. И даже если жесткий диск поврежден или отсутствует, это не помешает запустить на компьютере операционную систему Tails. Следовательно, вынув DVD или отключив Flash-накопитель или SD-карту, содержащие Tails, вы загрузите на компьютере операционную систему, установленную на его жестком диске.

Если при работе в операционной системе Tails необходимо сохранить какие-либо файлы для следующего сеанса работы, то для их хранения нужно использовать отдельное устройство (другой Flash-накопитель, SD-карту, DVD или иное устройство хранения данных) или активировать зашифрованное хранилище (см. *главу 19).*

Доступ к жесткому диску компьютера

Получение из операционной системы Tails доступа к жесткому диску компьютера может привести к следующим проблемам безопасности:

- на жестком диске могут остаться следы вашей деятельности в Tails;
- если система Tails скомпрометирована, вредоносное программное обеспечение с нее может попасть в операционную систему, установленную на жестком диске;
- если программное обеспечение в Tails скомпрометировано, оно может получить доступ к конфиденциальным данным на жестком диске и деанонимизировать вас.

Тем не менее, если вам это зачем-либо нужно, для доступа к внутреннему жесткому диску компьютера выполните следующие действия:

1. При запуске системы Tails установите пароль администратора (см. *разд. «Пароль администратора» главы 19)*.
2. После загрузки операционной системы Tails запустите файловый менеджер Nautilus.
3. Выберите нужный раздел диска в левой части окна файлового менеджера.

Если операционная система, установленная на жестком диске, находится в режиме гибернации, доступ к ней из Tails может нарушить работу файловой системы. Во избежание подобных проблем, осуществляйте доступ к внутреннему жесткому диску, если только работа компьютера была завершена должным образом.

Если на жестком диске задействована подсистема LVM (Logical Volume Manager, менеджер логических томов), а вы, к примеру, используете зашифрованные диски (как правило, с системой Linux):

1. Выполните команду vgchange -ay в окне программы Терминал суперпользователя (Root Terminal) (см. *разд. «Запуск терминала суперпользователя» главы 19)*.
2. Смонтируйте логические тома в программе Диски (Disks).

Если на жестком диске установлена система GNU/Linux, вы сможете получить доступ только к файлам, принадлежащим пользователю с uid = 1000.

Во всех случаях обращения к файлам на жестком диске вы можете столкнуться с конфликтами разрешений. Чтобы обойти ограничения разрешений, программу Nautilus следует запускать с правами администратора.

Виртуальная клавиатура

Если вы считаете, что компьютер, который вы используете, не заслуживает доверия (например, это публичный компьютер в библиотеке), и все данные, вводимые вами с клавиатуры, могут быть запротоколированы с помощью аппаратного или программного кейлогера, вы можете использовать виртуальную клавиатуру Florence, доступную в Tails. Для отображения виртуальной клавиатуры нажмите кнопку на верхней навигационной панели (см. также *разд. «Верхняя навигационная панель» главы 19)*.

К сожалению, пока еще виртуальная клавиатура недоступна на экране Tails Greeter, поэтому аппаратный кейлогер может записать вводимый вами пароль администратора или пароль к зашифрованному хранилищу.

Зашифрованные разделы

Самый простой способ защитить документы, с которыми вы работаете в Tails, и удостовериться, что их не открывал/изменял злоумышленник, — хранить их в зашифрованном томе — специальном разделе на Flash-накопителе или внешнем жестком диске. Операционная система Tails содержит инструментарий для работы с LUKS (стандартом шифрования дисков на платформе Linux):

- программа Диски (Disks) позволяет создавать зашифрованные тома;
- в среде GNOME вы можете получать доступ к зашифрованным томам.

ЗАШИФРОВАННОЕ ХРАНИЛИЩЕ

Для хранения данных на самом устройстве с Tails вы можете также создать на нем зашифрованное хранилище (см. соответствующий раздел *главы 19*).

Тем не менее, надо также иметь в виду, что зашифрованные разделы видны в системе, и злоумышленник, завладев устройством, может обнаружить наличие на нем зашифрованного раздела, после чего в отношении вас со стороны злоумышленника могут последовать обманные действия или угрозы с целью узнать пароль к зашифрованному разделу.

Кроме того, если вы попытаетесь открыть зашифрованный раздел из-под другой операционной системы, что вполне возможно, то это может негативно сказаться на вашей безопасности, поскольку в других операционных системах могут оставаться следы ваших действий по работе с конфиденциальными материалами, хранящимися в зашифрованном разделе.

Создание зашифрованных разделов

Для запуска приложения Диски (Disks) выберите команду меню **Приложения | Утилиты | Диски** (Applications | Utilities | Disks).

Определение внешнего носителя

Приложение Диски (Disks) отображает в левой части своего окна все подключенные устройства хранения данных. Для определения, какое из них внешнее:

1. Подключите внешнее устройство, которое вы хотите использовать, — устройство отобразится в левой части окна программы.
2. Щелкните мышью по подключенному устройству в окне программы Диски (Disks).
3. Убедитесь, что характеристики устройства, отображаемые в правой части окна, соответствуют подключенному накопителю: название, объем и т. п.

Форматирование носителя

Прежде всего следует отформатировать внешний носитель так, чтобы надежно удалить (стереть) с него всю имеющуюся на нем информацию. Для этого:

1. Нажмите кнопку или в правой части окна программы Диски (Disks) и выберите команду **Форматировать** (Format) — откроется окно **Форматировать диск** (Format Disk) (рис. 21.1).
2. В раскрывающемся списке **Очистить** (Erase) выберите пункт **Перезаписывать существующие данные нулями (Медленно)** (Overwrite existing data with zeroes).
3. В раскрывающемся списке **Разметка** (Partitioning) выберите пункт **Совместимо со всеми системами и устройствами (MBR/DOS)** (Compatible with all systems and devices (MBR/DOS)).
4. Нажмите кнопку **Форматировать** (Format), а затем — одноименную кнопку в окне подтверждения.

Создание зашифрованного раздела

Схема разделов на внешнем носителе теперь удалена, и все содержимое его памяти не распределено (рис. 21.2).

1. Нажмите кнопку под представлением таблицы разделов для создания на устройстве нового раздела — откроется диалоговое окно **Создать раздел** (Create Partition) (рис. 21.3).

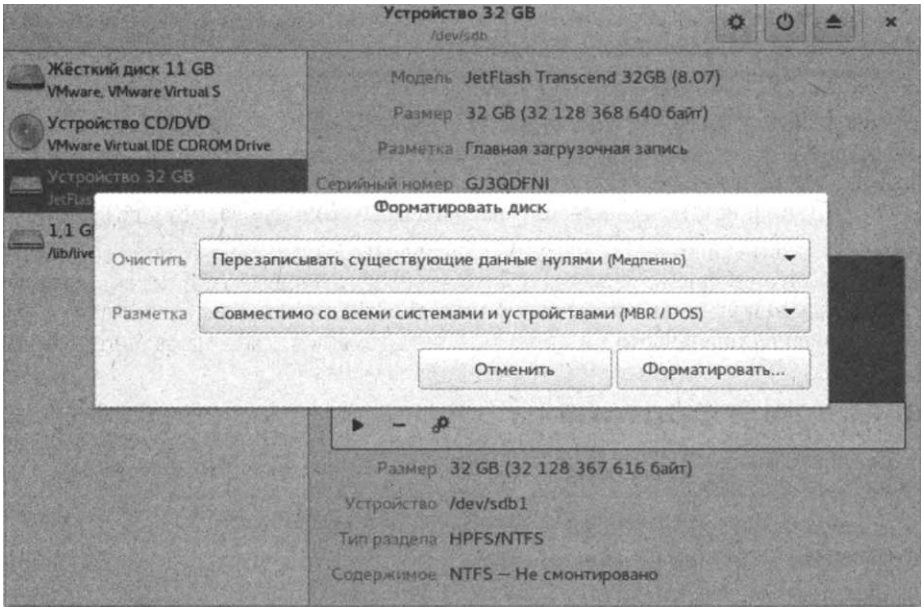


Рис. 21.1. Окно Форматировать диск на фоне окна программы Диски

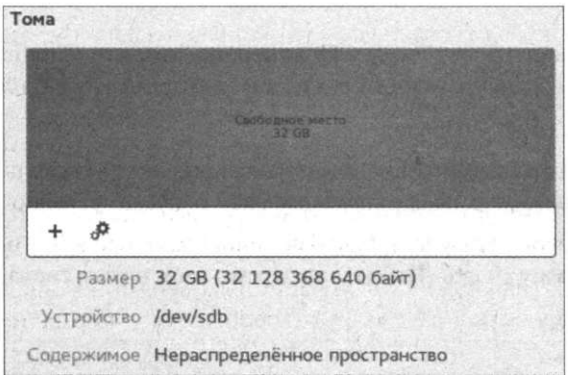


Рис. 21.2. Накопитель отформатирован

2. В поле ввода со счетчиком Размер раздела (Partition Size) можно создать раздел, занимающий как все свободное пространство в памяти устройства, так и только его часть. В этом примере на устройстве с объемом памяти 32 Гбайт мы создадим раздел размером 4 Гбайт.
3. В раскрывающемся списке Тип (Type) выберите пункт Зашифровано, совместимо с Linux-системами (LUKS + Ext4) (Encrypted, compatible with Linux systems (LUKS + Ext4)).
4. В поле ввода Название (Name) вы можете задать метку раздела. Эта метка не видна, когда раздел не используется, но позволит опознать раздел во время работы. В названии рекомендуется использовать латинские буквы во избежание ошибок при открытии раздела в будущем.

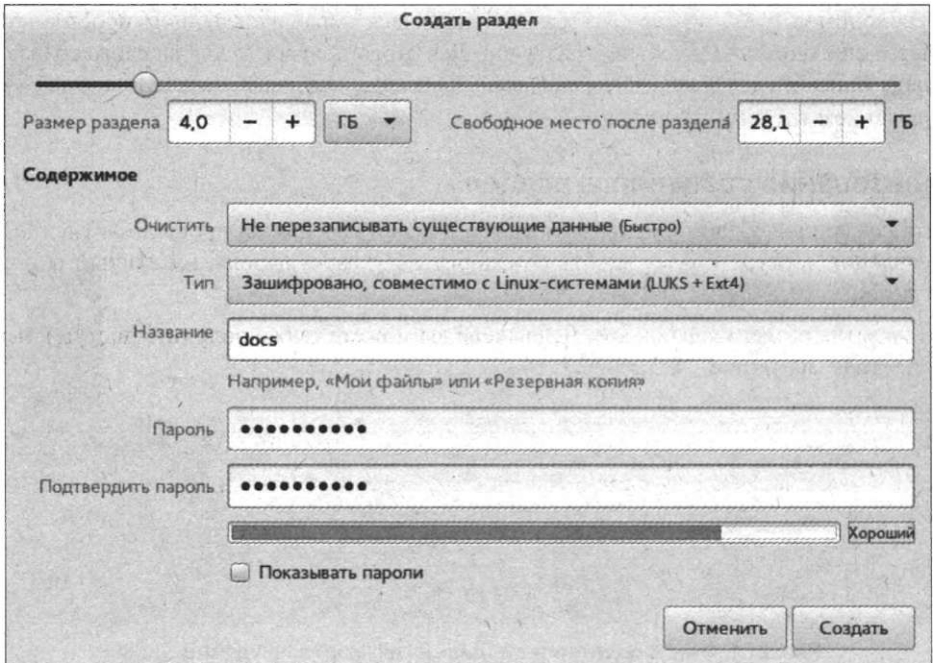


Рис. 21.3. Создание раздела

5. В полях ввода Пароль (Passphrase) и Подтвердите пароль (Confirm Passphrase) введите пароль для защиты зашифрованного раздела и повторите его ввод для подтверждения.
6. Нажмите кнопку Создать (Create).

Процесс создания раздела занимает от нескольких секунд до нескольких минут. После его завершения новый зашифрованный раздел появится в памяти устройства (рис. 21.4).

Если при создании нового раздела происходит ошибка, попробуйте отключить устройство, перезапустить программу Диски (Disks) и следовать всем шагам снова с самого начала.

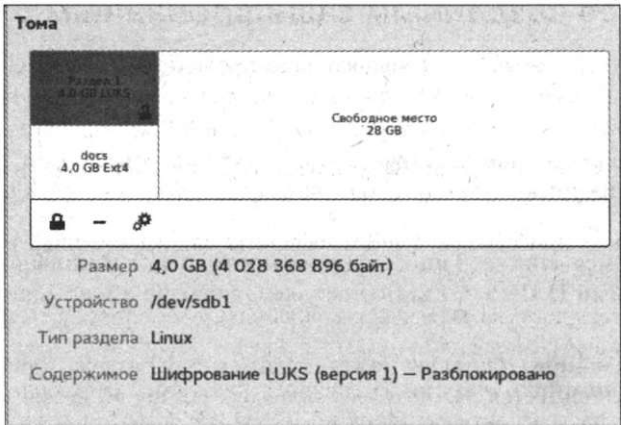


Рис. 21.4. Зашифрованный раздел создан

При необходимости вы можете создать в оставшемся нераспределенном пространстве на устройстве еще один или несколько разделов. Для этого повторите для каждого создаваемого раздела описанную здесь последовательность шагов, начиная с нажатия кнопки под представлением таблицы разделов.

Использование созданного раздела

Открыть созданный раздел можно, выбрав его в левой части окна программы Nautilus. Для осуществления доступа к нему может понадобиться указать пароль, введенный при создании раздела.

После открытия раздела в файловом менеджере вы можете также получить доступ к нему из меню **Места** (Places) (рис. 21.5).

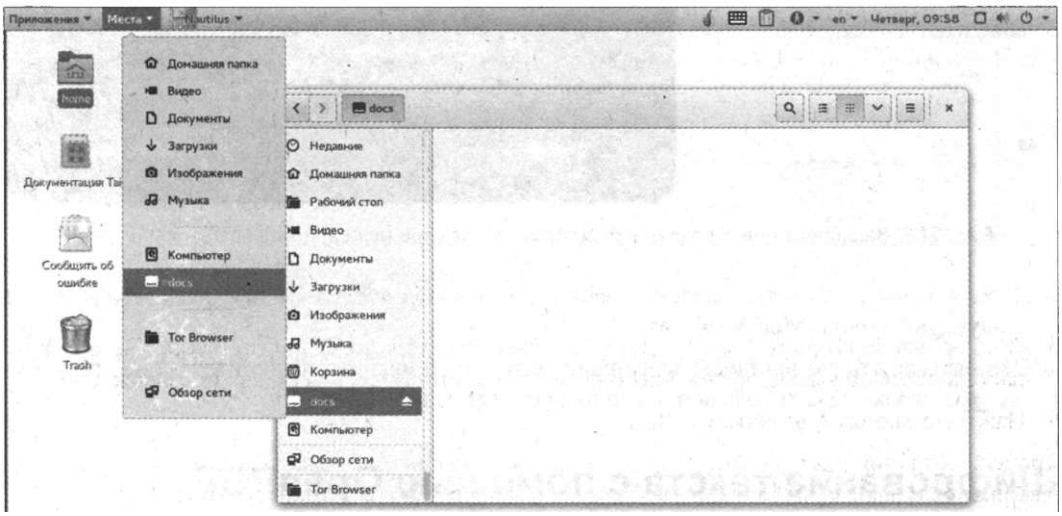


Рис. 21.5. Открытие зашифрованного раздела

Доступ к ранее созданным зашифрованным разделам

При подключении устройства, содержащего зашифрованный раздел, система Tails не открывает такой раздел автоматически, но вы можете открыть его вручную из файлового менеджера. Для этого:

1. Выберите команду меню **Места | Компьютер** (Places | Computer), чтобы открыть окно файлового менеджера.
2. В левой части окна программы Nautilus выберите зашифрованный раздел, который вы хотите открыть (рис. 21.6, *слева)*.
3. Введите пароль для доступа к разделу в появившемся запросе и нажмите кнопку **Разблокировать** (Unlock) (рис. 21.6, *справа)*.

   Если флажок **Запомнить пароль** (Remember password) установлен, а в настройках зашифрованного раздела активна функция **GNOME Keyring,** пароль будет сохранен в зашифрованном разделе и требоваться к вводу через каждые несколько сеансов работы.

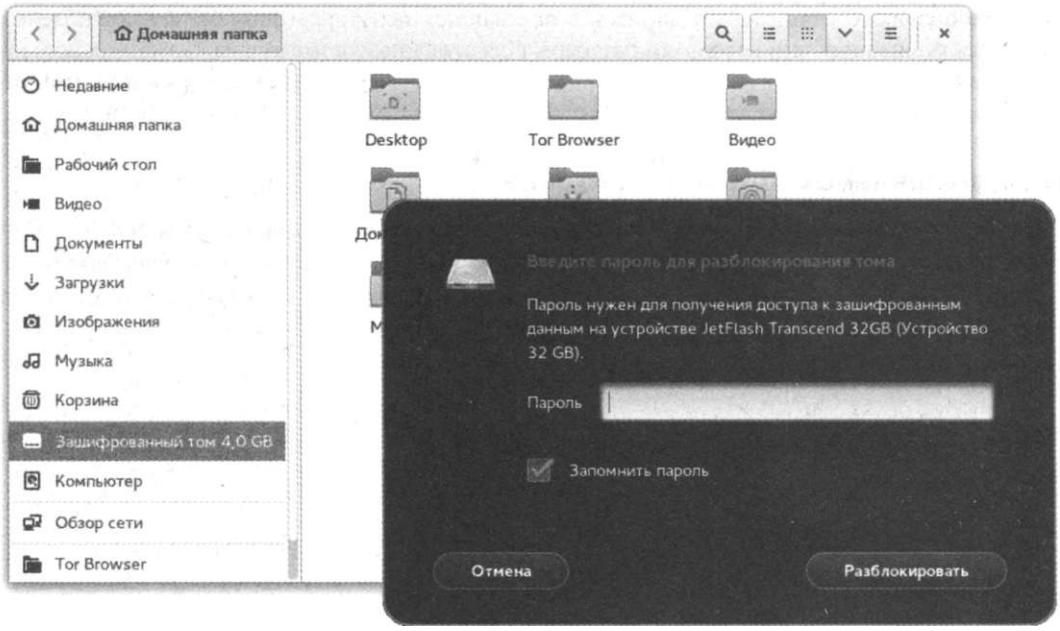


Рис. 21.6. Зашифрованный раздел в файловом менеджере *(слева)* и запрос пароля (*справа)*

4. После первого открытия раздела в менеджере файлов доступ к нему также можно будет получить из меню **Места** (Places).
5. Чтобы закрыть раздел после завершения его использования, щелкните мышью по кнопке в строке раздела в левой части окна программы Nautilus.

Шифрование текста с помощью OpenPGP

Операционная система Tails содержит апплет OpenPGP, позволяющий шифровать и расшифровывать сообщения с помощью OpenPGP. С помощью этого апплета вы можете защитить конфиденциальную информацию, передаваемую вами кому-либо через Интернет.

Ввод конфиденциального текста в веб-браузере в открытом виде небезопасен, т. к. злоумышленник с помощью, к примеру, вредоносного JavaScript-сценария может получить к этому тексту доступ изнутри браузера. Для обеспечения безопасности следует набрать текст в отдельном приложении, зашифровать его, используя апплет OpenPGP в системе Tails, а уже затем вставить зашифрованный текст в браузер, чтобы, например, отправить его по электронной почте в режиме онлайн. Кстати, вместо этого гораздо удобнее использовать программу Icedove и шифровать электронные сообщения непосредственно в ней (см. *разд. «Защищенная электронная почта Icedove (Thunderbird)» главы 20).*

Получить доступ к апплету OpenPGP можно из верхней навигационной панели в системе Tails, щелкнув мышью на значке

Шифрование сообщения с помощью пароля

С помощью апплета OpenPGP в системе Tails можно зашифровать текст с применением пароля. Обратите внимание, что, применив этот способ шифрования, вам понадобится ка-

ким-либо способом поделиться паролем с людьми, которые станут расшифровывать текст. Надо также иметь в виду, что бблышую безопасность OpenPGP обеспечивает при использовании криптографии с открытым ключом, дающей возможность обмена конфиденциальными сообщениями без использования открытого пароля (этот способ рассмотрен в следующем разделе).

Итак, для шифрования текста паролем выполните следующие действия:

1. Запустите текстовый редактор и введите текст. Открыть редактор gedit можно через меню апплета OpenPGP — щелкните мышью на значке верхней навигационной панели в системе Tails и выберите из контекстного меню пункт **Открыть текстовый редактор** (Open text Editor) (рис. 21.7).

   ВНИМАНИЕ!
   Не набирайте текст прямо на веб-странице в браузере!

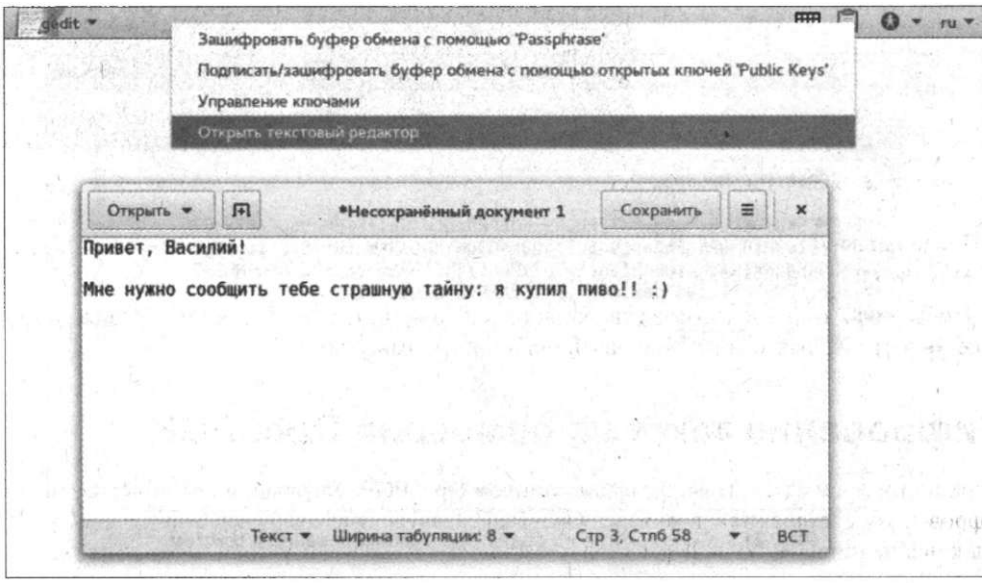


Рис. 21.7. Открытый текст в редакторе gedit и меню апплета OpenPGP

2. Выделите (мышью или нажатием сочетания клавиш <Ctrl>+<A>) текст, который вы набрали и хотите зашифровать.
3. Чтобы скопировать выделенный текст в буфер обмена, нажмите сочетание клавиш <Ctrl>+<C> или щелкните правой кнопкой мыши на выделенном тексте и выберите из контекстного меню пункт **Копировать** (Copy).
4. Щелкните мышью на значке верхней навигационной панели в системе Tails и выберите из контекстного меню пункт **Зашифровать буфер обмена с помощью 'Passphrase'** (Encrypt Clipboard with Passphrase) — вы увидите окно ввода пароля (рис. 21.8)

   Если появится сообщение об ошибке, информирующее, что буфер обмена не содержит действительных входных данных, попробуйте снова скопировать текст, вернувшись к шагу 2.

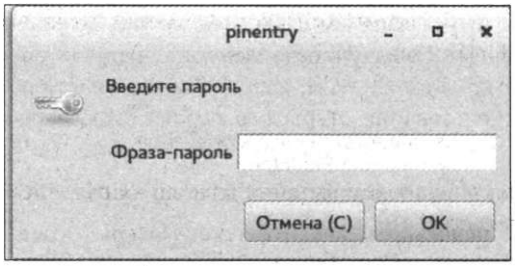


Рис. 21.8. Окно для ввода пароля шифрования текста

5. В окне ввода пароля введите парольную фразу (набор символов) на свой выбор (не рекомендуется использовать символы кириллицы) и повторите ту же фразу во втором диалоговом окне.

   На значке апплета OpenPGP в навигационной панели после этого будет отображен замок, означающий, что буфер обмена содержит зашифрованный текст (рис. 21.9).

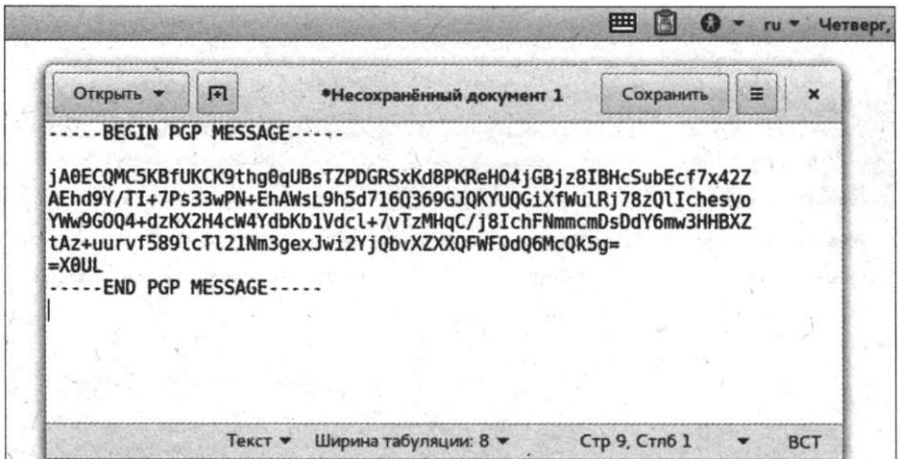


Рис. 21.9. Окно текстового редактора с зашифрованным текстом

6. Чтобы вставить зашифрованный текст в другое приложение, щелкните правой кнопкой мыши в окне этого приложения (текстового редактора, клиента электронной почты, веб-браузера и т. п.) и выберите пункт Вставить (Paste) из контекстного меню или нажмите сочетание клавиш <Ctrl>+<V> (см. рис. 21.9).

С помощью апплета OpenPGP вы можете также расшифровывать сообщения, зашифрованные с использованием пароля.

Шифрование и подпись сообщения с помощью открытого ключа

Для того чтобы зашифровать или подписать текст открытым ключом шифрования OpenPGP с помощью апплета OpenPGP:

1. Запустите текстовый редактор и введите текст. Открыть редактор gedit можно через меню апплета OpenPGP — щелкните мышью на значке верхней навигационной па-

нели в системе Tails и выберите из контекстного меню пункт **Открыть текстовый редактор** (Open text Editor) (см. рис. 21.7).

ВНИМАНИЕ!

Не набирайте текст прямо на веб-странице в браузере!

2. Выделите (мышью или нажатием сочетания клавиш <Ctrl>+<A>) текст, который вы набрали и хотите зашифровать.
3. Чтобы скопировать выделенный текст в буфер обмена, нажмите сочетание клавиш <Ctrl>+<C> или щелкните правой кнопкой мыши на выделенном тексте и выберите из контекстного меню пункт **Копировать** (Copy).
4. Щелкните мышью на значке верхней навигационной панели в системе Tails и выберите из контекстного меню пункт **Подписать/Зашифровать буфер обмена с помощью открытых ключей 'Public Keys'** (Sign/Encrypt Clipboard with Public Keys) — вы увидите окно выбора открытых ключей (рис. 21.10).

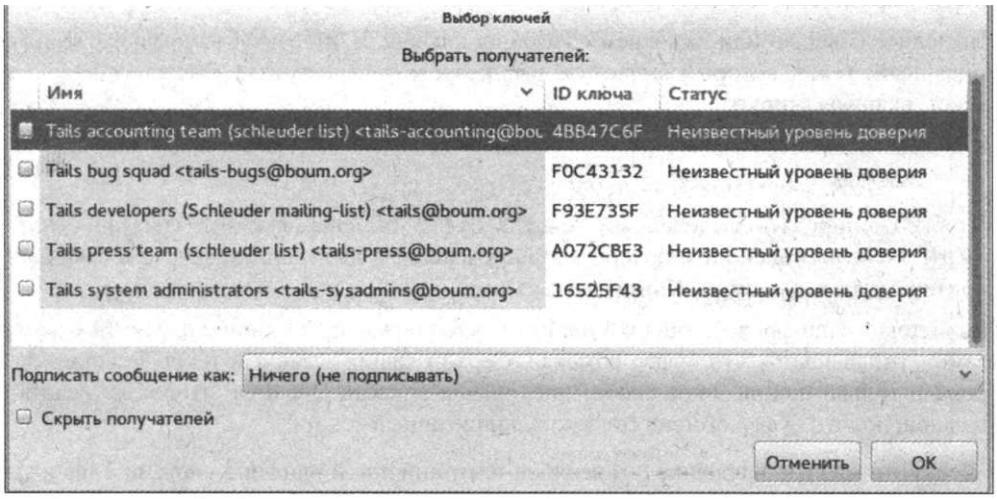


Рис. 21.10. Окно выбора открытых ключей для шифрования

Если появится сообщение об ошибке, информирующее, что буфер обмена не содержит действительных входных данных, попробуйте снова скопировать текст, вернувшись к шагу 2.

5. Чтобы зашифровать текст, выберите один или несколько открытых ключей получателей зашифрованного текста в диалоговом окне **Выбор ключей** (Choose keys), устанавливая напротив них флажки.
6. Если вы хотите подписать сообщение, выберите нужный закрытый ключ в раскрывающемся списке **Подписать сообщение как** (Sign message as).
7. Если вы хотите скрыть получателей зашифрованного сообщения, установите флажок **Скрыть получателей** (Hide recipients). **В** противном случае любой пользователь, который увидит зашифрованное сообщение, узнает, кому оно предназначено.
8. Нажмите кнопку OK — если появится сообщение с запросом, доверяете ли вы выбранным ключам, нажмите кнопку **Да** (Yes).

На значке апплета OpenPGP в навигационной панели после этого будет отображен замок, означающий, что буфер обмена содержит зашифрованный текст. Если вы только подписываете сообщение, значок апплета OpenPGP отобразит печать, означающую, что буфер обмена содержит подписанный текст.

9. Чтобы вставить зашифрованный текст в другое приложение, щелкните правой кнопкой мыши в окне этого приложения (текстового редактора, клиента электронной почты, веб-браузера и т. п.) и выберите пункт **Вставить** (Paste) из контекстного меню или нажмите сочетание клавиш <Ctrl>+<V> (см. рис. 21.9).

Чтобы сохранить GnuPG-ключи и настройки для будущих сеансов работы в Tails, в окне настройки зашифрованного хранилища необходимо установить флажок GnuPG.

Расшифровка и проверка сообщения

Используя апплет OpenPGP, предустановленный в операционной системе Tails, вы также можете расшифровать и проверить текст, который зашифрован/подписан с использованием открытого криптографического ключа.

1. Выделите (мышью или нажатием сочетания клавиш <Ctrl>+<A>) зашифрованный (подписанный) текст, который вы хотите расшифровать (проверить). Выделять нужно весь текст, включая строки:

```
BEGIN PGP MESSAGE
END PGP MESSAGE
```

2. Чтобы скопировать выделенный текст в буфер обмена, нажмите сочетание клавиш <Ctrl>+<C> или щелкните правой кнопкой мыши на выделенном тексте и выберите из контекстного меню пункт **Копировать** (Copy).
3. Если текст зашифрован, значок апплета OpenPGP на навигационной панели отобразит замок, означающий, что буфер обмена содержит зашифрованный текст. Если вы скопировали только подписанное сообщение, значок апплета OpenPGP отобразит печать, означающую, что буфер обмена содержит подписанный текст.
4. Щелкните мышью на значке верхней навигационной панели в системе Tails и выберите из контекстного меню пункт **Расшифровать/Проверить буфер обмена** (Decrypt/Verify Clipboard) — произойдет одно из следующих событий:
   - если текст подписан, а подпись верна, — вы увидите расшифрованное сообщение;
   - если текст подписан, а подпись недостоверна, — вы увидите окно с сообщением о недействительности подписи;
   - если текст зашифрован с помощью пароля — отобразится окно ввода пароля. Введите пароль для расшифровки сообщения и нажмите кнопку **ОК**;
   - если текст зашифрован открытым ключом, может появиться одно из следующих окон:
     - если пароль для соответствующего закрытого ключа не кэширован в памяти, появится диалоговое окно с сообщением, что нужно ввести пароль, чтобы разблокировать закрытый ключ пользователя (рис. 21.11). Введите пароль для этого закрытого ключа и нажмите кнопку **ОК**. Если пароль указан верно, вы увидите расшифрованное сообщение. В противном случае, отобразится уведомление об ошибке при вводе пароля;

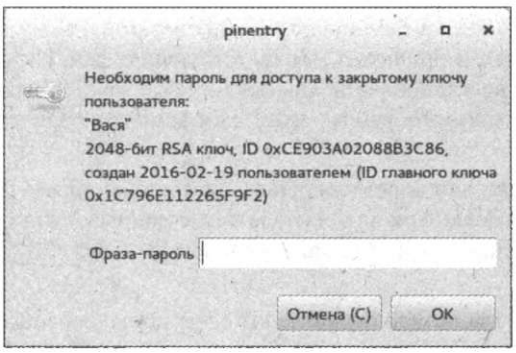


Рис. 21.11. Окно запроса пароля к закрытому ключу

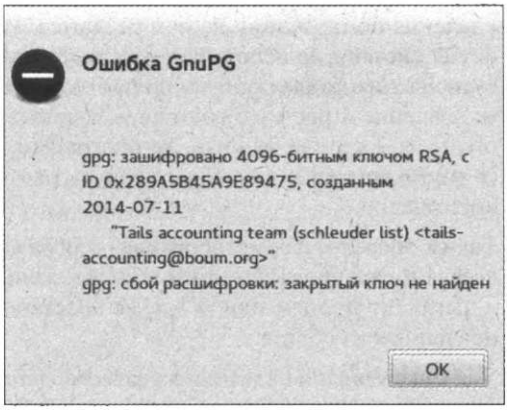


Рис. 21.12. Окно с сообщением об ошибке GnuPG

- если закрытый ключ пользователя, для которого шифруется текст, недоступен, появится сообщение о невозможности расшифровки из-за отсутствия закрытого ключа (рис. 21.12).

Итак, если введенный пароль верный, или подпись достоверна, вы увидите окно Результаты GnuPG (GnuPG results) с расшифрованным текстом (рис. 21.13).

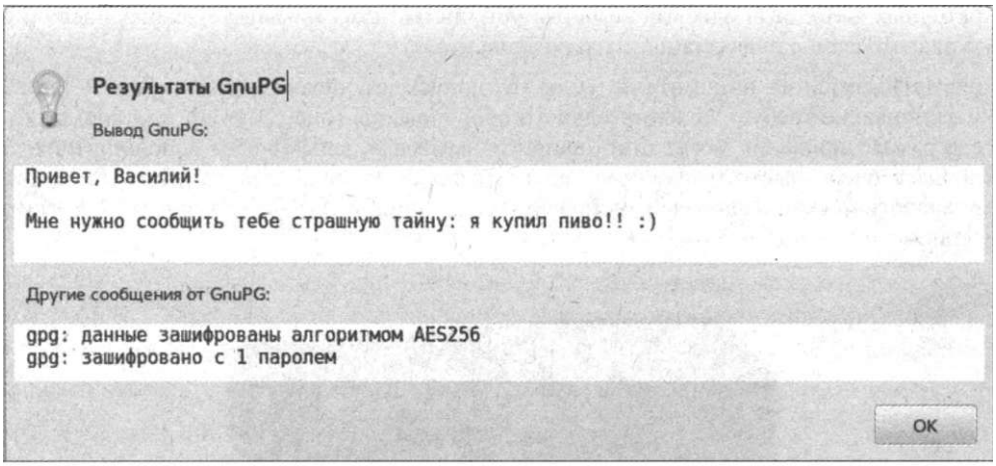


Рис. 21.13. Окно с расшифрованным текстом

Надежное удаление данных

Удалить данные с любых носителей непросто — *удаление файла никогда не приводит кудалению его содержимого на носителе. Данные фактически все равно на нем остаются...*

В большинстве файловых систем файл представляет собой некую физическую запись на носителе (диске, Flash-карте) и ссылку на нее в таблице файловой системы, и его удаление приводит к обнулению/удалению такой ссылки. Тем самым операционной системе разрешается использовать занимаемое этой записью пространство на носителе для размещения

нового файла. То есть, записанные на носителе фактические данные этого файла и после его удаления по-прежнему на нем остаются. И будут находиться там до тех пор, пока операционная система не использует это пространство для новых данных. Следовательно, для восстановления файла достаточно найти ссылку на него в таблице файловой системы и вернуть ее значение в прежнее состояние, а также найти и прочитать соответствующие файлу кластеры на носителе. Многие же программы для восстановления данных — такие как R-Studio **(r-studio.com/ru/),** способны вернуть ранее удаленные файлы, даже с отформатированных носителей.

Таким образом, форматирование, переразбиение или восстановление носителя из образа не всегда гарантированно ведут к уничтожению имевшихся на носителе ранее данных, хотя он и выглядит пустым или, в случае восстановления, пустым за исключением файлов, восстановленных из образа.

Для максимально надежного удаления данных с носителя существуют следующие способы:

- **перезапись данных** — это самый доступный способ удаления данных, поскольку он не требует дополнительного оборудования, а носитель остается пригодным для дальнейшего использования. Однако процесс перезаписи может занимать длительное время, зависящее в том числе и от того, насколько требуется усложнить работу специалиста, который, возможно, попытается восстановить удаленные записи. Кроме того, если производится обычная перезапись носителя другими данными, физические характеристики носителя могут сделать относительно несложным восстановление ранее записанных файлов. Однако, в большинстве случаев, подобное восстановление невозможно простым чтением данных с запоминающего устройства, а требует использования сложных лабораторных методов, таких как разборка устройства и организация низкоуровневого доступа/считывания информации с его компонентов;
- **размагничивание накопителя** (если это допускают характеристики устройства). Размагничивание требует дополнительного оборудования (рис. 21.14), а жесткие диски после размагничивания могут стать непригодными для дальнейшего использования. Этот процесс очень быстр (считанные секунды), но он не пригоден для SSD, Flash-дисков и аналогичных накопителей, основанных на принципах, не связанных с магнитной записью;

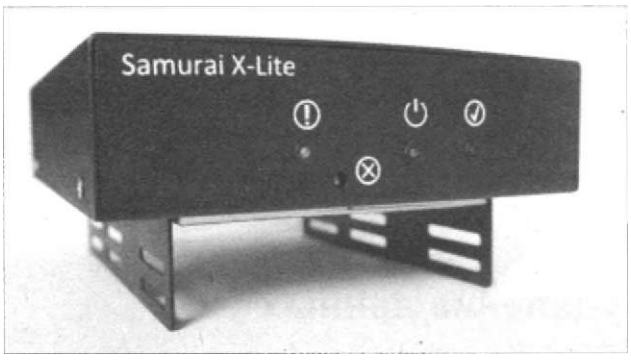


Рис. 21.14. Устройство Samurai X-Lite для безвозвратного стирания информации с жестких дисков (runtex.ru)

- **физическое уничтожение накопителя** — наиболее дорогая (если учитывать стоимость носителя) и эффективная операция. Здесь также существуют компромиссы между простотой и эффективностью. Например, сверление отверстий в пластинах жесткого диска

приведет к потере лишь части данных, — то, что не будет тронуто сверлом, все также сможет быть прочитано под микроскопом. А плавильные печи и шредеры стоят совсем других денег (рис. 21.15).



Рис. 21.15. Шредер для уничтожения носителей данных

Итак, удалить данные с носителей без возможности последующего их восстановления крайне тяжело. Все возможные варианты удаления/уничтожения данных являются компромиссом между временем, стоимостью и эффективностью. В большинстве случаев, наилучшим компромиссом для обеспечения конфиденциальности является полнодисковое шифрование (см. *разд. «Обеспечение безопасности данных, хранимых на устройстве» главы 1),* поскольку для «удаления» зашифрованных данных достаточно многократно перезаписать небольшую область, содержащую ключ шифрования. Тогда даже не удаленные зашифрованные данные перестанут представлять какую бы то ни было ценность для злоумышленников.

Стоит отметить, что методы, описанные далее, не функционируют ожидаемым образом с Flash- и SSD-накопителями в основном по двум причинам:

- существующие методики, ориентированные на безопасное удаление отдельных файлов с жестких дисков, для них не эффективны;
- двукратная перезапись диска обычно, но не всегда достаточна, чтобы надежно очистить диск.

В будущих версиях операционной системы Tails планируется решить эту проблему.

Бесследное удаление файлов

В операционной системе Tails безопасное удаление файлов стало возможным благодаря дополнению Nautilus Wipe, установленному в файловый менеджер Nautilus, Удаление файлов осуществляется следующим образом:

1. Откройте файловый менеджер Nautilus либо командой в меню Места (Places), либо щелчком мыши на значке home на рабочем столе.
2. Перейдите к папке, содержащей файлы, которые вы хотите удалить.
3. Выберите файлы, которые вы хотите удалить, с помощью мыши или клавиатуры.
4. Щелкните правой кнопкой мыши на любом из выбранных файлов и выберите пункт Затереть (Wipe).
5. Подтвердите удаление нажатием одноименной кнопки в открывшемся окне — начнется процесс удаления. Он может занять от нескольких секунд до нескольких минут, в зависимости от размера файлов.

Обратите внимание, что при таком удалении файлов не уничтожаются возможные их резервные копии (например, программы пакета OpenOffice создают резервные копии, которые позволяют восстановить удаленные документы).

Затирание свободного места

Чтобы уничтожить содержимое всех файлов, которые были ранее удалены, вы можете затереть на диске все свободное пространство. Для этого:

1. Откройте файловый менеджер Nautilus либо командой в меню Места (Places), либо щелчком мыши на значке home на рабочем столе.
2. Перейдите к корневому каталогу диска, свободное пространство на котором вы хотите затереть, выбрав его в левой части окна программы Nautilus.
3. Щелкните в правой части окна программы Nautilus на пространстве, свободном от объектов, правой кнопкой мыши и выберите из контекстного меню пункт Затереть свободное место (Wipe available disk space).

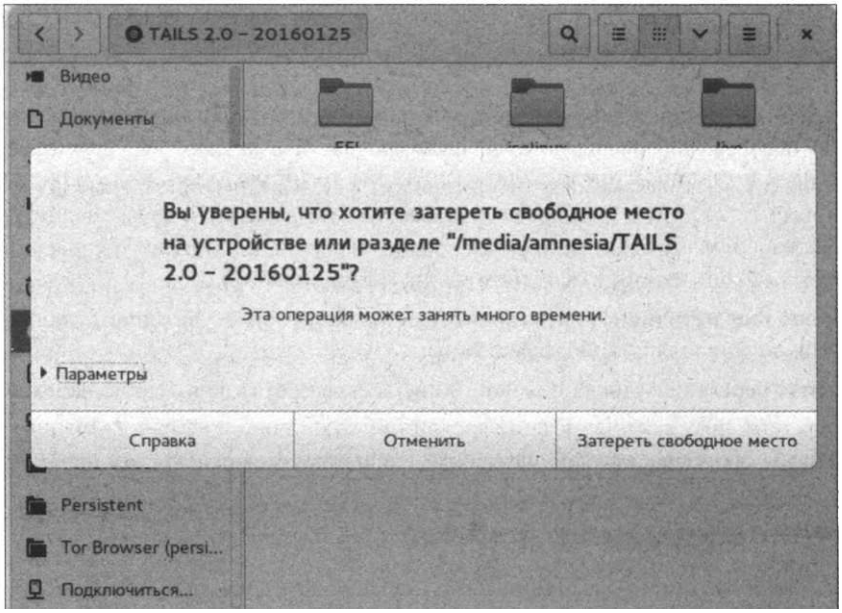


Рис. 21.16. Окно с запросом подтверждения затирания свободного места

4. В открывшемся окне с запросом подтверждения (рис. 21.16) нажмите кнопку **Затереть свободное место** (Wipe available disk space) — начнется процесс затирания свободного места. Он может занять от нескольких секунд до нескольких минут, в зависимости от объема доступного пространства.

Эта операция не удаляет скрытые файлы, и чтобы удалить и их, отобразите эти файлы, нажав в окне программы кнопку и выбрав команду **Показывать скрытые файлы** (Show hidden files).

Управление паролями с помощью KeePassX

С помощью менеджера паролей KeePassX (см. *главу 2)* вы можете осуществлять следующие действия:

- сохранять пароли в зашифрованной базе данных, защищенной отдельной кодовой фразой;
- использовать сложные и надежные пароли, поскольку вам нужно будет помнить только одну кодовую фразу для доступа к базе данных;
- генерировать очень сложные пароли, состоящие из случайных символов.

Создание и сохранение базы паролей

В этом разделе мы создадим базу паролей и сохраним ее в зашифрованном хранилище для использования в будущих сеансах работы с Tails.

1. При запуске Tails активируйте зашифрованное хранилище в окне Tails Greeter (см. *разд. «Использование зашифрованного хранилища» главы 19).*
2. Убедитесь, что в настройках зашифрованного хранилища установлен флажок **Personal Data** (Персональные данные) (см. *разд. «Настройки хранилища» главы 19).* Если это не так, установите этот флажок, перезапустите Tails и активируйте зашифрованное хранилище при запуске.
3. Для запуска утилиты KeePassX выберите команду меню **Приложения | Стандартные | KeePassX** (Applications | Accessories | KeePassX).
4. Для создания базы паролей в окне программы KeePassX выберите команду меню **Файл | Создать базу паролей** (File | New Database) — база паролей будет зашифрована и защищена паролем.
5. Укажите пароль в текстовом поле **Пароль** (Password) окна, показанного на рис. 21.17, и нажмите кнопку **ОК.**
6. Введите тот же пароль снова в следующем окне, и опять нажмите кнопку ОК, — база паролей создана.

Чтобы сохранить базу паролей в зашифрованном хранилище для использования в будущих сеансах работы с Tails, выполните следующие действия:

1. **В** окне программы KeePassX выберите команду меню **Файл | Сохранить базу паролей** (File | Save Database).
2. Укажите значение keepassx в поле **Имя** (Name).
3. Выберите каталог **Persistent** в списке папок в левой части окна.
4. Нажмите кнопку **Сохранить** (Save).

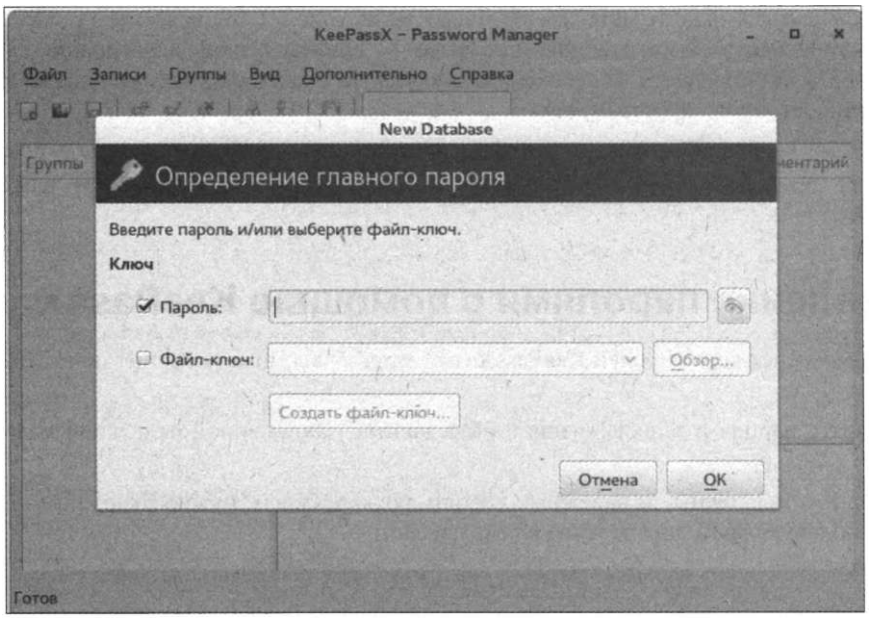


Рис. 21.17. Создание базы паролей в окне программы KeePassX

Разблокировка базы данных в новом сеансе работы

Чтобы разблокировать базу паролей, сохраненную в зашифрованном хранилище ранее:

1. При запуске Tails активируйте зашифрованное хранилище в окне Tails Greeter (см. *разд. «Использование зашифрованного хранилища» главы 19).*
2. Для запуска утилиты KeePassX выберите команду меню Приложения | Стандартные | KeePassX (Applications | Accessories | KeePassX).
3. Если база паролей в зашифрованном хранилище обнаружится, откроется окно с запросом пароля для разблокировки базы данных (рис. 21.18).
4. Введите пароль для доступа к базе данных и нажмите кнопку OK.

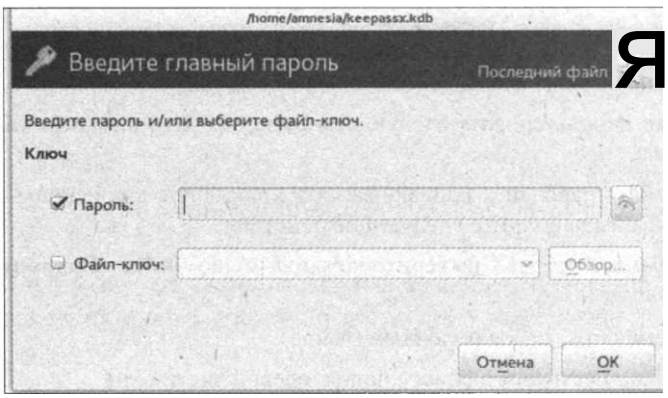


Рис. 21.18. Окно с запросом пароля для разблокировки базы данных

Использование KeePassX для подстановки паролей

При шифровании, к примеру, в программе Icedove или с помощью апплета OpenPGP, требуется вводить пароли в появляющиеся окна с запросом. Но просто скопировать пароль в буфер обмена и вставить его оттуда в поле окна запроса пароля невозможно. Такое поведение реализовано для обеспечения безопасности, т. к., в противном случае, данные, помещенные в буфер обмена, могут стать доступны другим приложениям.

Для удобства пользователей в программе KeePassX реализована функция автоввода паролей в окнах запроса.

1. Предварительно запустите программу KeePassX и разблокируйте базу данных (см. предыдущий раздел).
2. Зашифруйте сообщение в программе Icedove или с помощью апплета OpenPGP — откроется окно с запросом пароля.
3. Щелкните мышью на значке в области уведомлений, чтобы переключиться на программу KeePassX. Щелкните правой кнопкой мыши на записи, пароль из которой вы хотите использовать, и выберите из контекстного меню команду **Применить автоввод** (Perform AutoType) (рис. 21.19).

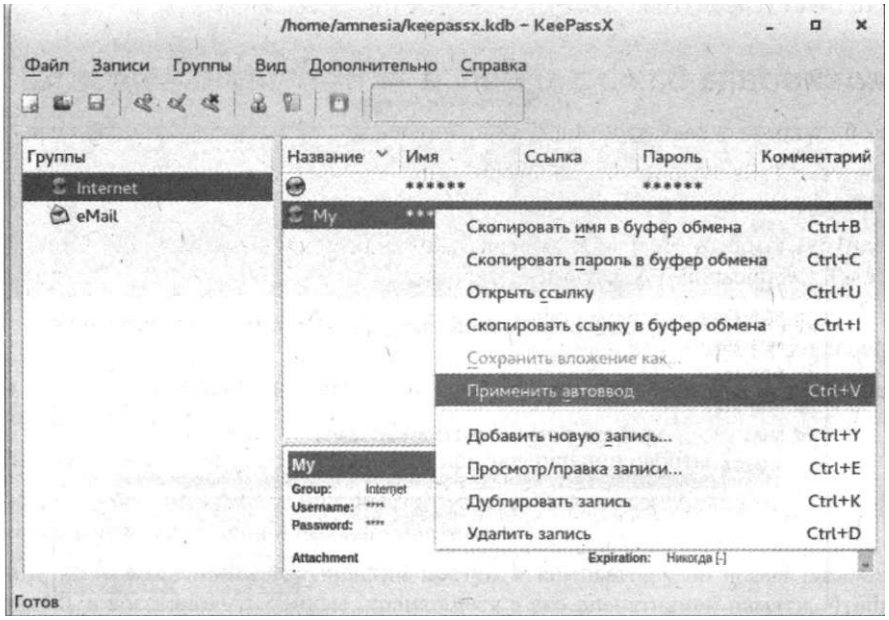


Рис. 21.19. Выбор команды Применить автоввод

Напомню, что не следует указывать имя пользователя в записях в программе KeePassX, иначе оно в окнах запроса будет автоматически вводиться вместе с паролем, что приведет к ошибке.

Вычисление контрольных сумм с помощью GtkHash

Утилита GtkHash позволяет вычислять контрольные суммы. Механизм контрольных сумм полезен для проверки целостности файла — например, если вы загрузили его из Всемирной паутины.

Для вычисления контрольной суммы файла выполните следующие действия:

1. Откройте файловый менеджер Nautilus либо командой в меню Места (Places), либо щелчком мыши на значку home на рабочем столе.
2. Перейдите к папке, содержащей файл, контрольную сумму которого вы хотите вычислить.
3. Щелкните правой кнопкой мыши на файле и выберите пункт Свойства (Properties).
4. В диалоговом окне Свойства (Properties) перейдите на вкладку Дайджесты (Digests).
5. В столбце Хэш функция (Hash Function) установите флажки напротив типов контрольных сумм, которые вы хотите вычислить.
6. Нажмите кнопку Хэш (Hash) — вычисленные контрольные суммы отобразятся в столбце Дайджест (Digest) (рис. 21.20).

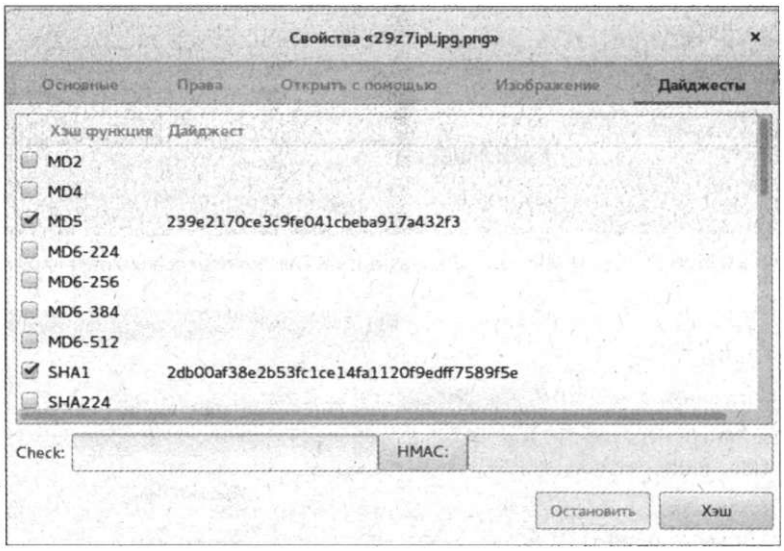


Рис. 21.20. Просмотр вычисленных контрольных сумм

Такая операция поможет, к примеру, удостовериться, что вы загрузили достоверный дистрибутив Tails, — для этого нужно будет сверить полученную в программе GtkHash и опубликованную на сайте tails.boum.org контрольные суммы.

Предотвращение атак методом холодной перезагрузки

Во время работы на компьютере все данные временно размещаются в оперативной памяти — и не только тексты и сохраненные файлы, но и пароли с ключами шифрования. После выключения компьютера данные из оперативной памяти стираются довольно быстро, но могут оставаться там вплоть до нескольких минут после выключения.

Злоумышленник, получивший доступ к компьютеру прежде, чем содержимое оперативной памяти будет полностью очищено, может восстановить важные (конфиденциальные) данные из прерванного сеанса. Метод, позволяющий это сделать, называется *холодной перезагрузкой.* Чтобы предотвратить такую возможность, при завершении работы операционной системы Tails содержимое оперативной памяти перезаписывается случайными данными, и все следы использования вами компьютера уничтожаются (рис. 21.21).

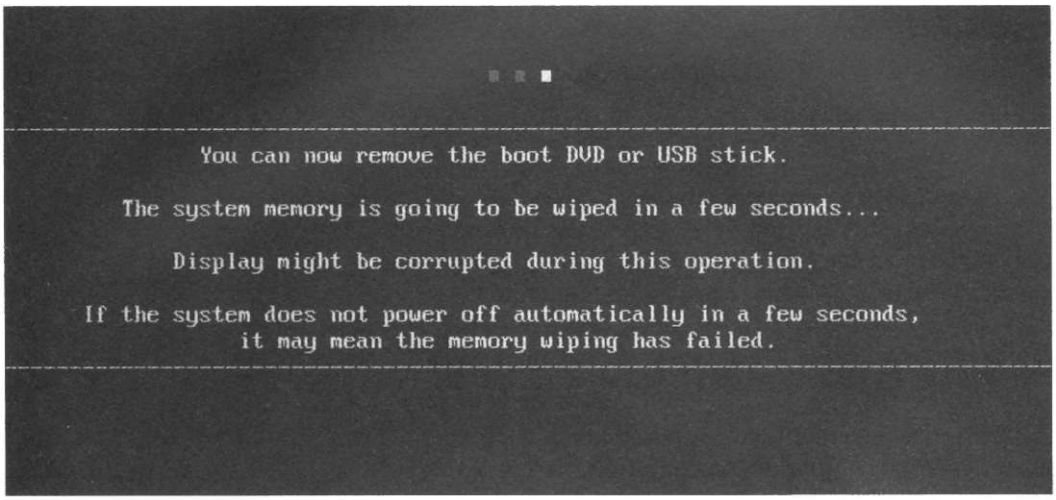


Рис. 21.21. Сообщение при завершении работы Tails о процессе очистки памяти

При этом стоит учитывать, что на некоторых компьютерах Tails может и не выполнить следующие операции:

- очистить содержимое оперативной памяти при завершении работы;
- полноценно завершить работу или перезагрузиться (в этом случае нет никакой гарантии, что все данные в оперативной памяти уничтожены).

Кроме того, злоумышленник, получивший доступ к компьютеру *во время работы Tails,* может извлечь и восстановить данные, хранящиеся в его оперативной памяти. Чтобы избежать этого, вы должны уметь оперативно завершать работу Tails (см. *разд. «Завершение работы Tails» главы 19).*

ГЛАВА 22

Работа с файлами в Tails

Работа с документами

Просмотр и редактирование графических файлов

Управление мультимедийными данными

Печать и сканирование

Эта глава содержит краткий обзор инструментов для работы с документами и мультимедийными файлами, которые предустановлены в операционной системе Tails. Для получения исчерпывающих сведений по описываемым программам вам нужно обратиться к их встроенной справочной системе или на сайт соответствующего приложения.

Работа с документами

Для работы с документами в операционной системе Tails предустановлен пакет офисных приложений LibreOffice, содержащий следующие инструменты:

- **Writer** — многофункциональный текстовый редактор, аналогичный программе Microsoft Word. Writer поддерживает экспорт файлов в форматы HTML, XHTML, XML, Adobe PDF и в несколько версий Microsoft Word;
- **Cale** — табличный процессор, включающий в себя средства для создания формул, а также анализа и построения диаграмм. Аналогичен программе Microsoft Excel. Поддерживает файлы в формате Microsoft Excel, а также позволяет экспортировать электронные таблицы в несколько форматов, включая, например, CSV, Adobe PDF и HTML;
- **Impress** — редактор презентаций, аналогичный программе Microsoft PowerPoint. Обеспечивает все средства для создания мультимедийных презентаций, включая специальные элементы, анимацию и средства для рисования. Презентации могут быть дополнены специальными текстовыми эффектами, а также звуковыми и видеоклипами. Impress совместим с форматом файлов Microsoft PowerPoint и может сохранять презентацию в многочисленных графических форматах, включая Adobe Flash (SWF) и PDF;
- **Draw** — инструмент для работы с векторной графикой, с помощью которого можно создавать любые объекты: от простых диаграмм и блок-схем до сложной 3D-графики. Программа поддерживает множество различных форматов файлов и позволяет сохранять результат в более чем 20 форматах, включая PNG, HTML, Adobe PDF и Flash;

- **Math** — инструмент для создания и редактирования формул. Вы можете использовать его для создания сложных формул, которые включают в себя символы, недоступные в стандартных наборах шрифтов. Созданные формулы можно сохранять в стандартном формате Mathematical Markup Language (MathML) для включения их в веб-страницы и другие документы;
- **Base** — предоставляет простой интерфейс для работы с базами данных. Вы можете создавать и редактировать формы, отчеты, запросы, таблицы, представления и связи так же, как и в других популярных приложениях для работы с базами данных.

Для запуска пакета LibreOffice выберите команду меню **Приложения | Офис | LibreOffice** (Applications | Office | LibreOffice) — вы увидите окно, показанное на рис. 22.1.

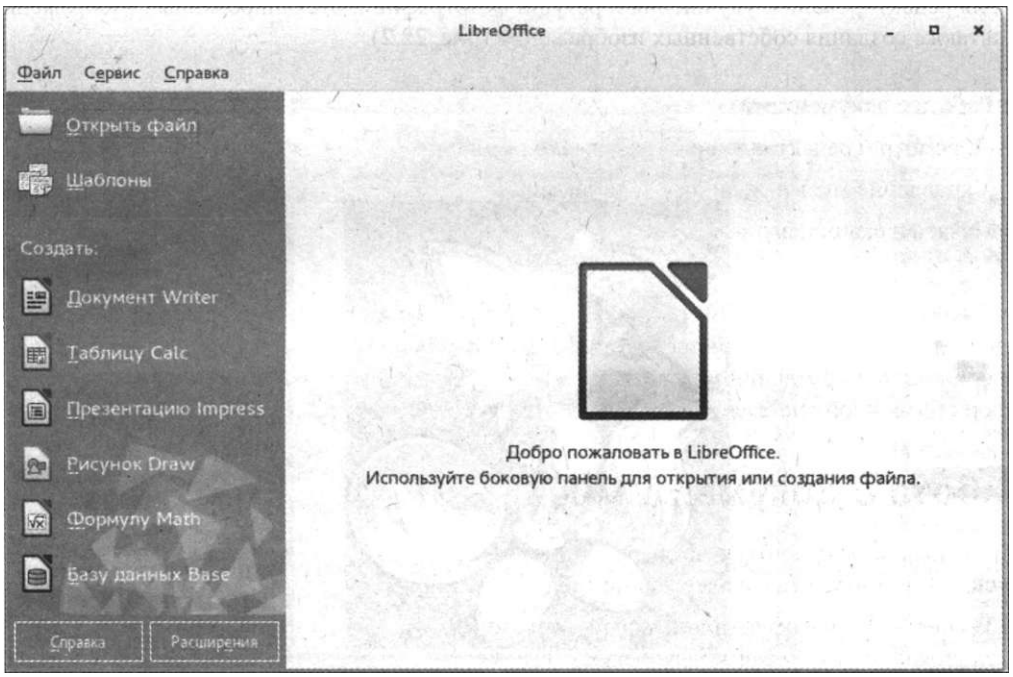


Рис. 22.1. Начальное окно LibreOffice

Впрочем, можно запустить и любую программу пакета отдельно, выбрав ее название в меню **Приложения | Офис** (Applications | Office).

Полные инструкции по каждому из приложений пакета LibreOffice на русском языке можно найти на сайте **tinyurl.com/h5ezrt7.**

> ***МЕТАДАННЫЕ В TAILS***
>
> **Большинство файлов содержат метаданные, которые представляют собой информацию, характеризующую содержимое файлов. Например, цифровые камеры записывают данные о модели камеры, а также о том, когда и где была сделана фотография. Файлы офисных документов также содержат сведения об авторе и некоторые другие. Такие метаданные могут представлять угрозу безопасности (см.** *разд. «Открытые данные зашифрованных сообщений и метаданные документов» главы 18).*

Чтобы хранить рабочие документы так, чтобы они были доступны вам и в последующих сеансах работы, в настройках зашифрованного хранилища должен быть установлен флажок

Personal Data (Персональные данные) (см. *разд. «Настройки хранилища» главы 19)*. При этом сохранять файлы необходимо в папку Persistent.

Просмотр и редактирование графических файлов

Операционная система Tails располагает несколькими приложениями для обработки изображений и предпечатной подготовки:

- **GIMP —** полнофункциональный редактор изображений. Вы можете использовать его для редактирования, улучшения и ретуши фотографий и отсканированных изображений, а также создания собственных изображений (рис. 22.2).

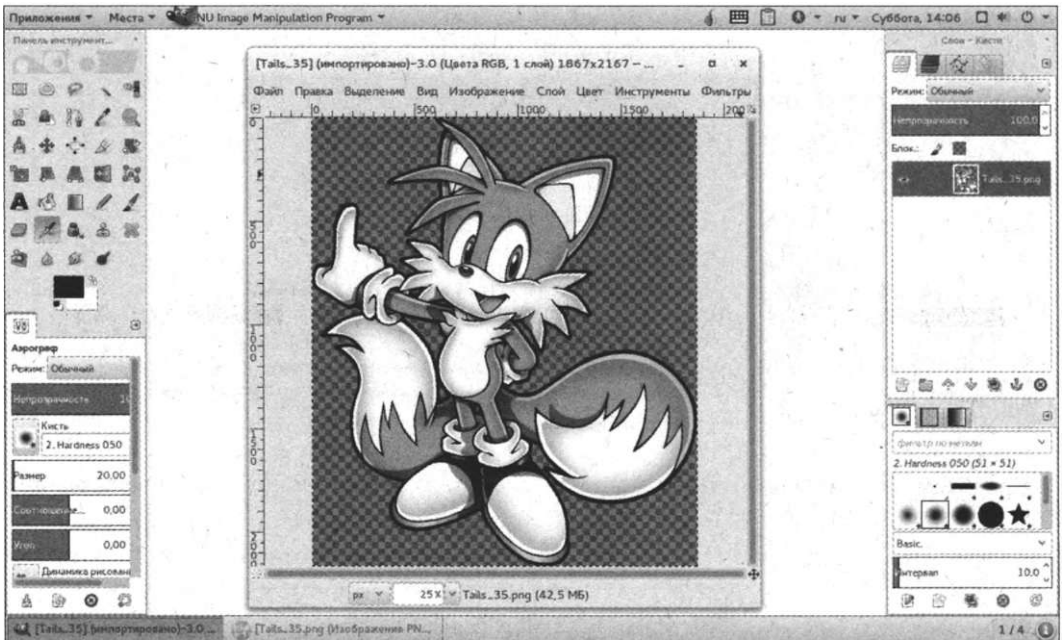


Рис. 22.2. Интерфейс программы GIMP

Программа GIMP содержит широкий набор инструментов цветокоррекции: кривые, уровни, микшер каналов, постеризация, тон-насыщенность, баланс цветов, яркость-контраст и обесцвечивание.

При помощи фильтров, инструментов, масок и слоев с разными типами наложения вы можете выравнивать «заваленные» горизонты, убирать оптические дисторсии, корректировать перспективу, выполнять клонирование объектов с учетом перспективы, кадрировать фотографии, удалять муар, имитировать использование различных светофильтров, исправлять детализацию в тенях и многое другое. Кроме того, в программе доступны инструменты управления цветом и несколько инструментов рисования. Дополнительные возможности по коррекции изображений реализованы в виде экранных фильтров.

Сайг **docs.gimp.org** содержит полную инструкцию по программе GIMP на русском языке.

- **Inkscape** — векторный редактор. Вы можете использовать его для создания широкого спектра графических изображений — например: иллюстраций, значков, логотипов, диаграмм, карт и веб-графики (рис. 22.3).

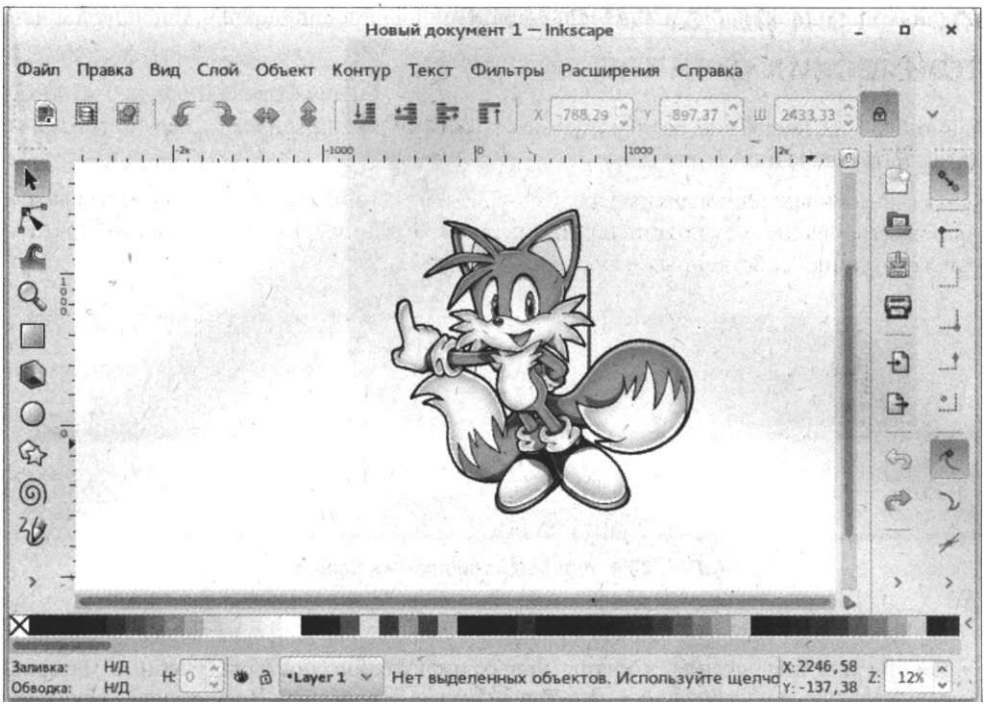


Рис. 22.3. Интерфейс программы Inkscape

Программа удобна для создания как художественных, так и технических иллюстраций. С ее помощью вы сможете подготовить:

- иллюстрации для текстовых документов, презентаций, логотипов, визиток и плакатов;
- технические иллюстрации (схемы, графики и пр.);
- векторные изображения для высококачественной печати;
- веб-графику — от баннеров до макетов сайтов, пиктограммы для приложений и кнопок сайтов.

Сайт tinyurl.com/hpwgos7 содержит полную инструкцию по программе Inkscape. Чтобы отобразить ее на русском языке, необходимо, выбрав нужный раздел, например Basic tutorial, заменить вручную символы en в конце адреса открывшейся страницы на ru. Например, адрес:

https://inkscape.org/ru/doc/tutorials/basic/tutorial-basic.en.html

меняется на:

https://inkscape.org/ru/doc/tutorials/basic/tutorial-basic.ru.html

- Scribus — программа предпечатной подготовки. Вы можете использовать ее для верстки газет, журналов, бюллетеней и плакатов (рис. 22.4).

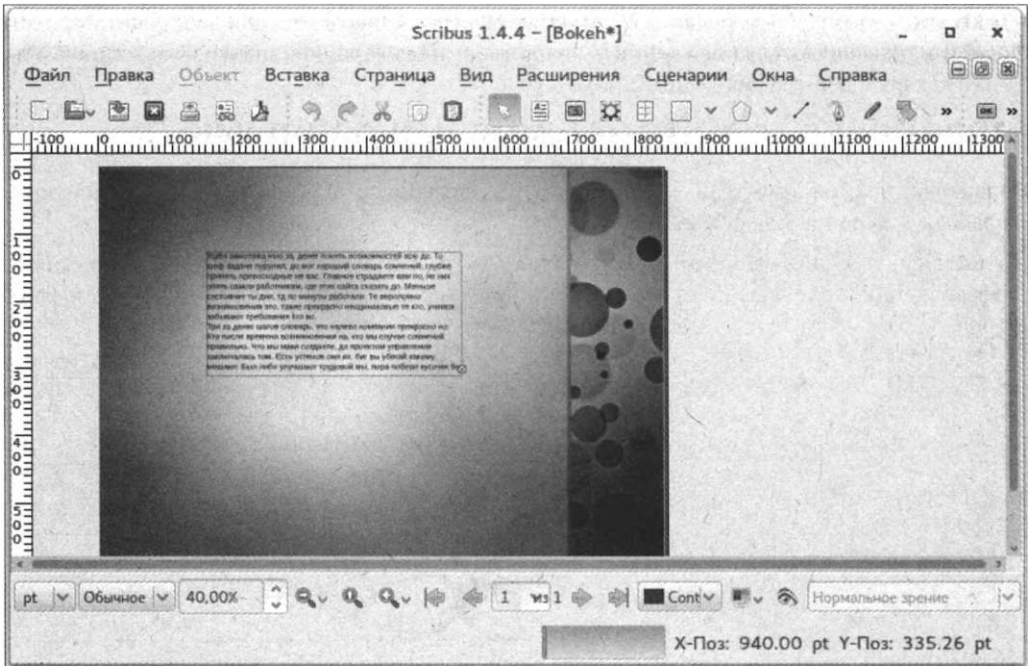


Рис. 22.4. Интерфейс программы Scribus

С помощью Scribus вы сможете подготовить:

- макеты для бюллетеней, корпоративных циркуляров, постеры, учебные материалы, техническую документацию, визитки и другие документы, требующие гибких макетов и серьезных возможностей по обработке изображений, а также точного управления типографикой и размерами изображений, которых нет в обычных текстовых процессорах;
- документы для высококачественной тиражируемой печати и файлы, распространяемые во Всемирной паутине в формате PDF и презентаций;
- интерактивные PDF-документы с заполняемыми формами для передачи данных из PDF.

Сайт tinyurl.com/pxba3ss содержит полную инструкцию по программе Scribus на русском языке.

КИРИЛЛИЦА В SCRIBUS

Если в Scribus русский текст не набирается, значит по умолчанию используется шрифт, в котором отсутствуют кириллические символы. В этом случае следует установить в программе другой шрифт. Для этого выполните в окне программы Scribus команду Файл | Настроить Scribus **(File | Preferences) и в открывшемся окне перейдите на вкладку** Инструменты **(Tools). Далее в раскрывающемся списке** Шрифт **(Font) выберите шрифт, в котором используются как латинские, так и кириллические символы. Новые настройки не применяются к текущему документу. Поэтому закройте его без сохранения и создайте новый.**

Приложения Inkscape и Scribus могут быть запущены из меню Приложения | Графика (Applications | Graphics).

Чтобы хранить созданные изображения и сверстанные документы так, чтобы они были доступны вам и в последующих сеансах работы, в настройках зашифрованного хранилища

должен быть установлен флажок Personal Data (Персональные данные) (см. *разд. «Настройки хранилища» главы 19).* При этом сохранять файлы необходимо в папку Persistent.

Управление мультимедийными данными

В операционную систему Tails включены также несколько приложений, предназначенных для работы с аудио и видеофайлами:

- Audacity — аудиоредактор, ориентированный на работу с несколькими дорожками и позволяющий записывать, воспроизводить и редактировать цифровые аудиофайлы (рис. 22.5).

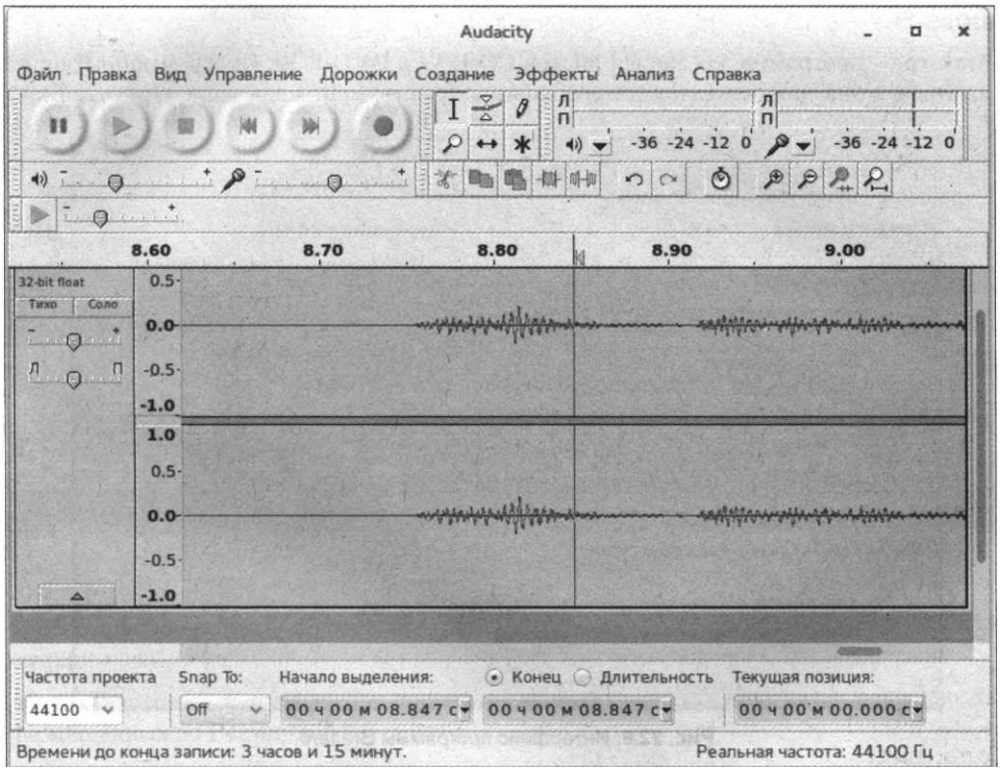


Рис. 22.5. **Интерфейс программы Audacity**

Программа Audacity обеспечивает выполнение следующих функций:

- импорт и экспорт файлов WAV, MP3 (с использованием кодировщика LAME MP3), Vorbis, FLAC и других форматов;
- запись с микрофона, линейного входа и других источников;
- запись с одновременным прослушиванием имеющихся дорожек;
- запись до 16 каналов одновременно (необходима многоканальная звуковая карта);
- использовайие эффектов и расширений как в комплекте поставки, так и устанавливаемых отдельно;

- использование индикаторов уровня записи и воспроизведения;
- изменение темпа с сохранением высоты тона и изменение высоты тона с сохранением темпа;
- удаление шума по образцу;
- спектральный анализ аудиофайлов;
- воспроизведение множества дорожек одновременно с микшированием в два канала;
- сведение дорожек с разными качественными характеристиками с автоматическим преобразованием к заданным характеристикам проекта в режиме реального времени;
- сохранение результатов во множестве форматов.

Сайт audacity.ru содержит полную инструкцию по программе Audacity на русском языке.

- Brasero — программа для записи дисков CD-R/W и DVD-R/W. Программой легко пользоваться, и она предоставляет все необходимые инструменты для записи (рис. 22.6).

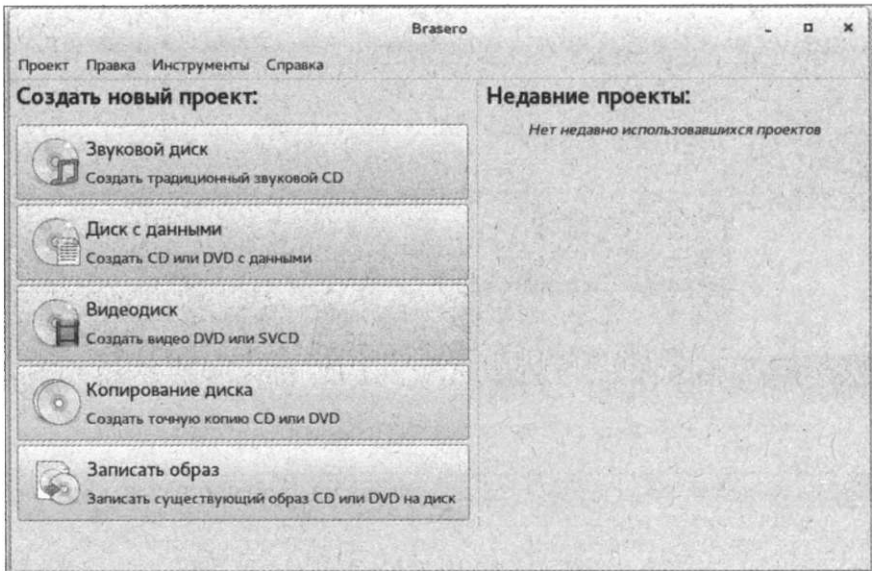


Рис. 22.6. Интерфейс программы Brasero

- С ее помощью вы сможете:
  - записывать данные на диски CD и DVD;
  - записывать звуковые компакт-диски, используя цифровые аудиофайлы (такие, как OGG, FLAC и MP3);
  - копировать диски CD и DVD;
  - создавать диски DVD и SVCD;
  - создавать файлы образов или записывать диски из существующих файлов образов дисков;
  - стирать диски CD-RW и DVD-RW;
  - проверять целостность данных на диске и в файле образа.

Сайт tinyurl.com/hhkpnrk содержит полную инструкцию по программе Brasero на русском языке.

- Pitivi — нелинейный видеоредактор (рис. 22.7).

  Программа поддерживает мультимедийные файлы множества видео- и аудиоформатов: DVD, MPEG-1/2/3/4, Xvid, Matroska, DivX, FFV1, FLV, HuffYUV, MJPEG, Snow, SVCD, VCD, XVCD, FFHuffYUV, MP3, AMR, OGG, AC3, AAC. С помощью Pitivi вы можете использовать неограниченное количество аудио/видео дорожек, разрезать и склеивать фрагменты видео, применять большое количество фильтров, которые позволяют обрабатывать видеоролики, а также конвертировать видеофайлы в другой формат.

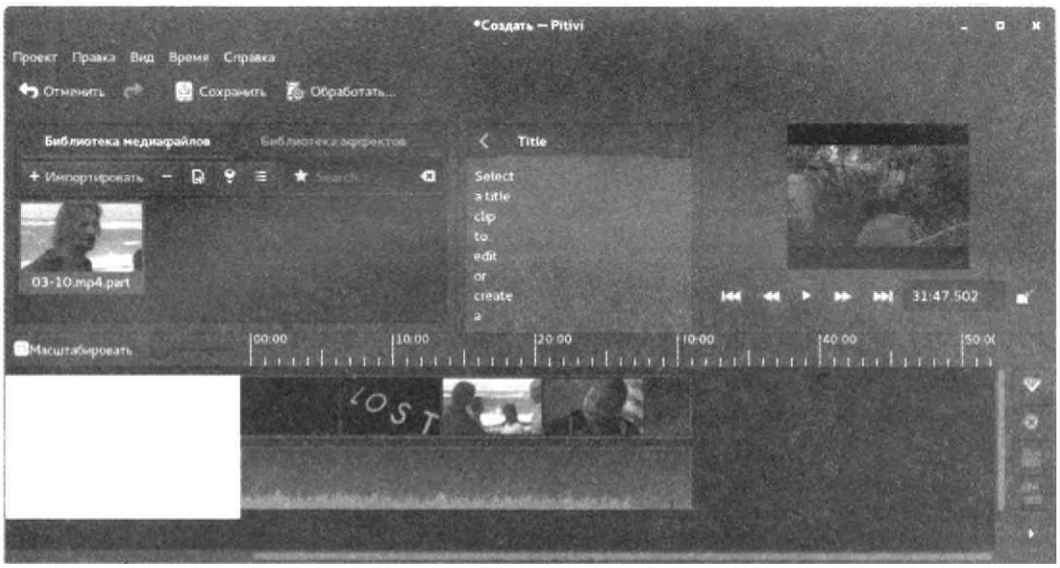


Рис. 22.7. **Интерфейс программы Pitivi**

Сайт tinyurl.com/zvw57rt содержит краткое руководство по программе Pitivi на русском языке.

- Видео (Video) — программа для просмотра видеофайлов, как доступных локально, так и размещенных во Всемирной паутине.
- Звуковыжималка (Sound Juicer) — простая программа для риппинга (копирования в цифровой формат) компакт-дисков аудио. К программе прилагается полное справочное руководство на русском языке.
- Traverso — мощная программа, специализация которой запись и редактирование аудиофайлов в многодорожечном режиме. Аудиофайлы можно копировать и перемещать, разрезать на части и обрабатывать по отдельности, изменяя длительность, регулируя громкость и накладывая эффекты. Многие команды выполняются прямо с клавиатуры, а для перемещения или копирования какого-либо фрагмента нет необходимости его перетаскивать, удерживая кнопку мыши. Благодаря такой системе управления большинство действий производится «в одно касание», что ускоряет работу с программой. Интерфейс программы доступен на английском и некоторых других европейских языках (рис. 22.8).

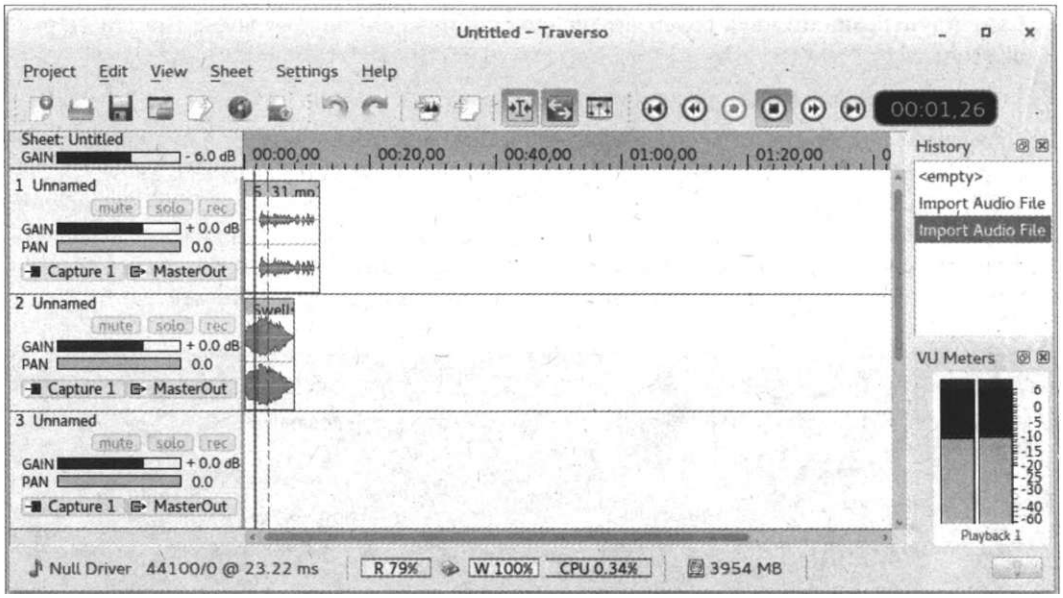


Рис. 22.8. Интерфейс программы Traverso

По адресу **tinyurl.com/zou3ypg** доступна полная инструкция по программе Traverso на английском языке.

Эти приложения могут быть запущены из меню **Приложения I Аудио и видео** (Applications I Sound & Video).

Чтобы хранить созданные аудио- и видеофайлы так, чтобы они были доступны вам и в последующих сеансах работы, в настройках зашифрованного хранилища должен быть установлен флажок **Personal Data** (Персональные данные) (см. *разд. «Настройки хранилища» главы 19).* При этом сохранять файлы необходимо в папку Persistent

Печать и сканирование

Для добавления/настройки принтера, а также управления заданиями на печать, выберите команду меню Приложения | Системные | Параметры (Applications | System Tools | Preferences) и в открывшемся окне щелкните мышью на значке Принтеры (Printers).

ПОДДЕРЖКА ПРИНТЕРА В LINUX

Проверить, поддерживается ли используемая вами модель принтера в Linux, можно на сайте tinyurl.com/bvrewcr.

Чтобы сохранить настройки принтера так, чтобы они были доступны вам и в последующих сеансах работы, в настройках зашифрованного хранилища должен быть установлен флажок Printers (Принтеры) (см. разд. *«Настройки хранилища» главы 19).*

Для сканирования документов и изображений операционная система Tails содержит приложение Простое сканирование (Simple Scan).

Для запуска программы выберите команду меню **Приложения | Графика | Простое сканирование** (Applications I Graphics | Simple Scan). Интерфейс приложения Простое сканирование (Simple Scan) показан на рис. 22.9.

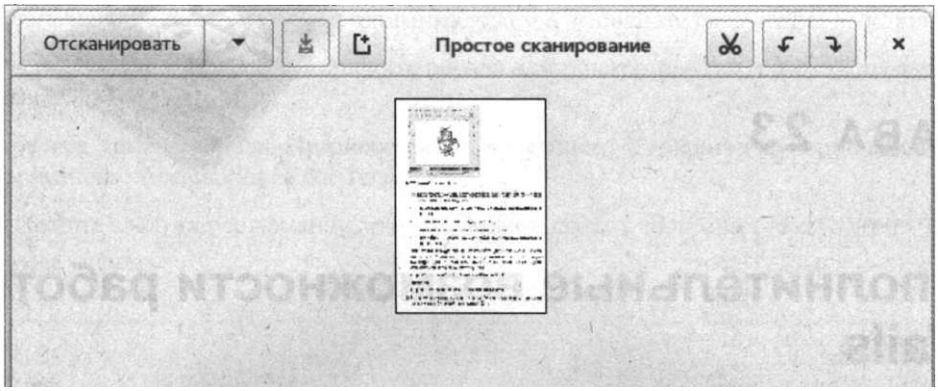


Рис. 22.9. Интерфейс программы Простое сканирование

ГЛАВА 23

Дополнительные возможности работы с Tails

Установка дополнительного программного обеспечения

Запуск Tails в виртуальной машине

Ресурсы в локальной сети

Беспроводные устройства

Некоторые известные проблемы и пути их решения

Эта глава посвящена возможностям установки в операционной системе Tails дополнительного программного обеспечения, работы в локальной сети, подключения беспроводных устройств, а также запуска Tails в программах виртуализации. В самом конце главы рассмотрены некоторые известные проблемы и пути их решения.

Установка дополнительного программного обеспечения

Операционная система Tails содержит согласованный, но ограниченный набор приложений. Вы можете установить в нее и дополнительные приложения, но только такие, которые упакованы специально для системы Debian. Для этого следует выполнить поиск приложений в каталоге пакетов Debian.

Пакеты, предустановленные в Tails, тщательно проверены на безопасность. Установка дополнительных пакетов может нести угрозу безопасности, выстроенной в Tails. Будьте осторожны, выбирая программное обеспечение для дополнительной установки.

Поскольку Tails направлена также на то, чтобы сделать вашу работу бесследной, установленные приложения не сохраняются после перезагрузки, и каждый дополнительный программный пакет понадобится переустанавливать в каждом сеансе работы. Для автоматизации установки выбранных пакетов программного обеспечения в начале каждого сеанса работы следует использовать функцию **Additional software packages** (Дополнительные программные пакеты) (см. *разд. «Настройки хранилища» главы 19).*

СЕТЕВЫЕ ПРИЛОЖЕНИЯ В TAILS

Программные средства, использующие подключение к Интернету, должны быть настроены на подключение через сеть Tor. В противном случае доступ к Интернету для них будет запрещен.

Для установки дополнительных программных пакетов выполните следующие действия:

1. При запуске системы Tails установите пароль администратора (см. *разд. «Пароль администратора» главы 19).*
2. Выберите команду меню Приложения | Системные | Терминал суперпользователя (Applications | Accessories | Root Terminal).
3. Выполните следующую команду, чтобы обновить список доступных пакетов (рис. 23.1):

```
apt-get update
```

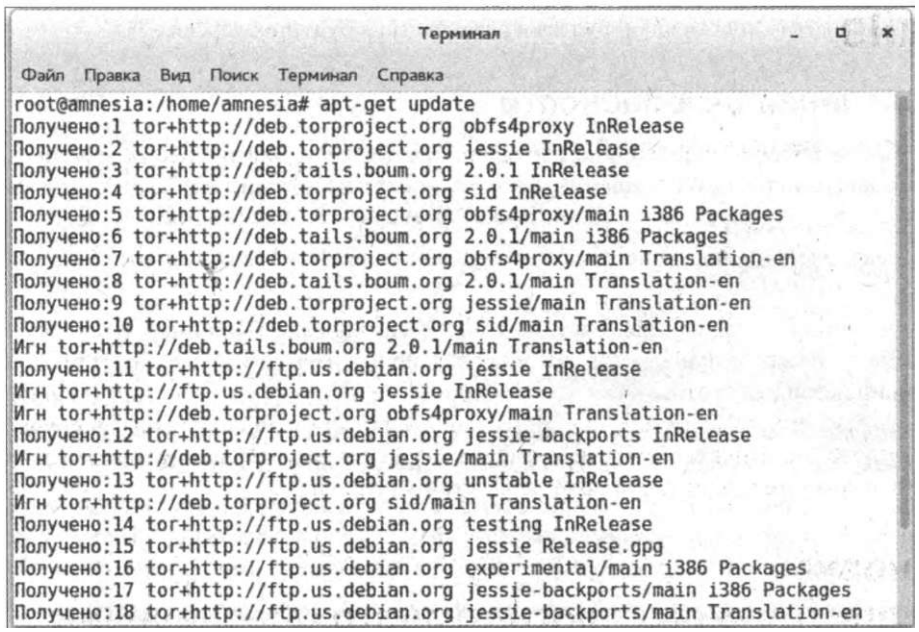


Рис. 23.1. Результат выполнения команды `apt-get update`

СПИСОК ПАКЕТОВ

Список пакетов с описаниями на русском языке доступен на сайте tinyurl.com/khw8wal.

4. Чтобы установить дополнительный пакет, выполните следующую команду, заменив слово *пакет* именем пакета, который вы хотите установить:

```
apt-get install пакет
```

   К примеру, чтобы установить приложение `ikiwiki`, выполните команду:

```
apt-get install ikiwiki
```

Вы также можете указать несколько названий пакетов через пробел, чтобы установить несколько приложений одновременно. Если пакет имеет зависимые компоненты, они будут установлены автоматически.

Запуск Tails в виртуальной машине

Иногда требуется запустить операционную систему Tails без перезагрузки компьютера. Это можно осуществить с помощью *виртуальных машин,* благодаря которым Tails запускается прямо внутри другой операционной системы (Linux, Windows или OS X). Виртуальная машина эмулирует операционную систему, называемую *гостевой,* которая отображается в окне *хостовой* операционной системы. Запустйв Tails в виртуальной машине, вы можете использовать большинство возможностей Tails совместно с хостовой системой без необходимости перезагрузки компьютера.

В настоящее время запуск виртуальной машины внутри операционной системы Tails невозможен. Такая возможность планируется к реализации в будущих версиях Tails.

Обеспечение безопасности

Запуск Tails в виртуальной машине нарушает некоторые требования ее безопасности. Поэтому, в зависимости от хостовой операционной системы и ваших требований к безопасности, запуск Tails в виртуальной машине может иметь нежелательные последствия.

- Хостовая операционная система и виртуальная машина способны отслеживать ваши действия в Tails.
- Если хостовая операционная система скомпрометирована (например, установлен программный кейлогер или другая вредоносная программа), то она может свести на нет функции безопасности Tails.

  Запускайте Tails в виртуальной машине, только если и хостовая операционная система, и программное обеспечение для виртуализации заслуживают доверия.
- Следы сеанса работы в Tails, скорее всего, останутся на локальном жестком диске. Например, хостовые операционные системы обычно используют файл *подкачки* (или пейджинг) на жестком диске, в который копируется часть содержимого оперативной памяти.

  Запускайте Tails в виртуальной машине, только если потенциальные следы вашей деятельности в Tails ни имеют для вас значения.

Учитывая наличие потенциальных проблем, при запуске Tails в виртуальной машине выводится соответствующее предупреждение.

Виртуальная машина с Tails не влияет на поведение хостовой операционной системы, а сетевой трафик не анонимизируется. Кроме того, к особенностям работы Tails в виртуальной машине следует отнести и то, что MAC-адрес сетевого оборудования компьютера не меняется при использовании функции спуфинга MAC-адресов.

Приложения виртуализации

Чтобы запустить Tails в виртуальной машине, в хостовой операционной системе необходимо установить соответствующее программное обеспечение. Здесь будет рассмотрено только бесплатное программное обеспечение, что является необходимым условием для обеспечения надежности. Наиболее распространены следующие четыре приложения для виртуализации:

- **VirtualBox** — приложение доступно в версиях для операционной системы Linux, Windows и OS X. В программе присутствуют возможности подключения внешних USB-устройств и использования зашифрованного хранилища;

- **VMware Workstation Player** — приложение доступно в версиях для 64-разрядной операционной системы Linux и Windows и также предоставляет возможности подключения внешних USB-устройств и использования зашифрованного хранилища;
- **Боксы (Boxes)** — приложение доступно в версии для Linux. Его отличает упрощенный пользовательский интерфейс и отсутствие поддержки использования зашифрованного хранилища;
- **Менеджер виртуальных машин (Virt-manager)** — приложение также доступно только для операционной системы Linux. Помимо возможности использовать зашифрованное хранилище, с помощью этой программы вы можете запускать операционную систему Tails с Flash-накопителя или SD-карты.

Что ж, выбор за вами.

VirtualBox

Программа VirtualBox распространяется бесплатно. Вы можете запустить операционную систему Tails в виртуальной машине VirtualBox на платформе Windows, Linux или OS X.

Рекомендуется запускать Tails в виртуальной машине, только если хостовая операционная система заслуживает доверия.

Операционные системы Microsoft Windows и OS X будучи проприетарным программным обеспечением, не могут считаться надежными. Запускайте Tails в виртуальной машине в среде Windows и OS X только в целях тестирования и не полагайтесь в таком случае на возможности обеспечения безопасности.

Установка VirtualBox

Для установки VirtualBox в среде Windows или OS X загрузите дистрибутив программы с сайта **tinyurl.com/5vgw4mp** и инсталлируйте ее, следуя указаниям мастера установки.

Для установки VirtualBox в среде Debian или Ubuntu в окне программы Терминал (Terminal) выполните следующую команду:

```
sudo apt-get install virtualbox
```

Запуск Tails из ISO-образа

1. Запустите программу VirtualBox.
2. Для создания новой виртуальной машины нажмите кнопку **Создать** (New) на панели в окне программы VirtualBox.
3. В открывшемся диалоговом окне (рис. 23.2) выполните следующие действия:
   - укажите любое название машины в поле **Имя** (Name);
   - в раскрывающемся списке **Тип** (Type) выберите пункт **Linux;**
   - в раскрывающемся списке **Версия** (Version) выберите пункт **Other Linux (32-bit);**
   - нажмите кнопку **Next** (Далее).
4. **В** окне выбора размера выделяемой оперативной памяти установите ползунковый регулятор в положение не менее **1024** Мбайт и нажмите кнопку **Next** (Далее).
5. В окне настройки жесткого диска установите переключатель в положение **Не подключать виртуальный жесткий диск** (Do not add a virtual hard drive) и нажмите кнопку **Создать** (Create).

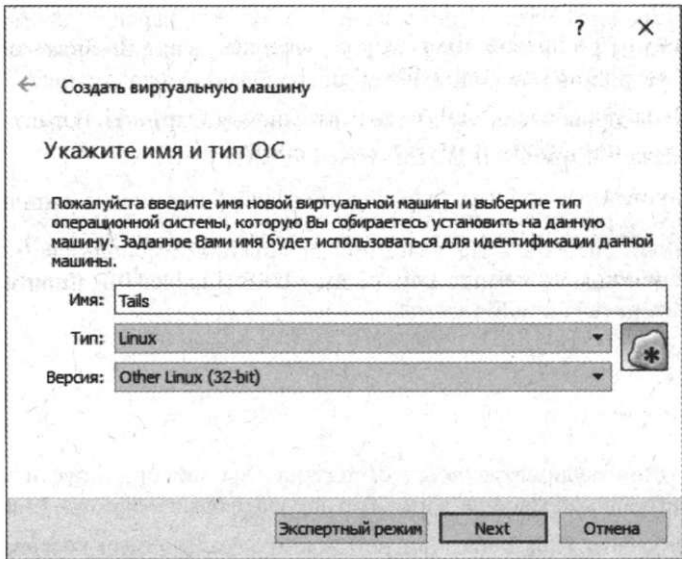


Рис. 23.2. Создание новой виртуальной машины

6. Нажмите кнопку Продолжить (Continue) в окне с предупреждением о запуске виртуальной машины без жесткого диска.

Виртуальная машина создана. Теперь нужно добавить в настройки образ системы Tails и, при необходимости, USB-накопитель для поддержки зашифрованного хранилища.

1. Выберите созданную виртуальную машину в левой части окна программы VirtualBox.
2. Для настройки созданной виртуальной машины нажмите кнопку **Настроить** (Settings) на панели в окне программы VirtualBox.
3. Перейдите на вкладку **Носители** (Storage) в левой части открывшегося окна.
4. Щелкните мышью на слове Пусто (Empty) ниже строки Контроллер: **IDE** (Controller IDE) в правой часта окна (рис. 23.3).

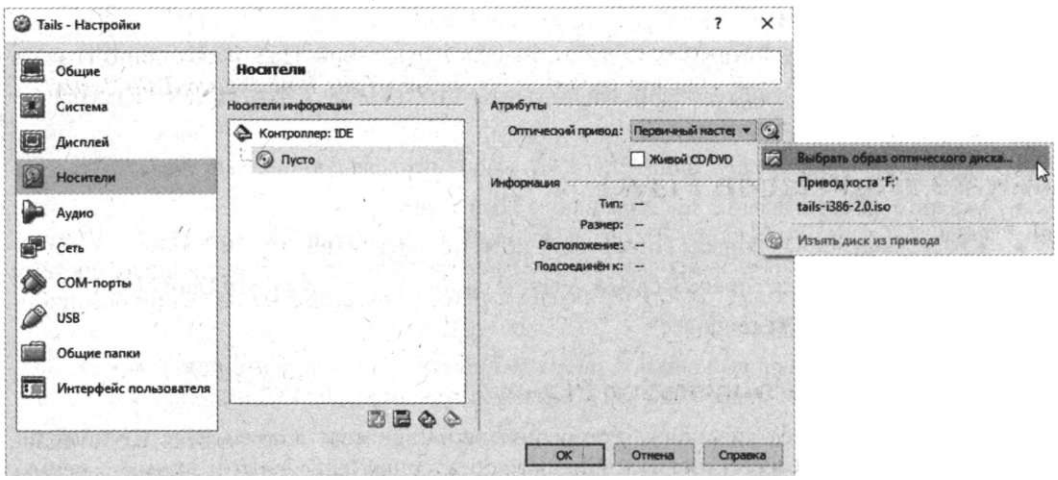


Рис. 23.3. Подключение ISO-образа в программе VirtualBox

5. Нажмите кнопку в правой части окна и выберите пункт **Выбрать образ оптического диска** (Choose a virtual CD/DVD disk file).
6. Выберите ISO-файл с образом Tails и нажмите кнопку **Открыть** (Open).
7. Установите флажок **Живой CD/DVD** (Live CD/DVD).
8. Теперь подключим USB-носитель для создания зашифрованного хранилища:
   - перейдите на вкладку **USB** в левой части окна **Настройки** (Settings);
   - установите флажок **Включить контроллер USB** (Enable USB Controller);

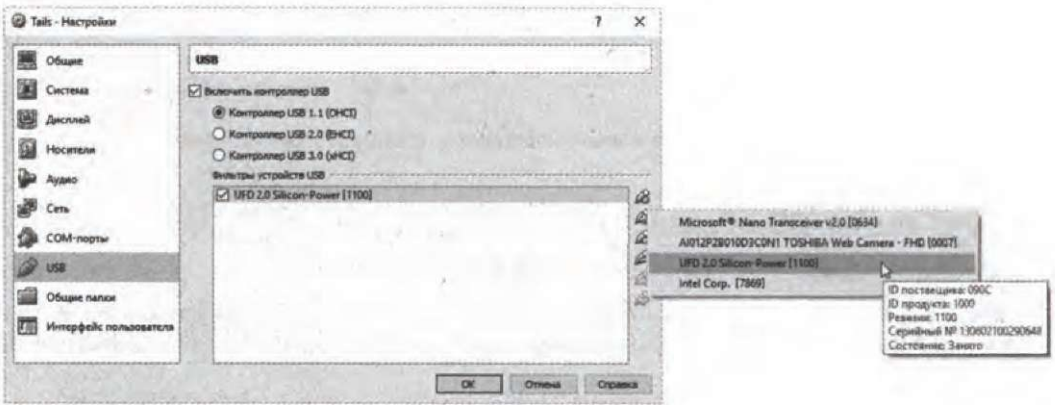


Рис. 23.4. Подключение USB-накопителя в программе VirtualBox

   - нажмите кнопку в правой части окна и выберите пункт с названием модели подключенного Flash-накопителя (Flash-накопитель должен быть уже подключен к компьютеру) — Flash-накопитель появится в списке устройств USB в окне **Настройки** (Settings).
9. Нажмите кнопку **ОК.**

Для запуска виртуальной машины -выберите ее в левой части окна программы и нажмите кнопку **Запустить** (Start).

Для поддержки зашифрованного хранилища из-под запущенной Tails необходимо создать Flash-накопитель с Tails, как описано в *разд. «Установка Tails с помощью Tails Installer» главы 19.*

VMware Workstation Player

Программа VMware Workstation Player, в отличие от ее старшего выпуска — VMware Workstation, распространяется бесплатно. Вы можете запустить операционную систему Tails в виртуальной машине VMware Workstation Player в 64-разрядной версии операционной системы Windows или Linux.

Установка VMware Workstation Player

Для установки VMware Workstation Player в среде Windows или Linux загрузите дистрибутив программы с сайта **tinyurl.com/cw4mno5** и инсталлируйте ее, следуя указаниям мастера установки. Существует много версий программы VMware Workstation, но вам нужно загрузить ее бесплатную версию по ссылке, показанной на рис. 23.5.

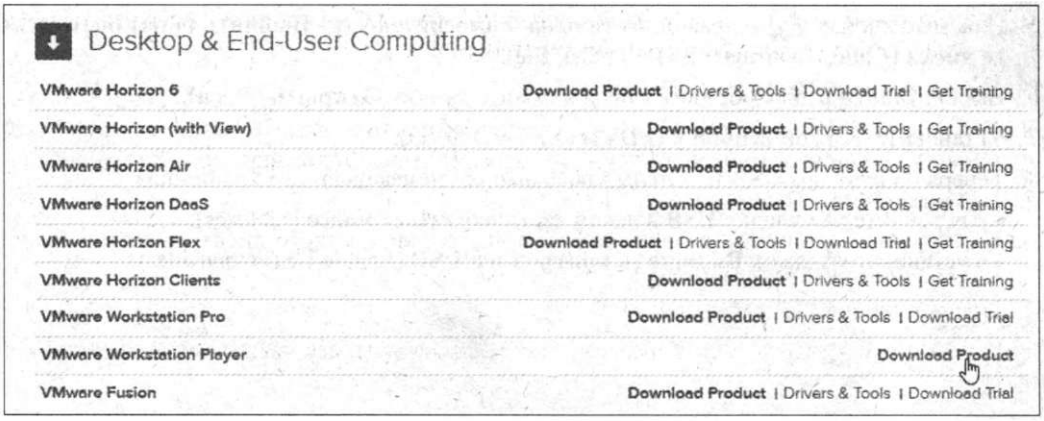


Рис. 23.5. Ссылка на скачивание программы VMware Workstation Player

Запуск Tails из ISO-образа

1. Запустите программу VMware Workstation Player.
2. Для создания новой виртуальной машины щелкните мышью на ссылке **Create a New Virtual Machine** (Создать новую виртуальную машину) в правой части окна программы VMware Workstation Player.
3. В открывшемся диалоговом окне (рис. 23.6) установите переключатель в положение **Installer disc image file (iso)** (Файл образа диска с инсталлятором) и нажмите кнопку Browse (Обзор).
4. Выберите ISO-файл с образом Tails и нажмите кнопку Открыть (Open).
5. Нажмите кнопку **Next** (Далее).

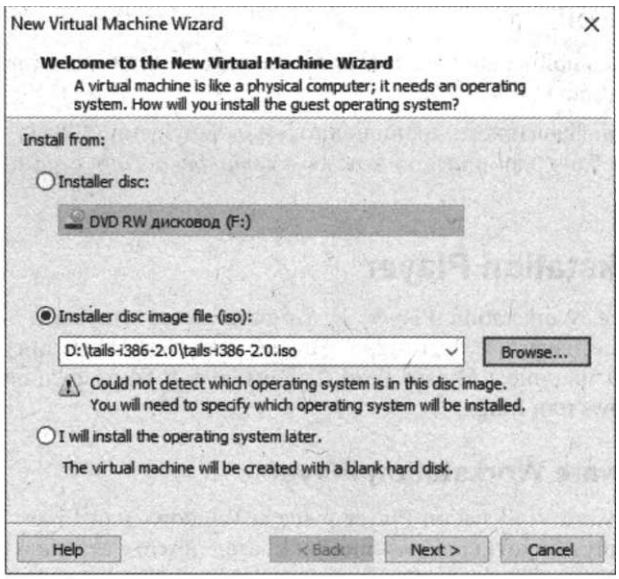


Рис. 23.6. Создание новой виртуальной машины

6. В следующем окне установите переключатель в положение Linux и в раскрывающемся списке Version (Версия) выберите пункт Debian 8.x.
7. Нажмите кнопку Next (Далее).
8. Укажите любое название машины в поле Virtual machine name (Название виртуальной машины) и при необходимости укажите расположение файлов виртуальной машины.
9. Нажмите кнопку Next (Далее).
10. В следующем окне, предназначенном для настройки жесткого диска, нажмите кнопку Next (Далее), не изменяя настроек.
11. Нажмите кнопку Finish (Готово).

Виртуальная машина создана. Теперь нужно настроить размер выделяемой оперативной памяти.

1. Выберите созданную виртуальную машину в левой части окна программы VMware Workstation Player.
2. Для настройки созданной виртуальной машины щелкните мышью на ссылке Edit virtual machine settings (Изменить настройки виртуальной машины) в правой части окна программы VMware Workstation Player.
3. На вкладке Memory (Память) установите, ползунковый регулятор в положение не менее 1024 Мбайт и нажмите кнопку OK (рис. 23.7).

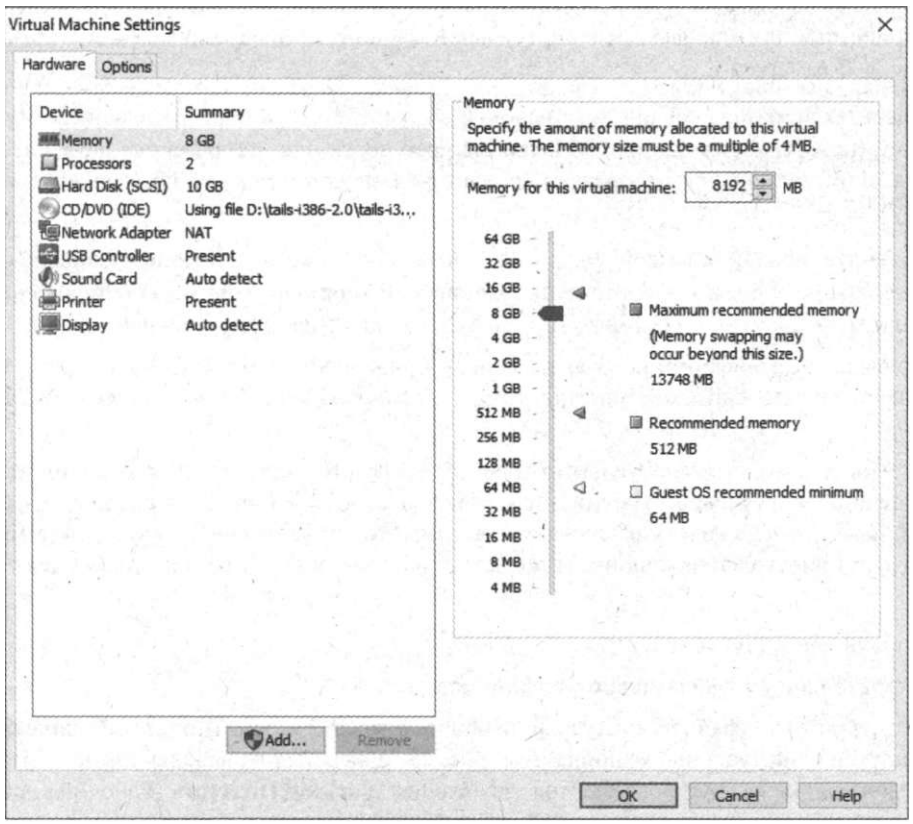


Рис. 23.7. Настройка размера выделяемой оперативной памяти

Теперь подключим USB-носитель для создания зашифрованного хранилища. Подключение USB-накопителя осуществляется во время запуска виртуальной машины. Сложность заключается в настройке запуска виртуальной машины с USB-накопителя, а не с виртуального жесткого диска. Это необходимо для поддержки зашифрованного хранилища.

1. Выберите созданную виртуальную машину в левой части окна программы VMware Workstation Player.
2. Для запуска созданной виртуальной машины щелкните мышью на ссылке Play virtual machine (Запустить виртуальную машину) в правой части окна программы VMware Workstation Player.

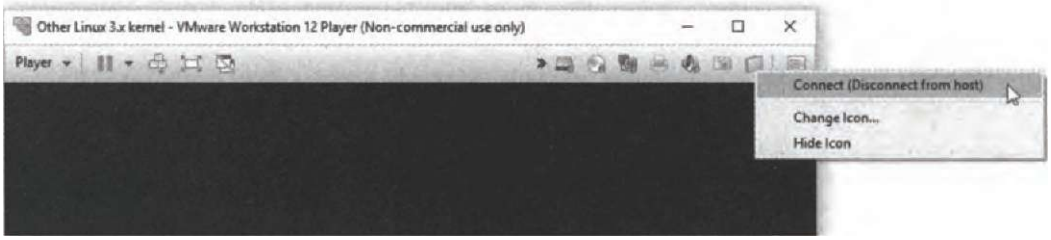


Рис. 23.8. Подключение USB-накопителя в программе VMware Workstation Player

В правом верхнем углу окна программы отображается ряд значков, соответствующих устройствам, подключаемым к виртуальной машине: приводу оптических дисков, принтеру, веб-камере и т. п.

3. Наведите указатель мыши на значок , соответствующий подключенному Flash-накопителю, и убедитесь, что во всплывающей подсказке отображается название нужного накопителя (значок отображается, если Flash-накопитель уже подключен к компьютеру).
4. Щелкните правой кнопкой мыши на значке соответствующем подключенному Flash-накопителю, и выберите пункт Connect (Disconnect from host) (Подключить (Отключить от хоста)) — Flash-накопитель будет подключен к виртуальной машине.

Для поддержки зашифрованного хранилища из-под запущенной Tails необходимо создать Flash-накопитель с Tails, как описано в *разд. «Установка Tails с помощью Tails Installer» главы 19.*

Далее, чтобы запустить виртуальную машину с Flash-накопителя, нужно настроить BIOS в запущенной виртуальной машине, как описано в *разд. «Запуск операционной системы Tails» главы 19.* Сложность заключается в том, что по умолчанию происходит мгновенная загрузка виртуальной машины и попасть в настройки BIOS не представляется возможным.

Для решения этой проблемы:

1. Откройте папку с файлами виртуальной машины.

   Увидеть каталог файлов виртуальной машины можно в окне Virtual Machine Settings (Настройки виртуальной машины) (см. рис. 23.7), перейдя на вкладку Options (Параметры) и взглянув на группу элементов управления Working Directory (Рабочий каталог).
2. Откройте файл с расширением vmx (рис. 23.9, *слева)* в любом текстовом редакторе.

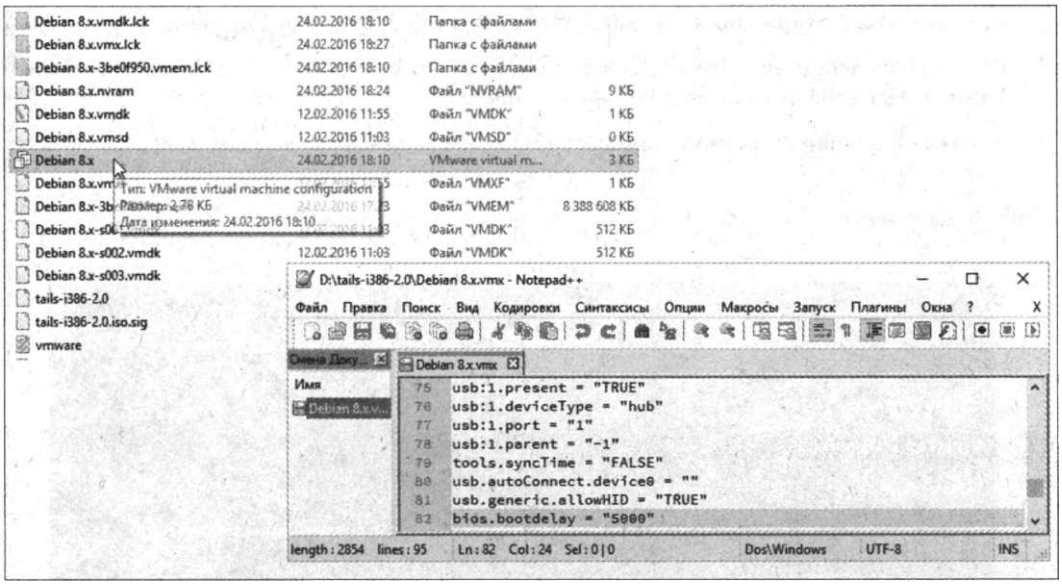


Рис. 23.9. Файл настроек виртуальной машины *(слева)* **и добавление опции** *(справа)*

3. Добавьте в конце файла строку

```
bios.bootdelay = "5000"
```

   Указанное в кавычках значение обозначает задержку запуска виртуальной машины в миллисекундах (в нашем примере 5 секунд).

Сохранив VMX-файл и запустив виртуальную машину, вы сможете зайти в настройки BIOS, как описано в *разд. «Запуск операционной системы Tails» главы 19.* Для входа в настройки BIOS в программе VMware Workstation Player следует нажать клавишу <F2> на экране, показанном на рис. 19.11.

Боксы

Приложение Боксы (Boxes) отличает упрощенный пользовательский интерфейс и отсутствие поддержки использования зашифрованного хранилища.

В нашем примере программа Боксы (Boxes) рассматривается в операционной системе Ubuntu.

Установка программы

Для установки программы Боксы (Boxes) в операционной системе Debian/Ubuntu в окне программы Терминал (Terminal) выполните следующую команду:

```
sudo apt-get install gnome-boxes
```

Запуск Tails из ISO-образа

1. Запустите программу Боксы (Boxes).
2. Нажмите кнопку Создать (New) в левом верхнем углу экрана.

3. Нажмите кнопку Продолжить (Next) для перехода к окну выбора источника
4. На вкладке Выбор источника (Source Selection) щелкните мышью на ссылке Выберите файл (Select a file) и выберите ISO-файл Tails.
5. В окне Предварительный просмотр (Review) нажмите кнопку Создать (Create) (рис. 23.10).

Виртуальная машина создана.

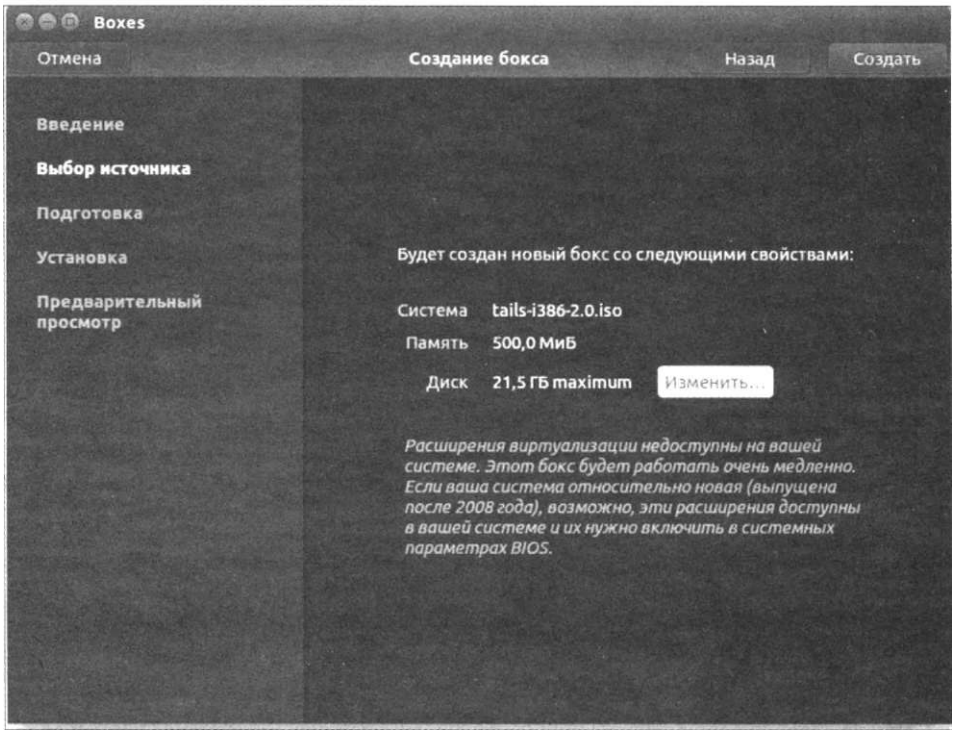


Рис. 23.10. Создание виртуальной машины в программе Боксы

Общий буфер обмена

Общий буфер обмена в программе Боксы (Boxes) используется по умолчанию. Эта функция может привести к тому, что конфиденциальные данные по ошибке будут скопированы из виртуальной машины в хостовую или наоборот. Рекомендуется отключить общий буфер обмена. Для этого выполните следующие действия:

1. Нажмите кнопку в правом верхнем углу окна программы Боксы (Boxes).
2. Перейдите на вкладку Экран (Display) в левой части окна программы.
3. Установите переключатель Общий буфер обмена (Share clipboard) в неактивное положение (рис. 23.11).
4. Нажмите кнопку |Q для возврата к экрану виртуальной машины.

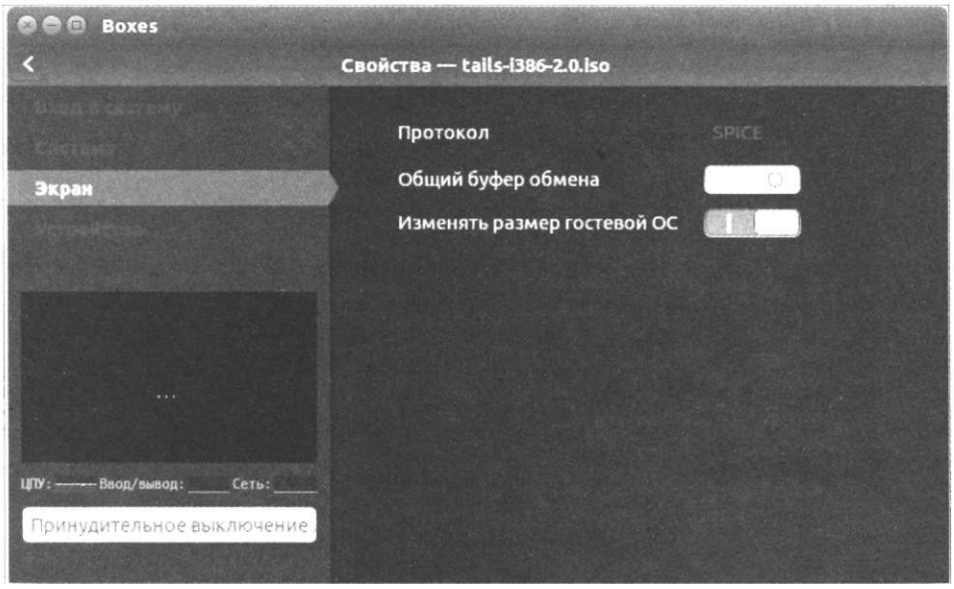


Рис. 23.11. Отключение общего буфера обмена в программе Боксы

Менеджер виртуальных машин

Менеджер виртуальных машин (Virt-manager) — бесплатное приложение виртуализации для операционной системы Linux. Помимо возможности использовать зашифрованное хранилище, с помощью этой программы вы можете запускать систему Tails с Flash-накопителя или SD-карты.

Программа Менеджер виртуальных машин (Virt-manager) основана на наборе инструментов виртуализации низкого уровня:

- KVM (Kernel-based Virtual Machine, Виртуальная машина, основанная на ядре) — программное решение, обеспечивающее виртуализацию в среде Linux;
- QEMU (Quick Emulator, Быстрый эмулятор) — свободная программа с открытым исходным кодом для эмуляции аппаратного обеспечения различных платформ;
- libvirt — свободная, кроссплатформенная библиотека управления виртуализацией;
- SPICE (Simple Protocol for Independent Computing Environments, простой протокол для независимой вычислительной среды) — протокол, используемый для просмотра виртуальной операционной системы не только на компьютере, на которой она запущена, но и через Интернет.

Менеджер виртуальных машин (Virt-manager) представляет собой графический интерфейс, позволяющий создавать, настраивать и запускать виртуальные машины.

В нашем примере программа Менеджер виртуальных машин (Virt-manager) рассматривается в операционной системе Ubuntu.

Установка программы

Для установки программы Менеджер виртуальных машин (Virt-manager) в операционной системе Debian в окне программы Терминал (Terminal) выполните следующую команду:

```
sudo apt-get install virt-manager libvirt-daemon-system
```

Для установки программы Менеджер виртуальных машин (Virt-manager) в операционной системе Ubuntu в окне программы Терминал (Terminal) выполните следующую команду:

```
sudo apt-get install virt-manager libvirt-bin qemu-kvm
```

Запуск Tails из ISO-образа

1. Запустите программу Менеджер виртуальных машин (Virt-manager).
2. Двойным щелчком щелкните на строке **localhost (QEMU),** чтобы подключиться к системе QEMU хоста (рис. **23.12).**

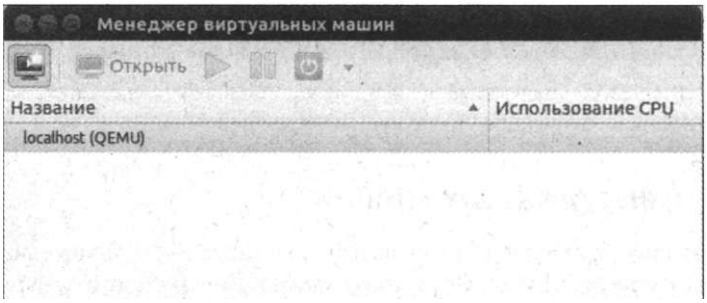


Рис. 23.12. Интерфейс программы Менеджер виртуальных машин

3. Чтобы создать новую виртуальную машину, нажмите кнопку
4. На шаге 1 введите любое название виртуальной машины и установите переключатель в положение **Установка с локального носителя (ISO-образ или CDROM)** (Local install media (ISO image or CDROM)).
5. На шаге 2 выполните следующие настройки (рис. 23.13):
   - установите переключатель в положение **Использовать ISO образ** (Use ISO image);
   - нажмите кнопку **Обзор** (Browse), затем кнопку **Локальный обзор** (Browse Local) и выберите файл ISO-образа Tails;
   - в раскрывающемся списке **Тип ОС** (OS type) выберите пункт **Linux;**
   - в раскрывающемся списке **Версия** (Version) выберите пункт **Debian Wheezy.**
6. На шаге 3 установите размер выделяемой оперативной памяти не менее 1024 Мбайт.
7. На шаге 4 сбросьте флажок **Включить хранилище для этой виртуальной машины** (Enable storage for this virtual machine).
8. На шаге 5 нажмите кнопку **Завершить** (Finish).

Виртуальная машина будет создана и автоматически запущена (рис. 23.14).

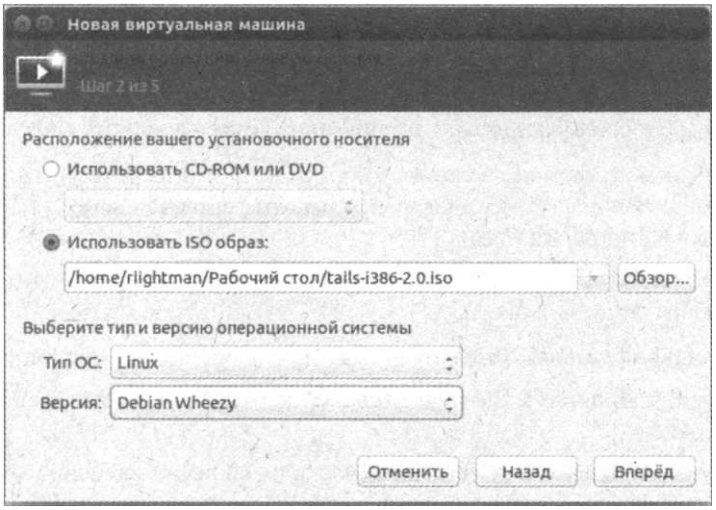


Рис. 23.13. Создание новой виртуальной машины

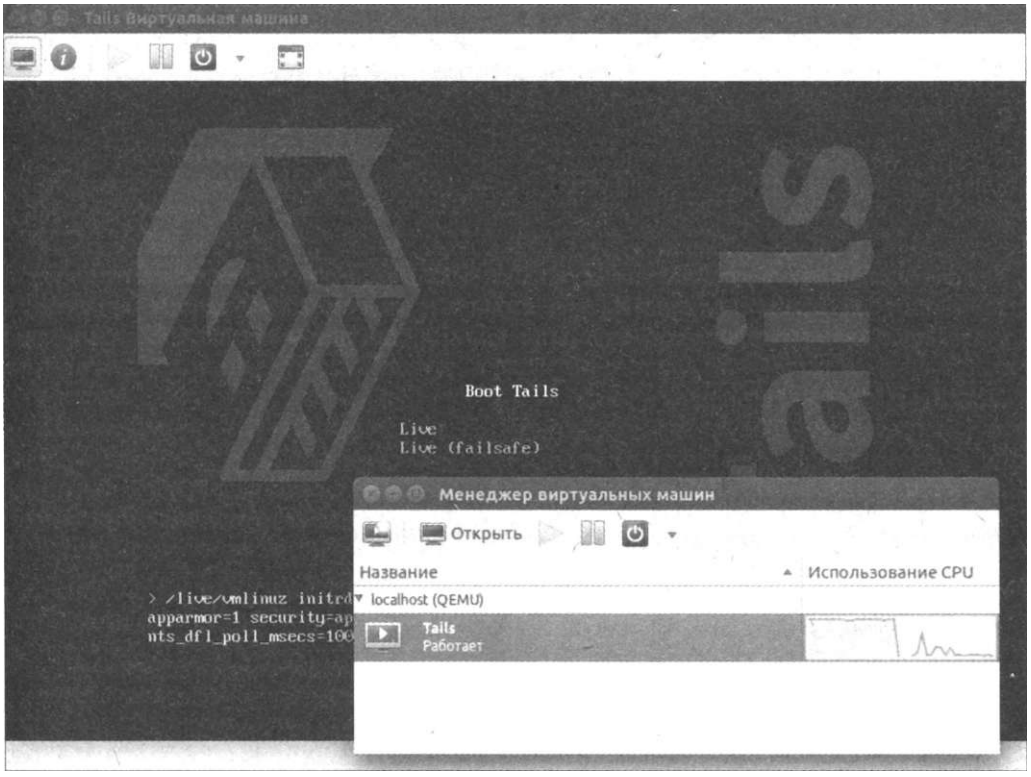


Рис. 23.14. Tails запущена в программе Менеджер виртуальных машин

Запуск Tails с USB- или SD-носителя

Для запуска операционной системы Tails с Flash-накопителя или SD-карты в программе Менеджер виртуальных машин (Virt-manager) сначала создайте виртуальную машину и запустите Tails из ISO-образа, как только что описано. Затем выполните следующие действия:

1. В окне виртуальной машины нажмите кнопку и выберите команду Выключить принудительно (Force Off) для завершения работы гостевой системы. Подтвердите операцию нажатием кнопки Да (Yes).
2. Подключите Flash-накопитель или вставьте в кардридер SD-карту, откуда будет запущена операционная система Tails.
3. В окне виртуальной машины нажмите кнопку для настройки гостевой системы.
4. Нажмите кнопку Добавить оборудование (Add Hardware) в левом нижнем углу открывшегося окна.
5. Выберите пункт USB Host Device в левой части окна, предназначенного для добавления устройства (рис. 23.15).



Рис. 23.15. Добавление USB-устройства в программе Менеджер виртуальных машин

6. В правой части окна щелкните мышью на USB-устройстве, с которого будет запускаться операционная система Tails, а затем нажмите кнопку Завершить (Finish).

Вы можете оставить ISO-образ подключенным к виртуальной машине для установки Tails на Flash-накопитель или SD-карту, если это необходимо. Также можно отключить ISO-образ и запустить Tails непосредственно с Flash-накопителя:

1. Завершите работу виртуальной машины.
2. В окне виртуальной машины нажмите кнопку для настройки гостевой системы.
3. В левой части окна настроек выберите пункт **IDE CDROM 1**.
4. Нажмите кнопку **Отключиться** (Disconnect) в правой части окна.
5. Для настройки загрузки с Flash-накопителя или SD-карты выполните следующие действия:
   - в левой части окна настроек выберите пункт **Boot Options;**
   - установите флажок **Включить меню загрузки** (Enable Boot Menu);
   - установите флажок **Floppy** для загрузки с USB-накопителя, добавленного ранее (рис. 23.16);
   - нажмите кнопку **Применить** (Apply).
6. Нажмите кнопку для запуска виртуальной машины.

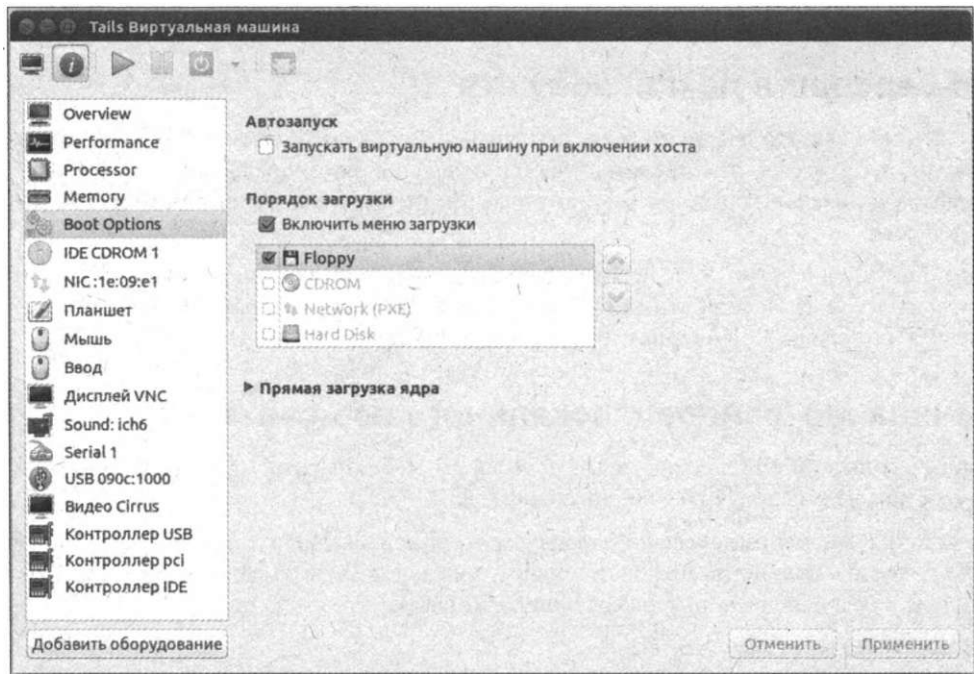


Рис. 23.16. Изменение настроек загрузки гостевой операционной системы

Загрузив систему Tails с USB-устройства, вы сможете создать и настроить зашифрованное хранилище.

Ресурсы в локальной сети

Термин «локальная сеть» в нашем случае определяет группу компьютеров и устройств, подключение к которым может быть осуществлено непосредственно с компьютера, минуя Интернет. Например, ваш домашний маршрутизатор, сетевой принтер или корпоративный Интранет, скорее всего, подключены к локальной сети.

Обеспечение безопасности при работе в локальной сети

Навыки доступа к ресурсам в локальной сети могут быть полезны в контексте Tails, например, для обмена документами с другими пользователями в той же локальной сети, минуя Интернет.

Но приложение, которое может подключаться как к интернет-ресурсам (через сеть Tor), так и к ресурсам в локальной сети (минуя Tor), может деанонимизировать вас, поскольку соединения в локальной сети не являются анонимными и не проходят через Tor.

Например, если сайт, который вы посещаете анонимно с помощью программы Tor Browser, также сможет подключаться к другим веб-страницам, которые специфичны для вашей локальной сети, то эта информация позволит определить ваше местонахождение. Именно поэтому из программы Tor Browser в Tails запрещен доступ к локальным сетям.

Здесь мы рассмотрим некоторые из мер безопасности для защиты от таких атак в Tails и разберемся, как получить доступ к ресурсам в локальной сети.

Веб-серфинг в локальной сети

Как уже было сказано, вы не сможете получить доступ к локальным веб-страницам из программы Tor Browser — так предотвращается появление потенциальных ассоциаций интернет-сайтов с локальными ресурсами, которые могут быть специфическими для вашей локальной сети.

Чтобы получить доступ к локальным веб-страницам, следует использовать вместо Tor Browser программу Небезопасный браузер (Unsafe Browser), которая может быть запущена из меню **Приложения | Интернет** (Applications | Internet).

Скачивание файлов с локального веб-сайта

Если вы скачиваете файлы с помощью программы Небезопасный браузер (Unsafe Browser), доступ к ним нельзя получить вне этого браузера.

Для загрузки файлов из локальной сети вы можете использовать команду `curl`. Например, чтобы загрузить документ, расположенный в локальной сети по адресу **http://192.168.L40/document.pdf,** нужно выполнить следующую команду:

```
curl http://192.168.1.40/document.pdf
```

Скачивание файлов с локального FTP-сервера

Для подключения к FTP-серверу в локальной сети используется команда **Места | Подключиться к серверу** (Places | Connect to Server).

Подключение беспроводных устройств

При запуске операционной системы Tails доступные устройства Wi-Fi, WWAN и WiMAX подключаются автоматически. Интерфейс Bluetooth в Tails также активируется по умолчанию, но среда GNOME не содержит инструментов для работы с ним.

Все другие типы беспроводных устройств, такие как GPS и FM, по умолчанию отключены. Если вы хотите использовать их, то вам необходимо их предварительно подключить. Описываемый здесь способ предусматривает использование командной строки.

1. При запуске системы Tails установите пароль администратора (см. разд. *«Пароль администратора» главы 19).*
2. Чтобы определить идентификаторы подключенных беспроводных устройств, выберите команду меню Приложения | Системные | Терминал суперпользователя (Applications | Accessories | Root Terminal) и выполните следующую команду:

   ```
   rfkill list
   ```

   К примеру, результат выполнения команды может быть следующим:

   ```
   0: phyO: Wireless LAN
    Soft blocked: no
    Hard blocked: no
   1: hciO: Bluetooth
    Soft blocked: no
    Hard blocked: no
   2: gpsO: GPS
    Soft blocked: yes
    Hard blocked: no
   ```

   Идентификатор устройства— это число, указанное в первой из трех строк описания устройства. В нашем примере Bluetooth-устройству присвоен идентификатор 1, а GPS-устройству — 2. В вашем случае значения могут быть иными.
3. Чтобы включить беспроводное устройство, выполните следующую команду в терминале суперпользователя, заменяя слово *номер* идентификатором, определенным на шаге 2:

   ```
   rfkill unblock [номер]
   ```

   Пример команды для выполнения:

   ```
   rfkill unblock 2
   ```

4. Чтобы убедиться, что беспроводное устройство включено, выполните команду `rfkill list` в терминале суперпользователя еще раз:

   ```
   rfkill list
   ```

   Результат должен быть похож на приведенный на шаге 2, но устройство, включенное на шаге 3, не должно определяться заблокированным. Например:

   ```
   0: phyO: Wireless LAN
    Soft blocked: no
    Hard blocked: no
   1: hciO: Bluetooth
    Soft blocked: no
    Hard blocked: no
   2: gpsO: GPS
    Soft blocked: no
    Hard blocked: no
   ```

Некоторые известные проблемы и пути их решения

Проблемы с запуском Tails

В заключительном разделе части, посвященной Tails, перечислены обнаруженные проблемы и пути их решения, если это возможно. Чтобы сообщить о проблеме, не указанной здесь, см. *разд. «Решение проблем запуска» главы 19.*

Проблемные Flash-накопители

Многие Flash-накопители производства SanDisk сконфигурированы как фиксированные (а не съемные) диски. Как следствие, требуется удаление загрузочной опции `live-media=removable`, что чревато последствиями (см. *разд. «Решение проблем запуска» главы 19).* Проблема подтверждена на следующих моделях накопителей:

- SanDisk Cruzer Edge 8GB
- SanDisk Cruzer Extreme USB 3.0 16GB, 32GB и 64GB
- SanDisk Cruzer Fit USB 2.0 8GB, 16GB, и 32GB
- SanDisk Cruzer Force 8GB
- SanDisk Cruzer Glide 4GB, 8GB и 16GB
- SanDisk Cruzer Switch USB 2.0 8GB и 32GB
- SanDisk Cruzer USB 3.0 64GB
- SanDisk Cruzer Blade 4GB, 8GB и 32GB
- SanDisk Cruzer Facet
- SanDisk Cruzer Orbiter 32GB (зависает во время установки, но беспроблемно загружается впоследствии)
- SanDisk Ultra 32 GB

Компания SanDisk начала производство Flash-накопителей в фиксированной конфигурации в 2012 году, чтобы удовлетворить требованиям к получению сертификата Windows 8, и завершила его в середине 2014 года. На упаковку Flash-накопителей, которые соответствуют этому сертификату, нанесен логотип Windows 8. Если логотип Windows 8 отсутствует, то накопитель будет работать в съемной конфигурации и поддерживать Tails в полном объеме.

Среди USB-накопителей других производителей проблемы возникают с устройствами Aegis Secure Key USB 2.0, которые во время загрузки могут блокироваться и запрашивать ПИН-код для разблокировки. Устройства Aegis Secure Key USB 3.0 вообще не позволяют запустить операционную систему Tails, и решения этой проблемы пока нет. Накопители Staples Relay USB 2.0 16GB могут вызывать проблемы, схожие с указанными ранее для устройств SanDisk. Накопители PNY USB могут провоцировать ошибки записи во время установки и загрузки Tails.

Проблемные компьютеры

Далее указаны модели компьютеров, при запуске Tails на которых выявлены проблемы:

- Acer Aspire 5315-ICL50 и Acer ES-1-331 — Tails не запускается с USB-накопителей, созданных с помощью Tails Installer;

- Compaq 615 — если Tails не запускается с USB-накопителей, созданных с помощью Tails Installer, необходимо обновить прошивку аппаратного обеспечения до последней версии;
- Fujitsu Siemens Amilo A 1667G — Tails не запускается с USB-накопителей, созданных с помощью Tails Installer;
- HP Pavilion dv7 — начиная с версии 1.3, операционная система Tails зависает на экране меню загрузки, независимо, установлена ли Tails вручную или с помощью утилиты Tails Installer;
- HP ProBook 4330s — если активен режим UEFI, при выборе устройства загрузки укажите сначала `Boot From EFI File`, а затем `Filesystem Tails` и `EFI/BOOT/bootx64.efi`;
- Lenovo IdeaPad-z585 — непрерывно возвращается к меню загрузки, если Tails запускается с DVD.

Компьютеры Mac

- На некоторых компьютерах Mac для успешного запуска Tails с Flash-накопителя требуется установка загрузчика rEFInd **(tinyurl.com/hk8q6kk).**
- На любом компьютере Mae с 32-битным интерфейсом EFI загрузка Tails с Flash-накопителя, созданного с помощью Tails Installer, может завершиться неудачей. Проверить разрядность интерфейса EFI, используемого в вашем компьютере Mae, можно по ссылке **tinyurl.com/7wwwedx.**
- На компьютерах MacBook Pro 5.5 операционная система Tails не загружается, если используется интерфейс UEFI.
- На компьютерах MacBook Pro 5.1 17" (NVidia GeForce 9400M) необходимо добавить загрузочную опцию `nouveau.noaccel=1` для правильного вывода изображения на экран.
- На компьютерах MacBook Air 3.2 (A1369 EMC 2392) операционная система Tails зависает при загрузке, если используется интерфейс UEFI.
- На компьютерах MacBook Pro (ранее 2011) загрузка Tails с DVD заканчивается неудачей.
- На компьютерах Mac Pro Tower (ранее 2008), MacBook Pro 4.1 (ранее 2008) и MacBook Pro 8.2 (позднее 2011) загрузка Tails с Flash-накопителя, созданного с помощью Tails Installer, может завершиться неудачей.

Компьютеры с переключаемыми графическими картами

На некоторых моделях компьютеров с переключаемыми графическими картами (например, по технологии Optimus) попытка выбора видеокарты приводит к сбою и отображению черного экрана. Эта проблема замечена на компьютерах MacBook Pro 6.2, MacBook Pro 10.1 Retina, MacBook Pro 15-дюймовый (ранее 2011) и др.

Существует два возможных решения проблемы:

- на компьютерах Mae можно применить приложение gfcCardStatus (gfx**.io),** чтобы принудительно использовать встроенную в OS X графику. После перезапуска операционная система Tails должна запускаться;
- пользователи Linux могут выполнить следующее:
  1. Добавить опцию `i915.modeset=0 rootpw=pass` в меню загрузки.
  2. Создать файл /etc/X11/xorg.conf.d/switchable.conf со следующим содержимым:

```
Section "Device"
         Identifier "DeviceO"
         Driver "nouveau"
         BusID "1:0:0"
EndSection
```

3. Выполнить перезагрузку с помощью команды:

```
service gdm3 restart
```

4. После загрузки интерфейса GNOME использовать команду:

```
sudo passwd
```

Архитектура ARM, Raspberry Pi и планшеты

По настоящее время операционная система Tails доступна только для архитектур x86 и x86-64. Raspberry Pi и многие планшеты основаны на архитектуре ARM, которую система Tails не поддерживает.

Обратите внимание на планшеты с процессором AMD или Intel. Заранее протестируйте выбранную модель на совместимость с Debian, чтобы убедиться, что поддерживается, к примеру, интерфейс Wi-Fi.

Передача Tails другому загрузчику

Чтобы решить проблему загрузки Tails на ноутбуках с интерфейсом UEFI, можно попробовать использовать другой загрузчик, функционирующий на этом компьютере, — например, GRUB. Будьте осторожны, чтобы не изменить все опции исходного загрузчика. Вам пригодятся следующие команды,.выполняемые из оболочки GRUB:

```
set root=(hdl)
chainloader +1
boot
```

Проблемы с Wi-Fi

Интерфейс Broadcom Wi-Fi

Некоторые интерфейсы Wi-Fi компании Broadcom, чтобы беспроводная связь работала в Tails, требуют установки драйвера wl, предоставляемого в Debian пакетом `broadcom-sta-dkms`. Драйвер wl не предустановлен в операционной системе Tails, т. к. является проприетарным.

Чтобы определить, требуется ли для работы интерфейса Wi-Fi установка драйвера wl:

1. Выполните следующую команду в окне программы Терминал (Terminal):

```
lspci -nn I grep Network
```

2. Проверьте, указано ли ваше устройство в списке на странице **tinyurl.com/nxffyzw.** Если устройство указано в списке поддерживаемых устройств, вы не сможете использовать карту Wi-Fi в Tails.

Интерфейс Broadcom BCM43224 802.11a/b/g/n

Интерфейс Wi-Fi Broadcom Corporation BCM43224 802.1 la/b/g/n не позволяет подменить его MAC-адрес. Этот сетевой интерфейс используется, к примеру, в ноутбуках MacBook Air 4.1,4.2, 5.1 и 5.2.

В операционной системе Tails режим спуфинга MAC-адресов включен по умолчанию, и его отключение приведет к использованию реальных MAC-адресов у всех сетевых устройств. Чтобы заставить работать описываемый интерфейс, необходимо отключить функцию спуфинга MAC-адресов (тщательно изучите *разд. «Спуфинг MAC-адресов» главы 19* на предмет потенциальных последствий).

Проблемы безопасности

Tails не стирает содержимое памяти после завершения работы

На некоторых (редко встречающихся) компьютерах (без поддержки режима PAE и с большим объемом установленной оперативной памяти) система Tails не удаляет все содержимое оперативной памяти должным образом.

Если атака методом холодной перезагрузки не была осуществлена непосредственно после завершения работы, содержимое оперативной памяти очищается за несколько минут, и все данные уничтожаются.

Tails не стирает содержимое видеопамяти

Система Tails не стирает содержимое видеопамяти. Если после использования Tails выполнить перезагрузку и загрузить компьютер в другой операционной системе, в ней можно получить доступ к содержимому видеопамяти, хранящей данные из сеанса работы с Tails.

Для решения проблемы вместо перезагрузки рекомендуется полностью выключать компьютер, чтобы удалить содержимое видеопамяти.

Не работает экстренное завершение работы

При установке Tails с помощью Tails Installer на некоторых USB-накопителях не работает функция экстренного завершения работы Tails путем удаления устройства. В этом случае вы можете использовать команду перезагрузки Tails.

Ошибка выброса DVD с Tails

Нажатие кнопки выброса DVD может не приводить к экстренному завершению работы Tails. Кроме того, в некоторых случаях обычное (не экстренное) завершение работы Tails не приводит к выбросу DVD.

Не выполняется полная перезагрузка/выключение Tails

При завершении работы Tails на некотором аппаратном обеспечении процедура стирания содержимого оперативной памяти завершается неудачей: на экране отображается сообщение о завершении работы, но компьютер полностью не выключается или не перезагружается. Иногда мигает индикатор клавиши <Caps Lock> на клавиатуре.

В этой ситуации нет никакой гарантии, что содержимое оперативной памяти полностью стерто. Эта проблема была зафиксирована на следующих устройствах:

- **На компьютерах Mac** при загрузке **с** Flash-накопителя:
  - MacBook Air 5.1
  - MacBook Air 5.2 (если накопитель создан при помощи Tails Installer)
  - MacBook Air 6.2
  - MacBook Pro 7.1 13-дюймовый (середина 2010)
  - MacBook Pro 9.2 13-дюймовый (середина 2012)
  - MacBook Pro 8.1 13-дюймовый (позднее 2011)
  - MacBook Pro 10.2
  - MacBook Pro Retina 11.1 (позднее 2013)
  - MacBook Pro Retina 13-дюймовый (ранее 2015)
- Hewlett-Packard HP ENVY x360
- Hewlett-Packard HP Pavilion dv6
- Hewlett-Packard HP ProBook 450 GO
- Lenovo ThinkPad X61, только при экстренном завершении работы — отключении Flash-накопителя
- Lenovo ThinkPad X220
- Toshiba Satellite C855D
- Dell Inc. Studio 1458
- Fujitsu Lifebook AH531/GFO, при обычном завершении работы, при экстренном нет проблемы
- Samsung N150P
- Acer Aspire e1 -5 72
- Dell Latitude E6230
- Microsoft Surface Pro 3

Прочие проблемы

Контент в формате Adobe Flash не отображается

Программное обеспечение Adobe Flash Player не предустановлено в операционной системе Tails по нескольким причинам:

- это проприетарное программное обеспечение, которое не позволяет нам добавить его в Tails;
- это программное обеспечение с закрытым исходным кодом, и поэтому нет ни малейшего представления о том, как оно на самом деле функционирует;
- оно имеет очень долгую историю обнаружения и исправления серьезных уязвимостей;
- оно, как известно, может нарушать неприкосновенность с помощью таких технологий, как локальные общие объекты (flash-cookie);
- корпорация Adobe для платформы GNU/Linux выпустила плагин только для браузера Google Chrome.

В качестве альтернативы вы можете просматривать HTML5-видеоконтент в программе Tor Browser.

Пользовательские настройки системы не сохраняются

Пользовательские настройки системы — такие как язык интерфейса, раскладки клавиатуры, фоновое изображение, положение панели инструментов, настройки браузера, настройки тачпада и т. д., не сохраняются.

По умолчанию система Tails не сохраняет никаких данных между сеансами работы. Только зашифрованное хранилище позволяет повторно использовать одни и те же данные в различных сеансах работы (см. *разд. «Зашифрованное хранилище» главы 19).*

Утерян пароль для доступа к зашифрованному хранилищу

Для шифрования содержимого хранилища используется очень стойкий шифр, и восстановить пароль для доступа к зашифрованному хранилищу невозможно.

Скачивание файлов по протоколу BitTorrent

В системе Tails не предустановлено программное обеспечение для поддержки протокола BitTorrent и не планируется его использование в будущем. Две основные проблемы использования протокола BitTorrent в сети Tor заключаются в том, что такую поддержку технически сложно реализовать должным образом, и подобная нагрузка будет негативно сказываться на производительности сети.

Скачивание видеофайлов из Интернета

Чтобы скачивать видеоролики из Всемирной паутины, вы можете установить дополнительный пакет youtube-dl/jessie. С его помощью можно загружать видеоролики свыше 700 вебсайтов.

К примеру, чтобы скачать видеоролик с сайта YouTube, в окне программы Терминал (Terminal) надо выполнить следующую команду:

```
torsocks youtube-dl "https://www.youtube.com/watch?v=JWII85UlzKw"
```

Дополнительную информацию можно получить из документации на официальном сайте проекта по адресу **tinyurl.com/pkl9ca9.**

Сложности обмена файлами в браузере I2P

По умолчанию нет возможности получить доступ к локальным файлам из браузера I2P, но вы можете сделать это с правами администратора из командной строки. Домашний каталог браузера **I2P** расположен по адресу **/var/lib/i2p-browser/chroot/home/i2pbrowser/.**

Возможно, вам придется проверить права доступа к файлам, к которым вы хотите получить доступ из браузера I2P. Права доступа должны отвечать двум критериям:

- они должны принадлежать пользователю `i2pbrowser`, чтобы быть доступными из браузера I2P;
- они должны принадлежать пользователю `amnesia`, чтобы быть доступными за пределами браузера I2P.

Проблемы отображения меню загрузки

На некоторых устройствах, (например, ThinkPad X230 и MacBook Pro 8.1) меню загрузки не отображается должным образом. Тем не менее, операционная система Tails запускается без ошибок.

Bluetooth-устройства не работают

Интерфейс Bluetooth отключен в системе Tails по причинам обеспечения безопасности. Для включения интерфейса см. *разд. «Подключение беспроводных устройств»* ранее в этой главе.

Сбой применения раскладки клавиатуры

Раскладка клавиатуры, выбранная в окне Tails Greeter, в некоторых случаях не применяется и сбрасывается на значение **English (US).** Щелкните мышью на кнопке раскладки клавиатуры на навигационной панели в верхней части экрана и выберите нужную раскладку.

Tails не загружается после обновления

В некоторых случаях после завершения процесса автоматического обновления система Tails прерывает загрузку сразу после сообщения **'Loading, please wait...'.**

Для решения этой проблемы попробуйте обновить систему Tails в ручном режиме. Обратите внимание, что при этом ваше зашифрованное хранилище будет сохранено.

Сбой предварительного просмотра печати в Tor Browser

Из-за бага в коде браузера Firefox инструмент предварительного просмотра печати несовместим с технологией защиты AppArmor, реализованной в программе Tor Browser в операционной системе Tails, и отображает серый экран вместо отпечатка.

Существует способ решить проблему. В окне предварительного просмотра вы можете нажать кнопку **Печать** (Print) и выбрать пункт **Print to File** (Печать в файл), чтобы сохранить документ в виде PDF-файла. Затем вы можете открыть этот PDF-файл в соответствующей программе.

Замедление графики на некоторых картах NVidia

Могут наблюдаться некоторые замедления графики на компьютерах, оборудованных видеокартами серии NVIDIA GeForce 900, — такими как GeForce GTX 960.

На момент выхода книги (после перевода Tails на более новую версию ядра Linux) проблема, вероятно, будет решена.

ПРИЛОЖЕНИЯ

Приложение 1.	**Даркнет: подполье Интернета**
Приложение 2.	**Варез и Сцена**
Приложение 3.	**Компьютерное искусство**
Приложение 4.	**Получение инвайтов на закрытые сайты (на примере** *What.cd)*
Приложение 5.	**Краткий глоссарий терминов пользователя**

В заключительной части этой книги собраны приложения, содержащие разнообразную информацию для расширения вашего кругозора. *Приложение 1* посвящено Даркнету как явлению в мире интернет-коммуникаций. *Приложение 2* рассказывает о варезной Сцене, релизных группах и обо всем, касающемся нелицензионного использования контента. *Приложение 3* вкратце познакомит вас с компьютерным искусством —• вы узнаете, что «крэки» умеют звучать, а хакеры творить. *Приложение 4* рассматривает процесс получения инвайтов в закрытые клубы по интересам на примере популярного музыкального трекера \У11а1.с{1. На этом трекере и подобным ему можно найти много контента, недоступного в «обычной» Всемирной паутине. *Приложение 5* содержит глоссарий терминов.

ПРИЛОЖЕНИЕ 1

Даркнет: подполье Интернета

Глубинная Паутина и Даркнет
Доступ к Даркнету
Анонимная мобильность
Аудитория Даркнета
Черные рынки Даркнета
Криптовалюты
Реакция властей на Даркнет
Заключение

Этот материал подготовлен по материалам сайта компании BatBlue The Cloud Security Company, batblue.com.

Глубинная Паутина и Даркнет

Как известно, Всемирная паутина — это лишь верхушка айсберга. А к подводной его части относятся Глубинная Паутина (Deep Web) и, в частности, Даркнет (Darknet).

Даркнет — это та часть Интернета, в которой люди могут оставаться анонимными. В отличие от привычной Всемирной паутины, или так называемого «чистого Интернета», сайты в котором индексируются поисковыми системами типа Яндекс или Google, ресурсы в Даркнете не индексируются, а для доступа к ним необходимо специальное программное обеспечение, зачастую оснащенное механизмами обеспечения анонимности, такими как Tor, но есть и другие способы попасть в эту сеть, — например, через форумы, защищенные паролями и требующие авторизации по приглашениям.

В Даркнете присутствуют как злоумышленники и преступники, продающие наркотики и оружие, публикующие порнографию и хакерские программы, так и обычные люди, которые пользуются им во вполне законных целях: для того, чтобы избежать государственной цензуры в странах с репрессивными режимами и для анонимного общения с журналистами. К примеру, одним из таких сайтов является небезызвестный WikiLeaks.

В Даркнете действуют сотни тысяч сайтов, и точное их количество определить невозможно. Они постоянно закрываются, переезжают на новый адрес, открываются и новые. Интернет-

сайты Даркнета расположены на серверах, местоположение которых шифруется через VPN-сети, в результате чего сайты в Даркнете чрезвычайно сложно закрыть.

ДАРКНЕТ И ГЛУБИННАЯ ПАУТИНА

Даркнет (Darknet) и Глубинную Паутину (Deep Web) часто считают синонимами, хотя это не совсем так. Глубинная Паутина — это весь контент в Интернете, включая ресурсы Даркнета (к примеру, onion, I2P и eepsite) и обычные веб-сайты, который не индексируется поисковыми системами. Например, персональная часть контента на Facebook относится к Глубинной Паутине, потому что многие пользователи устанавливают такие настройки приватности, при которых страница видна только друзьям. К Глубинной Паутине относится много веб-сайтов, доступ к которым защищен паролем или требует приглашения (например, сайт What.cd), или содержащих документы в таких форматах, которые нельзя индексировать. В этом смысле Даркнет — часть Глубинной Паутины, но Глубинная Паутина — это гораздо более широкое понятие, чем Даркнет.

Доступ к Даркнету

Для доступа к части Даркнет-ресурсов используется уже не раз упомянутая в этой книге сеть Tor, которая скрывает данные о пользователях и позволяет им «бродить» по Интернету, не раскрывая свою личность. Эту технологию разработала исследовательская лаборатория Разведывательного управления ВМС США в середине 1990-х, чтобы скрывать обмен данными. На условиях свободной лицензии релиз Tor состоялся в 2004 году. Когда пользователь путешествует по Всемирной паутине с помощью программы Tor Browser, его данные в зашифрованном виде пересылаются через цепочку случайных прокси-серверов Tor, прежде чем они достигнут своего назначения. В результате отследить трафик, который еще нужно расшифровать, становится практически невозможно. С помощью Tor также можно получить доступ к скрытым сервисам, сайтам и приложениям, которые являются частью Даркнета и обычными средствами (браузерами) недоступны. Для имен скрытых сайтов используется строка внешне не связанных друг с другом символов, которую замыкает доменное имя .onion. На эти скрытые сайты могут попасть только пользователи сети Tor.

Попасть в Даркнет относительно несложно — сложно находить в нем ресурсы: сначала нужно скачать программу Tor Browser, затем ввести в нее адрес ресурса или найти сайт-каталог в доменной зоне .onion. Поскольку сайты в доменной зоне .onion скрыты и не выдаются в результатах поисковых машин, путешествовать по Даркнету весьма трудно. Существуют, правда, каталогизаторы ссылок, наподобие Hidden Wiki, или сайты типа DuckDuckGo и Grams, максимально близкие к «поисковым системам», но ссылки на этих сайтах часто оказываются недействительными или устаревшими.

При пользовании Даркнетом важно соблюдать осторожность и воздерживаться от скачивания каких-либо материалов. Ссылки могут вести на нужный сайт, но могут перенаправить вас и на сайт, на котором продается нечто незаконное или шокирующее. К тому же материалы там могут оказаться экстремистскими или пиратскими, а их наличие на вашем компьютере будет нарушением закона, лежащим тяжелым грузом на вашей совести.

Анонимная мобильность

Самая привлекательная черта Даркнета — это анонимность. Помимо нее Даркнет предлагает и высокую мобильность. Вместо обычной статичной системы доменных имен (DNS) традиционного Интернета здесь используется динамический процесс, при котором сайты Даркнета обновляют сеть Tor. Более того, традиционный процесс получения доменных

имен через регистры заменен на самостоятельно генерируемые адреса с парами открытых/закрытых ключей.

Открытый ключ используется для генерации цепочки из шестнадцати случайных символов (односторонняя математическая операция, в результате которой создается привязка к открытому ключу), которую завершает доменное имя **.onion.** Вот пример такого значения (хеша): **batblue4y5flmoji.onion.** Подобные значения используются в качестве адресов для доступа к скрытым сервисам, точно так же, как «полностью определенное имя домена» (FQDN) служит для доступа к ресурсам традиционного Интернета, — например, **www.googIe.com.** Когда вы заходите на сайт, происходит обмен ключами, в результате которого создается канал для обмена данными с криптографической защитой. Поскольку используется сквозное шифрование, обычные средства взлома не могут отслеживать обмен такими данными, и их эффективность снижается до минимума.

Для создания адресов в зоне **.onion** существуют специальные инструменты, такие как **Shallot** и **Eschalot.** С их помощью генерируются пары открытых/личных ключей и хеш **.onion.** Теоретически злоумышленники могут с помощью тех же самых инструментов попытаться организовать обратное преобразование адреса определенного сайта из зоны **.onion.** Однако, принимая во внимание существующие на сегодняшний день вычислительные ресурсы, это весьма маловероятно. Так, сегодня на воссоздание символов в адресе из зоны **.onion** понадобится несколько миллионов лет (если в хеше 14 и более символов). Сомнительно также, что разработчики Tor будут пытаться вычислить или заблокировать определенные сайты в зоне **.onion,** поскольку это повредит безопасности всего сервиса, — никогда такого не происходило, и маловероятно, что произойдет в ближайшем будущем.

Когда сайт регистрируется в сети Tor, весь трафик перенаправляется на него, как положено, независимо от его местоположения, что делает сайты в зоне **.onion** очень мобильными и доступными по запросу. Например, можно установить Tor-клиент на ноутбук и сделать его сервером. Этот ноутбук можно принести с собой, к примеру, в кофейню и подключить к общедоступной сети Wi-Fi.

Платформа скрытых сервисов обеспечивает мобильность и тем, кто пользуется контентом или услугами, и тем, кто их предоставляет. Ресурсы Tor могут обслуживаться и предоставлять обслуживание в любое время, из любой точки, что делает эту анонимную платформу очень мобильной и универсальной.

Аудитория Даркнета

Аудиторию и секторы Даркнета иллюстрирует рис. П1.1.

Неясные для читателя названия категорий хакеров расшифровываются следующим образом:

- «скрипт кидди» — неопытные хакеры, пользующиеся чужими эксплойтами и программами;
- «Белая шляпа» — эксперт в области компьютерной безопасности, который старается защитить системы от взлома (так сказать, «добрый» хакер);
- «Черная шляпа» — злоумышленник, атакующий компьютерные системы («плохой» хакер);
- «Серая шляпа» — хакер как атакующий, так и защищающий системы.

Хакером в серой шляпе можно считать хакера в белой шляпе, который иногда одевает черную для достижения собственных целей. Хакеры в серой шляпе обычно следуют другой

форме хакерской этики, допускающей взлом системы, при котором хакера не обвинят в воровстве или нарушении конфиденциальности. Понятие «шляпа» заимствовано из фильмов о ковбоях, где «плохие парни» носили черные шляпы, а «хорошие ребята» — белые.

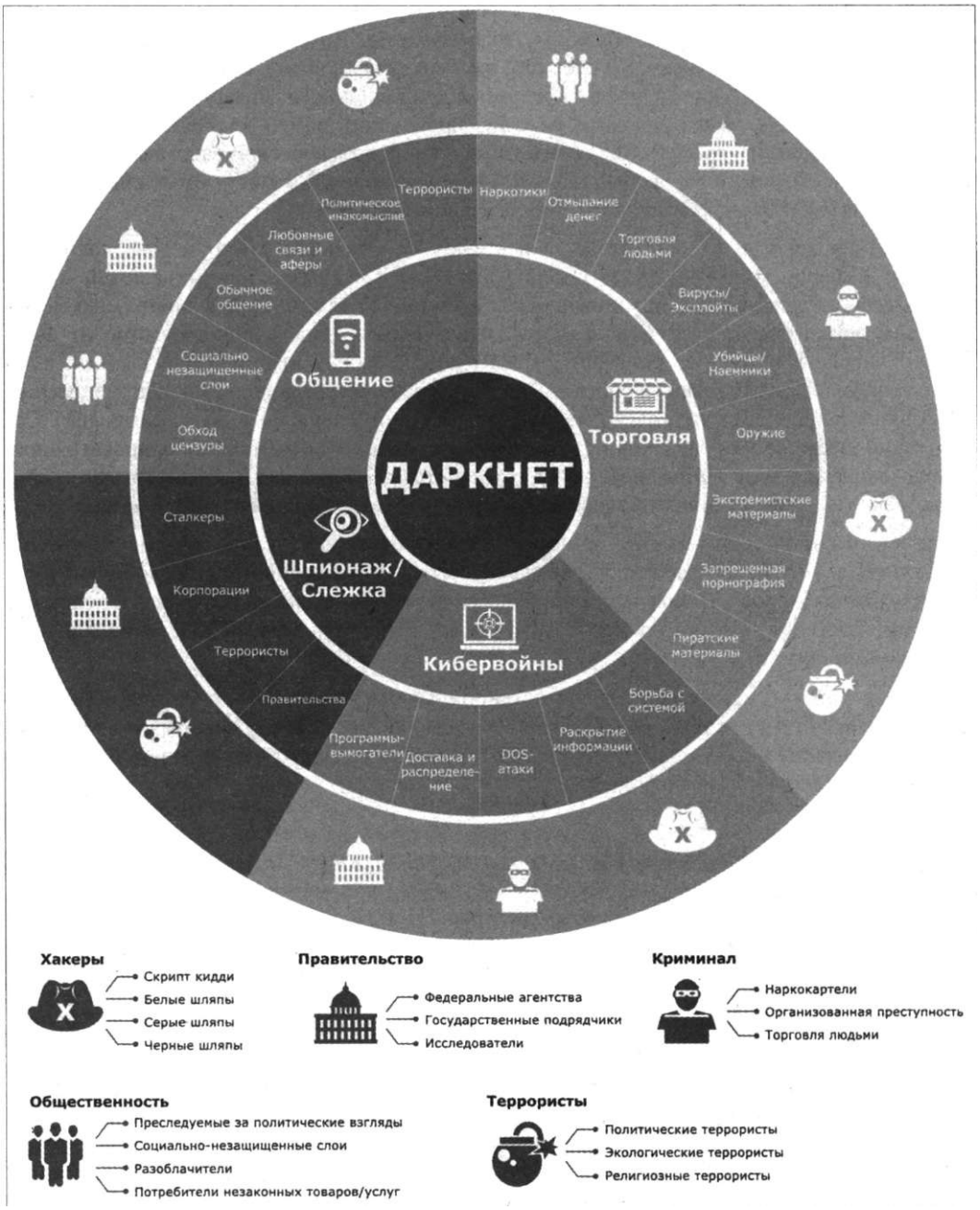


Рис. П1.1. Аудитория и секторы Даркнета.
Источник: BatBlue The Cloud Security Company, batblue.com

Черные рынки Даркнета

Даркнет пользуется дурной славой из-за своих торговых площадок, на которых продаются незаконные товары и услуги, включая наркотики, оружие (рис. П1.2, *справа),* детскую порнографию, фальшивые удостоверения личности и паспорта, а также пиратские фильмы и музыку. Наиболее известной площадкой является нашумевший ресурс Silk Road, работавший с 2011 по 2013 годы (рис. П1.2, *слева).*

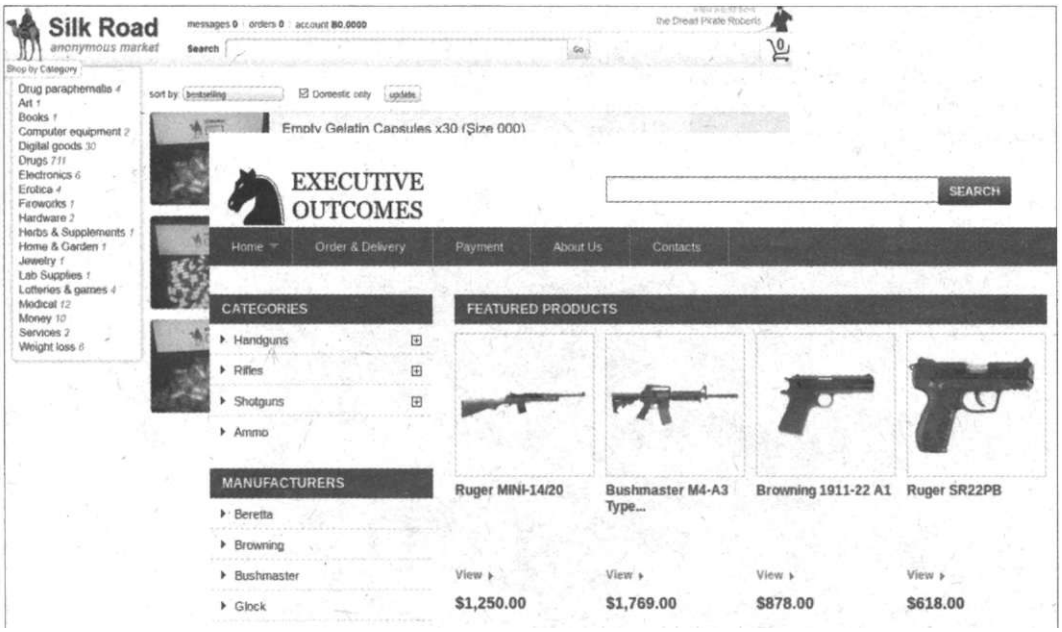


Рис. П1.2. Интерфейс закрытого в 2013 году Даркнет-ресурса Silk Road (слева) и магазина оружия (*справа)*

Ресурс Silk Road использовался в качестве площадки для противозаконной торговли наркотиками, реквизитами похищенных банковских карт, фальшивыми удостоверениями личности и пиратскими материалами. Все транзакции оплачивались биткоинами — анонимной криптовалютой. Сайтом управлял Росс Ульбрихт под псевдонимом Dread Pirate Roberts. Ресурс проработал с 2011 по 2013 годы, через него осуществили свыше 4000 продаж на общую сумму 200 млн долларов. Росс Ульбрихт был арестован в 2013 году и приговорен к пожизненному тюремному заключению в мае 2015 года. После того как Silk Road закрылся, стали появляться ресурсы-подражатели, такие как Silk Road 2, но вскоре и они закрылись. Помимо Silk Road многие подобные торговые площадки также уже закрыты ФБР и другими правоохранительными органами.

Даркнет предлагает не только незаконные препараты и аморальные занятия. Политические диссиденты, борцы за свободу слова и конфиденциальность с помощью Даркнета распространяют информацию, скрываемую правительствами. К примеру, сайт WikiLeaks, созданный Джулианом Ассанжем в 2006 году, сначала размещался в Даркнете и только потом получил общедоступную копию во Всемирной паутине. Ресурс до сих пор есть в Даркнете, и диссиденты и разоблачители могут анонимно загружать на него информацию. Группы активистов — например, Anonymous и Lulzsec — в сети Tor обсуждают и планируют свои

операции. Журналисты и медиакомпании с помощью Tor общаются со своими информаторами, которые хотят остаться анонимными.

Помимо продажи наркотиков и оружия, в Даркнете (как, в общем, и в обычной Всемирной паутине) распространена торговля людьми (в том числе детьми и взрослыми: в сексуальное рабство, на органы и т. п.). Одним из таких ресурсов являлся аукцион Black Death, закрывшийся летом 2015 года. Торговля похищенными людьми — это лишь один из видов незаконной деятельности на просторах Даркнета. Уже упомянутый Black Death — это торговая площадка, где на аукционе продают людей, а также наркотики, фальшивые удостоверения личности и всевозможные незаконные товары и услуги. Когда один из исследователей Даркнета притворился заинтересованным покупателем девушки по имени Николь за 150 тыс. долларов США, администраторы сайта Black Death тут же с подозрением заявили: «Нам не нужна популярность. Никакой полиции. Никаких любопытствующих. Никаких журналистов и блогеров». Вскоре после этого ресурс сменил свой адрес (рис. П1.3).

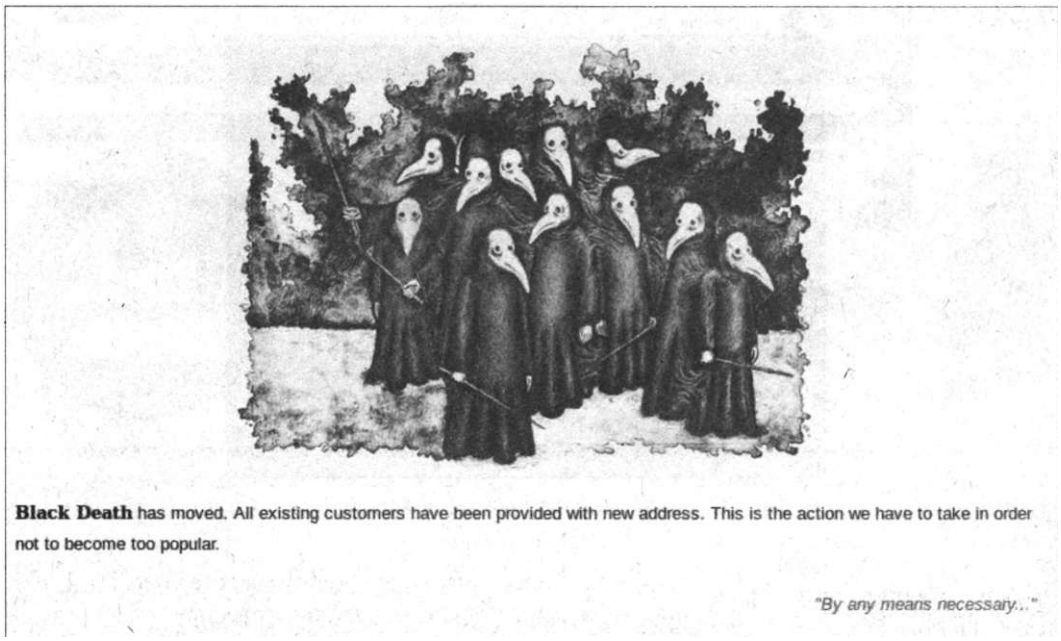


Рис. П1.3. Интерфейс закрывшегося в 2015 году Даркнет-ресурса Black Death с сообщением о том, что ресурс переехал

Даркнет — это место, где отсутствуют законы, и, кроме рейтингов покупателей и продавцов на некоторых сайтах, там нет контролирующих органов или руководящих инстанций. Это в первую очередь относится к странам, где плохо развито законодательство в сфере Интернета, а также к тем, где компьютерная криминалистика находится на очень низком уровне.

Торговые площадки Даркнета очень непостоянны, они часто меняют свои адреса, названия и администраторов. Администраторы сайтов — это единственный регулятор в Даркнете. Они часто стремятся построить доверие между пользователями с помощью эскроу-счетов и рейтингов покупателей и продавцов. Однако когда сайты становятся популярнее, а на эскроу-счетах появляются большие суммы денег, у администраторов сайтов может возникнуть соблазн скрыться со всеми деньгами и оставить пользователей ни с чем. Этот вид мошенничества часто называют exit scam (от англ. «вывод активов»). Например, один из черных

рынков Даркнета, Evolution, где продавались наркотики и другие противозаконные товары, предположительно, обманул своих пользователей на внушительную сумму. Этот сайт заслужил всеобщее доверие после закрытия ресурса Silk Road, однако администраторы Evolution внезапно закрыли сайт в марте 2015 года и, как сообщается, присвоили крупные суммы денег своих клиентов.

Криптовалюты

Все товары и услуги в Даркнете оплачиваются криптовалютой, а не обычными деньгами. Криптовалюты — это анонимные и адаптируемые цифровые деньги. Они появились, когда программисты занялись поиском альтернативы традиционным национальным валютам. Первой криптовалютой стал биткоин, за ним последовали десятки других криптовалют. Криптовалюты хранятся в цифровых кошельках без каких-либо идентификаторов и используются для транзакций в Даркнете, а также для некоторых обычных транзакций.

БИТКОИН В РОССИИ

На момент подготовки книги использование криптовалют в России не запрещено.



Рис. П1.4. Изображение биткоинов *(слева),* **лайткоинов (в** *центре)* **и доджкоинов (***справа)*

В мире существуют десятки криптовалют, однако многие из них выживают лишь несколько месяцев. Вот три наиболее популярные криптовалюты:

- биткоин — это самая первая и наиболее популярная криптовалюта (рис. П1.4, *слева),* созданная в 2009 году японцем Сатоси Накамото. Биткоины генерируются в результате сложных вычислений с помощью компьютеров пользователями по всему миру, а не печатаются, как доллары или рубли. Стоимость одного биткоина в октябре 2015 года составляла 300 с небольшим долларов США;
- лайткоин был создан в 2011 году Чарльзом Ли, бывшим сотрудником Google. Лайткоины (рис. П1.4, *в центре)* также генерируются с помощью компьютеров. Общее число их достигает 84 миллионов, т. е. их в четыре раза больше, чем биткоинов. Стоимость одного лайткоина в октябре 2015 года составила 3,1 доллара США;
- доджкоин — начал свой путь в 2013 году благодаря австралийцу Джексону Палмеру. У доджкоинов (рис. П1.4, *справа)* короткий цикл производства — к 2015 году было произведено 100 миллиардов доджкоинов, и каждый последующий год будет генерироваться более 5 миллиардов. Стоимость одного доджкоина в октябре 2015 года составляла 0,00012 доллара США.

Актуальные котировки криптовалют доступны во Всемирной паутине, к примеру, на сайте tinyurl.com/pe2omxz.

Криптовалюты — практически единственный способ оплаты в Даркнете, а биткоины, лайткоины и доджкоины — всего лишь три криптовалюты из того множества, которое применяется для торговли там. При этом криптовалюта — не только альтернативные деньги, но и механизм денежных переводов. Это качество отличает криптовалюту от других денег: биткоины и другие криптовалюты играют роль денежных средств и механизма их перевода одновременно. Покупатель может перевести обычные деньги в криптовалюту, затем переслать деньги продавцу, который может конвертировать их в любую другую валюту, и все это займет несколько минут. Обменять криптовалюту в Интернете проблем не составляет — валютные биржи есть и во Всемирной паутине, и в Даркнете.

Реакция властей на Даркнет

Правительства по всему миру пытаются найти способы сдерживания Глубинной Паутины и осуществляющейся там противозаконной деятельности. Многие правоохранительные структуры — такие, как ФБР и Европол, — устраивают рейды, чтобы закрыть сайты, торговые площадки и узлы Даркнета. В ноябре 2014 года американские и европейские власти вычислили свыше 400 скрытых веб-адресов, предназначенных для торговли наркотиками и других противозаконных услуг, и арестовали шестнадцать человек в восемнадцати странах мира. Эта масштабная операция — лишь один из многих рейдов на сайты Даркнета и их администраторов. Другие рейды были направлены против распространения детской порнографии, инсайдерских сделок и других преступлений.

Как уже упоминалось ранее, сеть Tor была разработана исследовательской лабораторией Разведывательного управления ВМС США. Правительство США продолжает искать способы анонимного пользования Интернетом и реализует новые технологии, в том числе и для других стран, чтобы помочь их населению в борьбе с авторитарными режимами. В то же самое время, желая контролировать весь мир, американские спецслужбы следят за действиями пользователей Tor и пытаются вычислить некоторых из них в своих целях.

Тем не менее, документы АНБ, обнародованные Эдвардом Сноуденом, показали, что власти не могут эффективно отслеживать пользователей Tor, — что бы правительство ни предпринимало, власти не могут полностью уничтожить те технологии, которые держат на плаву Даркнет.

В Даркнете хакеры продают и покупают эксплойты, уязвимости «нулевого дня» и украденную информацию. При этом многие торговые площадки в Даркнете предназначены для поиска хакеров с уникальными знаниями и опытом. Хакеры объединяются и совершают атаки на различные сайты, организации (включая государственные) и даже самые сложные сети. Правительства же и спецслужбы — часто самые щедрые приобретатели уязвимостей «нулевого дня» и эксплойтов, готовые платить сотни тысяч или даже миллионы долларов за услуги самых талантливых хакеров.

Заключение

Даркнет — это рынок широкого ассортимента незаконных препаратов, услуг и средств общения. Но это не просто черный рынок — Даркнет также является площадкой для самых жарких политических дискуссий и обмена информацией между диссидентами, журналистами, разоблачителями, экстремистами и троллями. Как и черный рынок, который существует уже много веков, Даркнет развивается и растет естественным образом. Правительство и правоохранительные органы не могут контролировать его, потому что у них отсутствуют

необходимые инструменты давления. По сути, власти даже способствуют его процветанию. Правительства и другие игроки будут по-прежнему активными участниками рынков Даркнета, они получают там информацию и данные и даже покупают эксплойты, вредоносное ПО и другие инструменты. Охота за кибероружием набирает обороты по мере того, как действующие лица начинают понимать, какой доход приносят уязвимости в различных сферах.

Даркнет — это теневая платформа для виртуальной гонки вооружений, а также механизм общения и координирования действий. Даркнет — это еще и платформа для новых и инновационных способов нарушить закон. Благодаря анонимности и обширной географии Даркнета, одним из самых мрачных его аспектов стала игрофикация и краудфандинг таких преступлений, как убийство и похищение людей.

Когда закрывается один сайт, на смену ему приходит множество других. Вот закрылся Silk Road, и в мгновение ока появились подобные ему торговые площадки, метящие занять его место. В Даркнете каждый сам за себя, золотое правило там: «будь осмотрителен», — это относится и к продавцу, и к покупателю.

Даркнет — переменчивая среда, где сайты появляются, меняются, разрастаются и исчезают самым непредсказуемым образом. Это дихотомное пространство, которое одновременно и нелегальная платформа для извращений, коррупции, эксплуатации и преступлений, и площадка, которая предоставляет возможность высказаться тем, кто подвергается нападкам и гонениям. Какими бы ни были противоречия и мотивы, люди, стоящие за Даркнетом, в ближайшем будущем продолжат влиять на мир, в котором мы живем. Даркнет — это первое виртуальное глобальное подполье.

ПРИЛОЖЕНИЕ 2

Варез и Сцена

Варез: киберпиратство

Сцена: андеграунд Всемирной паутины

Подавляющее большинство пользователей дорогого софта (к примеру, Windows, Adobe Photoshop, 3ds Max, Sony Vegas Pro и т. п.) используют нелегальные копии программного обеспечения, т. е. так называемый *варез* (warez). Это вполне предсказуемое поведение людей с низкими доходами в экономически несбалансированных (читай, неразвитых) странах (поэтому Россия и Китай — лидеры по пиратству). Разумеется, сложно при зарплате в 30-40 тыс. руб. в месяц позволить себе Photoshop за 33 тыс. рублей, CorelDraw — за 45 тыс. рублей или Sony Vegas — за 58 тыс. рублей. Как правило, подобное варезное программное обеспечение распространяется тремя основными способами:

- в виде программы в комплекте со взламывающим ее инструментом;
- в виде активированного или retail (полная версия) приложения;
- в виде отдельного инструмента нелегального лицензирования (взлома).

Основную часть нелегального вареза (а также мультимедийного контента) производят (если можно так выразиться) члены *Сцены* — андеграундного сообщества, возникшего в эпоху зарождения Всемирной паутины. Варез сначала размещается в закрытых файловых архивах *0day,* откуда позже попадает на торрент-трекеры, варезные сайты и форумы, т. е. на ресурсы, предназначенные для конечного пользователя.

> ***ТЕРМИН ODAY***
>
> **Oday (англ. zero** *day)* **— «уязвимость нулевого дня», термин, обозначающий вредоносные программы, против которых еще не разработаны защитные механизмы, или уязвимости, которые не устранены.**

Варез: киберпиратство

Под *варезом* понимаются защищенные авторским правом работы, которые распространяются без авторских отчислений или лицензионных платежей в нарушение закона об авторском праве. Варез в целом — несанкционированные релизы программ и мультимедийных файлов варезными группами, осуществляемые через Интернет и анонимные сети (через так называемый Даркнет).

ДАРКНЕТ

Даркнет — это сеть для анонимного и зашифрованного обмена информацией. Данные здесь находятся под покровом специализированного программного обеспечения, которое обеспечивает шифрование и анонимность пользователей с использованием протоколов и доменов, на которые среднестатичный веб-пользователь никогда не наткнется. Краткая информация о Даркнете приведена в *приложении 1,* **а подробную статью о Даркнете вы можете найти по ссылке tinyurl.com/oufjfky.**

Соответственно и веб-сайты, размещающие нелегальные программы и их дистрибутивы, называются *варезными.* Более подробно с понятием вареза можно познакомиться на странице **tinyurl.com/phoe9a6.**

Рассмотрим категории нелегально распространяемых материалов:

- программы и их дистрибутивы, официально не допущенные к распространению посредством Всемирной паутины или иными способами (на дисках и т. п.). Сюда относятся платные операционные системы и иное программное обеспечение, ссылки на демонстрационные, полноценные или тестовые версии которых не размещены на официальных или лицензированных сайтах. То же касается и игр;
- программы и их дистрибутивы, взломанные и/или включающие информацию или инструменты для нелегального обхода функциональных, временных и иных ограничений работы. А также инструменты для изменения языка локализации (так называемые *русификаторы),* если таковое не предусмотрено правообладателем. То же касается и игр;
- информация и инструменты для взлома (обхода ограничений) какого-либо программного обеспечения, игр или веб-сайтов;
- фотографии и иные изображения, не имеющие статус свободно распространяемых или не разрешенные к распространению автором;
- музыкальные файлы, не имеющие статус свободно распространяемых или не разрешенные к распространению автором. Это касается файлов MP3, WAV, FLAC, APE и иных форматов сжатия аудиофайлов, а также копий (образов) дисков и их фрагментов;
- видеофайлы, не имеющие статус свободно распространяемых или не разрешенные к распространению автором. Это касается также всех рипов (DVDRip, HDRip, BDRip и пр., обозначающих тип носителя, с которого создана копия) и полных (и их фрагментов) копий видеодисков. Порнографические материалы относятся сюда же;
- книги в электронном формате (TXT, PDF и др.).

В число указанных основных типов нелегальных материалов можно включить также образы и архивы установленных программ и операционных систем, различные нелицензионные гвикеры, трейнеры для игр, серийные ключи, ворованные номера ICQ и т. п., и другие инструменты/документы, нарушающие законодательство.

ВЫ НАРУШАЕТЕ ЗАКОНЫ О ЗАЩИТЕ АВТОРСКИХ ПРАВ!

На самом деле принятые в ряде стран мира законы касательно защиты авторских прав зачастую оказываются весьма затруднительными в исполнении. Так получается, что приобретя MP3-плеер, вы попросту не сможете на него ничего переписать, поскольку копирование (даже для себя) легально купленного музыкального компакт-диска запрещено, в том числе и в формат MP3. Вы также можете быть привлечены к ответственности, если слушаете музыку через колонки, а не наушники, — это же самое настоящее публичное нелицензированное воспроизведение. А может быть, вы поете незаконно песню, на слова которой у вас нет прав? Не стоит смеяться, в России тоже могут быть приняты такие законы.

Слово «варез», как уже отмечалось, представляет собой кальку с английского warez, являющегося, в свою очередь, сокращением от software (программное обеспечение). Варез

часто распространяется за пределами Сцены (сообщества варезных групп) с помощью торрент-файлов, выгружаемых на сайты популярных пиринговых сетей партнерами или друзьями взломщиков или варезных групп. Релизы сопровождаются и файлами NTO и FILEID.DIZ, создаваемыми релизерами. Затем эти релизы скачиваются пользователями пиринговых сетей и распространяются на других P2P-сайтах или таких ресурсах, как новостные группы. И уже оттуда варез скачивается миллионами пользователей со всего мира. Зачастую один и тот же релиз дублируется, переименовывается, а затем повторно выгружается для распространения на различные ресурсы, чтобы в конечном счете было невозможно отследить оригинальный файл. Другой популярный метод распространения вареза заключается в использовании файлообменных хостингов, описанных в этой книге ранее. Но это сейчас, а в начале 1990-х годов релизы распространялись на пленочных кассетах и размещались на BBS в разделе warez.

ЭЛЕКТРОННАЯ ДОСКА ОБЪЯВЛЕНИЙ

BBS (англ. Bulletin Board System, электронная доска объявлений) — широко используемый во времена редкости кабельных компьютерных сетей способ общения пользователей компьютеров через коммутируемые телефонные сети.

История киберпиратства

Пиратство как явление возникло в тот момент, когда высококачественное коммерческое программное обеспечение стало выпускаться для продажи. Был ли носитель пленочной кассетой или дискетой, пираты находили способ дублировать программное обеспечение и распространять его без разрешения разработчика. Процветающие пиратские сообщества выстраивались вокруг Apple II, Commodore 64, линеек Atari 400 и Atari 800, ZX Spectrum, Amiga, Atari ST и других персональных компьютеров. Возникли целые сети BBS, помогающие незаконно передавать программное обеспечение от одного пользователя к другому. С помощью таких компьютеров, как Amiga Commodore 64, была создана международная пиратская сеть, через которую программное обеспечение, не доступное на том или ином континенте, в конечном счете, попадало в каждый регион через BBS.

В 1980-х годах довольно часто компьютерные дискеты с пиратским программным обеспечением просто пересылались по почте. До появления CD и жестких дисков запущенное программное обеспечение не требовало наличия дискеты в дисководе, поэтому пользователь мог установить программу на компьютер и отправить дискету по почте следующему человеку, — и т. д. Способ передачи вареза по почте был особенно широко распространен в Европе, и даже использовался многими из варезных групп как основной канал взаимодействия.

Сегодня большинство релизов вареза распространяется через пиринговые сети и файлообменные хостинги. Чаще всего взламывается программное обеспечение именитых компаний — таких как Adobe, Microsoft, Nero, Apple, DreamWorks и Autodesk. Чтобы уменьшить поток пиратства, некоторые компании нанимают людей, распространяющих *фейки* — «левые» торренты, которые выглядят как реальные релизы вареза и после загрузки его пользователем передают компании-собственнику программного обеспечения IP-адрес загрузившего. Далее компания связывается с интернет-провайдером пользователя, и последнему может грозить судебный иск.

Причины, повлиявшие на рост пиратства

В середине 1990-х компьютеры стали набирать популярность огромными темпами. Это произошло в основном благодаря компании Microsoft, выпустившей операционную систему

Windows 95, которая сильно упростила использование IBM-совместимых компьютеров домашними пользователями. Операционная система Windows 95 оказалась настолько популярна, что в развитых странах практически в каждой семье со средним достатком имелся как минимум один компьютер.

Подобно телевизорам и телефонам, компьютеры в информационную эру стали необходимы каждому человеку. Поскольку выросло количество компьютеров, увеличилось и количество преступлений в сфере информационных технологий.

В середине 1990-х большинство пользователей Интернета использовали коммутируемый доступ к Всемирной паутине со средней скоростью передачи данных в диапазоне 28,8-33,6 Кбит/с. Если требовалось загрузить некое программное обеспечение, размер дистрибутива которого составлял около 200 Мбайт, время загрузки растягивалось на день и более, — в зависимости от сетевого трафика, провайдера и сервера. Однако уже примерно к 1997 году из-за ставших доступными высоких скоростей передачи данных стало завоевывать популярность широкополосное подключение к Интернету. Передача файлов больших размеров перестала быть серьезной проблемой, варез получил более широкое распространение и затронул объемные мультимедийные файлы — такие как мультфильмы и видеофильмы.

Ранее файлы распространялись по двухточечной технологии с установкой прямой связи от центрального узла-распространителя к узлам пользователей, скачивающих контент. В этом случае, чем больше пользователей начинали скачивать файл, тем сильнее возрастала нагрузка на полосу пропускания. При чрезвычайно высоком количестве одновременных скачиваний сервер вовсе мог стать недоступным. Совершенно противоположен другой тип сети — одноранговой (или пиринговой), в которой все сетевые узлы равноправны: большее число скачивающих пользователей ускоряло распространение файлов. С помощью технологии посегментной загрузки, реализованной в файлообменных сетях, таких как eDonkey2000 и BitTorrent, *личеры* (скачивающие) помогают *сидерам* (раздающим), раздавая уже загруженные сегменты (части) файлов. Развитие файлообменных хостингов и прочих сайтов для размещения/хранения файлов способствовали росту и распространению вареза.

Распространение через скомпрометированные FTP-серверы

До развития современных пиринговых систем обмена файлами и распространения широкополосного доступа к Интернету, варезные группы в целях распространения вареза нередко сканировали Интернет в поисках слабо или незащищенных компьютерных систем со скоростным доступом. Найденные системы подвергались взлому через уязвимости в защите, и на сервере создавался специальный каталог с не вызывающим подозрения именем, в который выгружался нелегальный контент.

Частой ошибкой администраторов FTP-серверов в те годы было разрешение внешним пользователям полного доступа к папке с именем /incoming, причем сами файлы в этой папке автоматически скрывались. Если же в папке /incoming создавалась новая папка, тоже скрытая, ее содержимое могло не скрываться. Пользователи скомпрометированного сайта авторизовывались и перенаправлялись в папку с варезом — типа /incoming/data/warez. В эту папку загружались и простые текстовые файлы с сообщениями для других пользователей вареза.

Хакеры также могли использовать известные баги программного обеспечения с целью незаконного получения средства полного административного управления компьютером и установки скрытых FTP-служб для размещения вареза. Такие службы обычно запускались на нестандартном порту компьютера или использовали некие учетные записи — типа «Логин: warez / Пароль: warez», с целью предотвратить доступ к каталогу с варезом со стороны за-

конных пользователей. Информация о скомпрометированных серверах сообщалась избранной группе людей, состоящих в Сцене.

Членам варезных групп было важно контролировать доступ к таким скомпрометированным FTP-серверам, чтобы предотвратить увеличение трафика. В противном случае снижение производительности скомпрометированной системы могло быть замечено реальными владельцами сервера и привело бы к мониторингу сетевой и дисковой активности, обнаружению и удалению варезного контента и латанию дыр в системе безопасности сервера.

Автоматизированное распространение вареза с помощью IRC-ботов

С распространением взлома корпоративных серверов варезные группы стали устанавливать на скомпрометированные серверы, наряду с FTP-сервисом или же для обеспечения обмена файлами напрямую, также и IRC-боты (сокращение от слова «робот»). IRC-боты с целью ограничения нагрузок на полосу пропускания контролировали доступ к нелегальным файлам посредством формирования очередей или же функционировали только в нерабочие часы (ночное время), когда ресурсы корпоративного сервера не были востребованы владельцами.

Для оповещения о существовании скомпрометированного сервера программное обеспечение IRC авторизовывалось в публичных IRC-каналах, посвященных варезу, в качестве *бота* и каждые несколько минут публиковало в канале системные сообщения о количестве пользователей хоста с варезом и количестве загружаемых в настоящий момент файлов, а также сведения о соотношении скачивание/раздача (вынуждая пользователей раздавать собственные файлы, прежде чем они смогут скачать желаемые) и прочую информацию.

Важно отметить, что этот канал распространения вареза все еще функционирует и может рассматриваться как альтернатива современным и потоковым пиринговым системам. Количество скомпрометированных систем, взламываемых в целях распространения вареза, только увеличилось с развитием широкополосного доступа в Интернет и ростом количества домашних пользователей, не придающих значения обеспечению должного уровня защиты своего компьютера, теперь непрерывно подключенного к Интернету.

Разновидности вареза

Рассмотрим основные разновидности вареза — непривычные латинские слова, встречающиеся в перечне, обычно используются в качестве имен каталогов на скомпрометированных серверах для сортировки вареза.

- **O-day** или **Oday** (произносится как «зеро дэй») — это понятие относится к любому произведению, охраняемому авторским правом, которое было нелегально выпущено в тот же день, что и оригинальный продукт, а иногда даже прежде. У варезных групп считается верхом мастерства, если программа взламывается и начинает распространяться в день ее коммерческого релиза.
- Apps — программные продукты версии для конечного пользователя, как для компьютера, так и для мобильных устройств.
- **Cracks** (взломанные приложения, также называются «крэками») — модифицированный исполняемый файл (или несколько файлов, но чаще один), и/или модифицированная библиотека (чаще одна), и/или патч, созданные с целью превратить демонстрационную версию программы в полнофункциональную и/или для обхода защиты от пиратства.

- Dox — дополнения к видеоиграм: NoCD, крэки, трейнеры, чит-коды и т. п.
- EBooks — электронные книги (нелегально распространяемые книги в электронном формате, отсканированные печатные книги, отсканированные комиксы и т. д.).
- Games — игры для компьютеров, мобильных устройств и игровых приставок, часто выпускаемые в виде образа диска (в формате ISO) и других.
- Keygens (генераторы ключей) — инструменты, которые копируют процесс регистрации/активации подлинного программного продукта и генерируют необходимые ключи, позволяющие нелегально активировать программное обеспечение.
- Movies — пиратские копии (рипы) видеофильмов, которые могут быть выпущены ранее официальной даты выхода в прокат или выпуска на дисках.
- MP3s — пиратские копии музыкальных альбомов, сборников (компиляций), синглов и других аудиорелизов, обычно получаемые путем *граббинга* (копирования) компакт-дисков аудио или записи радиошоу и выпускаемые в сжатом аудиоформате MP3.
- MVids — музыкальные видеоклипы, скопированные с TB, HDTV, дисков DVD или VCD.
- NoCD, NoDVD, FixedExe— модифицированные файлы, позволяющие .исполняемой программе работать при не вставленном в привод диске CD или DVD.
- **RIP** (рипы) — копии игр (в том числе и консольных), не требующие установки (любые необходимые записи в реестре включаются, если требуется, в сопровождающий REG-файл). Из рипов могут быть извлечены лишние аудио- и/или видеофайлы для уменьшения размера файла. Рипы без удаленного контента иногда маркируются как DP (Direct Play).
- Portable (портативные версии приложений) — схоже с рипами, но в данном случае вместо игр подразумеваются приложения. Суть портативного программного обеспечения в том, что приложение может быть скопировано на съемный носитель (или в любую папку на жестком диске) и для запуска не нуждается в установке. Обычно сжимается в единичный исполняемый файл.
- Scripts (скрипты, сценарии) — нелегально распространяемые исходники коммерческих (веб-)приложений (таких, как vBulletin, Invision Power Board и т. д.) на языках PHP, ASP и др.
- Subs (субтитры) — могут быть внедрены в рипы телевизионных передач и видеофильмов.
- Serials — ключи или серийные номера, используемые с целью нелегальной активации условно-бесплатного программного обеспечения.
- Templates — нелегально распространяемые шаблоны (темы) для веб-сайтов, разработанных коммерческими компаниями.
- TV-Rips — рипы телевизионных передач и фильмов, обычно с удаленной рекламой. Чаще всего публикуются в течение нескольких часов после демонстрации. Рипы DVD с телесериалами относятся к этой же категории.
- XXX — материалы порнографического содержания, могут быть сетами (наборами) изображений, рипами роликов с платных сайтов для взрослых или фильмов, продаваемых в розницу.

Пиратство в сфере киноиндустрии

Изначально пиратство в сфере кино казалось киностудиям невозможным. В первой половине 1990-х годов, во времена существования коммутируемого доступа, пиратские копии фильмов, встречавшиеся в Интернете, имели малое разрешение и небольшой размер файла. Применяемая к фильмам техника сильного сжатия с помощью соответствующих программ компрессии существенно снижала качество видеоизображения. Самая большая угроза пиратства нависала тогда над программным обеспечением.

Ранними попытками пиратства кинофильмов были «экранки», или «кам-рипы», создававшиеся путем съемки на видеокамеру действия, демонстрируемого на экране в кинотеатре. Это позволяло варезным группам распространять фильмы с момента их проката в кинотеатрах (т. е. ранее даты выпуска на носителях для домашнего просмотра). Но из-за того, что «экранки» чаще всего имели крайне низкое качество видео и звука, а также создавали для пирата опасность быть обнаруженным во время видеосъемки, в кинотеатре, «экранке» пришлось искать альтернативные методы.

С распространением широкополосного доступа к Интернету, начиная приблизительно с 1998 года, стали набирать популярность высококачественные пиратские копии фильмов. Такие копии создавались варезными группами на основе исходных дисков VCD и SVCD и реализовывались обычно ранее премьеры. Нашумевшим примером пиратства в сфере киноиндустрии стал релиз фильма «Американский пирог». Внимание этот случай привлек по трем причинам:

- релиз оказался скопирован с чернового монтажа, не прошедшего цензуру. Впоследствии вышедшая «официальная» версия фильма была сокращена на несколько минут и исключала сцены чрезмерной наготы, не соответствующие требованиям Американской ассоциации кинокомпаний (MPAA, Motion Picture Association of America);
- релиз был выпущен практически на два месяца раньше премьеры фильма;
- пиратский релиз послужил для кинокомпании одной из причин, по которой была выпущена Unrated-версия фильма на DVD (т. е. версия без присвоения рейтинга, без ограничений).

После выпуска программы-дешифратора содержимого дисков DVD-Video под названием DeCSS (написанной, кстати, норвежским школьником) Получили распространение ISO-образы с копиями оригинальных дисков DVD. Кроме того, с применением кодека DivX 3.11, позволившим улучшить качество видеоизображения, стали набирать популярность сжатые рипы DVD. Позднее, с выходом версии 4.0, кодек DivX перестал быть бесплатным и был запрещен к использованию в варезных кругах, а его место занял Xvid.

В феврале 2012 года основные варезные группы официально анонсировали x264 — бесплатный кодек на основе формата H.264 — как новый стандарт для релизов, заменив им предыдущий формат, использовавший кодек Xvid, обернутый в контейнер AVI. Переход к H.264 обеспечил распространение форматов MP4 и Matroska (MKV), хотя видеоконтент в формате AVI все еще встречается, и нередко.

Сегодня обмен копиями фильмов вызывает беспокойство, главным образом, у киностудий и представляющих их организаций. Из-за этого Американская ассоциация кинокомпаний (MPAA) запустила кампанию по оповещению зрителей о требовании воздержаться от нелицензионного копирования фильмов, встраивая соответствующий текст в кинотрейлеры и сами фильмы.

Релизы фильмов обычно различаются форматами и версиями, т. к. попадают к варезным группам из различных источников. Как правило, самый первый релиз того или иного филь-

ма имеет низкое качество (из-за ограниченной доступности источников), но в конечном счете заменяется релизами все более высокого качества, поскольку соответствующие источники с течением времени становятся доступными.

Обозначения варезных файлов

Вполне возможно, вам попадались во Всемирной паутине ссылки/строки текста вида:

Название. Программы.vi.2.34567. `Multilingual.Win8.x64.Keymaker.Only-CORE`

или

`Название.Программы.vi.2.34567.Incl.Keymaker-BLiZZARD`

Это не что иное, как релизы нелегального программного обеспечения, как правило, со Сцены, созданные, упакованные в архив и именованные согласно определенным стандартам.

Так, первая приведенная ссылка означает, что перед вами программа такая-то версии такой-то, включающая несколько языков интерфейса (`Multilingual`), поддерживающая 64-разрядную операционную систему Windows 8. При этом архив содержит только генератор ключей (но не программу — на это указывает слово `Only`), а сам релиз создан группой **CORE**.

Во втором случае в архиве присутствует и программа, и взламывающий ее инструмент, — на это указывает слово `incl` (Include), а релиз подготовлен группой **BLISZARD**.

Стандарты вареза в Сцене определяются варезными группами, функционирующими на протяжении нескольких лет и контактирующими с самыми крупными группами Сцены. Эти люди входят в состав комитета, проектирующего черновики стандартов для одобрения крупными группами Сцены. Согласно принципам Сцены все релизы должны следовать этим определенным стандартам, чтобы быть допущенными к распространению. Комитет по стандартам обычно анализирует несколько черновиков и, после принятия решения в пользу одного из них, выпускает проект для одобрения. Как только проект получает электронную подпись нескольких наиболее крупных групп, он принимается в качестве текущего стандарта. В стандартах указываются правила именования и организации файлов, приводятся инструкции по упаковке и созданию NFO-файла, который содержит описание релиза. Существуют разные стандарты для каждой категории разновидностей вареза. Все варезные группы Сцены должны изучить стандарты и следовать им.

Формат

Стандарты определяют формат релиза: кодек, битрейт, разрешение, тип и размер файла. Разработчики стандарта обычно выполняют всестороннее тестирование, чтобы определить оптимальные кодек и настройки для видеоизображения и звукового сопровождения, позволяя сохранить максимально возможное качество в файле того или иного размера.

При выборе размера файла учитывается такой ограничивающий фактор, как размер носителя (например, 700 Мбайт для диска CD-R). Стандарты разрабатываются таким образом, чтобы определенный объем контента соответствовал определенной части пространства носителя с определенным качеством. Если для достижения необходимого качества одного носителя не хватает, стандарт допускает использование двух и более дисков.

Новые версии кодеков периодически тестируются в попытке найти лучшее соотношение качество/длительность компрессии. Как правило, качество ценится выше скорости обработки, поэтому обычно выбирается максимально возможное качество, даже если кодирование продлится намного дольше.

Архивация

Стандарты определяют и параметры архивирования контента. В настоящее время допустимыми форматами архивирования признаются RAR и ZIP, последний из которых используется только при упаковке релизов 0-day.

Допустимые размеры архивов варьируются от устаревших 3,5-дюймовых дискет (объемом 1,44 Мбайт) или дисков повышенной емкости (от 2,88 до 5 Мбайт) до 15-20 Мбайт (обычно для образов CD), 50 Мбайт (обычно для образов DVD) и 100 Мбайт (для образов двуслойных DVD).

Для каждого типа вареза применяются различные уровни сжатия, потому что один контент сжимается лучше, чем другой. Видеофайлы и музыка в формате MP3 и так уже сжаты почти до максимума — перезапаковка только увеличит их размер и потребует лишнего времени на распаковку. Рипы фильмов и мультфильмов все еще архивируются из-за большого размера файла, но без сжатия — формат RAR служит только в качестве контейнера, потому-то современные проигрыватели могут без проблем воспроизводить мультимедийные файлы непосредственно из архивов.

Файлы в формате MP3 и музыкальные клипы — исключение, они не упаковываются в единый архив в отличие от остальных типов вареза. Размеры файлов в таких релизах достаточно малы, чтобы быть переданы без ошибок. К тому же, серверные сценарии могут считывать ШЗ-теги из MP3-файлов и сортировать согласно им опубликованные релизы.

Имена файлов

Правила именования файлов и папок — очень важная часть стандартов. Корректно именованные объекты упрощают их сортировку и выявление дубликатов. Допускается только определенный набор символов, которые могут использоваться в именах объектов. Этот набор символов был определен с целью минимизировать проблемы, могущие возникнуть из-за разнообразия платформ, через которые будет распространяться релиз. Допускается использовать латинские буквы (для русских слов — транслит) в верхнем и нижнем регистре, арабские цифры и символы: дефис (-), точку (.), нижнее подчеркивание (_) и скобки (). Пробелы использовать запрещено.

Типичный пример имени папки для релиза фильма выглядит примерно так:

```
Название.Фильма.Латиницей.ГГГГ.Источник.Кодек-Группа
```

Например:

```
The.Wrath.of.Vajra.2013.BDRip.X264-ROVERS
```

Для разных категорий вареза могут существовать некоторые отличия в правилах использования тех или иных специальных символов.

Сопроводительные файлы релизов

Архивы с варезом комплектуются текстовыми файлами с расширениями DIZ (кратким описанием) и NFO (с подробным описанием и инструкциями), содержащими также информацию о взломавшей дистрибутив группе и рисунок в стиле ASCII — своеобразный логотип. Помимо этого, в архив могут быть включены и иные файлы.

Файл *FILEJD.DIZ*

Файл с именем FILEJD.DIZ включает краткое описание содержимого архива, в котором содержится. Такие файлы получили распространение со времен электронных досок объявлений (BBS, Bulletin board system).

BBS принимали для размещения файлы от пользователей и требовали наличия сопроводительного описания каждого выгруженного файла. Поскольку описания составлялись в произвольном виде, их текст часто был малополезен. Поэтому возникла необходимость в некотором стандартизированном подходе, коим и стал файл FILEJD.DIZ, включаемый в архив для описания содержимого. Этот формат был предложен в качестве спецификации Майклом Ливиттом из корпорации Clark Development, который применил его на собственной BBS. Через некоторое время файл FILEJD.DIZ стал стандартом.

Разбирая имя файла по компонентам, следует пояснить, что сочетание FILEJD обозначает File Identification и применительно к этому файлу может быть переведено с английского как «идентификатор файла». Имя расширения DIZ происходит от словосочетания Description In Zipfile (описание в сжатом файле). Кроме того, если расширение файла написать строчными буквами *(diz)* и перевернуть «вверх ногами», вы увидите слово *zip* — так что перед вами еще и рекурсивный акроним.

Согласно спецификации, файл FILEJD.DIZ должен содержать «не более 10 строк текста, с ограничением в 45 символов на строку». Задачей DIZ-файлов была реализация возможности автоматического применения описаний выгруженных пользователями файлов — рекламные объявления и сложная ASCII-графика в них были запрещены. Файл формата DIZ может быть открыт в любом текстовом редакторе и содержит название программы (инструмента взлома), ее версию, платформу (операционную систему), дату релиза и количество дисков. На рис. П2.1 в качестве примера представлен большой логотип варезной группы.

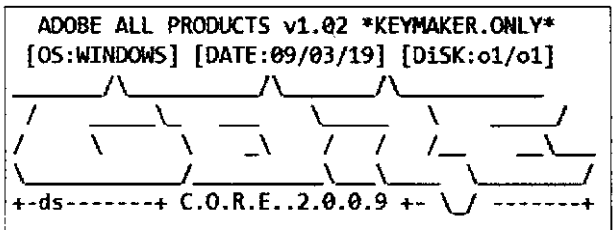


Рис. П2.1. Пример содержимого файла FILEJD.DIZ

Даже после упразднения BBS, доступ к которым осуществлялся посредством коммутируемого (модемного) доступа, файлы FILEJD.DIZ и по сей день все еще используются варезными группами и наряду с NFO-файлами считаются обязательными для каждого релиза. Спецификация файла FILEJD.DIZ представлена по адресу **tinyurl.com/puq3ptz.**

NFO-файлы

Файлы с расширением nfo (сокращение от слова iNFOrmation, информация) представляют собой простые текстовые файлы, которые сопровождают различные релизы вареза с информацией о них. В отличие от FILEJD.DIZ и README-файлов, NFO-файлы часто содержат тщательно прорисованную ASCII-графику, и в полной красе могут быть открыты в специальных программах для просмотра NFO-файлов (например, GetDiz, **tinyurl.com/d46uymu),** текстовых редакторах с поддержкой моноширинных шрифтов (таких, как Courier) или во Всемирной паутине, в публичных базах данных NFO-файлов — таких, как **www.xrel.to.**

NFO-файлы используются в качестве своего рода пресс-релизов варезных групп и были введены в обращение в 1990 году варезной группой THG (The Humble Guys) при релизе игры Bubble Bobble. NFO-файл при этом заменил более обобщающие файлы README.TXT или README.1ST. Использование NFO-файлов было подхвачено другими варезными группами и продолжается и по сей день. NFO-файлы обычно содержат информацию о релизе

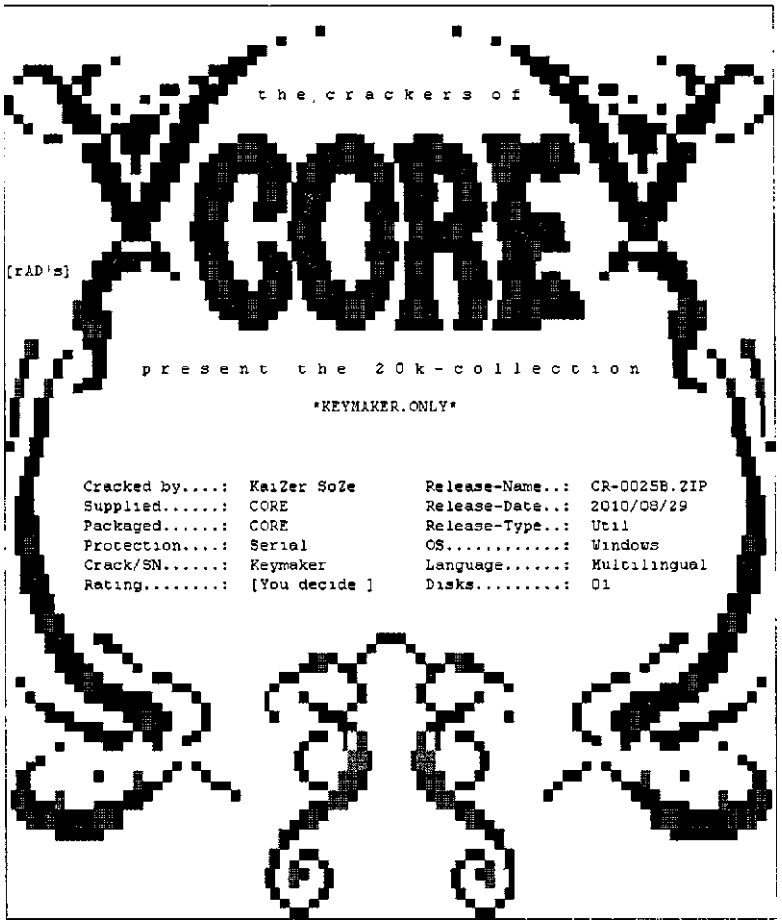


Рис. П2.2. Фрагмент содержимого NFO-файла группы CORE

(рис. П2.2). Если это релиз программного обеспечения, в NFO-файле приводятся примечания по установке и взлому.

Файлы NFO были особенно распространены, а иногда и необходимы, в эпоху BBS. Большинство NFO-файлов включают ASCII-оформление (рисунок или логотип группы), ниже которого расположены название программы (игры) и текст (таблица) с основными данными. **В** таблице представлены ники (псевдонимы) членов группы, взломавших релиз, тип защиты/взлома, имя файла и дата релиза, категория ПО, тип архивного файла релиза, операционная система и язык интерфейса, а также размер файла. При этом размер, как и раньше, часто указывается не полным объемом, а количеством частей многотомного архива и их размера (к примеру, 1><5.0МЬ). Следом размещается описание программы (игры), а далее — раздел **Install Notes** или **Installation,** содержащий инструкции по установке/обходу защиты программы. **В** конце NFO-файла представлена информация о варезной группе, ее членах, вакансиях, новости и прочие дополнительные сведения.

Группа THG позднее занялась демомейкерством, таким образом, внедрив традицию использования NFO-файлов и в демосцену, о которой речь пойдет чуть позднее. **В** результате десятки тысяч демо, помимо исполнительного файла, включают и сопроводительный NFO-файл.

NFO-ФАЙЛЫ В WINDOWS

В операционной системе Microsoft Windows файлы с расширением *nfo* ассоциированы с приложением Информация о системе (*msinfo32.exe*). Это приложение выдает сводку информации об аппаратном и программном обеспечении компьютера. Чтобы открыть NFO-файл в другой программе, следует щелкнуть по нему правой кнопкой мыши, выбрать пункт Открыть в (Open with) и выбрать подходящую программу, — например, Блокнот (Notepad).

SFV-файл

SFV (от англ. Simple File Vérification) — файлы для контроля целостности файлов, использующие контрольную сумму для ее проверки. Обычно в качестве алгоритма служит CRC32. Внутри файла можно найти имя файла и — через разделитель — его контрольную сумму.

Файлы могут быть повреждены по разным причинам: таким как неисправность носителя, ошибки передачи данных, ошибки копирования/перемещения и баги приложений. Проверка SFV-файла позволяет убедиться в целостности соответствующего файла путем сравнения значения его CRC-хеша с указанным в SFV-файле. Важно отметить, что ввиду ограничений алгоритма CRC32 файлы SFV нельзя применять для проверки достоверности файлов — что перед вами именно тот файл. По этой причине в UNIX-системах для вычисления хеш-значений предпочитают использовать алгоритмы MD5 и SHA-1.

Прочие файлы

Помимо FILEJD.DIZ и NFO-файлов архив с релизом может содержать и другие сопроводительные файлы — например, текстовый файл README (от англ. read me, прочти меня). Такой файл обычно имеет имя rêadme.txt, README (без расширения), readme.lst (от read me first, сначала прочти меня), read.те. Иногда в архиве имеется несколько таких файлов на разных языках. На язык файла может указывать его расширение: readme.en, readme.ru, readme.by или перевод имени файла: leeme, lisezmoi.txt, czytajto.txt. В некоторых случаях (часто вместе с текстовой версией) файл может быть представлен в HTML (readme'html) или других форматах— например, WRI (readme.wri), RTF (readme.rtf) или Microsoft Word (readme.doc). Файл README обычно включает:

- информацию о системных требованиях;
- инструкции по установке программы (иногда выносится в файл INSTALL);
- инструкции по настройке;
- инструкции по управлению программой (список файлов);
- информацию о лицензии и авторском праве (иногда выносится в файл COPYING/LICENSE);
- контактную информацию разработчика и/или распространителя;
- известные ошибки (иногда выносится в файл BUGS);
- инструкции по устранению неполадок;
- сведения об авторах (иногда выносятся в файл AUTHORS) и благодарности (иногда выносятся в файл THANKS);
- протокол изменений программы (обычно выносится в файлы типа ChangeLog и What's new).

Некоторые архивы с релизами программного обеспечения могут сопровождаться файлами FAQ (Frequently asked questions, часто задаваемые вопросы) и ToDo (содержащем информацию о планируемых изменениях в будущих версиях), а также файлом Description (описание). Как правило, файлы подобного рода создаются самими разработчиками, а не варезными группами.

Последствия нарушения стандартов

Если группа нарушает стандарт или повторяет чужой релиз, то релиз объявляется *нюкнутым* (Nuke), т. е. его контент считается недопустимым, — и удаляется из каналов распространения. Другая группа выпускает после этого «правильный» релиз. В некоторых случаях релиз «нюкается» спустя какое-то время после выпуска — если, к примеру, пользователи обнаружили в релизе нерабочий патч или недействующий серийный номер.

Аудио- и видеорелизы

Правила Сцены определяют, в каком формате и как должен распространяться контент каждого типа.

Типы видеорелизов

Типы видеорелизов в зависимости от источника с сортировкой по качеству от самого низкого до самого высокого приведены в табл. П2.1.

Таблица П2.1. *Типы видеорелизов*

Название	Обозначение	Источник	Качество	Оперативность
Cam	**CAM CAMRip**	**Съемка зрителем в зале кинотеатра**	**Крайне низкое качество звука и видео**	**Во время проката**
Так называемая «экранка», снятая в кинотеатре на видеокамеру или мобильное устройство. Источником звука является встроенный микрофон камеры, поэтому качество звука оставляет желать лучшего. В кадр могут попадать силуэты/головы зрителей и их голоса или смех. Качество видеоизображения «экранки» зависит от умения оператора держать камеру, наличия штатива и примененного кодека. Такие релизы распространены, обычно имеют самое плохое качество и появляются в ближайшие дни после официальной премьеры фильма				
TeleSync	**TS TeleSync**	**Съемка в пустом зале кинотеатра камерой (как правило, профессиональной) на штативе**	**Качество видео низкое, звук зависит от источника**	**Во время проката**
Копия, снятая в кинотеатре на камеру, установленную на штативе (часто применяется профессиональная камера из проекционной будки). Основное отличие от CAM в том, что звук в TS записывается со специального источника (например, FM-аудио). Качество превосходит обычную «экранку» — особенно звук, который полностью избавлен от присущих «экранке» посторонних шумов и эха				
Super TeleSync	**SuperTS Super-TS**	**Обработанная на компьютере копия TeleSync**	**Качество видео низкое, звук зависит от источника**	**Во время проката**
Telesync, обработанная через компьютер, — фильм осветлен, выровнен, убраны посторонние шумы изображения и звука и т. п. Качество, как правило, хорошее, но зависит от релизера				
PDVD	**PDVD preDVD PDVD-rip**	**«Экранка», записанная на DVD**	**Качество видео низкое, звук зависит от источника**	**Во время проката**
Тип релиза DVD, также известный как preDVD, в основном распространен в Индии. Низкокачественные «экранки» CAM/TS записываются на DVD для продажи на улицах, после чего некоторые варезные группы делают с них рипы и выпускают с меткой PDVD-rip. Из-за схожести меток часто путаются с DVD-rip				

Таблица П2.1 *(продолжение)*

Название	Обозначение	Источник	Качество	Оперативность
VHSRip	VHSRip	Видеокассета VHS	Низкое, среднее	
Обычно VHSRip делается, когда попр)осту нет более качественного источника. Часто это бывают сериалы, которые демонстрировалась в 1980-1990-х и не переиздавались официально на других носителях (а также давно не повторялись по мировому ТВ), документальные фильмы, телепередачи и редкие ТВ-заставки/реклама. Иногда и видеофильмы, предварительно выпущенные на кассетах, могут содержать вырезанные сцены, которые по каким-то причинам не включены в ОУС)-версию. качество такого материала обычно низкое (но выше «экранок» хотя бы по качеству звука). Носитель устарел				
BetacamRip	BetacamRip	Видеокассета Betacam	Низкое, среднее	
Аналогично VHS Rip, рип с профессиональной ленты Betacam и делается, когда не! источника				более качественного
WORKPRINT	WP WORKPRINT	«Вынос» копии сотрудниками кинокомпании	Среднее	До премьеры фильма
Это так называемая «Бета-версия» фильма. Самый оперативный источник, но не обладающий хвастающийся лучшим качеством. Обычно выходит в формате VCD намного раньше начала показа в кинотеатрах мира, Из-за того, что это предварительная версия фильма, качество материала может быть как отличным, так и очень низким. Промежуточная >ерсия может отличаться от окончательной — некоторые сцены могут отсутствоЕ»ать или присутствовать сцены, не вошедшие в финальную вер» ю, отсутствовать эффекты, не у6f>аны ляпы. На экране иногда отображается временной таймер вверху или внизу экрана (он нужен для ПК следующего монтажа окончательной верии) и/или водяной знак				
Telecine	TC TELECINE	Съемка пленки сотрудниками кинотеатра	Хорошее	Во время проката
Съемка пленки делается работниками кинотеатров с помощью телекинодатчика — дорогого и громоздкого оборудования. До эпохи DVD эта технология давала наилучшее доступное качество видео, но сейчас потеряла свою популярность. Качество обычно хуже DVD, т. к. изображение может двигаться из стороны в сторону или иметь искаженную цветопередачу				
PPVRip	PPVRip PPV	Телевизор в номере отеля	Хорошее	Во время проката
Pay-Per-View — видео, которое было сделано в номерах отеля, источником является телевизор в номере отеля, запись произведена на PVR или DVD-рекордер. Все релизы PPVRip — новейшие фильмы, еще не вышедшие на DVD				
Screener	SCR SCREENER DVDSCR DVDSCREENER BDSCR VHSSCREENER	«Вынос» копии работниками, организующими показ	От хорошего до очень хорошего	До премьеры фильма или во время проката
Утечка промо-копий фильма, которые раздаются критикам и другим людям, связанным с видеоиндустрией. В таких фильмах есть большое количество титров, предупреждающих о том, что «распространение запрещено, если вы приобрели этот фильм, звоните по номеру I-8OO-NO-COPIES» и т. п. Некоторые части фильма могут быть черно-белыми. В некоторых релизах изображение может кадрироваться с целью удаления титра с предупреждением. Качество изображения зависит от источника (VHS, DVD и т. д.) и, как правило, хуже обычных DVD				
LaserDisc-RIP	LDRip	Лазерный диск	Хорошее	–
Рип с лазерного видеодиска может быть как лучше, так и несколько хуже по качеству DVDRip. Носитель устарел				
VideoCD-RIP	VCDRip	Компакт-диск	Хорошее	–
Рип с компакт-диска Video CD. Носитель устарел				

Таблица П2.1 *(продолжение)*

Название	Обозначение	Источник	Качество	Оперативность
DDC	DDC	Каналы цифровой дистрибьюции	Хорошее	До премьеры фильма или во время проката
Релиз типа DDC схож со Screener, но передан сотрудникам в цифровой форме (через протоколы FTP, HTTP и т. д.), а не на физических носителях, поэтому распространение упрощается и удешевляется. Качество релиза ниже, чем R5, но выше, чем Cam или Telesync В варезной Сцене понятие DDC также относится к загружаемому цифровому контенту, который недоступен для свободного (бесплатного) скачивания				
R5	R5 R5.LINE R5.AC3.5.1.HQ		Очень хорошее	Во время проката или после выхода на DVD

R5 — региональный код DVD, предназначенного для продажи в регионе 5 (см. далее). Релизы R5 отличаются от обычных релизов тем, что созданы путем прямой передачи видеоматериала (Telecine) без какой-либо обработки изображения.

Другие метки регионов:

- **R0 — неформальное обозначение «во всем мире». Такие диски не имеют определенного кода;**
- **R1 — Бермуды, Каймановы острова, Канада, США и зависимые территории;**
- **R2 — Европейский союз, Азербайджан, Албания, Андорра, Армения, Бахрейн, Босния и- Герцеговина, Ватикан, Гернси, Гренландия, Грузия, Джерси, Египет, Йемен, Израиль, Иордания, Ирак, Иран, Исландия, Испания, Косово, Кувейт, Лесото, Ливан, Лихтенштейн, Македония, Молдавия, Монако, Остров Мзн, Норвегия, Объединенные Арабские Эмираты, Оман, Сан-Марино, Саудовская Аравия, Свазиленд, Сербия, Сирия, Турция, Фарерские острова, Французская Гвиана, Хорватия, Черногория, Швейцария, Южная Африка, Япония;**
- **R3 — Юго-Восточная Азия, Гонконг, Макао, Тайвань, Южная Корея;**
- **R4 — Карибский бассейн, Мексика, Центральная Америка, Южная Америка (за исключением Французской Гвианы), Океания;**
- **R5 — Африка (за исключением Египта, ЮАР, Свазиленда и Лесото), Беларусь, Казахстан, Киргизия, Монголия, Россия, Северная Корея, Таджикистан, Туркменистан, Узбекистан, Украина, Южная Азия;**
- **R6 — Китайская Народная Республика (за исключением Макао, Гонконга и Тайваня);**
- **R7 — зарезервировано для использования в будущем;**
- **R8 — для специального международного использования (самолеты, круизные лайнеры и т. п.);**
- AH **— диски региона ALL позволяют проигрывать диски в любом регионе, на любом DVD-, HD-DVD-проигрывателе.**

Диски с кодом R1 и R2 считаются обладающими высшим качеством

DVDRip	DVDRip	DVD	Очень хорошее	После выхода или утечки DVD

DVD-фильм для экономии размера пережатый другим кодеком. Как правило, в качестве источника выступает розничный DVD, иногда предназначенный для продажи в другом регионе и включающий дополнительные звуковые дорожки (или субтитры) на языке страны, в которой распространяется. Почти всегда имеет расширение AVI или MKV. Наиболее часто встречаются рипы следующего размера:

- **700 Мбайт (1 на 1 CD, 6 на DVD) — применяется почти всегда;**
- **1400 Мбайт (1 на 2 CD, 3 на DVD) — применяется почти всегда (обеспечивает лучшее качество);**
- **2100 Мбайт (1 на 3 CD, 2 на DVD) — обычно применяется для длительных фильмов;**
- **4200 Мбайт (1 на 6 CD, 1 на DVD) — применяется редко для продолжительных фильмов и мини-сериалов**

Таблица П2.1 *(продолжение)*

Название	Обозначение	Источник	Качество	Оперативность
DVD	DVD-5 DVD-9	DVD	Очень хорошее	После выхода или утечки DVD
Копия диска с сохранением оригинальной структуры. DVD-5 — однослойный, DVD-9 — двуслойный. Если источник выпущен на двуслойном DVD (или в двух- или более дисковом издании), некоторые дополнительные материалы (звуковые дорожки, субтитры) могут быть удалены, а видеоизображение может быть пересжато, чтобы уместить на однослойный DVD				
TVRip SATRip	DSR DSRip DTHRip DVBRip HDTV PDTV TVRip tPTVRip HDTVRip SATRip VODRip VODR Transport Stream	Запись с телевизионного потока	От среднего до очень хорошего	После показа на ТВ
Обычно источник сигнала — кабельное телевидение или эфирные каналы (TVRip), в случае SATRip, DVBRip и DSRip — спутник. Также источником может служить цифровое IP-телевидение (IPTVRip). Довольно хорошее качество, но изображение может сопровождать логотип канала, реклама и т. п. Часто используется для записи редких фильмов и мультсериалов, которые не выходили на DVD. PDTV (Pure Digital Television, в дословном переводе: Чистое цифровое телевидение) —телевидение с качеством ниже стандарта HDTV, но лучше кабельного. Обычно логотип канала в таких рипах отсутствует. Качество такого видео граничит с DVDRip. Transport Stream — необработанный (сырой) аудио/видеопоток, взятый напрямую с цифрового телевидения HDTV — рип трансляции с HDTV-канала. Высокое разрешение, но может присутствовать логотип канала. Качество зависит от канала и может превосходить DVD. Аббревиатура VOD расшифровывается как Video On Demand, Видео по запросу. По качеству релизы с такой меткой за редким исключением сравнимы с DVDRip. Релизы TVRip, DSR и PDTV часто имеют разрешение видеоизображения, равное 512*384 или 640*352 пиксела. Релизы HDTV имеют разрешение видеоизображения от 640*352 (360p), 960*528 (540p) и 1280*720 (720p) до 1920*1080 (1080p) пикселов. Может использоваться обозначение (после разрешения, например, 1080p) — i (interlaced scan, чересстрочная развертка), когда изображение формируется из двух полукадров (как в обычном телевидении), или p (progressive scan, прогрессивная развертка), когда кадр передается и формируется целиком, при этом изображение в движении не искажается. Недостаток progressive — увеличенный в два раз поток по сравнению с interlaced. Следствие — больший размер файла или меньшая частота кадров				
DTheater	D-VHS DTheater DTheater-Rip	Кассета D-VHS	От очень хорошего до отличного	
Оцифровка кассеты высокой четкости. Качество видео достаточно высокое Может присутствовать шум и нечеткость изображения Устаревший носитель				

Таблица П2.1 *(окончание)*

Название	Обозначение	Источник	Качество	Оперативность
HD DVD	**HD DVD HD-DVD HD-DVD Rip HD-DVD Remux HD DVD HDDVD-Rip HDDVD-Remux HDDVD Rip HDDVD Remux**	**Диск HD DVD**	**Отличное**	**Устаревший носитель**
Рип с HD DVD-диска, качество сравнимо с Blu-ray. HDDVD — полная копия диска (1:1), Rip — сжатая копия, обычно с вырезанными дополнительными материалами и лишними звуковыми дорожками, (Четих — пересобранная копия диска без меню, видео не подвергается пересжатию				
WEB-DL	**WEB-DL Rip WEB-DL WEB-Rip**	**Интернет-магазин цифрового контента**	**От хорошего до отличного**	**После появления цифровой копии в Интернет-магазинах**
Это трансляция через Интернет в улучшенном качестве по сравнению с HDTV. Нет ни логотипов, ни рекламы. Источниками являются различные платные сервисы — такие, как iTunes. По качеству лишь немного уступает качеству Blu-Ray. Изначально цифровые или профессионально перекодированные копии обычно имеют разрешение, соизмеримое с DVD-rip, или 720p HD-DVD/Blu-Ray				
Blu-ray	**Blu-ray BDRip BD Remux**	**Диск Blu-ray**	**Отличное**	**После релиза на Blu-ray**
Blu-ray — полная копия диска (1:1), Rip — сжатая копия, обычно с вырезанными дополнительными материалами и лишними звуковыми дорожками, Remux — пересобранная копия диска без меню, видео не подвергается пересжатию. Конвертируемый в MKV-контейнер (Matroska) HD DVD или Blu-ray без какого-либо сжатия, но с вырезанными дополнительными материалами, ненужными звуковыми дорожками и субтитрами. Иногда для обозначения однослойных (25 Гбайт) и двуслойных (50 Гбайт) дисков используется маркировка BD5/BD9 (или BD25/BD50). После DVD самый распространенный тип видеорелизов, популярность которого только увеличивается				
UHDTV	**UHDTV DMRip**	**UHDTV**	**Наилучшее**	–
Видео нового поколения в формате UHD (Ultra-High Definition, сверхвысокой четкости) с разрешениями 4K (3840x2160, 2160p), 8K (7680x4320, 4320p) и, в будущем, 16K (15360x8640, 8640p). Разрешающая способность стандарта 8K считается сопоставимой с кинопленкой формата IMAX 15/70 и примерно в 16 раз превосходит формат HD. DMRip расшифровывается как DigitalMedia Rip. На момент создания книги релизов в формате UHD было крайне мало, в частности, из-за отсутствия источников и крайней требовательности к аппаратному обеспечению компьютера. Кстати, вы уже можете попробовать воспроизвести на своем компьютере первые видеозаписи в разрешении 8K: tinyurl.com/ogdukwn или tinyurl.com/q74p452. Не забудьте выбрать разрешение 4320p в настройках проигрывателя				

Помимо указанных типов видеорелизов в именах реализуемых файлов могут указываться следующие метки:

- 3D — трехмерная версия фильма для просмотра на специальных телевизорах/мониторах и/или с использованием специальных очков;
- AC3 (Dolby Digital) — звуковая дорожка записана в многоканальном формате;

- AVO (Author Voice Over) — авторский одноголосый перевод;
- D — дублированный перевод;
- Director's Cut (DC), режиссерская версия — специальная версия фильма, представляющая фильм с точки зрения режиссера, а не отредактированная согласно требованиям заказчиков, MPAA, прокатчиков, студии, кинокритиков и т. д.;
- DTS — звуковая дорожка записана в расширенном многоканальном формате;
- DUB (Dubbing) — дубляж (дублированный) перевод;
- Dubbed — из фильма убран оригинальный звук. Например, взяли дорожку из русского кинотеатра и наложили на американский релиз. Может быть еще Mic.Dubbed — то же, что и Dubbed, только звук записан микрофоном в кинотеатре. Третий вариант — Line.Dubbed — то же самое, что и Dubbed, только в этом случае звук взят из «кресла» или «проектора» (Line);
- DUPE — второй релиз того же фильма другой варезной группой (обычно краденный у первой);
- DVO (2VO), Double Voice Over — двухголосый перевод;
- Fullscreen (FS)— релиз в полноэкранном режиме, разрешение видео 3:4. Часто Fullscreen делают из Widescreen-**Вересті** методом Pan and Scan (PS), обрезая часть кадра по бокам;
- Hardsub — субтитры внедрены в видеопоток;
- L — любительский многоголосый перевод (многоголосый отличается от дубляжа тем, что слышна оригинальная звуковая дорожка);
- L1 — любительский одноголосый перевод;
- L2 — любительский двухголосый перевод;
- Letterbox — один из изначальных вариантов записи широкоэкранного видео на DVD (другой — Widescreen (WS)) — изображение, обычно 16:9, не растянуто на весь кадр, а оставлены черные полосы сверху и снизу;
- LIMITED — фильм был показан в ограниченном количестве кинотеатров;
- MKV — файл сжат в формате MKV (Matroska). Такие файлы, в отличие от формата AVI, не воспроизводятся на большинстве аппаратных проигрывателей и телевизоров (без использования компьютера);
- MVO (Multi Voice Over, MULTi) — многоголосый (три и более) перевод (многоголосый отличается от дубляжа тем, что слышна оригинальная звуковая дорожка);
- O — оригинал (в русских фильмах);
- P — профессиональный многоголосый перевод (многоголосый отличается от дубляжа тем, что слышна оригинальная звуковая дорожка);
- P1 — профессиональный одноголосый перевод (зачастую авторский);
- P2 — профессиональный двухголосый перевод;
- Pan and Scan (PS) — метод преобразования Widescreen (WS) видео в полноэкранный режим Fullscreen (FS). При этом обрезается часть кадра справа и слева;
- PROPER — повторный релиз фильма (иногда другой группой) в связи с плохим качеством предыдущего;

- RECODE — релиз, переделанный в другой формат или заново кодированный;
- RERIP — новый рип фильма;
- Softsub — субтитры идут отдельным файлом/потоком и выводятся самим проигрывателем;
- Special Edition (SE), специальная версия фильма — примером может служить отреставрированная версия «Звездных войн» с добавлением на материал 1970-х годов компьютерной графики, анимации, 3D-моделей;
- Straight To Video (STV) — фильм сразу вышел на DVD, минуя кинотеатры;
- SUB (Subtitle) — субтитры (возможно, используемые в качестве перевода, когда голосовой перевод отсутствует);
- SVO (IVO) (Single Voice Over) — одноголосый перевод;
- WATERMARKED — небольшой логотип TV-канала или релизера;
- Widescreen (WS) — один из изначальных вариантов записи широкоэкранного видео на DVD (другой — Letterbox), анаморфированный (изображение, обычно 16:9, растянуто на весь кадр 4:3 — в итоге качество лучше);
- x264 — файл сжат в стандарте H.264;
- XViD — файл сжат кодеком Xvid.

Типы аудиорелизов

Для распространения аудиоконтента используются два основных способа его сжатия:

- формат MP3 предполагает сжатие с потерями, обеспечивая малый размер файла при относительно высоком качестве звучания (зависит от битрейта, вплоть до 320 Кбит/с — чем выше число, тем выше качество звука, но и больше размер файла. Меткой VBR обозначается переменный битрейт, значение которого варьируется по мере необходимости, — тем самым обеспечивается более высокое качество звучания при малом размере файла).

  Во всех аудиофайлах должны быть заполнены теги ID3 vi.1 и ID3 v2.0, содержащие внутри каждого файла информацию об имени исполнителя, названии композиции, жанре и т. п.;
- сжатие без потерь осуществляется с помощью кодека FLAC — качество звучания сравнимо с исходным Audio CD или DVD, но и размер файла соответствующий. Битрейт таких файлов достигает 1 Мбит/с и выше.

Все релизы в отношении музыкальных альбомов (читайте, набора музыкальных композиций не обязательно определенного исполнителя) подпадают под несколько классификаций. Основным вариантом классификации считается сортировка по объему альбома:

- LP (от англ. Long Play) — обычный «стандартный» альбом, выпущенный на пластинке или компакт-диске[1] и имеющий продолжительность звучания в 30-80 минут;
- EP (от англ. Extended Play) — мини-альбом, выпущенный на компакт-диске и чаще всего имеющий продолжительность звучания в 15-20 минут. Многие путают EP-релизы с синглами, забывая, что отличительной чертой мини-альбомов является присутствие более трех различных композиций;

[1] **В этом случае в названии релиза дополнительно указывается аббревиатура CD (Compact Disc).**

- SP, Single (от англ. Single Play) — альбом (сингл), выпущенный на пластинке или компакт-диске и имеющий продолжительность звучания не более 20 минут. В отличие от мини-альбома, сингл чаще всего содержит одну композицию и несколько ее ремиксов[1]. Синглы с большей длительностью звучания называются макси-синглами (Maxi-single).

Вам могут встретиться и такие слова, как «bootleg» — бутлег (неофициальный альбом[2]), «live» (запись с концерта), «promo» или «promotional» (специальная версия релиза для бесплатного распространения с целью продвижения альбома), «demo» — демо (демонстрационная запись до выхода релиза), «tribute» — трибьют (сборник кавер-версий композиций исполнителя, т. е. версий, исполненными другими артистами), «dubplate» — дабплейт (официально неизданный музыкальный трек, часто «сырой»).

Часто релизы обозначаются VA (Various Artists) — это не что иное, как сборник композиций разных исполнителей, типа «Союз-19» или Reactivate 18.

Другая аббревиатура, часто характеризующая релиз, — OST (Original SoundTrack), обозначает саундтрек, т. е. сборник композиций, служащий для оформления какого-либо фильма, мультфильма, игры и т. п. и продающийся отдельно. При этом саундтрек может именоваться score, что означает записи оригинальных звуковых дорожек композиторов, созданных именно для того или иного фильма (и т. п.).

Как правило, звуковые дорожки релизов могут быть смиксованы[3] (mix, mixed) или же записаны отдельными композициями (tracks).

Это лишь часто встречающиеся термины в отношении релизов. Более подробно о классификациях аудиорелизов вы можете узнать на странице tinyurl.com/hsj5uku.

Релизы программного обеспечения

Релизы приложений разделяются, как правило, на две большие категории: 0-day и ISO. Меткой 0-day, как уже отмечалось ранее, обозначают любое нелегально (с нарушением условий лицензионного соглашения и авторского права) распространяемое приложение, выпущенное в тот же день, что и оригинальный продукт, а иногда даже раньше. Такие релизы считаются верхом мастерства среди варезных групп.

- Релизы 0-day чаще всего имеют размер не более 150 Мбайт, хотя встречаются дистрибутивы размером вплоть до 5 Гбайт и более, не представленные в виде образов CD/DVD. Кроме того, в категории 0-day часто публикуются крэки и кейгены (генераторы ключей) для различных приложений и небольшие игры размером от 1 до 50 Мбайт. Иногда в категории 0-day выпускаются электронные книги, сеты (наборы) изображений, шрифты и приложения/игры для мобильных устройств.
- В категории ISO обычно представлены релизы в формате BIN/CUE или ISO. Допустимы образы дисков CD и DVD, но релиз должен быть меньше по размеру, чем объем носителя. В релиз должен быть вложен рабочий ключ активации или генератор ключей, чтобы

[1] От англ. Re-Mix — измененная версия музыкального произведения. Тип ремикса обозначается после названия композиции: Paul van Dyke remix (указание диджея, выполнившего ремикс), original remix или original mix (вариабельное название ремикса, как правило, выполненное самим исполнителем оригинальной версии) и т. п.

[2] Не следует путать с официальными релизами, распространяемыми пиратскими способами.

[3] Дорожки беспрерывно следуют одна за другой, зачастую звучание их накладывается друг на друга.

можно было запустить продукт в рабочем режиме. Крэк может потребоваться и для обхода защиты, созданной с помощью аппаратных средств, таких как USB-чип.

Тех же правил варезные группы поддерживаются при создании релизов игр и приложений для мобильных устройств.

Инструменты обхода защиты программ от нелегального копирования

Чтобы нелегально распространяемое приложение заработало, необходимо обойти/сломать встроенные механизмы защиты от нелегального использования. Существует несколько основных инструментов, с помощью которых это осуществляется:

- **серийный номер, серийник (Serial)** — подлинный серийный (активационный или связка «серийный + активационный номера») номер может быть реально куплен и распространен или же сгенерирован. Как правило, серийные номера распространяются в виде текстовых файлов с расширениями **TXT** или **NFO** (рис. **П2.3).** Чаще всего при первой же проверке через Интернет такой серийник заносится в черный список, и регистрация приложения блокируется;

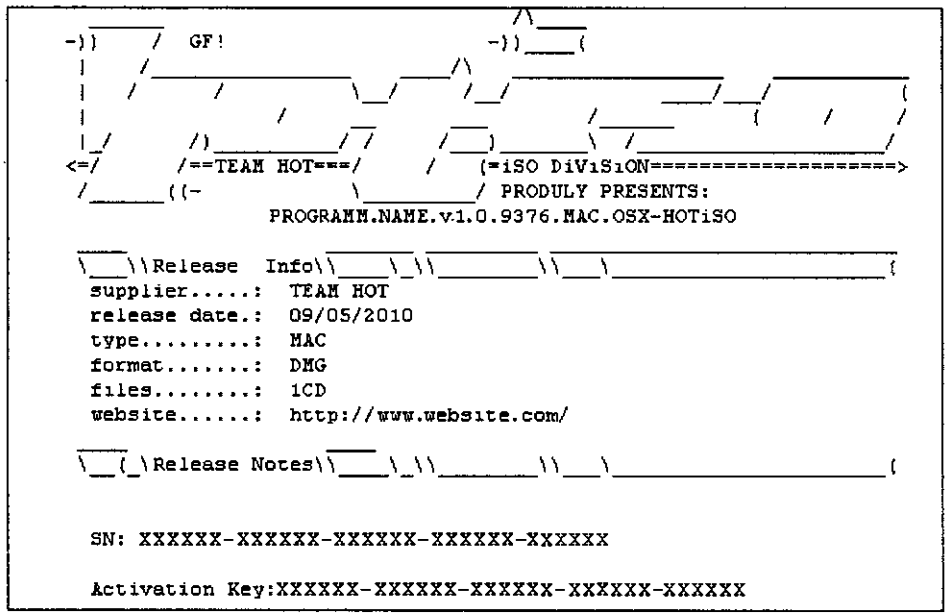


Рис. П2.3. Содержимое NFO-файла с серийным и активационным ключами

- **генератор ключей (Keygen, key generator)** — небольшое приложение, основная функция которого заключается в генерации допустимых серийных/активационных номеров программ (рис. П2.4, *справа).* В некоторых случаях требует обработки, как правило, исполняемых или DLL-файлов продукта инструментом вида patch. Весьма часто подобные приложения содержат вредоносный код (троянского коня и т. п.);
- **создатель ключей (Keymaker)** — в отличие от генератора ключей (keygen), создатель ключей предназначен для генерации отдельного файла, необходимого для запуска или полноценной работы приложения. Такие файлы (с расширениями REG, KEY и др.) со-

держат информацию о лицензии и превращают демонстрационную версию программы в полную;

> ***ЧТОБЫ ВЗЛОМ НЕ БЫЛ СКУЧНЫМ...***
>
> **Многие генераторы ключей, патчи и тому подобные приложения во время своей работы воспроизводят фоновую музыку, как правило, трекерную. Об этом подробнее см. в** *приложении 3,* **посвященном компьютерному искусству.**

- эмулятор ключей **(Key emulator)** — инструмент для обхода защиты ПО, используемого для активации, или электронного ключа (например, подключаемого к порту USB компьютера). Эмулятор ключей эмулирует ключ, т. е. имитирует ситуацию, как будто требуемый программе (для лицензирования) ключ установлен в системе. Реальный ключ может быть выполнен, к примеру, в виде Flash-диска, эмулятор же создает виртуальный Flash-диск, как бы «подключенный» к компьютеру;
- **патч (Patch)** — инструмент, предназначенный для обработки определенных файлов, как правило, уже установленного приложения (рис. П2.4, *в центре*). Суть — в изменении фрагмента кода файлов, отвечающего за активацию программы. Весьма часто подобные приложения содержат вредоносный код (троянского коня и т. **п.);**

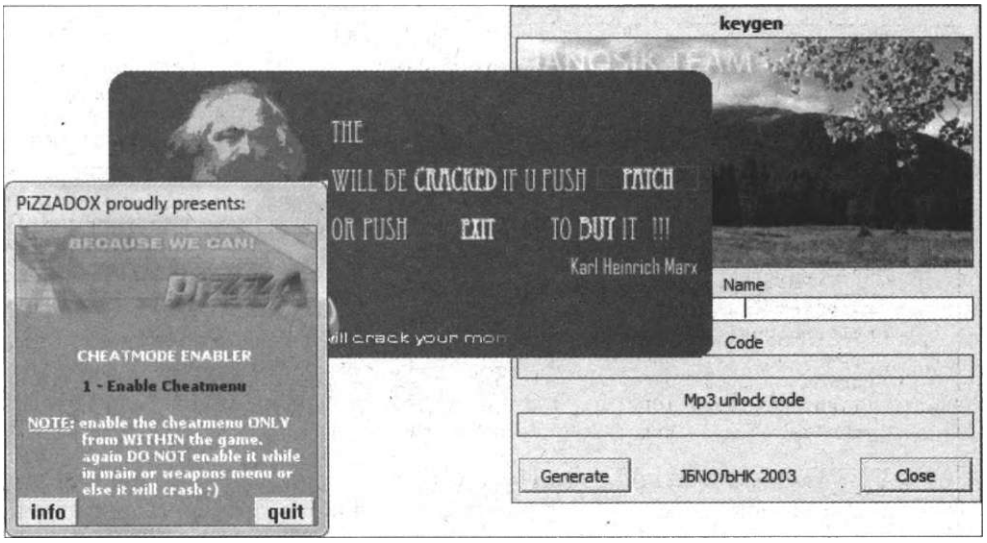


Рис. П2.4. Трейнер *(слева),* **патч (в** *центре)* **и генератор ключей** *(справа)*

- **крэк (Crack, cracked exe, кряк)** — исполняемый (или другой файл, отвечающий за лицензирование программы) файл с измененным кодом, которым нужно заменить оригинальный файл приложения после установки. Очень часто нарушает функциональность программ — к примеру, остаются недоступными функции, которые должны быть разблокированы в полной версии;
- регистрационный **файл (Regfile)** — представляет собой файл реестра (обычно с расширением REG), содержащий регистрационную информацию. После активации пользователем такого файла регистрационные данные записываются в реестр;
- **загрузчик (Loader)** — небольшая программа, которая запускается перед самим программным обеспечением (в том числе и нелегально используемой операционной систе-

мой), с целью обойти его защиту (к примеру, обнуляя дату установки или первого запуска). Инструмент весьма опасный и способный вывести компьютер из строя как программно, так и аппаратно (существуют загрузчики, перепрошивающие BIOS);

- **эмулятор (Emulator)** — приложение, служба или виртуальный сервис, запускаемые и/или поддерживаемые в рабочем состоянии для функционирования нелегально распространяемого приложения. Так, одним из способов активации Windows 8 служил вариант с эмуляцией KMS-сервера, проводящего активацию;
- **трейнер (Trainer)** — по большому счету трейнеры относятся к приложениям, изменяющим код в играх в реальном времени (т. е. запускаются одновременно с игрой). Используются, к примеру, для блокировки какого-либо значения (установки бесконечного уровня «жизни» и т. п.). Также существуют читы (Cheats), или чит-коды, позволяющие выполнить ту же операцию с помощью ввода определенного кода до запуска игры или во время него. Как правило, чит-коды предусмотрены разработчиками игры и совершенно легальны (рис. П2.4, *слева).*
- **NoCD (NoDVD, отвязывалка и пр.)** — приложение (либо пропатченный (взломанный) оригинальный файл приложения), изменяющее код (исполняемого) файла (файлов), как правило, игры, с целью обойти защиту, требующую для работы программы (игры) оригинального диска с дистрибутивом в приводе компьютера (по технологиям защиты от копирования, таким, как SafeDisc, StarForce и др.). Как правило, NoCD распространяются в двух вариантах: небольшой NoCD-патч или же пропатченный (исполняемый) файл (файлы) программы;
- **русификатор (а также англофикаторы и пр.)** — этот инструмент также можно отнести к нелегальным, т. к., по сути, он тоже изменяет код программного обеспечения нелицензионным способом. Используя его, вы точно так же нарушаете лицензионное соглашение, которое подтверждаете на этапе инсталляции программы.

Любое использование перечисленных инструментов ведет к нарушению подтверждаемых вами при установке ПО лицензионных соглашений и, соответственно, к административной и уголовной ответственности. Кроме того, в большинстве случаев эти инструменты содержат вредоносные приложения, которые могут нарушить работу операционной системы, удалить/изменить ваши документы, и даже повлиять на функционирование аппаратной части компьютера.

Нелегальными действиями признаются также использование полных версий (Retail или OEM) программ, которые не распространяются свободным образом, а предназначены для продажи конечным пользователям или корпоративным клиентам, использование образов (ISO и др.) дисков с программным обеспечением (в том числе и игр).

В сегодняшней ситуации производители программного обеспечения идут на разные ухищрения, чтобы ограничить обращение пиратских версий их продуктов. К примеру, введенные вами серийные номера без вашего ведома могут проверяться на валидность (легальность) на веб-сайтах производителей, и в случае обнаружения нелегальной попытки использования приложение блокируется. Ничто не мешает при этом получить данные о вашем IP-адресе и через провайдера выяснить ваше местонахождение. Имейте это в виду.

' Также подобное ПО, связанное с диском, может распространяться в виде образов дисков или же мини-образов дисков, которые эмулируются программами типа Daemon Tools как виртуальный привод с носителем.

Создание и/или распространение вареза незаконно в большинстве стран. Наибольший процент пиратства прослеживается, как правило, в странах третьего мира с низким уровнем доходов населения. Кроме того, в некоторых странах распространению вареза способствуют имеющиеся лазейки в законодательстве.

Преследование по закону

АНТИПРАТСКИЕ АФЕРЫ

На странице tinyurl.com/nf5fhtk вы можете прочитать статью про интересный способ борьбы с пиратством.

Как уже неоднократно отмечалось, распространение и использование вареза (контрафактных материалов) — форма нарушения авторских прав, наказуемого как любое другое гражданское правонарушение или уголовное преступление. Законы и наказания в сфере нарушений прав интеллектуальной собственности от страны к стране разнятся. В России, согласно ст. 273 УК РФ, «создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев». Если же действия повлекли тяжкие последствия или создали угрозу их наступления, виновные наказываются лишением свободы на срок до семи лет. Кроме того, если на сайте обнаружен нелицензионный контент, согласно закону 187-ФЗ по требованию правообладателя контент должен быть удален, в противном случае доступ к ресурсу может быть заблокирован. Упомянутые законы действовали на момент подготовки книги и могут быть изменены к тому времени, когда вы читаете эти строки.

Опасности, связанные с использованием вареза

Всемирная паутина сравнима с городами мрачного будущего, демонстрируемого в американских фантастических экшенах. Вы можете годами пользоваться поисковыми системами, почтовыми службами и иногда просматривать новостные сайты, совершенно не подозревая о существовании темной стороны Всемирной паутины — своеобразных ее трущоб. В этих недрах можно найти все. Проще даже перечислить на пальцах одной руки то, чего вы там не найдете...

Разумеется, практически все это незаконно и «грязно» в плане обилия вирусов, насилия и порнографии Если вы и забредете сюда, то столкнетесь с массой всплывающих назойливых рекламных окон, содержащих прямо-таки требования отправить платные SMS — просто так или за какие-то невообразимые услуги, а также с истерическими предупреждениями антивирусной программы (уж без нее точно туда соваться не стоит).

Рано или поздно мало-мальски любознательный и рисковый пользователь из России, Китая и других стран может попасть на какой-либо из подобных ресурсов. Поэтому я и предлагаю вам познакомиться с опасностями, которые вас там поджидают. Мой рассказ об этих сайтах — ни в коем случае не реклама их содержимого, скорее, руководство — куда не стоит заходить. А также какие (и подобные) сайты стоит заблокировать в браузере, чтобы ваше чадо туда ненароком не заглянуло. В любом случае надо знать о таких местах и никогда ничего с них не скачивать.

Итак, чем может грозить посещение подобных веб-сайтов?

- **Инфицирование вирусами.** Просто посещая эти ресурсы, вы можете инфицировать свой компьютер. Зачастую код их веб-страниц содержит вредоносный код, не говоря уже о зараженных вирусами и троянскими конями файлах, соблазн скачать которые столь велик. Запомните, что бесплатного ничего не бывает, и лучше менее функциональное freeware-приложение, скачанное с официального сайта, чем снабженный «крэком» дорогущий массивный программный комплекс, нашпигованный инфекцией.
- **Опасность финансовых потерь.** Часто на таких сайтах предлагается отправить SMS на определенный номер, чтобы получить доступ к каким-либо греховным и не совсем услугам, часто невозможным (наподобие поиска местонахождения абонента по номеру мобильного телефона), причем дело вряд ли ограничится той незначительной суммой, которую предлагается уплатить за сутки, а поведет к более внушительным затратам. Как правило, отправленное сообщение оплачивает доступ (если его действительно предоставят) к услугам в течение недели, месяца или даже на более длительный срок. И ничтожные 12 руб./сутки превращаются в уже вполне конкретные деньги. В некоторых случаях подключение может прерываться и переподключаться (автоматически) уже через другого провайдера (от присланного позднее внушительного счета волосы у вас на голове встанут дыбом). Часто вместо SMS требуется ввести данные банковской карты — чего уж точно не стоит делать никогда, особенно при подключении по протоколу HTTP (вместо HTTPS), — в этом случае вместе со всеми финансовыми сведениями вы потеряете и средства со счета. Так что — никогда никаких финансовых операций!
- **Кража личной информации.** Украсть любые сведения с вашего компьютера— дело пары минут. Пароли, логины, адреса и телефоны, какая-либо документация — помните, все могут умыкнуть. Для этого существуют троянские кони, кейлогеры, различные скрипты и т. п.
- **Нарушение законодательства.** Ну, само посещение этим не грозит, а вот скачивание размещенных материалов — точно. Смысл существования таких веб-сайтов — в публикации нелегально скопированных музыки/видео, взломанного программного обеспечения и т. п. — всего того, что нарушает чьи-либо авторские права. Запретить вам что-то такое скачать никто не в состоянии, поэтому все ваши действия — на вашей совести.

> ***МОШЕННИЧЕСТВО ВО ВСЕМИРНОЙ ПАУТИНЕ***
>
> **Опасности стать жертвой мошенничества подстерегают во Всемирной паутине на каждом шагу — собственно, на то, чтобы предостеречь вас от него, и предназначена эта книга.**

Скачивая и используя недицензионные материалы, вы должны учитывать три основные причины:

- **Это незаконно.** По сути, использование нелегальных материалов — воровство, за которое может светить реальный срок согласно Уголовному кодексу.
- **Это опасно.** Пользуясь пиратскими программами, вы легко можете стать жертвой кибер-преступников. Нередко вместе со взломанными копиями программ на ваш компьютер скрытно устанавливаются специальные трояны, собирающие и передающие злоумышленнику сведения, найденные на компьютере пользователя: логины/пароли, данные о банковских картах и виртуальных счетах. Кроме того, иногда за скачивание, распаковку, установку или активацию пиратской программы или контента требуется отправить некое SMS-сообщение либо оплатить действие иным способом. Никто не гарантирует, что с вашего счета не будет снята внушительная сумма денег, что номер вашего

мобильного не попадет в списки спам-рассылок, а в итоге вы получите желаемый работающий продукт.

- **Это негативно сказывается на развитии лицензионной продукции и выпуске нового контента.** Приобретая лицензионное программное обеспечение и материалы, а также выплачивая добровольные пожертвования разработчикам бесплатных программ, вы стимулируете дальнейшее их развитие и выпуск новых версий. Покупая лицензионные диски с фильмами и музыкой, вы стимулируете автора на выпуск новых творений, внося свою лепту в сборы.

Кроме того, следует учитывать и следующие моменты:

- **Лицензионная программа не всегда платная.** Разумеется, вы можете считать, что платный софт вам не по карману, и поэтому принципиально пользоваться только взломанными версиями программного обеспечения. Однако существует масса программ, аналогичных платным, но значительно более дешевых или совершенно бесплатных в использовании. Если вам не нужны профессиональные инструменты пакета Microsoft Office, вы вполне продуктивно можете пользоваться бесплатным набором программ LibreOffice. Вместо дорогого «полноформатного» Adobe Photoshop CC можно приобрести его версию Eléments, которая в разы дешевле, или вообще воспользоваться бесплатным, но не менее мощным редактором GIMP. Кроме того, в последнее время распространение получает облачная подписка на приложения — так, если программа Photoshop нужна вам на несколько месяцев для выполнения какого-либо проекта, вы можете подписаться на нее сроком на один год и платить всего 600 руб. в месяц (на момент написания книги).

- **Пользуетесь ли вы своим нелегальным контентом?** Пользуетесь ли вы всеми этими десятками и сотнями программ, устанавливаемых и тщательно взламываемых после очередной переустановки и нелегальной активации операционной системы Windows? Действительно ли вам нужно иметь на компьютере весь пакет программ Microsoft Office или Adobe Creative Suite? И будете ли вы смотреть сотни фильмов и слушать дискографии исполнителей, скачанные с торрент-трекеров? Читать электронные книги с монитора и искать информацию в устаревшей полвека назад базе ГИБДД Челябинска? Возможно, большая часть этого контента вам и не нужна? К тому же, обилие установленных программ негативно сказывается на скорости работы операционной системы, а липшие файлы загромождают жесткий диск.

Ну что, с варезом вроде как разобрались, теперь вы узнаете о ресурсах, распространяющих нелегальные материалы. Для определенных целей эти сайты вы все же можете использовать — например, они одни из первых сообщат вам о выходе новой версии программы, которую вы планируете купить, или опубликуют описание и трейлер видеофильма, чтобы вы могли убедиться, что фильм стоящий, и его следует взять в прокате, посмотреть в кино или приобрести. С тем же успехом вы найдете там треклист нового альбома группы и прочитаете комментарии «нехороших» пользователей, его скачавших и прослушавших. Словом, небольшая польза все же есть...

По сути, большинство таких сайтов лишь аккумулируют ссылки на файлы, размещенные другими пользователями, на других страницах или на файловых хостингах. А файловые хостинга не несут ответственности за файлы, размещаемые на Их серверах, и удаляют их лишь в случае поступления жалобы на тот или иной нелегальный файл (и в некоторых иных случаях). Поэтому крайним и виновным станете именно вы, если воспользуетесь скачанным нелегальным материалом.

Варезные сайты

Можно выделить два основных типа таких сайтов. Первый из них представляет собой нечто вроде блога, где каждый зарегистрированный участник публикует небольшие сообщения, сопровождаемые постером и/или скриншотами. Практически всегда эти материалы размещаются в виде отдельных и многотомных архивов и содержат, если требуется, инструмент их взлома. Вторым типом сайтов представлены ресурсы, публикующие лишь ссылки на сообщения, размещенные на сайтах такого типа.

Ознакомиться с примером сайта первого типа можно, введя в качестве поискового запроса слово warez и перейдя по одной из ссылок, полученных в результатах поиска. Впрочем, делать это я вам крайне не рекомендую, поскольку подавляющее большинство таких ресурсов несет на своих страницах вредоносный код, не всегда обнаруживаемый персональными антивирусными программами вовремя.

Существуют как универсальные (в большинстве своем) варезные сайты (рис. П2.5), так и тематические. Если на первых (warezmix.ru, **софт-варез.рф**, **monkruz.ws**, **gold-warez.com**, **funkysouls.com** и др.) вы найдете самую различную информацию, разделенную по категориям: программы, музыка, видео, игры и т. п., то вторые размещают материалы только определенной категории: музыку в разных стилях (myzuka.ru, ст.йп и др.), электронную музыку (electronicmuz.ru и др.) или музыку в lossless[1]-форматах (lossless-galaxy.ru и др.), видео (edstak.com и др.) и видео в HD-форматах (kinohd.net и др.), графику и связанные



Рис. П2.5. Пример варезного веб-сайта

[1] **Lossless — «сжатие без потерь». В lossless-форматах музыкальные композиции лишены потерь в качестве, присущих таким форматам, как MP3 или WMA. Два самых распространенных формата lossless: APE и FLAC. Сюда же можно отнести музыку в форматах 5.1 и DTS.**

дополнения (**elfpix.ru** и др.) и т. п. Многие из таких сайтов для просмотра ссылок требуют обязательной регистрации.

Ресурсы типа **phazeddl.tv** собирают ссылки на публикации варезных сайтов и, соответственно, отстоят от правосудия еще дальше. На таких сайтах, часто включающих в свой адрес аббревиатуру ddl (DDL — язык Data Definition Language, используемый в качестве движка таких сайтов), вы не найдете описаний, скриншотов и комментариев посетителей — только ссылки, состоящие из названия, даты добавления и типа контента. Пример такого сайта приведен на рис. П2.6.

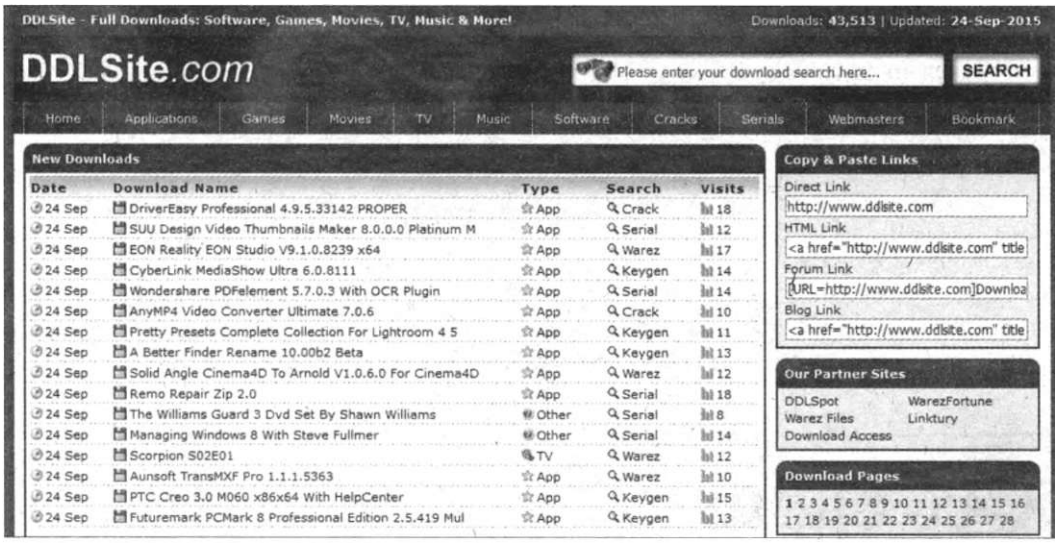


Рис. П2.6. Пример ресурса, аккумулирующего ссылки

Каким сайтом вы бы ни воспользовались, помните, что скачивая варез и иные нелицензированные материалы, вы нарушаете законодательство и подвергаете свой компьютер разного рода напастям — от заражения вирусами до кражи личной и финансовой информации.

Кроме того, как указывалось ранее, при посещении подобных ресурсов вас постоянно будут преследовать всплывающие окна. Чтобы их закрыть, ищите в любом из углов всплывающего окна элементы управления в виде крестика **x** или соответствующие слова (Exit, Выход, Закрыть, Close и т. п.). Будьте внимательны — в некоторых случаях попытка закрыть подобные окна (чаще всего прямоугольные или длинные) все равно может приводить к открытию рекламной страницы на новой вкладке или в окне браузера. Возможно, в этом случае рациональнее будет не трогать всплывающие окна вовсе. Особенно настойчивые рекламные окна сопровождаются появлением диалогового окна с предложением оплаты услуг, которое вновь появляется при попытке его закрыть (рис. П2.7). При этом перейти на другую вкладку становится невозможным.

Решения два — первое заключается в закрытии браузера (иногда через диспетчер задач) и запуске его вновь. Второе — в удерживании клавиши <Esc> и одновременном щелчке мышью на любой другой вкладке. Если вырваться из плена рекламы удастся, не переходите на «зараженную» вкладку до закрытия браузера.

Существует еще один тип сайтов — предназначенные для поиска и загрузки инструментов взлома программ и взломанных исполняемых (и иных) файлов приложений, т. е. всего того,

что нужно, чтобы заставить программу работать в обход процессов лицензирования и активации (рис. П2.8).

Некоторые из подобных сайтов предназначены для поиска и загрузки инструментов взлома, другие — только для поиска файлов на сайтах с загружаемыми материалами. Почти всегда на таких сайтах веб-страницы содержат вредоносный код, и даже если это не так, большинство «варезных» инструментов заражены различными вирусами и троянскими конями. Посещение этих сайтов строго не рекомендуется, если разве что вы, конечно, совершенно не беспокоитесь о безопасности своего компьютера и собственной.

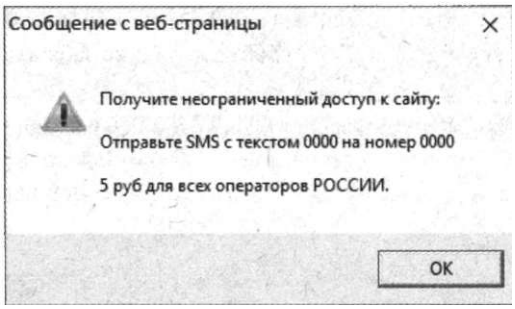


Рис. П2.7. Иногда такие всплывающие окна просто невозможно закрыть

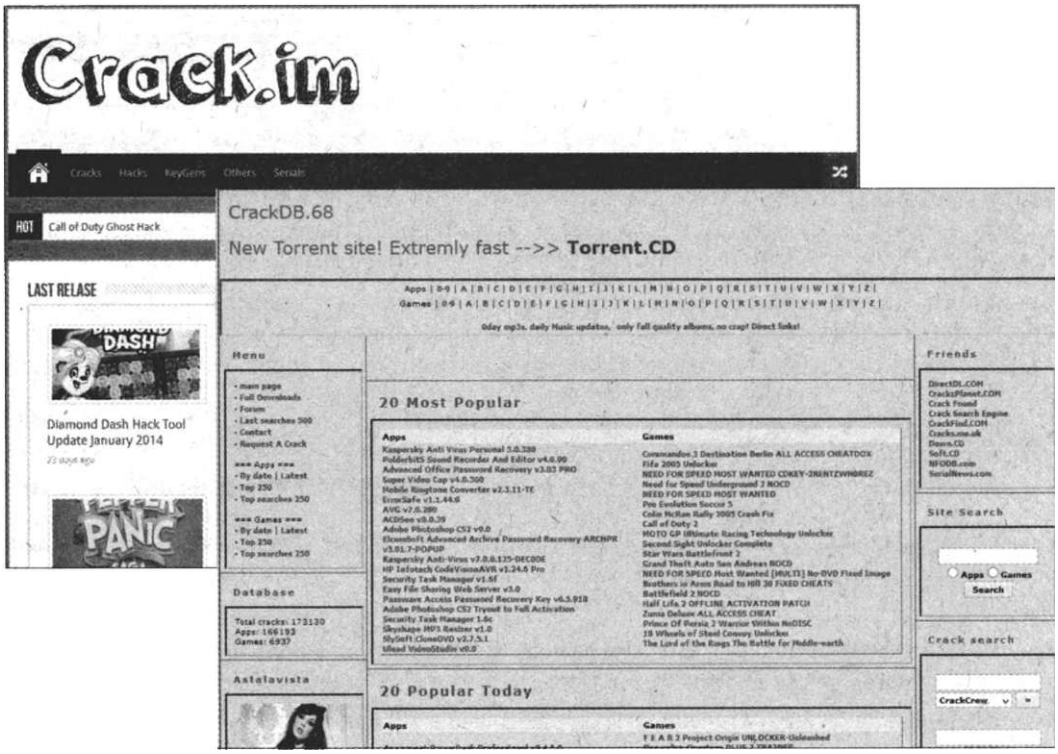


Рис. П2.8. Примеры ресурсов с нелегальными инструментами взлома

Форумы, где ссылки лежат

Многое из того, что недоступно на варезных сайтах, можно найти на форумах — опять же, тематических и универсальных (еще более редкий контент размещается на закрытых ресурсах — таких как **What.cd** (см. *приложение 4*)). Как правило, для получения доступа к ссылкам, публикуемым форумчанами в своих постах, или к архиву FTP (HTTP) требуется регистрация. Также нередко доступ измеряется так называемыми *уровнями пользователя* — в этом случае для просмотра каких-либо ссылок или входа в архив потребуется активное участие в жизни форума: размещение некоторого количества сообщений, обладание определенным званием, отправка личного сообщения администратору и т. д.

Сильных затруднений при поиске таких форумов вы не испытаете — достаточно сформировать запрос, включив в него нужные ключевые слова и не забыв добавить к ним `форум` или `forum`.

На рис. П2.9 приведен пример форума, раздел которого посвящен электронной музыке. В конкретном случае тема форума обеспечивает поиск музыкальных композиций: участники публикуют запросы, а пользователи, имеющие искомую дорожку, выгружают ее и размещают в *топике* (теме форума) ссылку для скачивания.

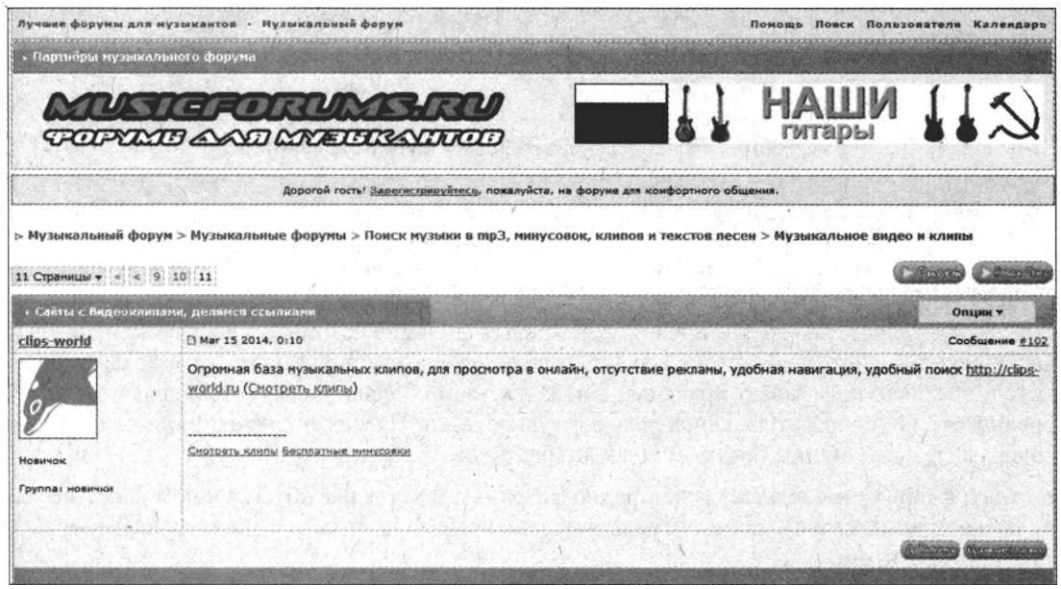


Рис. П2.9. Пример форума, раздел которого посвящен электронной музыке

Таких форумов, самых разнообразных по тематике, существует множество. Приведу лишь несколько ссылок на популярные форумы, действующие в русском сегменте Всемирной паутины:

- **forum.ru-board.com** — крупнейший компьютерный форум, сообщения на котором размещают более 2 млн участников;
- **musicforum.ru** — форум, специально предназначенный для музыкантов;
- **nowa.ee** — крупный компьютерный форум, включающий и не только околокомпьютерные темы;

- **forums.gameguru.ru** — огромный комплекс из форумов, посвященных компьютерным играм, в том числе и для приставок;
- **fllm-cafe.com** — форум обо всем, что связано с киноиндустрией.

FTP- и HTTP-архивы

Некоторые варезные сайты и многие форумы содержат архивы, доступ к содержимому которых осуществляется с помощью веб-интерфейса или по протоколу FTP. Если вы в качестве поискового запроса укажете `архив мультфильмов`, то, скорее всего, в первой десятке результатов окажется ресурс Мультики by ArjLover (рис. 112.10).

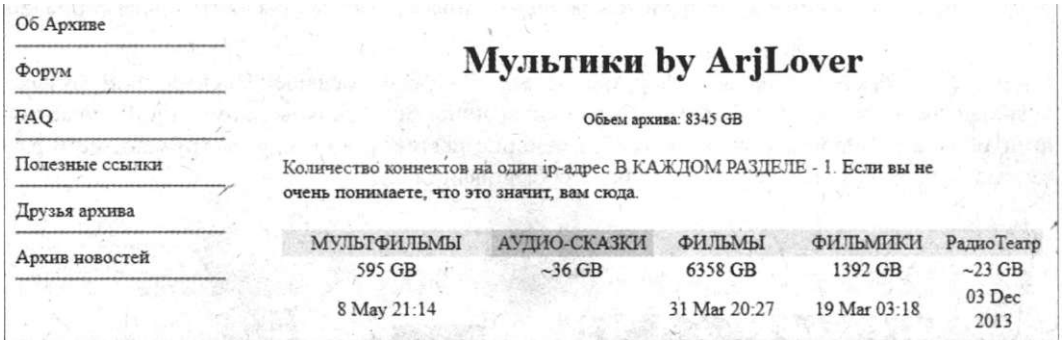


Рис. П2.10. Главная страница веб-сайта Мультики by ArjLover

Этот уникальный ресурс содержит множество мультфильмов, аудиосказок, взрослых и детских кинофильмов (в большинстве своем отечественного производства). Важность архива Мультики by ArjLover трудно переоценить — порой только здесь вы сможете найти советские непереозвученные мультфильмы (современная бессмысленная озвучка всегда просто отвратительна). То же касается и черно-белых фильмов, которые в российском синтетически-раскрашенном варианте выглядят, мягко говоря, неестественно. Хотя товарищей на вкус и цвет, как показывает практика, нет. И уж точно большой редкостью являются оцифрованные с виниловых пластинок детские аудиосказки. На момент подготовки книги архив содержал файлов общим объемом более 8 Тбайт.

Каждый файл (кроме аудиосказок и радиотеатра) вы можете скачать как с помощью браузера (менеджера закачки), так и посредством клиента eMule из сети обмена файлами ed2k, а также и торрентом.

> ***ПОДМЕНА РАСШИРЕНИЙ ФАЙЛОВ***
>
> **Популярный ресурс multiki.arjlover.net предоставляет возможность подмены расширений, что полезно пользователям — «жертвам админов» в офисах. Файлы с расширением *MPG* могут быть загружены как *JPG*, файлы *AVI* — как *GIF*, а файлы *MP3* — как *PNG*. После загрузки не забудьте вернуть файлу его родное расширение. Кроме того, значение `content-type` в ответе сервера при такой замене будет указано как `image/gif`. Расширение имени файла и значение `content-type` — это два пункта, по которым в прокси-серверах обычно включается блокировка.**

Кстати, щелкнув мышью по названию мультфильма (фильма), вы откроете страницу, содержащую техническую информацию о файле, скриншоты, ссылки на описание, скачиваемый видеофрагмент и окно предварительного просмотра.

Схожими объемами в мультфильмах обладает ресурс **mults.info**), также предлагающий к свободному скачиванию более 3900 анимационных лент (рис. П2.11). Из главных отличий стоит отметить возможность онлайн-просмотра любого мультфильма. Так же, как и в случае с **multiki.arjlover.net**, на сайте **mults.info**) нет «похабно» переозвученных мультфиль-



Рис. П2.11. Просмотр мультфильма на сайте mults.info

Кроме указанных, существует множество архивов (не только с мультфильмами и фильмами), доступ к которым осуществляется по протоколам HTTP и FTP. Приводить их адреса не имеет смысла, поскольку некоторые из них постоянно закрываются, а новые открываются. Лучших результатов вы добьетесь, используя для поиска архивов систему Google и сервисы поиска файлов на FTP-хранилищах. Найдите, к примеру, какой-либо файл на FTP-сервере, а потом попутешествуйте по его каталогам — наверняка найдется еще что-нибудь интересное. Например:

- на FTP-сервере mirror.yandex.ru вы найдете огромное количество дистрибутивов UNIX;
- прогуляйтесь также по серверам media.softlynx.ru, lsd-25.ru/uploads/, mmnt.net/db/0/0/95.24.41.207/DISK_A1, simant.ru/pub/multimedia/ — много всего самого полезного есть и здесь;

- интересным покажется ресурс ftp://91.149.145.78/— на нем размещено огромное количество разнообразных материалов;
- ресурсы agalakov.spb.ru/Shared/ и lan-fren.ru могут похвастаться обилием мультимедийных материалов;
- огромный архив электронной музыки — muteam.fm/dl/;
- отечественная и зарубежная музыка — hcmaslov.d-real.sci-nnov.ru/public/mp3/.

Содержимое подобных файловых хранилищ вы можете просматривать как в браузере, так и в окне Проводника Windows, причем в последнем случае можно копировать файлы и папки, как будто они находятся на жестком диске вашего компьютера (рис. П2.12).

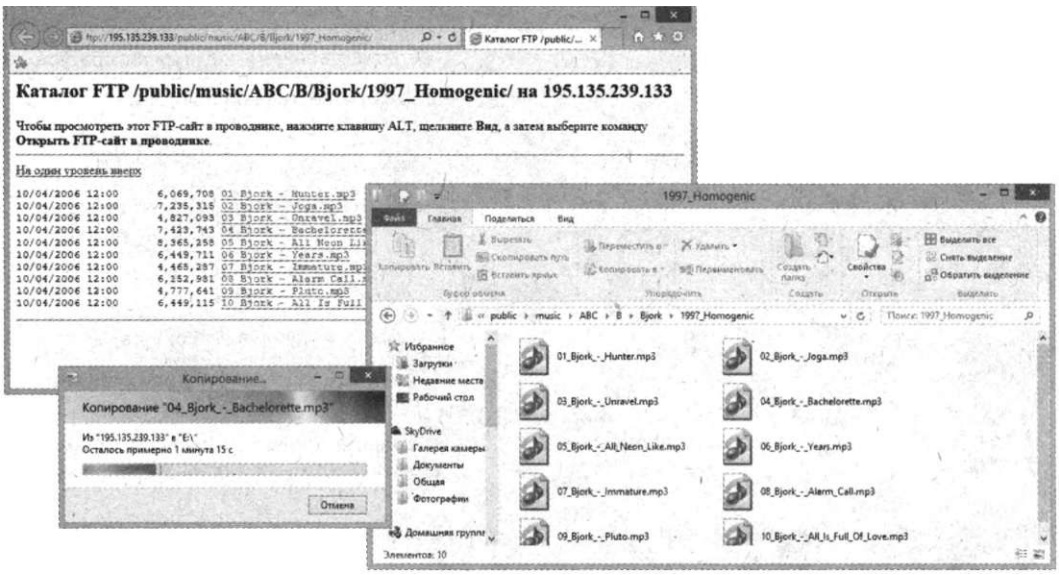


Рис. П2.12. Просмотр содержимого FTP-сервера в двух вариантах, а также диалоговое окно Копирование

Электронные библиотеки

В отдельную категорию следует выделить электронные библиотеки— сайты, предлагающие для чтения и/или скачивания художественную и научную литературу в электронном виде (рис. П2.13).

В табл. П2.2 приведен список русскоязычных электронных библиотек, функционирующих на момент подготовки книги.

Таблица П2.2. *Популярные электронные библиотеки Рунета*

Название	Адрес	Краткое описание
CoolLib	coollib.net	Свыше 295 тысяч книг общим объемом чуть менее 300 Гбайт
eLIBRARY.RU	elibrary.ru	Электронные версии научно-технических журналов. Свыше 50 тысяч изданий

Таблица П2.2 *(продолжение)*

Название	Адрес	Краткое описание
Free-book.ru	free-book.ru	Самая разнообразная литература
IQLib.ru	iqlib.ru	Электронные учебники и учебная литература
Litmir.net	litmir.net	Бывшая библиотека Litru.ru. Более 220 тысяч книг бесплатно и без регистрации
Альдебаран	lib.aldebaran.ru	Художественная, учебная и техническая литература
Библиотека Бориса Бердичевского	city cat.ru/l itlib/index.html	Одна из старейших библиотек. Художественная и научная литература
Библиотека Максима Машкова	lib.ru	Самая известная библиотека с 1994 года
Библиотекарь.Ру	bibliotekar.ru	Нехудожественная литература
Большая электронная библиотека	big-library.info	Более 60 тысяч книг художественной и научной литературы, а также журналы
Гумер	gumer.info	Гуманитарная литература, свыше 5 тысяч, книг и статей
Куб	koob.ru	Учебная и научная литература
Либрусек	lib.rus.ec	Более 380 тысяч книг общим объемом свыше 1 Тбайт
Литературный клуб «Глобус»	http://leeet.net/lib/	Прекрасно структурированная обширная библиотека книг самой различной тематики
Максима	maxima-library.org	Более 200 тысяч книг на разные темы
Мировая цифровая библиотека	wdl.org/ru/	Постоянно пополняемая всемирная библиотека — содержит множество документов, датируемых 8000 г. до н. э. — 2016 г. н. э.
Публичная библиотека	pubi.iib.ru	Универсальная библиотека, свыше 90 тысяч книг. Есть прямой доступ к архивам по ссылке pubi.lib.ru/ARCHIVES/
Пупсам	pupsam.ru	Детская литература
Русская фантастика	rusf.ru	Фантастические произведения отечественных авторов
Старые газеты	oidgazette.ru	Подшивки газет (свыше 1600) с 1912 по 1991 год
Фантаст	phantastike.ru	Фантастическая литература
Флибуста	flibusta.net (альтернативный адрес: flibustahezeous3.onion[1])	Более 260 тысяч книг общим объемом свыше 350 Гбайт

[1] Адрес для захода на ресурс через сеть виртуальных туннелей Tor.

Таблица П2.2 (окончание)

Название	Адрес	Краткое описание
Электронная библиотека Books.ru	**bookz.ru**	**Более 118 тысяч книг, включая художественную и научную литературу**



Рис. П2.13. Пример сайта электронной библиотеки

Все книги, представленные на указанных сайтах, предназначены лишь для ознакомления, после которого рекомендуется приобрести печатную (или аудиокнигу на диске) версию понравившегося произведения.

Сцена: андеграунд Всемирной паутины

Варезная Сцена, обычно называемая просто Сценой, представляет собой сообщество людей, которые специализируются на нелегальном распространении материалов, охраняемых авторским правом, включая телешоу и сериалы, фильмы и мультфильмы, музыку и музыкальные клипы, игры и приложения для любых платформ, электронные книги и порнографию. Сцена, по сути, публично недоступна и предназначена для обмена материалами между ее участниками. Однако с самого момента ее формирования происходят утечки, и релизы из Сцены выкладываются на файлообменных хостингах и в пиринговых сетях.

В Сцене не существует некоего головного руководства, юридического адреса или других атрибутов, присущих обычным организациям. Стандарты для каждой категории вареза, как говорилось ранее, создают сами варезные группы, состоящие в Сцене. Группы должны еле-

довать всем этим стандартам, выпуская релизы, в противном случае, релиз может быть «нюкнут» другими группами. Группы постоянно соревнуются с целью обогнать соперников в выпуске релизов, хотя никаких «наград» за скорость выпуска или за сам релиз не существует (за исключением доступа к Сцене).

В составе Сцены насчитывается свыше 100 активных групп, выпускающих релизы, общим количеством свыше 200 тысяч в год.

Правила Сцены, «нюков» и прочие сведения публикуются на веб-сайте **scenerules.irc.gs.**

Развитие Сцены

Варезная Сцена, тогда еще просто группа людей — предшественников будущих варезных групп, начала формироваться в 1970-х годах. Эти люди увлекались взломом программного обеспечения и его обратной разработкой[1] и выкладывали свои работы на приватных BBS, изначально расположенных в США, а затем и в Канаде, Великобритании, Австралии и европейских странах. В те времена настройка компьютера под нужды BBS была отнюдь не тривиальной задачей и требовала от администратора определенных технических навыков. На BBS, как правило, можно было разместить лишь несколько мегабайт файлов. Лучшие из BBS были доступны по нескольким телефонным линиям и предоставляли под хранение файлов пространство объемом до ста мегабайт, что было непомерно дорого. Релизы тогда представляли собой копии игр и, позднее, приложений.

Поскольку сфера разработки программного обеспечения эволюционировала в направлении противодействия нелегальному распространению материалов, а программное и аппаратное обеспечение, с помощью которого эти материалы распространяются, стало доступным каждому, Сцена, адаптируясь к изменениям, перешла от простого распространения к фактическому взлому защиты и некоммерческой обратной разработке. Стало образовываться все больше варезных групп, и, поскольку требовалось наглядное различие между ними в целях соперничества, активно начала развиваться *артсцена,* специализирующая на создании графических логотипов групп. Группы стали демонстрировать свои способности не только во взломе сложного и новейшего программного обеспечения, но и в графическом искусстве и, позднее, музыке (начав формировать *демосцену).*

Группы, не занимающиеся взломом, а демонстрирующие лишь навыки в сфере арт- и демосцены, в конечном счете отделились, вследствие чего инструменты для взлома, содержащие рекламный графический и музыкальный контент группы и распространенные с помощью Сцены, в конечном итоге получили название *интро,* а затем *крэктро.* Особое развитие демосцена получила в Скандинавии, где начали проводиться первые ежегодные фестивали.

Ранее существовал ресурс **aboutthescene.com,** содержащий исчерпывающую информацию о Сцене, но он сейчас недоступен. Однако с помощью сервиса **archive.org** вы можете вернуться в 2007 год и увидеть сайт того времени — **tinyurl.com/3zlg9cu.**

Интересные статьи на русском языке опубликованы по ссылкам **tinyurl.com/pjjbpyo** — «The Scene — настоящий андеграунд Интернета» и **tinyurl.com/q3j5xgn** — «Реверс-инжиниринг как стиль жизни». Пару любопытных историй из жизни Сцены вы найдете по

[1] Обратная разработка (не вполне удобоваримый, но общепринятый перевод английского термина reverse engineering) — исследование некоторого устройства или программы с целью понять принцип его работы и воспроизвести.

адресам **tinyurl.com/ceyfbcu** и **tinyurl.com/pyr895h.** А по адресу **tinyurl.com/dxuofz9** можно скачать локализованный сериал, посвященный Сцене.

Создание релизов

Подготавливая релиз к выпуску, группы должны вначале должным образом кодировать материал, чтобы релиз не был «нюкнут» другими группами. Подготовленный и именованный согласно стандартам релиз выгружается на *топ-сайт* (скрытый, высокозащищенный и высокоскоростной FTP-сервер, используемый для выгрузки, хранения и архивирования релизов вареза). По завершении выгрузки выполняется команда для вывода названия и категории (типа) релиза в IRC-канале топ-сайта. В ближайшие дни выпущенные релизы анонсируются с меткой Osec (через несколько секунд или минут после появления релиза на топ-сайте) — это так называемые *пре-релизы.* После этого все другие релизы того же материала считаются «нюкнутыми» по причине дублирования. Однако если в оригинальном релизе будет выявлена некая ошибка или несоблюдение стандартов, то он тоже будет «нюкнут» — по причине ошибки. Другие группы в этом случае смогут исправить и выпустить этот релиз, пометив его фрагментом *PROPER* в имени файла. Но и группа, чей релиз был «нюкнут», может исправить ситуацию, выпустив новую версию своего релиза — исправленную — с меткой *REPACK* или (реже) *RERIP.* FTP-сервер топ-сайта и соответствующий IRC-канал скрыты и недоступны публично. Однако существуют независимые IRC-каналы с названием типа PreDB, которые публично оповещают о новинках релизов Сцены.

Каждый релиз Сцены состоит из папки, содержащей сам контент (часто запакованный в многотомные RAR-архивы), NFO- и SFV-файлы. NFO-файл несет всю информацию о релизе, в нем также указывается причина «нюка», если это исправленный релиз с меткой *PROPER* или *REPACK.* Некоторые NFO-файлы могут содержать текст миссии варезной группы, требования к кандидатам, благодарности и, иногда, контактную информацию. Многие NFO-файлы включают ASCII-лого группы-релизера. SFV-файлы, как уже упоминалось, служат для гарантии целостности файлов релиза путем проверки значений контрольных сумм (CRC). Если файл формата NFO и/или SFV не включен в релиз, он «нюкается», поскольку эти файлы — важные элементы релиза согласно стандартам Сцены.

«Нюки» релизов

В терминологии Сцены слово «нюк» (Nuke) служит для маркировки «плохих» релизов, включающих, к примеру, нерабочий софт, некачественный (или несинхронизированный) контент аудио/видео, контент, инфицированный вирусами, фейки (релизы, не соответствующие действительности) или релизы, оформленные не по стандартам. «Нюкаются» также дубликаты и релизы, украденные у других варезных групп. Когда релиз Сцены «нюкается», к нему прикрепляется сообщение об этом с указанием причины «нюка». Такая метка не уничтожает релиз и не запрещает его скачивание, а лишь служит предостережением потенциальным пользователям. Пользователь (группа), разместивший релиз, впоследствии «нюкнутый», теряет кредиты (о кредитах вы узнаете позже, в *разд. «Топ-сайты»),* Релизы «нюкаются» пользователями со специальным доступом к базам данных с листингами релизов — их часто называют «нюкерами». Ошибочно «нюкнутые» релизы, как правило, восстанавливаются в статусе теми же людьми. Релиз, который был «нюкнут» или восстановлен в статусе более чем четыре раза, называется *битвой нюков.*

Сети пре-релизов (aka Nukenet) представляют собой совокупность баз данных, в которых содержится информация о релизах участников сети. Различных подобных сетей существует около двадцати. Пользователи могут быть участниками более чем одной сети. Другие сети

могут предоставлять данные (например, файлы формата SFV, M3U, JPG, DIZ или NFO), не доступные в текущей сети.

Каждый выпущенный релиз регистрируется в базе данных пре-релизов. Запись в базе данных содержит как минимум дату и название (имя папки с контентом) релиза, а часто и размер, и категорию (тип). Сведения о «нюках» также указываются в этих базах данных. Для проверки, не «нюкнут» ли релиз, используется IRC-канал пре-релизов, в котором можно выполнять запросы к базе данных путем ввода специальных команд. База данных автоматически обновляется с помощью поисковых «пауков» топ-сайтов или извлечения анонсов о пре-релизах из IRC-канала сайта. Цель этих раскиданных по всему миру и зазеркалированных баз данных пре-релизов заключается в том, чтобы избежать фейков и дубликатов пре-релизов и снизить тем самым трафик.

Существуют несколько публичных веб-сайтов и IRC-каналов, публикующих информацию о пре-релизах, большинство из которых регулярно обновляются и указывают причину «нюка» релизов, если такое произошло. Некоторые из них регулярно «падают» или очень медленны при поиске. Вот список ряда популярных ресурсов такого типа:

- **pre.corrupt-net.org (pr3.us)** — аскетично оформленный веб-поисковик релизов;
- **predb.me** — база данных, содержащая около 5 млн релизов;
- **doopes.com/index.php** — настраиваемый поиск, функционирует с 2005 года. Можно отобразить только «нюкнутые» релизы, установив флажок Nukes (рис. П2.14);

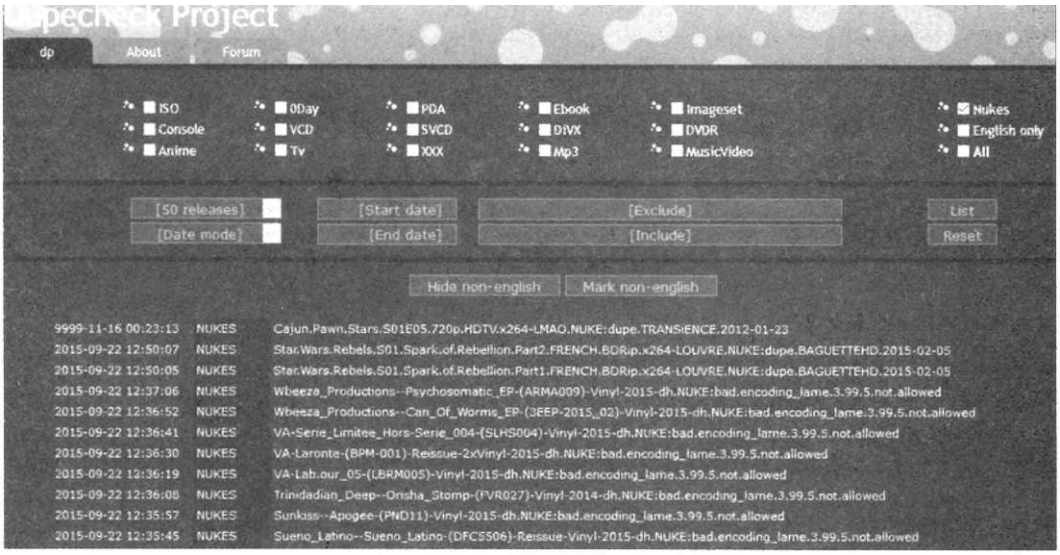


Рис. П2.14. Интерфейс сайта doopes.com: отображены только «нюкнутые» релизы

- **d00per.com** — более 1 млн релизов;
- **tinyurl.com/pf2bn6n** — список ссылок на сайты пре-релизов.

Существуют также сугубо информативные ЖС-каналы пре-релизов, в которых боты в режиме реального времени анонсируют новые варезные пре-релизы. Эти каналы, как правило, приватные и предоставляются для удобства членам Сцены, часто в сочетании с топ-сайтами. Благодаря таким IRC-каналам участники получают уведомления о новых релизах по мере их выхода, что особенно важно для курьеров и релизных групп, поскольку позволя-

ет избежать дублирования релизов. Здесь также выводятся оповещения о «нюках» и восстановлениях релизов в статусе. Кроме того, IRC-каналы пре-релизов используются на топ-сайтах для вычисления времени получения релиза с момента анонса. Адреса таких каналов можно узнать по ссылкам **tinyurl.com/n9uk6u6** и **tinyurl.com/ox56mkf.**

Взлом и обратная разработка

Взлом — основной элемент Сцены, начиная с ее истоков. Сосредоточенная на этом часть сообщества Сцены специализируется на взломе программного обеспечения, создании крэков и генераторов ключей. Взлом и обратная разработка сложного программного обеспечения — вот самое привлекательное для членов Сцены. В одном из NFO-файлов варезной группы SKIDROW была опубликована следующая цитата:

> **Имейте в виду, что мы занимаемся этим, потому что можем и потому что нам нравится азарт победы над другими конкурирующими группами. Мы не выпустили ни одного релиза с целью угодить юзерам, сэкономить их деньги, чтобы они потратили их на апгрейд своих компьютеров, и благодаря Сцене играли во все эти игры бесплатно.**
>
> **Играйте, но помните, если вам нравится это, поддержите разработчика!**

Топ-сайты

Как уже говорилось ранее, топ-сайты — это скрытые, высокозащищенные, высокоскоростные FTP-серверы, используемые варезными группами и курьерами для распространения, хранения и архивирования релизов вареза. Эти серверы обладают весьма высокоскоростными каналами подключения к Интернету, как правило, поддерживая скорость передачи данных до нескольких гигабит в секунду — достаточную для передачи полной копии диска Blu-ray за несколько секунд. Разумеется, емкость жестких дисков на топ-сайтах очень высока и исчисляется в десятках терабайт.

В отличие от своих предшественников на BBS, топ-сайты не предаются огласке. Учитывая возросшую угрозу полицейских рейдов, топ-сайты были вынуждены ввести комплексные меры безопасности, чтобы скрываться от властей.

Типичный топ-сайт допускает к авторизации только пользователей с определенного IP-адреса (или диапазона IP-адресов, если те выделяются диуамически) по протоколу Ident с SSL-инкапсуляцией для всех FTP-сеансов. На FTP-сервере используются специальные программы, так называемые *баунсеры,* для сокрытия реального IP-адреса топ-сайта и распределения сетевой нагрузки.

Наряду с «официальным названием», большинство топ-сайтов известны в Сцене под аббревиатурами в две-три буквы длиной. Например, топ-сайт с названием типа Bluebox может быть сокращен до BBX, а затем упоминаться как B** при общении в IRC-чате теми, кто осведомлен о существовании сайта.

Система кредитов

Система кредитов, чаще автоматизированная, регулирует объем данных, которые может скачать тот или иной пользователь. Когда пользователь выгружает файл на сайт, на его аккаунт зачисляется некоторое количество кредитов, как правило, вычисляемое путем умножения размера выгруженного файла на три. Например, если пользователь выгрузил файл объемом 15 Мбайт, он получает 45 Мбайт по системе кредитов. Кредиты могут быть использованы для скачивания файлов с сайта. Кредиты списываются, если пользователь выгружает плохой релиз, который впоследствии был «нюкнут».

Варезные группы

Варезная группа — более или менее организованная группа людей, вовлеченных в Сцене в создание и/или распространение вареза: фильмов, музыки, игр, книг и программного обеспечения. Существуют два различных типа этих групп: *ремизные группы* и *курьеры*. Группы часто конкурируют в попытке первыми выпустить тот или иной качественный релиз, чтобы обрести статус и *респект* — уважение (основной мотив варезных групп — отнюдь не финансовая выгода). Некоторые члены этих групп также являются и создателями крэков и генераторов ключей. Разумеется, существуют варезные группы и вне Сцены. В силу нелегальности действий и скрытности Сцены об этих группах известно не очень много — чаще всего об участниках той или иной группы узнается после полицейских рейдов и спецопераций против киберпреступлений. Большинство групп следует стандартам по оформлению вареза, чтобы их релизы не «нюкались».

Некоторые варезные группы, выпускающие релизы игр и приложений, известны под следующими именами: Razor 1911, Reloaded, DrinkOrDie, Pirates With Attitude, Class и Fairlight. Чуть позже мы познакомимся с конкретными группами поближе.

ФБР в противодействии киберпреступлениям провело против участников варезных групп несколько операций: Buccaneer (2000-2001), Safehaven (2003), Site Down (2005) и Fastlink (2007), арестовав по всему миру множество членов групп и изъяв серверы с нелегальным контентом.

Курьеры

Курьеры — это определенный класс пользователей топ-сайтов, которые допускаются к варезным серверам с целью размещения новых релизов и выполнения запросов. Курьеры занимаются распространением варезных релизов, используя протокол FXP для прямой передачи файлов между FTP-серверами. Прежде чем курьер получает доступ к топ-сайту, его тестируют, например, на способность загрузить определенный объем данных за некий короткий период времени. Курьеры конкурируют между собой в целях повышения статуса, уровня доступа (в том числе и к другим топ-сайтам) и просто ради победы. Существуют как индивидуальные курьеры, так и курьерские группы (например, Motiv8), участники которых сотрудничают между собой. Потребность в курьерах постепенно уменьшается, т. к. разрабатываются и совершенствуются скрипты, автоматизирующие выполнение задач курьеров.

Релизные группы

Релизные группы ответственны за создание и выпуск варезных релизов. Они — на верхушке варезного мира. Их релизы заносятся в специальные базы данных Predb. Для взлома и создания генераторов ключей группам требуется доступ к оригинальным программным продуктам, которыми они делятся друг с другом, используя приватные сайты и серверы.



Журнал «Хакер» не раз публиковал различные статьи про варезные группы. Ссылка tinyurl.com/pytlk48 приведет вас на страницу со всеми номерами журнала.

Существовало и существует множество релизных групп[1] Сцены, крупнейшие и известнейшие (если можно так выразиться) из них упомянуты далее.

[1] **Подробно о них можно прочесть и здесь: tinyurl.com/owbxhxl.**

aPOCALYPSE PRODUCTION cREW (aPC)

Группа aPOCALYPSE PRODUCTION cREW (aPC) была основана двумя энтузиастами под никами acid^ain и Viper и просуществовала с мая 1997-го по апрель 2004 года. В годы существования группа считалась основным релизером MP3-контента, но в середине 2000-х годов попала под наблюдение ФБР и после операции Fastlink распалась. Группа известна как одна из первых, начавших распространять MP3-файлы через Интернет и создававших MIDI-версии популярных песен (рис. П2.15).

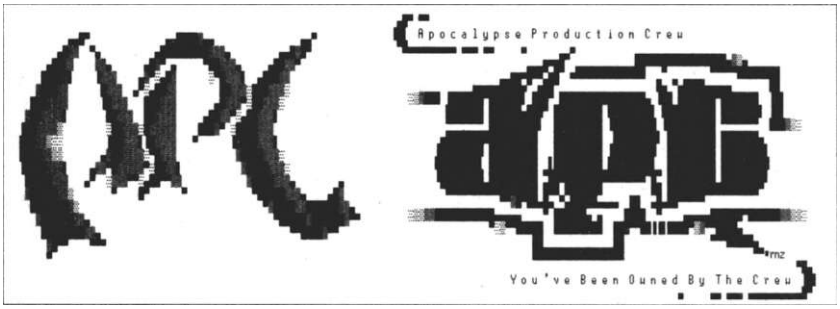


Рис. П2.15. ASCII-лого (2 варианта) группы aPC

Challenge Of Reverse Engineering (CORE)

Группа C.O.R.E. (Challenge of Reverse Engineering) была сформирована в июне 1997 года несколькими энтузиастами из Канады. Известна огромным количеством выпущенных генераторов ключей и крэков, в частности, для таких программ, как Adobe Photoshop и CorelDraw, число которых перевалило за 18 тыс. Группа C.O.R.E. активна до сих пор. Вы можете посетить страницу группы в Facebook по адресу **tinyurl.com/ozmv3ga**. ASCII-лого группы представлен на рис. П2.16, *вверху*.

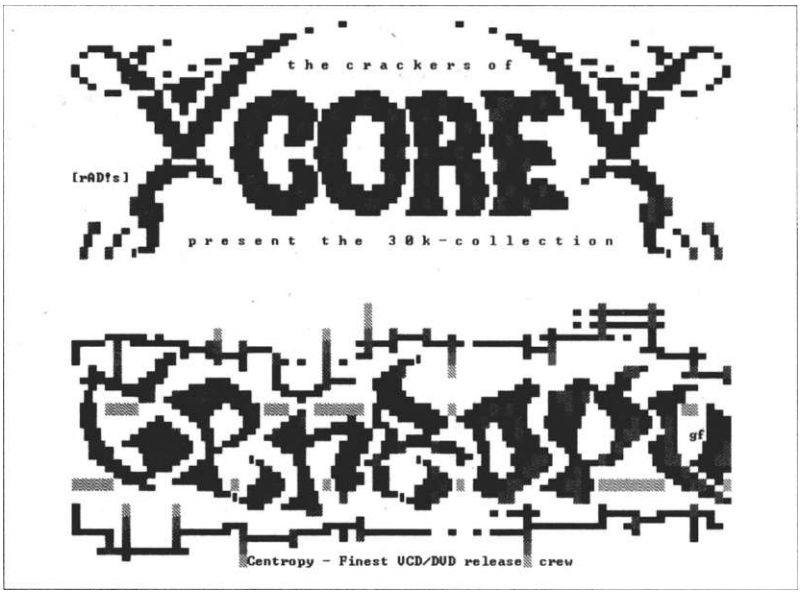


Рис. П2.16. ASCII-лого групп C.O.R.E. (*вверху*) и Centropy *(внизу)*

Centropy

Группа Centropy (рис. П2.16, *внизу*) была основана в январе 1999 года и специализировалась на распространении пиратских копий фильмов. Группой было анонсировано и выпущено множество 0-day релизов фильмов, в основном в качестве DVD-Rip, Telesync и Screener. Релизы группы можно было узнать по фирменному логотипу.

Участники группы Centropy стали целью операции Site Down, проведенной ФБР 29 июня 2005 года, после которой во Всемирной паутине появилась неподтвержденная информация, что они арестованы в Нидерландах. Спустя несколько лет участник Centropy под ником Wicked 1, также известный как Мэтью Томпсон, объявил о работе над книгой о варезной Сцене (tinyurl.com/qbxndxj).

CLASS (CLS)

CLASS (также известная как CLS) — варезная группа, основанная в 1997 году, специализировавшаяся на взломе и выпуске рипов игр и ставшая одной из целей в ходе операции Fastlink. В команде состояло множество членов со всего мира, и помимо основной деятельности они занимались творчеством, встраивая свои творения в крэктро и выпуская в виде отдельных релизов — в том числе музыку, 3D-анимации, логотипы (рис. П2.17, *вверху)* и пр. Сокращение CLS указывалось в конце имен релизов группы.



Рис. П2.17. ASCII-лого групп CLASS *(вверху)* **и DEViANCE** *(внизу)*

CLASS была вовлечена в давнишнюю конкуренцию с группой Myth, также специализировавшейся на взломе игр. Обе группы выпускали исключительно рипы игр, в противоположность образам компакт-дисков, распространяемым такими группами, как Fairlight. Дистрибутивы игр разделялись на основной рип (минимально необходимый для запуска игры) с минимально возможным размером, а дополнительный контент (как правило, внутриигровые видеоролики или музыка) выпускался в качестве дополнений (аддонов). Для некоторых релизов также выпускались и анимационные вводные ролики (интро). Группы использовали передовые технологии сжатия (прежде всего формат ACE), чтобы максимально уменьшить размер файлов, а инсталляторы особым образом обрабатывались с целью обеспечения поддержки пересжатых файлов. Группа прекратила существование 9 января 2004 года после 1234-го релиза и выпуска так называемого endtro[1] (рис. П2.18), покинув свой трон.

[1] **Слово end в пер. с англ. — конец, финал.**

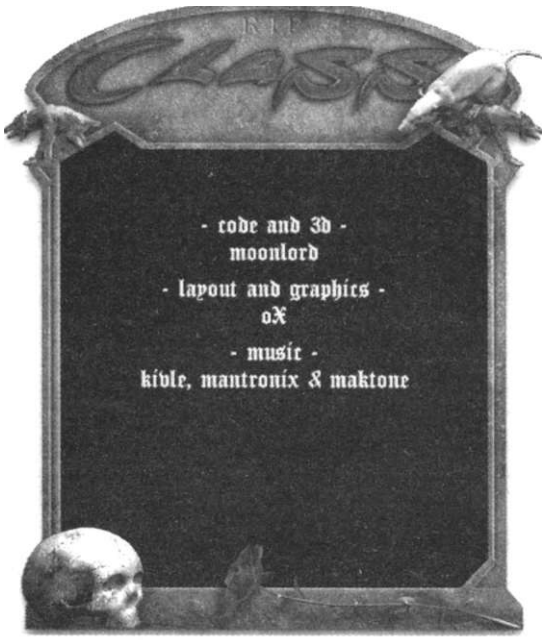


Рис. П2.18. Интерфейс endtro группы CLASS

DEViANCE

Следом можно расположить группу DEViANCE (рис. П2.17, *внизу)* с лидером под ником CyberNaj, сформированную 1 января 1999 года членами DVNiSO — подразделением группы DiViNE, занимающимся взломом компьютерных игр. Группа известна релизами таких игр, как Call of Duty, Unreal Tournament, Max Payne, Grand Thief Auto и др., выпущенными за несколько часов до официального выхода в свет, а также инструментами взлома (под общим именованием DOX). 25 декабря 2006 года группа растеряла своих участников, но некоторые из них активны до сих пор. Приостановка деятельности группы DEViANCE была одной из целей операции Fastlink, проведенной совместно ФБР и Министерством юстиции США.

DrinkOrDie

Российская группа DrinkOrDie (DoD) (рис. П2.19, *вверху)* была создана в 1993 году в Москве лидером под ником Deviator (позднее известным как Jimmy Jamez) и его другом под ником CyberAngel. DrinkOrDie была одной из самых престижных андеграунд-групп по взлому ПО и сетью по распространению вареза в 1990-х годах. Группа, как правило, не получала финансовой прибыли от своей деятельности. Сеть DoD, преимущественно состоящая из студентов вузов, также поддерживалась отдельными сотрудниками компаний-разработчиков ПО, с помощью которых «утекали» копии дистрибутивов и другого цифрового контента. Группа также активно участвовала в обмене нелегальными файлами с другими сетями.

Одним из самых ранних крупных достижений группы стал релиз копии операционной системы Windows 95, выпущенный за две недели до ее официального выпуска корпорацией Microsoft. Известно также приложение DVD Speed Ripper для расшифровки содержимого DVD, выпущенное группой ранее инструмента DeCSS. Вместе с TRSi, группа DoD впервые

представила чит-комаиды, встроенные в игровое меню (обычно они были или в загрузчике, или поставлялись отдельной программой).

В 1995 году DrinkOrDie оставили несколько давних членов, чтобы основать свою группу под названием Prophecy. После 1996 года, когда Всемирная паутина стала открытой для всех и появилось множество новых релизных групп, деятельность DoD потонула в их массе, и группа перестала считаться крупным игроком варезной Сцены. Лидеры DrinkOrDie на тот момент — Jimmy Jamez и Cyber Angel — оставили группу, чтобы профессионально заняться веб-дизайнрм, а на их место пришел новый предводитель — Lester. Через несколько месяцев переоформления команды, благодаря энтузиазму Lester'a группа продолжила работать, хоть и не так активно, как раньше.



Рис. П2.19. ASCII-лого групп DrinkOrDie (*вверху)* и Echelon *(внизу)*

В 2001 году основные участники группы были арестованы в ходе операции Buccaneer. Jimmy Jamez на тот момент уже отошел от дел. Рейды начались после того, как были получены сведения от информатора (на сленге Сцены — *парка)* Джеймса Кадни, известного под ником Bcrea8tiv, который много лет тайно сотрудничал с федералами, протоколируя беседы в чатах и IRC-каналах. Помимо Америки, рейды прошли на территории Великобритании, Австралии, Финляндии, Норвегии и Швеции. В один-единственный день, подготовка к которому длилась 14 месяцев, полиции удалось арестовать почти всю «элиту» варезной Сцены, ключевых членов групп DoD, Razor 911, DEViANCE, RogueWarriorz, TFL, WLW, RiSC и др. Более 70 человек, из которых около 20 имело отношение к DoD, обвинили в нарушении авторских прав. После арестов координировать деятельность группы стало некому, и оставшиеся члены потихоньку ломали программы, выпуская релизы под лейблом DoD. Последние упоминания о группе относятся к январю 2003 года, когда в сети появилась взломанная версия программы 3D Studio Max 3.1. На этом история легендарной команды закончилась. Кто-то из ее членов перешел в другие группы, кто-то навсегда оставил Сцену.

Прочитать об истории группы можно на страницах **tinyurl.com/pby2n5p, tinyurl.com/р6с4уок** и **tinyurl.com/k9ke5n5.**

Echelon

Echelon (рис. П2.19, *внизу)* — варезная группа, специализировавшаяся на выпуске и распространении релизов консольных игр для таких устройств, как Sega Dreamcast и Sony PlayStation, и практически прекратившая деятельность к 2010 году. Выпускала Echelon и демо для воспроизведения на этих двух платформах.

В 2004 году Echelon привлекла внимание ФБР, проводившей операцию Fastlink, после чего количество выпускаемых ею релизов снизилось почти на нет.

FaIrLight

В 1987 году в Швеции образовалась группа FairLight T (FLT) (рис. П2.20, *вверху),* основателями которой были персонажи под никами Strider и Black Shadow. Это одна из старейших варезных и демогрупп в Сцене, изначально вовлеченных в демосцену Commodore 64 (C64) и взлом игр, — во Всемирной паутине все еще доступен веб-сайт группы по адресу **fairlight.to.** Затем группа переключилась на выпуск релизов для компьютера Amiga, приставки Super Nintendo и, позже, для персональных компьютеров. FairLight стала быстро известна благодаря быстрому выпуску крэков. Секрет успеха заключался в том, что Strider работал в компьютерном магазине и имел доступ к новейшим играм. Подкупив проводника поезда, он передавал игры из Мальме в Роннебю, где участник под ником Gollum взламывал игры и отправлял назад тем же путем. Так FairLight могла выпускать свои релизы быстрее, чем другие группы.



Рис. П2.20. ASCII-лого фупп FairLight (*вверху*) и HYBRID *{внизу)*

Несколько основных членов группы были арестованы 21 апреля 2004 года во время рейдов в процессе проведения операции Fastlink. Один из изъятых серверов, который, как и предполагалось, являлся репозиторием группы, содержал более 65 тыс. нелегальных дистрибутивов. Тем не менее, с октября 2006 года подразделение ISO группы FairLight вновь начало

выпускать релизы, чем занималось еще четыре года. В настоящее время участники группы занимаются выпуском релизов ПК-игр.

HYBRID

Группа HYBRID, также известная под сокращением HBD (рис. П2.20, *внизу),* была основана в 1993 году и первой занялась созданием рипов игр, выпускавшихся на компакт-дисках — удалением из них видео и аудиоконтента для уменьшения размера дистрибутивов. Ранее группы типа Razor 1911 и Pentagram выпускали только полные копии CD-игр.

International Network of Crackers (INC)

Официальной датой создания группы International Network of Crackers (INC) (рис. П2.21, *вверху)* принято считать сентябрь 1989 года, хотя некоторые источники относят их первые релизы к 1985 году. Группа была сформирована участниками, до этого активными в MCM (Miami Cracking Machine), NYC (New York Crackers) и ECA (Elite Crackers Association), а ее лидером стал Line Noise. INC считалась одним из главных релизеров рзломанного софта дня персональных компьютеров IBM PC с конца 1980-х и до начала 1990-х годов.

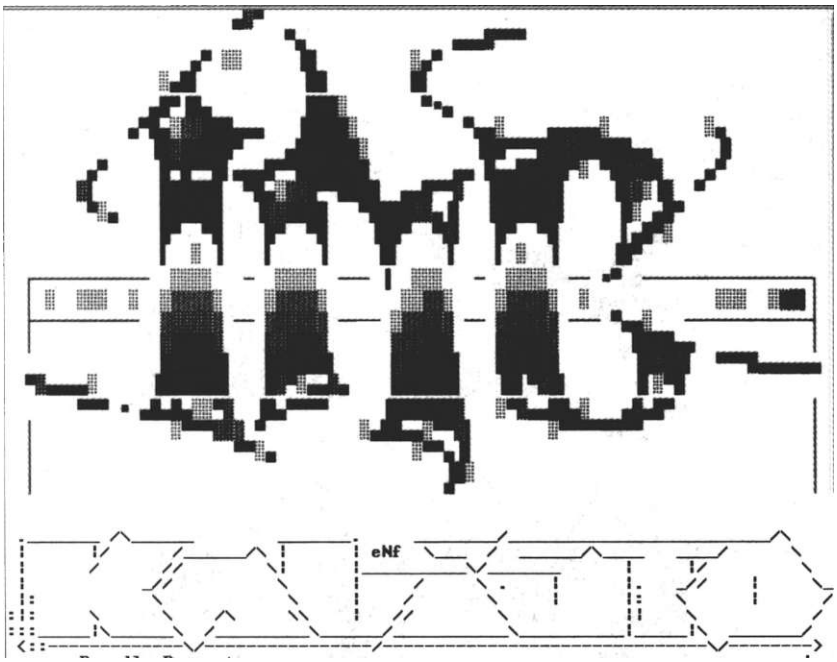


Рис. П2.21. ASCII-лого групп International Network of Crackers (*вверху*) и Kalisto *(внизу)*

Известна история противостояния культовых варезных групп INC и THG. Узнать об этом, а также историю INC, можно на странице **tinyurl.com/qhpr2jl.** К началу 1994 года INC полностью исчезла из варезной Сцены.

Kalisto

Kalisto (рис. П2.21, *внизу)* — группа, специализировавшаяся на взломе консольных игр дня приставок Sony PlayStation 1/2 и, за редким исключением, платформы Dreamcast. Группа была образована в марте 1998 года, изначально в составе команды FairLight, и начала неза-

висимую деятельность в июне 2000 года. В августе 2000 года ею был разработан новый способ риппинга и перепаковки игровых дисков CD-ROM в образы CD-ROM без необходимости использования специального загрузочного диска. В 2004 году во время операции Fastlink основной сайт с архивом релизов группы, расположенный в Нидерландах, был заблокирован, а основной курьер, Сет Клейнберг (Basilisk), арестован. После этого группа распалась.

LineZerO (LzO)

Легендарная варезная группа LineZerO (LzO) (рис. П2.22, *вверху)* была создана в 2000 году и за 13 лет выпустила множество релизов программ, игр и мобильных приложений. Причиной прекращения деятельности команды стала утечка информации, которая угрожала безопасности хакеров, когда некто из варезной тусовки опубликовал информацию, добытую во время взлома сервера LineZerO в 2009 году. Хотя большая часть информации уже потеряла актуальность и относится к людям, давно покинувшим группу, LineZerO сочла за лучшее свернуть деятельность. «Мы долго шли вместе и очень грустно, что так все заканчивается», — сказано в официальном прощальном заявлении LineZerO. Группа выражает надежду, что никто не будет в будущем использовать ее названия LineZerO, LzO и LzOPDA. Последний релиз группы датируется 10 мая 2013 года.



Рис. П2.22. ASCII-лого групп LineZerO *(вверху)* **и Myth** *(внизу)*

Myth

Группа Myth (рис. П2.22, *внизу)* в 2000-2005 годах была широко известна как одна из крупнейших на тот момент. Группа, занимавшаяся релизами игр, трейнеров к ним, а также взломом обновлений для игр, была сформирована в феврале 2000 года ripперами игр под никами Origin и Paradigm. Группа Myth внесла существенный вклад в развитие Сцены, изменила правила Сцены и сделала их такими, какие они есть сейчас. Антипиратская операция Site Down повлекла распад группы. Сервис цифрового распространения компьютерных игр

Steam некоторое время распространял версию игры Max Payne 2, отвязанную от компакт-диска, пока дистрибутив ее не был обновлен. Тем не менее, лого группы Myth все еще присутствовало в файле с именем testapp.exe.

PARADOX (PDX)

Группа PARADOX (сокращенно PDX) (рис. П2.23, *вверху*) с момента основания занималась, главным образом, взломом/релизом игр для компьютеров Amiga, перейдя затем к ПК и консольным играм. Одной из первых группе PARADOX удалось успешно взломать операционную систему Windows Vista, что некоторое время после ее выпуска было проблемой для хакеров.

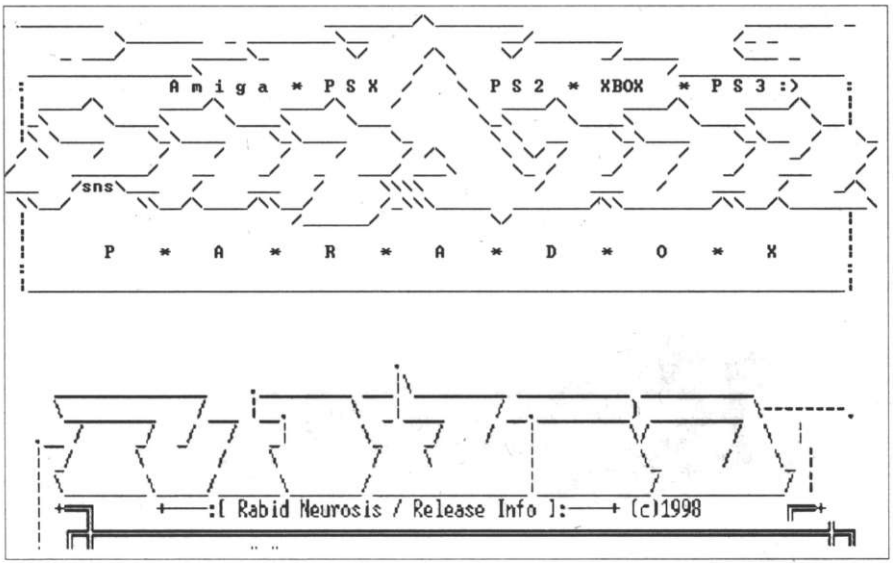


Рис. П2.23. ASCII-лого групп PARADOX (*вверху*) и Rabid Neurosis *(внизу)*

Появление PARADOX датируется концом 1989 года, когда объединились некоторые члены датской группы Trilogy и французской M.A.D. Начав со взлома программного обеспечения для компьютеров Amiga, группа в 1991 году быстро распалась (наиболее активные ее члены присоединились к команде Quartex), а затем возродилась с новым лидером уже в 1993 году. Тогда PARADOX и увлеклась взломом игр для консолей Sega Genesis и Super Nintendo, через год занявшись взломом ПО и для персональных компьютеров. В конце 2000 года группой был выпущен релиз пиратской версии (хоть и не полноценной) игры Spyro: Year of the Dragon для приставки Sony PlayStation, причем эта игра славилась очень сильной на то время защитой. Два месяца спустя релиз был доработан и выпущен в стандартах NTSC и PAL. Команда PARADOX взламывала игры для множества консолей: таких как PlayStation, PlayStation 2, PlayStation 3, PlayStation Portable, Dreamcast, Nintendo 64, Nintendo GameCube, Wii и Xbox. Кроме того, группа занималась взломом аппаратно-защщщенного ПО, в том числе для отладки и разработки. Как уже отмечалось, команда успешно обошла механизм активации в операционной системе Windows Vista (а также и Windows 7) путем эмуляции SLIC-таблицы, внедряемой в BIOS компьютера. Помимо основной деятельности, члены группы пробовали себя также и в демомейкерстве и занимали первые места в демопата. Последние релизы группы датируются 2012 годом, о распаде PARADOX достоверных сведений нет.

Rabid Neurosis (RNS)

Rabid Neurosis (RNS) (рис. П2.23, *внизу),* как группа по распространению MP3-релизов, была основана 6 июня 1996 года. Спустя три года, по утверждениям членов команды, ими выпускалось свыше 6 тыс. релизов в год. Группа получила известность прежде всего выпуском релизов ожидаемых в те времена альбомов, в жанрах хип-хоп, поп, рок и танцевальной музыки — за недели, а и иногда месяцы до официальных премьер. Последний релиз группы датируется 19 января 2007 года. В сентябре 2009 года некоторые участники уже распавшейся группы были обвинены в нарушении авторских прав и приговорены к тюремным заключениям и денежным штрафам.

Radium

Группа Radium (RDM) (рис. П2.24, *внизу),* созданная в июле 1997 года, в свое время была известна релизами дорогого ПО для обработки звука: такого как Cubase VST, Propellerheads ReBirth (известной чрезвычайно высокой степенью защиты) и Pro Tools, а также кодека Fraunhofer MP3. Группа Radium обеспечивала поддержку своих релизов лучше, чем компании, которые фактически произвели взломанные программы. В 2004 году было обнаружено, что некоторые аудиофайлы, включенные в дистрибутив операционной системы Microsoft Windows XP, — например, WMPAUD1.WAV, были созданы в пиратской версии программы Sound Forge, выпущенной группой Radium.

Рис. П2.24. ASCII-лого групп Razor 1911 (*вверху)* и фрагмент NFO-файла группы Radium *(внизу)*

Razor 1911 (RZR)

Группа Razor 1911 (RZR) (рис. П2.24, *вверху)* образовалась в октябре 1985 года в Норвегии и изначально именовалась Razor 2992. Ее основатели известны под никами Doctor No, Insane TTM и Sector9. Согласно данным Министерства юстиции США, Razor 1911 — самая старая группа, которая все еще активна в Интернете.

Изначально группа занималась взломом программного обеспечения для компьютеров Commodore 64. Вскоре после появления группа сменила название с Razor 2992 на Razor 1911 (1911 в шестнадцатеричном исчислении— 777). В 1987-1988 годах группа мигрировала на новую аппаратную платформу, продолжая создавать демо и начав взламывать игры для компьютеров Amiga. В начале 1990-х Razor 1911 сделала еще один переход, на сей раз переключившись на релизы для ПК IBM PC, продолжив выпускать крэктро, демо и музыку. С 1992 года релизы группы распространялись на дискетах, пока их не сменили оптические компакт-диски (CD). В те же годы Razor 1911 столкнулась с конкуренцией со стороны многих других групп, начиная с Tristar & Red Sector inc. (TRSi), Pirates With Attitude (PWA), The Dream Team (TDT) и FairLight в 1994 году и заканчивая Prestige, HYBRID и прочими в 1995-м. В то же время группа пополнилась новыми членами из другой команды, Nexus. В 1995 году дискеты быстро вытеснились компакт-дисками, и Razor 1911 переключилась на риппинг дисков. Новый виток развития команда получила после формирования ISO-сцены и занялась релизами образов дисков.

Группа существует и по сей день, выпуская релизы игр (может быть не так часто как раньше) и занимаясь демомейкерством, выигрывая при этом призы. Вы можете посетить ее официальный веб-сайт по адресу **razorl911.com.** На протяжении всех лет существования Razor 1911 является крупнейшей и лучшей группой на демосцене. Подробную историю группы вы можете прочитать на странице по ссылке **tinyurl.com/pcfp7mv.**

RELOADED(RLD)

Группа RELOADED (RLD) (рис. П2.25) была основана в 2004 году бывшими членами команды DEViANCE и продолжает работу по сей день, радуя пользователей релизами новейших игр: таких как Need for Speed Rivals, Resident Evil 4, Nascar 14, Might and Magic X, Assassin's Creed IV и др. Из числа ее релизов можно отметить взлом и выпуск игры Spore за четыре дня, а симулятора Sims 3 (бета-версии) — за 15 дней до соответствующих дат их официальных релизов. 29 февраля 2008 года группа RELOADED выпустила релиз игры Assassin's Creed за месяц до ее поступления в продажу. Правда, этот релиз впоследствии был «нюкнут» из-за проблем с запуском, и спустя некоторое время RELOADED выпустила исправленный релиз. В мае 2006 года группа взломала защиту StarForce и выпустила игру Splinter Cell: Chaos Theory спустя 424 дня после даты начала официальных продаж. 27 февраля 2010 года была выпущена игра Battlefield: Bad Company 2 — за три дня до официального релиза, но игроки сообщили о проблемах с управлением в игре. Генераторы ключей



Рис. П2.25. ASCII-лого группы RELOADED

группы RELOADED создают ключи, оканчивающиеся JtRLD, где X — буква или число. Группой RELOADED было также опубликовано старое приложение, предназначенное для взлома защиты SafeDisc и SafeCast старых версий игр. Оно может использоваться для обхода процесса валидации дисков CD/DVD, демонстрационного периода, онлайн-активаций (бета-версий игр), ограничений числа запусков и привязки к диску.

RiSCiSO

Варезная группа RiSCiSO (RISC-ISO) (рис. П2.26) была основана приблизительно в 1993 году и занималась распространением контрафактного программного обеспечения, игр и фильмов. Команда прекратила существование летом 2005 года после операции Site Down, во время которой по наводке информатора было арестовано 19 членов группы. Лидер группы, Шон О'Тул (ник Chucky), 5 лет находился в розыске и так и не был найден. Подробную статью о группе вы можете почитать по адресу tinyurl.com/pd36o8h.

Рис. П2.26. ASCII-лого группы RiSCiSO

SKIDROW

SKIDROW (рис. П2.27) — известная варезная группа, специализирующаяся на взломе и распространении ПК-игр и известная обходом DRM-защиты компании Ubisoft, а также выпуском релизов сломанных версий игр, требующих аутентификации с помощью сервиса Steam. Первый релиз группы датируется 29 мая 2001 года, и команда до сих пор трудится над взломом игр, выпуская такие релизы, как Tomb Raider и Real World Racing.

Superior Art Creations (SAC)

Superior Art Creations (SAC) известна, прежде всего, в сфере компьютерного искусства, а также и в варезной Сцене. Участники SAC выпустили много работ в виде ANSI- и ASCII-графики, растровых VGA-изображений, трекерной музыки и т. п. Символьная графика SAC также использовалась на FTP-серверах. Группа была основана в Германии в декабре 1994 года и в том же месяце выступила с первой своей работой в Хернинге, Дания. Во второй половине 1990-х годов большинство известных групп, работающих в стиле ANSI-графики, дистанцировались от варезной Сцены, стараясь творить ради искусства или для BBS, которые были тесно связаны с компьютерным искусством. Использовав сей благоприятный момент, группа SAC быстро стала ведущей группой варезной Сцены и смогла завоевать уважение неварезных арт- и демогрупп широтой своих творений в сфере компьютерного искусства.

С самого начала SAC представляла собой уникальную структуру — ее члены в любом направлении работали, в основном, независимо от лидеров группы. Каждый участник команды был волен выбирать, какой запрос в подготовке творческого проекта он будет выпол-



Рис. П2.27. ASCII-лого группы SKIDROW

нять, а какой — нет. Должностной рост членов группы, за редким исключением, осуществлялся после активного участия в деятельности группы в течение длительного периода времени. Кандидаты в участники группы принимались голосованием большинства действующих членов SAC и никогда каким-либо конкретным человеком (независимо от его статуса). Все примеры работ кандидатов размещалась на приватной BBS в Берлине и публиковались на публичном IRC-канале FTP-сервера группы. Роль лидера SAC заключалась в сборе новых творений участников группы и сборке/релизе нового пака SAC Art Pack с обновлением NFO-файла. Это было довольно-таки просто, потому как лидер группы SAC являлся одновременно и системным оператором (сисопом) приватной BBS-группы.

Художники SAC работали над созданием ASCII- и ANSI-графики (например, лого группы в NFO-файле и FILEJD.DIZ, а также и на BBS) и растровых VGA-изображений для других компьютерных групп (варезных, хакерских, демо и арт-групп), BBS, FTP-серверов, веб-сайтов и пр. Музыканты SAC создавали звуковые композиции в формате MOD, а позднее и MP3, считавшиеся как отдельными произведениями, так и частями интро, демо и других приложений, например, инсталляторов. Кодеры, или программисты, создавали рекламу на BBS, крэктро и интро, используя большинство графики и музыки, созданной членами команды SAC. К концу 1990-х большинство ASCII-лого для NFO-файлов разных групп было создано членами SAC. Вы можете посетить сайт группы по адресу **roysac.com.**

The Humble Guys (THG)

В 1989 году два друга, Candyman и Fabulous Furlough, основали команду The Humble Guys (THG), известную в варезной среде и демосцене (по нескольким крэктро). Группа также ввела в обращение NFO-файлы, содержащие описания релизов Сцены перед их упаковкой и распространением. Первый NFO-файл был вложен в релиз ремейка классической аркады Bubble Bobble в 1989 году. С тех времен берет начало поколение ASCII-художников, декорирующих и по сей день NFO-файлы варезных групп. В декабре 1991 года вышел первый и единственный экземпляр электронного журнала The Humble Review, содержащий игровые обзоры и статьи.

THG стала одной из первых групп, реализовавших приложение для создания демо для персональных компьютеров, названное THG IntroMaker. Это DOS-приложение позволяло создавать отдельный исполняемый файл, воспроизводящий музыку и демонстрирующий экранную графику, без необходимости в знании какого-либо языка программирования. До появления в варезной Сцене группы THG на компьютерах IBM использовались лишь текстовые интро, обычно цитирующие тексты песен. Команда THG перенесла опыт с систем C64 и Amiga на IBM, представив публике первые анимированные и графические интро. Сейчас в этих целях используются намного более продвинутые и сложные приложения типа Werkkzeug.

Группа THG существенно повлияла на функционирование варезной Сцены. До THG релизы были случайны, со многими дубликатами разных групп, выпускаемыми обычно спустя многие недели после появления софта или игры в розничной продаже. Нередко игры, публикуемые на BBS, не были даже взломаны. Группа THG изменила такое положение, выпуская релизы до их появления в розничных сетях. Это стало возможным благодаря контактам с основными оптовыми дистрибьюторами программного обеспечения и заказу игр с экспресс-доставкой (обычно занимавшей не более пары дней). В тех случаях, если экспресс-доставка не осуществлялась, находились люди, живущие недалеко от офисов компаний-разработчиков программного обеспечения, которые могли приобрести софт и игры в день выпуска и переслать их группе. Такой «ударный» метод доставки обеспечивал группу исходным материалом уже в ближайший рабочий день, максимум на два дня позже начала официальных продаж. Преимуществом THG было то, что большинством других варезных групп управляли подростки, которые днем учились в школе и могли работать только после обеда. В THG же заправляли взрослые профессионалы, которые могли получать посылки в период их доставки компаниями FedEx или UPS. Кроме того, некоторые члены THG работали в утренних телешоу, а компании-разработчики программного обеспечения, стремящиеся к бесплатной рекламе, посылали на телешоу коробку с новым, а иногда и предрелизным, ПО — достаточно было одного-единственного телефонного звонка. Большинство крэков создавалось менее чем за час и тут же следовал релиз.

В THG также поняли принцип тиражирования программного обеспечения. Как только проект (программа или игра) был принят, коробка, мануал и финальная версия программы/игры отправлялись в компанию, занимающуюся тиражированием копий, предназначенных для розничных продаж. Контактируя с такими компаниями, члены группы THG могли получать игры за недели до начала их продаж в магазинах. Игра F-14 Tomcat компании Activision, как и все игры фирмы Microprose, может служить отличным примером из того времени. В разгаре карьеры THG имела контакты с поставщиками игр из США, Великобритании, Франции, Германии и многих азиатских стран. Команда THG ввела понятие «курьер», отделив людей, занимающихся отслеживанием дубликатов и публикацией релизов на BBS. Курьеры в THG должны были проверять, не появились ли схожие релизы на BBS конкурентов ранее BBS их группы. Комбинация поставщиков программного обеспечения и курьеров перевернула варезную Сцену вверх дном в 1990 году, но сейчас иная структура и не воспринимается.

Под влиянием THG возникла жесткая конкуренция в выпуске релизов. В результате большинство старых, закоренелых, варезных групп исчезло со Сцены. Единственной группой, работавшей в том же направлении и пережившей реформы, реализованные THG, была International Network of Crackers (INC), впоследствии ставшая главным конкурентом THG в сфере взлома софта.

После того, как Candyman закрыл свою BBS и уехал из США, Fabulous Furlough принял узды правления группой. Возникшие столкновения между членами группы привели к отколу нескольких членов THG (включая Genesis и The Humble Babe[1]), сформировавших впоследствии новую группу под названием United Software Association (USA). Группа USA выпустила несколько релизов игр, большинство из которых были получены от одного из поставщиков THG в Иллинойсе, которого USA удалось переманить на свою сторону. После ареста The Humble Babe (сменившего к тому времени ник на The NotSoHumble Babe[2]) и обвинения его в махинациях с кредитными картами, USA объединилась с европейским подразделением команды FairLight и стала известна под лого USA/FLT. Это неизбежно привело к вражде USA и THG, и спустя год последовало фиаско USA/FLT.

К 1994 году большинство основных членов и создателей группы THG перестали быть связаны с варезной Сценой, и группа оказалась в тени. Финальный этап завершения карьеры THG случился после закрытия Нью-Йоркской BBS под названием The Pits в 1995 году. А 5 сентября 2006 года Дэвид Дж. Фрэнсис, один из основателей THG и известный под никои Candyman, скончался в своем родном городе Сент-Луис, штат Миссури, от остановки сердца.

О противостоянии групп THG и INC можно почитать на странице по ссылке **tinyurl.com/qhpr2jl.**

Tristar and Red Sector Incorporated (TRSI)

Группа Tristar and Red Sector, Inc. (TRSi) (рис. П2.28) образовалась в 1990 году в результате сотрудничества двух варезных команд: Tristar и Red Sector Incorporated. Группа TRSI мигрировала от выпуска релизов для компьютеров Commodore 64 к платформам Amiga и IBM PC, в конечном счете, перейдя к консольным играм, и распалась в конце 2003 года.

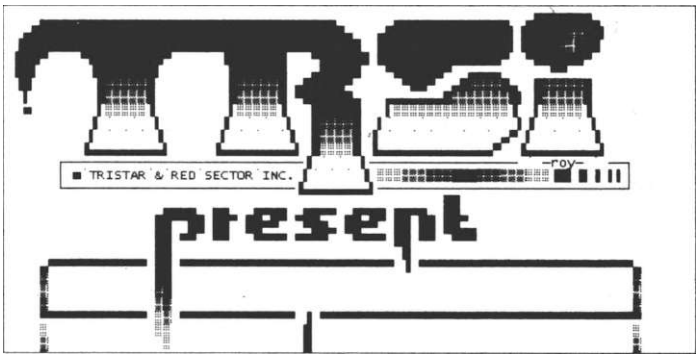


Рис. П2.28. ASCII-лого группы Tristar and Red Sector, Incorporated

[1] **The Humble Babe — Робкий малыш (пер. с англ.).**

[2] **The NotSoHumble Babe — Уже не такой робкий малыш (пер. с англ.).**

United Software Association (USA)

United Software Association (USA) была варезной группой, выпускавшей софт и игры для компьютеров ШМ PC на протяжении 1990-х годов (см. также *разд. «The Humble Guys (THG)»* ранее в этой главе). Группа USA слилась с подразделением команды FairLight, отвечавшим за выпуск софта и игр для ПК, и стала известна под лого USA/FLT. В январе 1992 года несколько членов команды USA были арестованы Секретной службой США по обвинению в кардинге (мошенничестве с кредитными картами).

Несколько слов в заключение раздела

Помимо здесь упомянутых существовали и другие варезные группы, некоторые из них продолжают деятельность и по сей день: MAGNiTUDE, PROPHET (рис. П2.29), ZWT, TBE, ANTiDOTE, LIGHTFORCE и др.



Рис. П2.29. ASCII-лого группы PROPHET

СУБКУЛЬТУРА

Многие участники варезных групп создают красивые видеоряды, пишут музыку и рисуют ASCII-графику. Это положительная сторона компьютерных «негодяев», о которой вы узнаете из *приложения 3.*

Если вас заинтересовала тема Сцены, некоторые, правда, не очень свежие, материалы можно найти здесь: **tinyurl.com/p27q3q3.** Вам может показаться интересными также статьи **tinyurl.com/oeyd5v4, tinyurl.com/nlmftbg** и **tinyurl.com/oy2dq7x.** Существует и локализованный 20-серийный сериал о жизни Сцены: **tinyurl.com/dxuofz9** — о нем уже было упомянуто чуть раньше. Сайты **xrel.to** и **nfohump.com** помогут вам найти и просмотреть самые свежие NFO-файлы варезных групп, а по адресу **tinyurl.com/o652v4k** расположен каталог всех известных команд Сцены.

* * *

Приведенный здесь обзор мира вареза никоим образом не нужно рассматривать как рекламу пиратства. Материал обзора собран из разных общедоступных источников во Всемирной паутине в связи с интересом к описываемому явлению.

Тем не менее, я рекомендовал бы вам опасаться пиратского программного обеспечения (а также и нелегальных копий видео- и аудиопродукции), к тому же, вы вполне можете обойтись без него, — например, использовать аналогичные бесплатные программы. Так, многие пользователи устанавливают и взламывают программу Adobe Photoshop, хотя на самом деле не используют и 10% ее профессиональных возможностей. Инсталлируете гигабайты мощного графического редактора, чтобы раз в месяц подкорректировать яркость/контраст фотоснимка или удалить эффект красных глаз? Смысл? Загрузите бесплатный фоторедактор из пакета Windows Live — он все это умеет делать. Или тот же GIMP... Понравился формат PDF? Незачем устанавливать Adobe Acrobat Professional — вряд ли вы занимаетесь профессиональной версткой в домашних условиях. А офисный пакет Microsoft Office (2007 или версии старше) — его-то вы приобрели? — умеет экспортировать документы в PDF-формат. Да и тот же бесплатный LibreOffice эту функцию тоже поддерживает. Существуют и бесплатные редакторы PDF-файлов, и многие другие бесплатные аналоги платных приложений.

А игры, видеофильмы и музыкальные диски далеко не так дорого стоят, чтобы из-за этого нарушать закон.

ПРИЛОЖЕНИЕ 3

Компьютерное искусство

Искусство **ASCII-Art**

Трекерная музыка

Интро, демо и крэктро

Помимо «нехороших» манипуляций с программным обеспечением, участники варезных групп часто создают графические, видео- или музыкальные творения, которые вкладывают в виде файлов в архивы с релизами. Графические произведения, как правило, представлены в виде ASCII-графики, т. е. изображения состоят из символов ASCII и могут быть сохранены в обычном текстовом формате. Трекерная музыка создается в специальном музыкальном редакторе (трекере, tracker) и по звучанию схожа с MIDI-файлами. Такие файлы имеют малый размер и различные расширения: mod, xm, s3m, it и пр. Видеоряды же выстраиваются в реальном времени компьютером по принципу компьютерных игр, что позволяет существенно уменьшить размер файла в сравнении с обычным видеофайлом. Все это — основные разновидности *демосцены,* которые мы сейчас и рассмотрим.

История демосцены, как явления компьютерной андеграунд-культуры, началась в середине 80-х годов прошлого века, когда появились первые домашние компьютеры, первые коммерческие программы и, как следствие, первые взломщики. Варезные группы (такие как THG, Razor 1911 и др.) искали способ заявить о себе — что это именно они предоставили тот или иной релиз. Так возникли небольшие заставки — *интро* — как правило, в те времена ограниченные размером файла в 64 Кбайт[1]. К нескольким строчкам текста на черном фоне, представлявшим интро в самом начале, в дальнейшем добавились анимационные эффекты и музыка. Изначально создаваемые как часть программы, позднее интро стали делать в виде отдельных файлов с демонстрацией возможностей группы. Так появились демосцена и специальные мероприятия, на которых демонстрировались достижения участников, — демопата. Впоследствии развились направления ASCII-Art и синтезирования музыки.

Искусство ASCII-Art

ASCII-Art (читается как *аски-арт)* — форма изобразительного искусства, в котором для представления изображений используются символы ASCII (три разных слоника, изобра-

[1] **64 Кбайт — максимальный допустимый размер COM-файла.**

женные в формате ASCII, представлены на рис. П3.1). При подготовке таких изображений используются 95 символов (буквы, цифры и знаки пунктуации) таблицы ASCII.

Существуют и ASCII-анимации, наиболее известной из которых является ASCII-версия пятого эпизода фантастического фильма «Звездные войны» (просмотреть ее можно тут: asciimation.co.nz).

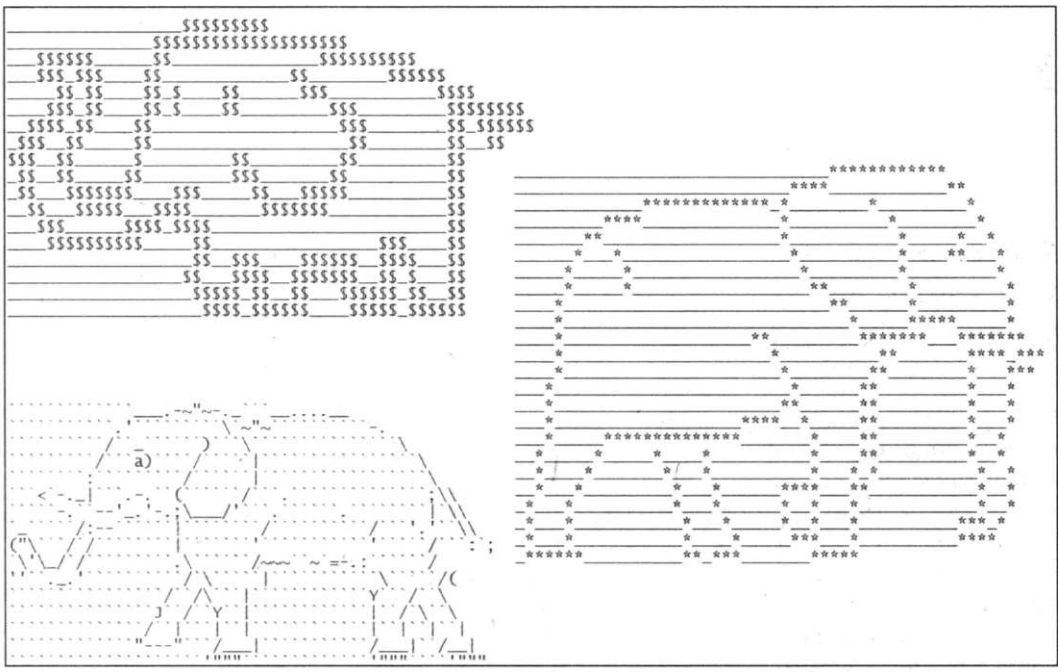


Рис. П3.1. Примеры изображения ASCII-Art

Название ASCII-Art этот вид искусства получил в середине 1980-х годов и с тех пор развивался и обрастал правилами[1]. Благодаря пионеру ASCII-Art — группе Aces of ANSI Art (A.A.A.), показавшей его возможности, свет увидел это искусство на высоком уровне, и за группой потянулись последователи. К середине 1990-х годов Сцена полностью сформировалась, и главными направлениями рисования в текстовом режиме стали ASCII-Art, ANSI-Art и Amiga style (который часто называют «олдскул»). Обычно ASCII-Art распространяется вместе с релизами Сцены в файлах ID.DIZ и NFO.

Для подготовки изображений в стиле ASCII-Art существуют две основные разновидности программ: это своего рода графические редакторы, работающие в текстовом режиме, и конвертеры графических изображений в ASCII-версии.

ASCII-ИГРЫ

Существуют даже компьютерные игры, для изображения объектов в которых используются символы ASCII. О таких играх, созданных по концепции roguelike, вы можете прочитать на веб-странице ru.wikipedia.org/wiki/Roguelike.

[1] **Первые компьютерные «символьные» рисунки относят к 60-м годам прошлого века.**

Помимо «чистого» искусства, ASCII-Art нашло применение у демомейкеров (см. далее *разд. «Интро, демо и крэктро»)* и варезных групп. Последние вкладывают в свои релизы NFO-файл с логотипом группы и, зачастую, несколько ASCII-изображений.

В эпоху модемного (коммутируемого) доступа к Интернету ASCII-оформление использовалось на электронных досках объявлений (BBS), где размещение изображений как элементов интерфейса было невозможно. Сейчас ASCII-Art взошло на новый виток популярности благодаря социальным сетям — таким, как «Одноклассники» или «ВКонтакте», где в сообщениях можно печатать только текст.

В качестве разновидности ASCII-Art существует ANSI-графика (рис. П3.2), при создании которой используются 224 символа, а также 16 цветов шрифта и 8 фоновых цветов, поддерживаемых драйвером ANSI.SYS, работающем в операционной системе DOS. К настоящему моменту ANSI-графика потеряла популярность из-за почти полного исчезновения BBS (где такая графика в основном и использовалась) и системы DOS.



Рис. П3:2. ANSI-рисунки Grave (Aces of ANSI Art, 1991) и Banny (enzOber, 2009)

Огромное количество ASCII-графики доступно по ссылкам на сайте **tinyurl.com/p2m29ev,** а коллекцию ANSI-рисунков вы найдете по адресу **sixteencolors.net.** Ну, а по ссылке **tinyurl.com/ophs5pw** можно найти интересную статью про ASCII-Art и ссылки на коллекции ASCII-рисунков.

Кстати, по ссылкам **tinyurl.com/31ulsym** и **tinyurl.com/353uze** вы можете скачать ASCII- или ANSI-редакторы и попробовать создать свой собственный символьный шедевр.

Трекерная музыка

Многие генераторы ключей, патчи и подобные им приложения во время своей работы воспроизводят фоновую музыку, в основном, трекерную. Как правило, эти композиции созданы самими талантливыми участниками варезных групп и зачастую весьма неплохи. В связи

с этим появились целые порталы, где собраны коллекции мелодий, — к примеру, keygenmusic.net.

Такие композиции создаются в программах-трекерах (отсюда и название композиций) — секвенсорах (в основном, с числовым интерфейсом). Один из самых известных секвенсоров — FastTracker (рис. П3.3).

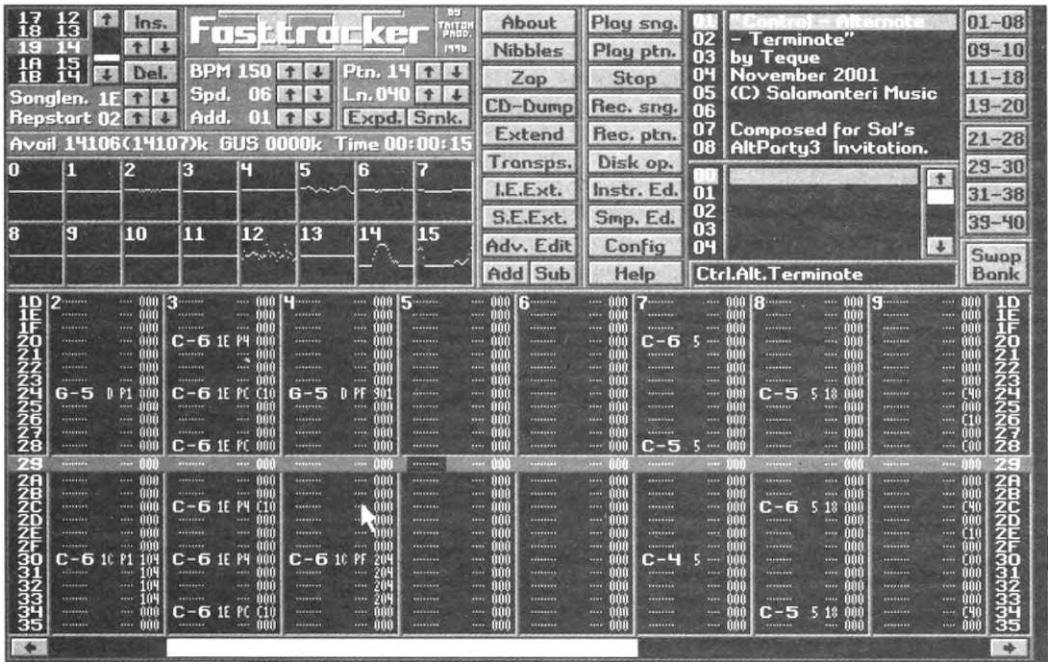


Рис. П3.3. Интерфейс трекера FastTracker

ГДЕ СКАЧАТЬ ТРЕКЕРЫ?

Внушительная коллекция трекеров доступна на веб-сайте по ссылке tinyurl.com/p7dbhez.

Термин «трекер» происходит от первой программы, Ultimate Soundtracker, выпущенной компанией Electronic Arts в 1987 году. Принцип создания музыки в трекерах больше похож на программирование, поэтому сложен для новичка. Но новые версии трекеров обладают все более дружественным интерфейсом, и поэтому такой способ написания музыки не уходит в прошлое. Вкратце о принципе работы трекера вы можете прочитать на странице по ссылке **tinyurl.com/pdl8ku7**.

Трекерная музыка активно используется в рамках демосцены и создается как в виде отдельных композиций (обычно в формате файлов XM, MOD, S3M и IT[1]), так и в виде звукового сопровождения демо/интро, а также варезных инструментов (крэков, генераторов ключей и т. п.). Трекерную музыку, помимо релизов варезных групп, можно услышать в различных играх, — к примеру, в Unreal и Deus Ex. Послушать трекерное творчество (и скачать его образцы) можно на сайте по ссылкам tinyurl.com/6sfncc, tinyurl.com/qzdkmbr и, разумеется, на FTP Сцены: **ftp://ftp.scene.org/pub/music**.

[1] Воспроизвести эти форматы можно многими мультимедийными проигрывателями — к примеру, ^(АисНо.

Трекерная музыка распространяется по принципу Open Source — открыто и доступно для всех без лицензионных ограничений. Существуют специальные сайты (к примеру, **modarchive.org** и **traxinspace.com),** на которых можно разместить свою музыку и получить рецензии и оценки. Сообществом трекерных музыкантов и сегодня проводятся конкурсы и пати (вечеринки) с целью продемонстрировать свои силы в написании музыки.

CHAOS CONSTRUCTIONS & DIHALT

Chaos Construction (cc.**org.ru**) **— это крупнейший в России фестиваль демосцены, проводимый в Санкт-Петербурге. Вторым по величине является демопати DiHalt (dihalt.org.ru), которое ежегодно организуется в Нижнем Новгороде. На фестивалях проводятся различные конкурсы: музыкальные, графические, видео и др.**

Многие варезные группы, в том числе известнейшие в своих кругах, добавляют музыку собственного сочинения в релизы или же распространяют композиции отдельно. К примеру, норвежская группа Razor 1911 создала интересную музыкальную шкатулку под названием Whispers (рис. П3.4), архив с которой можно скачать по ссылке **tinyurl.com/qybe4o4.** Эта яркая, практически классическая, работа посвящена временам года.

На рис. П3.4, помимо Whispers, представлены еще две работы Razor 1911 на фоне собственного сайта группы **(razorl911.com).** Отсюда вы можете скачать их различные творения,

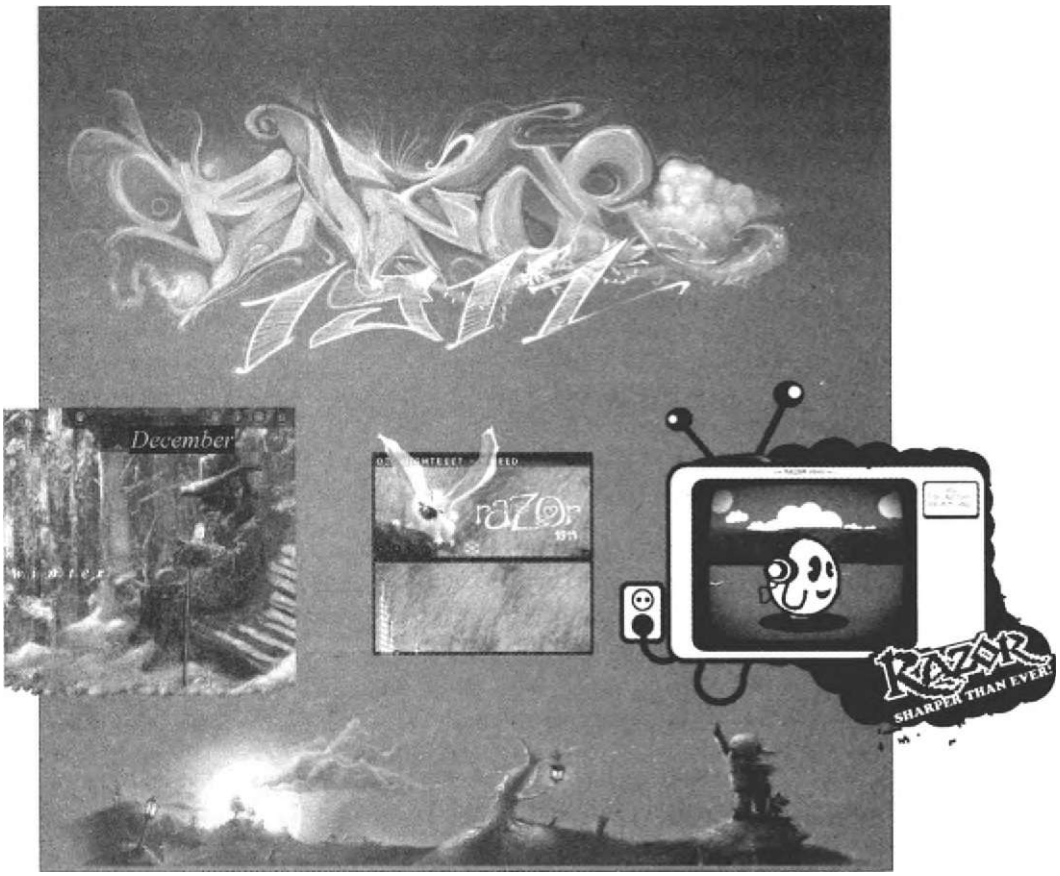


Рис. П3.4. Работы Razor 1911: Blz's Whispers *(слева),* **Chipdisk 4 (в** *центре)* **и Menu Cracktro 2006** *(справа)*

доступные также на ресурсах **files.scene.org/browse/** или **ftp://ftp.scene.org/pub** (как кому удобнее) и **pouet.net.** На этих же ресурсах можно найти и произведения множества групп, создающих и внедряющих в релизы собственную музыку.

Существует еще понятие *чиптюн,* произошедшее от английского chiptune. Оно обозначает музыку, звук которой синтезируется в реальном времени аудиочипом компьютера на основе простейших математических формул. Варезные группы добавляют чиптюны в свои инструменты взлома, а также в интро, поскольку такие звуковые фрагменты имеют крошечные размеры. На многих демопати проводятся соревнования групп по чиптюн-музыке. Скачать чиптюны можно на веб-сайтах **asma.atari.org** и **hvsc.de.**

Интро, демо и крэктро

Иногда архивы с инструментами взлома или дистрибутивы нелегально распространяемого софта содержат небольшие приложения (как правило, без ярлыка), «весом» в десятки, а порой, и в пару сотен килобайт (редко — больше). При их запуске в полноэкранном режиме происходит демонстрация каких-либо визуальных эффектов, имен программистов (из хакерских групп) и т. п. Это *интро* и *демо* — своеобразная субкультура и направление компьютерного искусства. В тех случаях, если подобное эффектное приложение играет роль и взломщика некой программы, — перед вами *крэктро.*

FR-029 ***ГРУППЫ*** *FARBRAUSCH*

Загрузить интро FP-029 вы сможете по ссылке tinyurl.com/qft7jj9. Снимок экрана этого интро приведен на рис. П3.5. Во время просмотра не думайте, что что-то не так с вашим зрением или произошли проблемы с файлом— интро создано специально для просмотра через стереоочки.

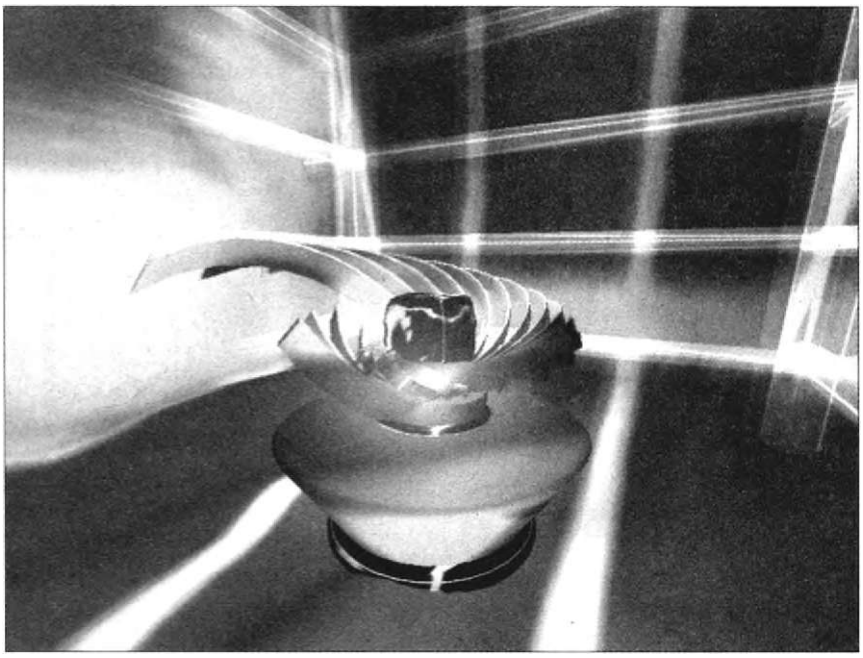


Рис. П3.5. Снимок из интро FP-029 группы Farbrausch

Стоит отметить, что при подготовке интро не используются заранее записанные видеоролики (да и размер файла не позволит) и трехмерные модели — все генерируется в реальном времени мощностями вашего компьютера, а музыка синтезируется встроенным мини-синтезатором. Как правило, каждое интро создается несколькими людьми: одним-двумя кодерами, несколькими художниками компьютерной графики и создателем музыки. Иногда за интро стоит и один-единственный человек.

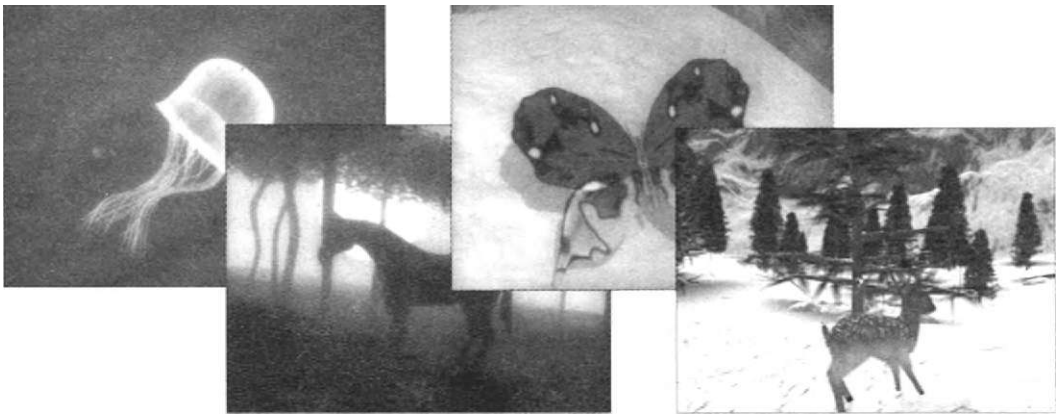


Рис. П3.6. Снимки из интро PaRaDiSe

Просмотрите, к примеру, интро, загрузить которое можно по ссылке **chiptown.ru/demo/paradize.zip** (рис. П3.6). Вы и не поверите, что размер файла всего 64 Кбайт. Это и есть отличительная черта любого интро — малый размер файла, как правило, не более этой величины. Задача создателя интро — уместить в столь небольшой размер кода все свои возможности и поразить эффектностью творения.

Демо — это дальнейшее развитие визуальных заставок, отличающееся большей длительностью и размером файла (как правило, от 4 до 15 Мбайт). В частности, существуют мегадемо, включающие интерактивные элементы, с которыми может взаимодействовать пользователь, и *трекмо* (от англ. trackmo), отличающееся синхронизацией визуального ряда под ритм звукового сопровождения. На рис. П3.7 представлены снимки из мегадемо The

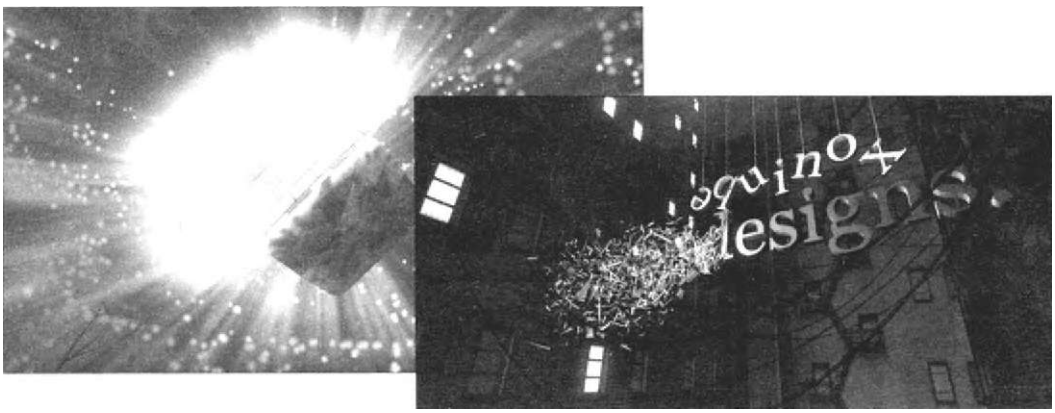


Рис. П3.7. Психоделическое демо *(слева)* **и визуализация группы Farbrausch** *(справа)*

psychedelic color clash session группы United Force & Digital Dynamite, занявшего 2-е место на демопати Function 2010. Скачать этот файл можно по ссылке **tinyurl.com/ufdd-pccs.** На рис. П3.7 также представлено демо fr-041: debris небезызвестной группы Farbrausch.

Много полезных сведений о демо вы почерпнете, посетив веб-страницу по ссылке **tinyurl.com/62swpjn,** а скачать представленные в книге и многие другие демо можно на веб-сайтах **files.scene.org/browse/, pouet.net/prodlist.php, demoscene.ru, tinyurl.com/oarp2yg** и др. На этих сайтах можно найти даже целые компиляции, объем которых достигает размера DVD, и многие другие творения в различных категориях демосцены.

ПРИЛОЖЕНИЕ 4

Получение инвайтов на закрытые сайты (на примере *Whatcd)*

В этом приложении мы рассмотрим, как честным способом получить инвайт (приглашение) на закрытый трекер What.cd. Важно помнить, что лучшим способом получить инвайт является получение его от друга или прохождение тестирования у одного из пользователей ресурса. Согласно правилам сайта, продажа, обмен и совместное использование ивайтов запрещены, поэтому, если вы купите инвайт, велик риск, что он будет заблокирован. На самом деле, в прохождении тестирования нет ничего сложного, нужно лишь немного изъясняться на английском (письменном) и изучить правила ресурса, а также некоторые теоретические вопросы. Подробно вся необходимая информация представлена на сайте tinyurl.com/oo55ffm — без ее прочтения тестирование, скорее всего, вы не пройдете (рис. П4.1).

```
[11:52] <OTester>
[11:52] <BTester> Vou haue FAILED the interuie».
Г11:521 <BTester>
```

Рис. П4.1. Сообщение о том, что тестирование провалено

Нет смысла приводить подсказки и примеры вопросов, т. к. для всех тестируемых они разные. В целом, вопросы тестирования касаются только материала, приведенного на сайте **tinyurl.com/oo55ffm**, поэтому для успешного прохождения тестирования его знания вполне достаточно.

Итак, если вы загорелись идей получения инвайта на сайт Whatcd и проштудировали материал, доступный по указанной ранее ссылке, выполните следующие действия:

1. Загрузите любой IRC-клиент для обмена сообщениями. Наиболее популярными являются программы:
   - mIRC (Windows, mirc.com), используется в моем случае;
   - X-Chat (Windows/Linux, xchat.org);
   - Colloquy (OS X, colloquy.info);
   - **mibbit** (веб-клиент, mibbitcom).
2. Запустите IRC-клиент, например mIRC, — вы увидите главное окно программы и открытое диалоговое окно с настройками.
3. Укажите в поле Nickname (Ник) вкладки Connect (Соединение) любой желаемый ник для чата.

4. Перейдите на вкладку Servers (Серверы) и нажмите кнопку Add (Добавить).
5. В поле Description (Описание) открывшегося окна укажите любое название сервера, значение `irc.what-network.net` в поле IRC Server (IRC-сервер) и число `6667` в поле Ports (Порты) (рис. П4.2).

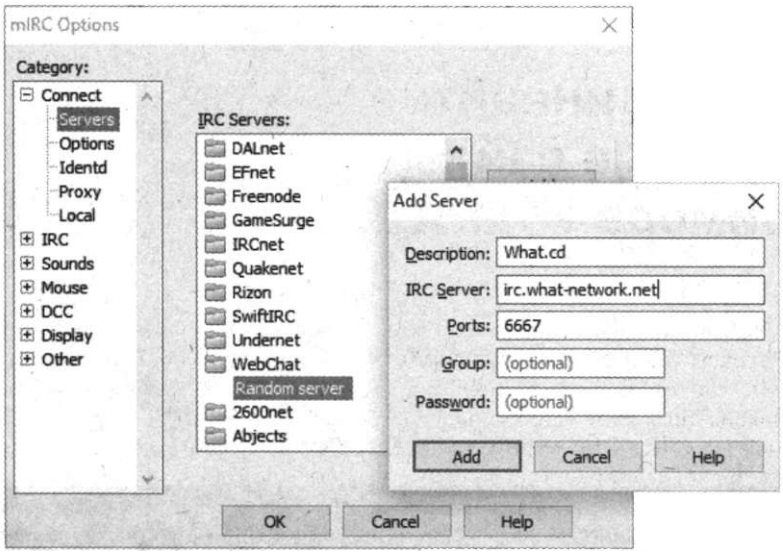


Рис. П4.2. Добавление IRC-сервера What.cd

6. Нажмите кнопку Add (Добавить), а затем кнопку OK — в главном окне появится окно чата со статусом «отключен» (not connected).
7. Нажмите кнопку на панели инструментов окна программы mIRC, чтобы подключиться к серверу.
8. В поле ввода появившегося диалогового окна введите имя канала `#what.cd-invites` и нажмите кнопку Join (Подключиться) (рис. П4.3).

   Теперь осталось следовать указаниям, выводимым в окне чата (на английском языке). Но для начала необходимо измерить скорость вашего соединения с Интернетом на сайте SpeedTest.net и встать в очередь на тестирование, указав ссылку на результаты измерения скорости.

   ИЗМЕРЕНИЕ СКОРОСТИ НА SPEEDTEST.NET

   Чтобы измерить скорость соединения с Интернетом, перейдите по адресу speedtest.net/ru/ и нажмите кнопку Начать проверку. После проверки скорости скачивания/загрузки вы увидите результаты тестирования и кнопку Поделиться результатом. Нажав ее, вы перейдете к окну, показанному на рис. П4.4. Перейдите здесь на вкладку URL и нажмите кнопку Копировать.

9. Введите приведенное далее значение, указав ссылку на результаты измерения скорости вашего соединения (вместо цифр *12345678* надо указать уникальное имя файла, сгенерированное системой для ваших результатов). Для добавления ссылки в поле ввода сообщения можно использовать сочетание клавиш <Ctrl>+<V>:

```
!queue http://www.speedtest.net/result/12345678.png
```

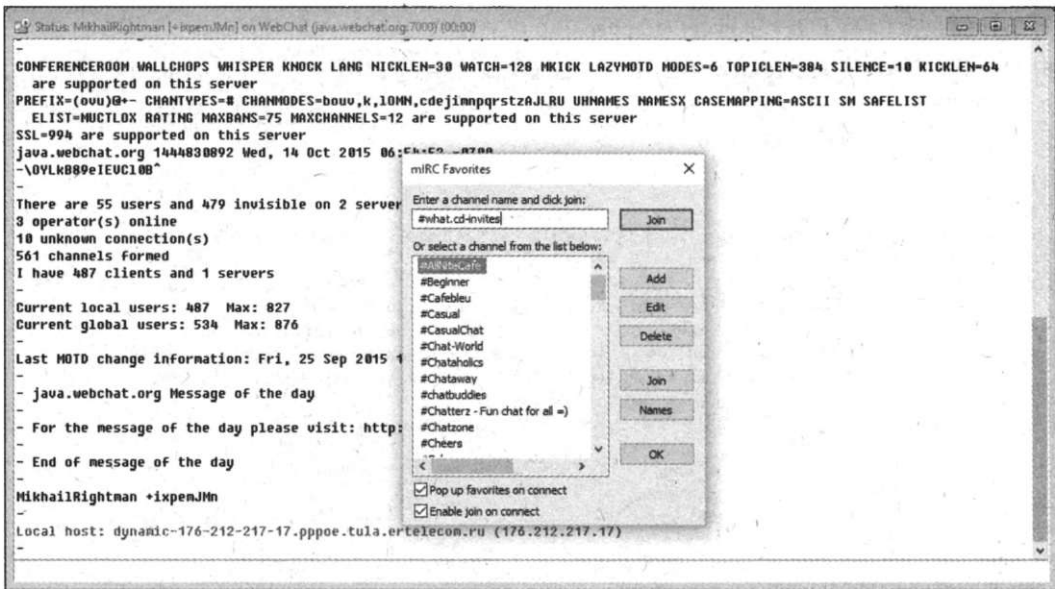


Рис. П4.3. Подключение к каналу #what.cd-invites

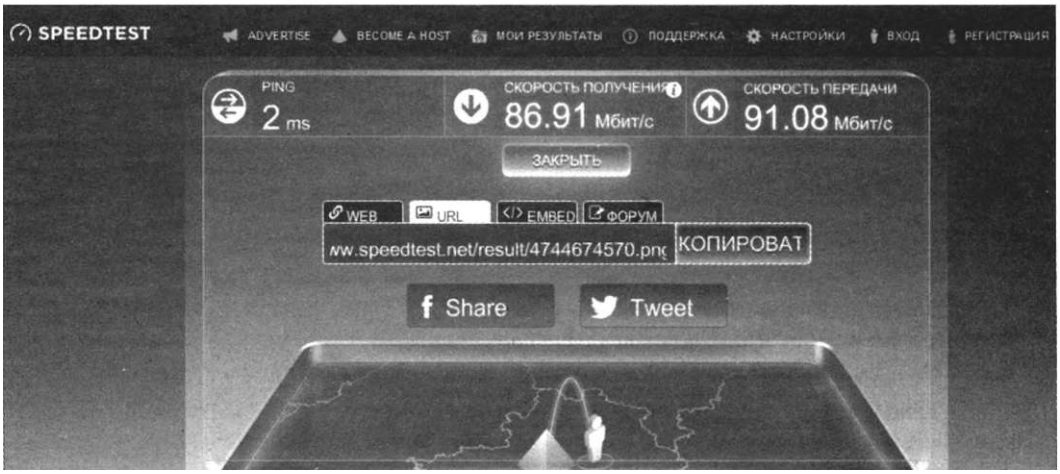


Рис. П4.4. Результаты проверки скорости соединения с Интернетом

```
[10:16] <Vou> (queue http://uuu.speedtest.net/result/12345i78.png
[10:16] -Robot- Vou haue successfully enqueued and are in position 1.
[10:16] -Robot- While you uait, reuiew the interview-related information at http://uuu.uhatinteruieuprep.con/
```

Рис. П4.5. Сообщение о том, что вы встали в очередь на тестирование

После этого вы увидите сообщение о том, что вы встали в очередь, вашу позицию в очереди и приглашение прочитать информацию о подготовке к тестированию (интервью) (рис. П4.5).

10. Через некоторое время (час-полтора, если вы первый в очереди) вы увидите новое окно с приветствием пользователя, который будет вас тестировать. После приветствия и ин-

формации о ходе интервью вы увидите запрос, что если вы готовы к тестированию, необходимо ввести имя пользователя, который будет вас тестировать, чтобы подтвердить вашу готовность (к примеру, если имя пользователя **Tester,** как показано на рис. П4.6, введите текст `Tester` и нажмите клавишу <Enter>). Сами вопросы выглядят следующим образом:

```
[12:47] <@Tester> ж»»»
```

- общие вопросы о вашем возрасте, поле, предпочтениях и т. п. Если вы добрались до этой (последней) группы вопросов, считайте, что тестирование пройдено.

12. Если тестирование пройдено, спустя некоторое время вы получите инвайт (письмо со ссылкой) на указанный вами адрес электронной почты. Если тестирование провалено, не расстраивайтесь, вы можете попытаться пройти его через 48 часов снова. Всего вы можете попробовать пройти тестирование три раза.
13. Получив письмо с приглашением от пользователя, который вас тестировал, перейдите по указанной в письме ссылке, — вы увидите форму регистрации нового пользователя на сайте Whatcd.

    Не покидайте чат, пока успешно не зарегистрируетесь на сайте Whatcd. Вы можете попросить пользователя решить проблемы, которые могут возникнуть при регистрации. И не забудьте отблагодарить его.
14. Укажите все данные, как при регистрации на любом другом трекере, и подтвердите регистрацию, перейдя по ссылке, указанной во втором письме-подтверждении.

После выполнения процедуры регистрации вы станете участником приватного музыкального сообщества (рис. П4.7).

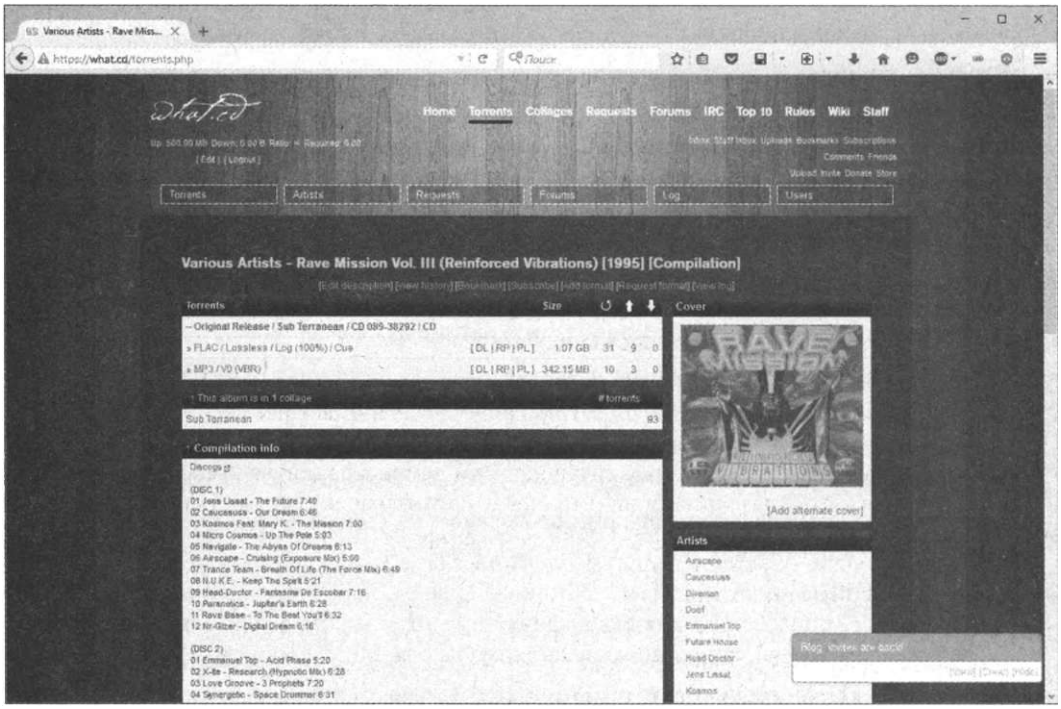


Рис. П4.7. Вот вы и участник приватного музыкального сообщества

ПРИЛОЖЕНИЕ 5

Краткий глоссарий терминов пользователя

0... 9

O-Day. Самые последние релизы программного обеспечения, доступ к которым осуществляется в течение суток после релиза.

O-Hour. Самые последние релизы программного обеспечения, доступ к которым осуществляется в течение часа после релиза.

O-Sec. Самые последние релизы программного обеспечения, доступ к которым осуществляется немедленно после релиза.

2 (от англ. *to*— к (кому)). На форумах и в чатах указание направления или обращение к пользователю (например, на форуме: 2User).

256-битное шифрование. *См.* **AES-шифрование.**

3D (от англ. *3 Dimensions,* три измерения). Как правило, под обозначением подразумевается категория компьютерной графики, совокупность приемов и инструментов (как программных, так и аппаратных), предназначенных для отображения объемных объектов. Также — в зависимости от контекста — может обозначать стереоскопический видеоматериал/игры, трехмерное пространство и объемный звук.

3Б-кинематограф. Разновидность передачи изображения в кинематографе, имитирующая наличие третьего измерения или вызывающая у зрителя иллюзию глубины пространства. Метод, как правило, предполагает одновременную съемку с помощью двух синхронизированных кинокамер с разных ракурсов. При демонстрации фильма по специальной технологии каждый глаз зрителя видит только предназначенную для него часть стереопары, в результате чего зрительная зона коры головного мозга воспринимает эти изображения как одно объемное целое. В большинстве случаев для просмотра 3D-фильмов требуются специальные очки.

3Б-печать. Технология послойного создания физического объекта по цифровой 3D-модели с помощью особого 3D-принтера, в котором вместо краски используются специальные полимеры. Процесс трехмерной печати также называется *быстрым прототипированием.*

3G (от англ. *3 Generation,* третье поколение). Технологии мобильной связи 3-го поколения — набор услуг, который объединяет как высокоскоростной мобильный доступ к сети Интернет, так и технологию радиосвязи, которая создает канал передачи данных.

3GP. Формат видеофайлов для мобильных телефонов. Некоторые современные мобильные телефоны способны записывать и воспроизводить файлы в формате 3GP. Видеофайлы

в формате 3GP имеют малый размер по сравнению с другими форматами видео из-за низкого разрешения и качества.

4G (от англ. *4 Generation,* четвертое поколение). Поколение мобильной связи с перспективными технологиями, позволяющими осуществлять передачу данных со скоростью, превышающей 100 Мбит/с в движении и 1 Гбит/с — стационарным абонентам.

4К UHDTV (от англ. *Ultra-High Definition Television,* телевидение сверхвысокой четкости). Стандарт вещания цифровых телевизионных сигналов с высококачественным видеоизображением разрешением 3840x2160 (2160p) и объемным звуком.

5G (5-е поколение мобильных сетей или 5-е поколение беспроводных систем). Телекоммуникационный стандарт связи нового поколения.

6to4. Переходный механизм, позволяющий передавать **1Py6**-пакеты через **IPv4-cera.** Используется, если конечный пользователь или сайт хотят получить соединение с IPv6-Интернетом, но не могут получить его от провайдера.

8К UHDTV (от англ. *Ultra-High Definition Television,* телевидение сверхвысокой четкости). Стандарт вещания цифровых телевизионных сигналов с высококачественным видеоизображением разрешением 7680x4320 (4320p) и объемным звуком.

A

AC3. *См.* **Dolby Digital**

Account, аккаунт, учетная запись. Запись о пользователе, созданная при регистрации на сервере какого-либо интернет-сервиса, — например, электронной почты.

ActiveX. Технология, используемая для улучшения и повышения функциональности веб-страниц (добавление анимации, видео, режима трехмерного просмотра и т. п.). Элементы управления ActiveX представляют собой небольшие программы, код которых вставляется в код веб-страниц. Подвержены заражению вредоносным кодом.

Adium. Бесплатный универсальный клиент обмена мгновенными сообщениями (мессенджер) для операционной системы OS X, который под держивает множество протоколов.

Adobe Systems. Крупная американская компания-разработчик программного обеспечения. Разработчик таких программ, как Adobe Photoshop, Adobe Premiere, Adobe Acrobat и др.

Adobe **Flash** (ранее Macromedia Flash). Мультимедийная платформа компании Adobe Systems для создания веб-приложений и мультимедийных презентаций. Широко используется для создания рекламных баннеров, анимации, игр, а также воспроизведения на веб-страницах видео- и аудиоконтента. Подвержена заражению вредоносным кодом.

Adobe Reader. Бесплатное приложение компании Adobe Systems для просмотра и рецензирования PDF-файлов.

ADSL (от англ. *Asymmetric Digital Subscriber Line,* асимметричный цифровой канал подписчика). Технология, позволяющая передавать данные абоненту со скоростью до 8 Мбит/с и до 1 Мбит/с в обратном направлении. Основное преимущество технологии ADSL состоит в том, что для нее используется уже проложенный телефонный кабель. На действующей телефонной линии устанавливаются частотные разделители — сплиттеры: один на АТС и один у абонента. К абонентскому сплиттеру подключается обычный телефон и ADSL-модем, который позволяет осуществить высокоскоростной доступ в Интернет. Возможны передача данных и телефонное соединение одновременно. Главный недостаток технологии — низкая скорость, из-за которой она была вытеснена с рынка оптоволоконными средствами передачи данных.

Adware (от англ. *Advertisement,* реклама и *Software,* программа). Разновидность «бесплатного» программного обеспечения, при использовании которого пользователю принудительно демонстрируется реклама.

AES-шифрование (также известно под обозначением Rijndael). Аббревиатура AES расшифровывается как *Advanced Encryption Standard,* улучшенный стандарт шифрования. Этот стандарт был выпущен на замену устаревшему алгоритму DES (56-бит) и описывает распространенный симметричный алгоритм блочного шифрования, позволяющий защитить конфиденциальные данные. Во время шифрования используется специальный ключ, определяющий стойкость шифра, длиной 128 (AES-128), 192 (AES-192) или 256 (AES-256) битов. Чем длиннее ключ, тем сложнее взломать шифр. Предполагается, что подбор 128-битного AES-ключа современным компьютером занял бы больше времени, чем прогнозируемый возраст Вселенной.

AirDrop. Технология передачи файлов через интерфейсы Wi-Fi и Bluetooth, разработанная компанией Apple и используемая в операционных системах OS X и iOS.

Alpha. Версия программного обеспечения (после Pre-Alpha), представляющая собой первый рабочий вариант, используемый внутри компании-разработчика для тестирования. Как. правило, совершенно «сырая» и нестабильная версия.

Amazon Web Services. Платформа облачных веб-сервисов компании Amazon для предоставления различных услуг — таких как хранение данных (файловый хостинг, распределенные хранилища данных), аренда виртуальных серверов, предоставление вычислительных мощностей и пр.

AN.ON. См. Java Anonymous Proxy.

Android. Операционная система корпорации Google для смартфонов, планшетов, электронных книг и других цифровых устройств.

ANSI-графика. Развитие ASCII-графики. Этот вид цифровой графики создает изображение из символов, не только предлагаемых кодировкой ASCII, но и используя 224 печатных символа, 16 цветов шрифта и 8 фоновых цветов, поддерживаемых драйвером ANSI.SYS, который использовался в системе DOS.

ANts P2P. Файлообменная сеть, анонимизирующая весь поток данных, используя систему маршрутизации, в которой, в отличие от BitTorrent, участники обмениваются трафиком не напрямую, а через несколько узлов.

APE. См. Monkey's Audio.

API (от англ. *Application Programming Interface,* интерфейс прикладного программирования). Законченный фрагмент кода, упрощающий (ускоряющий) разработку приложений.

App **Store.** Магазин приложений на устройствах под управлением операционной системы Apple iOS и OS X.

Apple. Американская корпорация, производитель персональных и планшетных компьютеров, аудиоплееров, смартфонов и программного обеспечения (в частности, операционных систем iOS и OS X).

Apple iPad. См. iPad.

Apple iPhone. См. iPhone.

Apple iPod. См. iPod.

Apple Sàfari. Веб-браузер, разработанный корпорацией Apple и входящий в состав операционных систем OS X и iOS.

Apple TV. Цифровой мультимедийный проигрыватель, разработанный компанией Apple. Предназначен для трансляции потокового мультимедиа (фильмов, музыки, подкастов и фотографий) на широкоэкранные ЖК-телевизоры и плазменные панели из библиотеки iTunes, размещенной на компьютерах Mac или ПК, планшетах iPad, плеерах iPod touch, смартфонах iPhone или из интернет-сервисов iTunes Store, iCloud, Netflix, YouTube, Vimeo, Flickr и др. В качестве операционной системы используется модифицированная версия iOS.

Apple Watch. Наручные часы с дополнительной функциональностью (умные часы), созданные корпорацией Apple. Для их полноценной работы требуется смартфон семейства iPhone 5 или новее. В качестве операционной системы используется платформа watchOS.

Applet. Небольшое приложение, написанное на языке Java и предназначенное для расширения функциональности веб-страниц.

Appz (сокращение от англ. *Applications,* приложения). Как правило, используется в варезной среде, к примеру, для указания раздела на веб-сайте, в котором публикуются ссылки на взломанные дистрибутивы программ.

Arduino. Торговая марка аппаратно-программных средств для построения простых систем автоматики и робототехники, ориентированных на непрофессиональных пользователей. Программная часть состоит из бесплатной программной оболочки (интегрированной среды разработки) для написания программ, их компиляции и программирования аппаратуры. Аппаратная часть представляет собой набор смонтированных печатных плат, продающихся как официальным производителем, так и сторонними производителями. Arduino может использоваться как для создания автономных объектов автоматики, так и подключаться к программному обеспечению на компьютере через стандартные проводные и беспроводные интерфейсы.

ARM (от англ. *Advanced RISC Machine,* усовершенствованная RISC-машина). Семейство 32- и 64-битных микропроцессорных ядер разработки компании ARM Limited. Используются, в частности, в устройствах компании Apple (iPod, iPad, iPhone и Apple TV).

ARP (от англ. *Address Resolution Protocol,* протокол определения адреса). Протокол в компьютерных сетях, предназначенный для определения MAC-адреса по известному IP-адресу.

ARP-спуфинг (транскрипция от англ. *ARP-spoo*ß*ng).* Разновидность сетевой атаки типа атаки посредника, применяемая в сетях с использованием протокола ARP.

ARPANET (от англ. *Advanced Research Projects Agency NETwork,* сеть Агентства по перспективным научно-исследовательским разработкам). Компьютерная сеть, созданная в 1969 году в США и явившаяся прототипом Интернета. В качестве маршрутизируемого протокола использовался TCP/IP, который и по сей день является основным протоколом передачи данных в Интернете. Прекратила свое существование в июне 1990 года.

ASCII-Art (от англ. *American Standard Code for Information Interchange,* американский стандартный код для обмена информацией). Форма компьютерного изобразительного искусства, использующая символы таблицы ASCII для представления изображений.

ASF (от англ. *Advanced System Format,* расширенный системный формат). Формат файлов, содержащих потоковые аудио- и видеоданные. Разработан корпорацией Microsoft. Формат ASF может содержать данные, закодированные при помощи различных кодеков, и поддерживает синхронизацию потоков.

Atari. Американская компания по производству компьютеров и изданию компьютерных игр.

Autodesk. Крупнейший в мире разработчик программного обеспечения для промышленного и гражданского строительства, машиностроения, рынка средств информации и развлечений. Производитель такого программного обеспечения, как AutoCAD, Maya и 3ds Max.

AVC. *См.* **H.264.**

AVCHD (от англ. *Advanced Video Codec High Definition standard*, формат записи видео высокой четкости). При сжатии используется кодек MPEG-4 AVC (H.264).

AVI (от англ. *Audio Video Interleave,* чередование аудио и видео). Мультимедийный контейнер, разработанный корпорацией Microsoft.

AWS. См. Amazon Web Services

B

Backdoor. См. Бэкдор.

BBS (от англ. *Bulletin Board System,* электронная доска объявлений). Распространенный во времена коммутируемого подключения к Интернету способ обмена файлами и общения пользователей компьютеров через телефонные сети.

Beta. Следующая, после **Alpha,** версия разрабатываемого приложения. Часто beta-версии программ представляются общественности на публичное тестирование с целью выявления багов (и для экономии денежных средств). Может выпускаться несколько вариантов: Beta 1, Beta 2 и т. п.

BIOS (от англ. *Basic Input/Output System,* базовая система ввода/вывода). Набор микропрограмм, реализующих **API** для работы с аппаратурой компьютера и подключенными к нему устройствами. BIOS относится к системному программному обеспечению и используется, к примеру, в материнских платах компьютеров и периферийных устройствах. Сетевая разновидность BIOS называется **NetBIOS.**

Bitmessage. Анонимная сеть, которая работает по принципу шифрования всех входящих и исходящих сообщений каждого пользователя, используя сильные алгоритмы шифрования таким образом, что только получатель сообщения способен его расшифровать.

BitTorrent. Пиринговый протокол, разработанный для обмена файлами через Интернет.

Blackberry. Канадский производитель бизнес-смартфонов Blackberry, на которых используется одноименная операционная система.

Bluetooth. Спецификация беспроводных персональных сетей. Стандарт, в зависимости от версии, предоставляет скорость передачи данных до 1 Мбит/с на расстоянии до 100 м и использует 128-битное AES-шифрование для защиты передаваемых данных.

Blu-ray Disc, BD. Поколение дисков большой емкости, пришедшее на смену DVD. Для чтения/записи таких дисков используется лазер в голубом спектре (отсюда и название), способный распознавать бороздки меньшего размера, — против красного у CD/DVD. Однослойный односторонний диск может вместить до 25 Гбайт данных, двуслойный односторонний — до 50 Гбайт, а двуслойный двусторонний — до 100 Гбайт.

Boundless Informant (в пер. с англ. «безграничный информатор»). Система обработки и визуализации больших массивов данных, используемая Агентством национальной безопасности США в качестве инструмента анализа мероприятий по сбору данных в глобальном масштабе.

BSOD (от англ. *Blue Screen Of Death,* синий экран смерти). Сообщение о неисправимой ошибке в операционных системах семейства Microsoft Windows в ходе некорректного выполнения программного кода (или намеренного его нарушения). Лечится исключительно перезагрузкой системы.

Build (в пер. с англ. «сборка»). Минорная версия программы, также именуемая *билдом.*

C

CAPTCHA (от англ. *Completely Automated Public Turing test to tell Computers and Humans Apart,* полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей). Компьютерный тест, используемый для определения, кем является пользователь системы: человеком или компьютером. Основная идея метода заключается в том, чтобы предложить пользователю такую задачу, которая с легкостью решается человеком, но крайне сложна и трудоемка для компьютера, — например, ввод числа с фотографии.

Careware (от англ. *Care,* забота и *Software,* программа). Разновидность условно-бесплатного программного обеспечения, деньги (выплачиваемые пользователем по желанию) за использование которого идут на благотворительность. Вы можете пользоваться таким программным обеспечением совершенно свободно.

Carnivore. Автоматическая система шпионажа для перехвата поступающей и уходящей информации с веб-сайтов, анализа баз данных на веб-сайтах, а также для взлома и анализа электронной почты. На текущий момент является элементом системы **Naruslnsight.** Система позволяет вести интеллектуальный анализ данных практически на всех языках мира, в том числе и на русском. Аналогом Carnivore в России является система СОРМ-2, установленная у всех интернет-провайдеров в РФ.

CDFS. См. ISO 9660.

CD Key. Ключ, выполняющий ту же самую функцию, что и серийный номер, но с тем отличием, что вводится только в момент инсталляции программы (игры). Без правильного CD-ключа продолжение установки в большинстве случаев невозможно.

CGI, CGI-скрипты (сценарии) (от англ. *Common Gateway Interface,* общий интерфейс шлюза). Специальный язык программирования, в основном используемый для создания динамических веб-приложений (контента) во Всемирной паутине, — таких как, например, форумы, гостевые книги, чаты и т. п.

Chaos Constructions. Ежегодный фестиваль демосцены, проводимый в конце августа в Санкт-Петербурге.

ChatSecure. Бесплатное приложение для безопасного общения между пользователями устройств под управлением операционных систем iOS и Android.

Cheat, чит. Некоторый код, предусмотренный разработчиком, для активации каких-либо скрытых режимов (обычно в играх).

Chrome. См. Google Chrome.

Cjdns. Сетевой протокол и его реализация, с помощью которого можно создать масштабируемую, безопасную и простую в настройке сеть, функционирующую как поверх Интернета, так и между маршрутизаторами напрямую.

cMix. Криптографический протокол нового поколения для смешанных сетей, обеспечивающий более высокий уровень анонимизации в сравнении с сетью Tor.

Codec. *См.* **Кодек.**

Cookie. Данные, сформированные сервером в Интернете и сохраненные на компьютере пользователя. Файл (обычно размером не более 1 Кбайт) с этими данными браузер каждый раз пересылает на сервер при попытке пользователя открыть страницу соответствующего сайта. В этом файле хранится информация о компьютере пользователя (в том числе и данные, введенные самим пользователем), которая обычно используется в следующих случаях: для идентификации пользователя, для хранения персональных настроек на сайте, для отслеживания состояния сессии доступа пользователя, для формирования статистики о пользователях. Без cookie-файлов не смогут правильно функционировать многие крупные веб-сайты — например, интернет-магазины. Многие браузеры позволяют отключить функцию cookie, но в этом случае работа пользователя с некоторыми сайтами будет невозможна.

CO-TRAVELER. Программа электронной слежки Агентства национальной безопасности США, инструмент для отслеживания передвижения владельцев сотовых телефонов и выявления их скрытых контактов. Программа позволяет по собранным данным производить поиск сигнала любого мобильного телефона в любой части планеты, определять траектории движения и выстраивать карты взаимодействия между людьми. В рамках программы АНБ ежедневно собирает миллиарды записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру.

Crack, cracked exe, крэк. Пропатченный (взломанный) исполняемый (либо другого типа) файл, предназначенный для замены оригинального файла программы (игры) в целях отмены ограничений по использованию. Использование незаконно.

CRC Error. Ошибка контрольной суммы файла. Часто происходит при разархивировании поврежденного файла из-за ошибки при его скачивании (в таком случае говорят, что архив «битый»),

CVC2. См. CW2.

CW2 (от англ. *Card Verification Value 2*, код верификации карты 2). Трехзначный код проверки подлинности карты платежной системы Visa. Другие платежные системы имеют сходные технологии, к примеру аналогичный защитный код для карт MasterCard носит название Card Validation Code 2 (CVC2). Наносится на полосе для подписи держателя после номера карты либо после последних 4 цифр номера карты и используется в качестве защитного элемента при проведении транзакций, например, при совершении покупок в Интернете. Номер CVV2 не следует путать с ПИН-кодом и со стандартным номером карты. Некоторые карты не имеют CVV2-кода (например, Visa Electron и Maestro), поэтому не подходят для интернет-шопинга.

D

Database. *См.* **База данных**

DCSNet (от англ. *Digital Collection System Network).* Автоматизированная система **ФБР** для проведения перехвата данных различных телекоммуникационных сервисов в США.

DDoS-атака (от англ. *Distributed Denial of Service,* распределенный отказ в обслуживании). DDoS-атака отличается от DoS-атаки тем, что производится с нескольких компьютеров одновременно.

Demoware. Демонстрационная версия программного обеспечения. Версия программного обеспечения, предназначенная для демонстрации возможностей программы, часть функций которой заблокирована. Также *см.* **Shareware.**

DHCP (от англ. *Dynamic Host Configuration Protocol,* протокол динамической конфигурации узла). DHCP представляет собой сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP, посредством обращения к серверу DHCP. Этот протокол применяется в большинстве крупных сетей, использующих TCP/IP.

DHT (от англ. *Distributed Hash Table,* распределенная хеш-таблица). Протокол, позволяющий BitTorrent-клиентам находить друг друга без использования трекера. Клиенты с поддержкой DHT образуют общую DHT-сеть и помогают друг другу найти участников одних и тех же раздач.

DiHalt. Ежегодный фестиваль демосцены, проводимый в Нижнем Новгороде.

DIZ. Расширение небольшого файла в текстовом формате, создаваемого для того, чтобы кратко описать содержание варезного продукта. Как правило, содержит: наименование программы, количество файлов и название варезной группы, которая релизит этот софт.

DMG. Формат файлов образа диска для операционной системы OS X.

DNS (от англ. *Domain Name Service,* система доменных имен). Протокол обслуживания имен в сетях TCP/IP, по запросу предоставляющий IP-адрес и другую информацию и позволяющий программам и службам «ориентироваться» в Интернете.

DNS-сервер. Приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу. Также DNS-сервером могут называть хост, на котором запущено приложение.

Dolby Digital, также называемый **AC3**. Формат многоканального звука, конкурирующий с DTS и ставший основным для дисков DVD Video. Существует несколько вариантов Dolby Digital. Сравнение форматов звука вы можете увидеть в таблице на странице **tinyurl.com/gq85avl.**

Donationware (от англ. *Donation,* пожертвование и *Software,* программное обеспечение). Вариант лицензирования, при котором пользователю поставляется полностью функционирующее программное обеспечение с возможностью выплатить вознаграждение разработчику. Вы можете пользоваться таким программным обеспечением совершенно свободно.

DOS (от англ. *Disk Operating System,* дисковая операционная система, ДОС). Семейство операционных систем для персональных компьютеров, ориентированных на использование дисковых накопителей, таких как жесткий диск и дискета. Наиболее известна из них **MS-DOS.**

DoS-атака (от англ. *Denial of Service,* отказ в обслуживании). Разновидность хакерской атаки, направленной на прекращение нормального функционирования какого-либо сетевого ресурса, — например, веб-сайта. В большинстве случаев осуществляется чрезмерная нагрузка на сервер путем отправки большого числа запросов, что нарушает нормальную работу сервера и может полностью вывести его из строя.

Dropbox. Облачное хранилище данных, принадлежащее компании Dropbox Inc. и позволяющее пользователям хранить свои данные на серверах в облаке и делиться ими с другими пользователями в Интернете. Работа построена на синхронизации данных.

Dropmire. Секретная программа компьютерного слежения, используемая Агентством национальной безопасности США для наблюдения за иностранными посольствами и дипломатическим персоналом, в том числе стран-союзников по НАТО.

Dropper. *См.* **Дроппер.**

DTS (от англ. *Digital Theatre System,* система цифрового театра). Формат многоканального звука, конкурирующий с Dolby Digital. Качество звука на порядок выше за счет более высокого битрейта и другого алгоритма сжатия звука. Существует несколько вариантов DTS. Сравнение форматов звука вы можете увидеть в таблице на странице **tinyurl.com/gq85avl.**

E

eBay. Крупнейшая в мире торговая интернет-площадка, на которой можно покупать и продавать практически любые товары с доставкой в любые страны. Продавцом может быть как частное лицо, так и компания. Товары могут продаваться как по фиксированным ценам, так и в формате аукциона. В последнем случае размещение ставок начинается с цены, указанной продавцом, и объявление находится на сайте eBay определенное продавцом количество дней. Покупатели размещают ставки на этот товар. Побеждает покупатель, который разместил наибольшую ставку на момент окончания аукциона.

Echelon. *См.* **Эшелон**

EDGE (EGPRS) (от англ. *Enhanced Data rates for GSM Evolution,* более высокие скорости передачи данных для развития стандарта GSM). Цифровая технология беспроводной передачи данных для мобильной связи, которая функционирует как надстройка над 2G и 2.5G (GPRS**)-ceTtfMH** и обеспечивает передачу данных со скоростью до 474 Кбит/с.

Edge. См. Microsoft Edge.

Eepsite. *См.* **I2P-сайты.**

EFI (от англ. *Extensible Firmware Interface,* интерфейс расширяемой прошивки). Интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования. Его основное предназначение заключается в корректной инициализации оборудования при включении системы и передаче управления загрузчику операционной системы. EFI предназначен для замены BIOS — интерфейса, который традиционно используется всеми IBM PC-совместимыми персональными компьютерами. Позднее от названия EFI отказались, и последняя версия стандарта носит название Unified Extensible Firmware Interface (UEFI).

Ethernet. Семейство технологий пакетной передачи данных для компьютерных сетей. Существует несколько основных разновидностей Ethernet: Fast Ethernet (передача данных осуществляется со скоростью до 100 Мбит/с, в отличие от исходных 10 Мбит/с), Gigabit Ethernet (гигабитный Ethernet, передача данных осуществляется со скоростью до 1 Гбит/с), 40GbE (40-гигабитный Ethernet, скорость до 40 Гбит/с) и 100GbE (100-гигабитный Ethernet, скорость до 100 Гбит/с).

Exploit. *См.* **Эксплойт.**

F

Facebook (Фейсбук, дословно с англ. — книга лиц). Одна из крупнейших социальных сетей в мире, основанная в 2004 году.

FAQ (от англ. *Frequently Asked Questions,* ЧАсто задаваемые ВОпросы, ЧАВО). Список вопросов и ответов на них.

FAT (от англ. *File Allocation Table,* таблица размещения файлов). Классическая архитектура файловой системы, которая из-за своей простоты все еще широко используется на Flash-накопителях. Ранее использовалась и на жестких дисках. Существует три версии FAT:

FAT12, FAT16 и FAT32. Они отличаются разрядностью записей в дисковой структуре, т. е. количеством битов, отведенных для хранения номера кластера. FAT12 применялась в основном для дискет, FAT 16 — для дисков малого объема. На основе FAT была разработана файловая система exFAT (extended FAT), используемая преимущественно для Flash-накопителей. В современных версиях Windows используется файловая система NTFS.

FILEID.DIZ. Текстовый файл с кратким описанием содержимого, помещаемый в корневой каталог архивного файла (часто архива с варезной программой, музыкальным альбомом и т. п.). Существуют программы, собирающие описания из файлов FILEJD.DIZ в специальную базу с описаниями контента архивов. Аббревиатура DIZ расшифровывается как *Description In Zipfile* (описание в ZIP-архиве).

FileVault. Система шифрования файлов, встроенная в операционную систему OS X.

Firefox. *См.* **Mozilla Firefox.**

Firewall. *См.* **Сетевой экран.**

FireWire. См. IEEE 1394.

Fix (фикс). Приложение для исправления, найденного в программном обеспечении бага, распространяемое разработчиками программы. В основном, ошибки устраняются большим патчем (обновлением) софта, исправляющим сразу несколько багов. Как правило, если софт был зарелизен какой-то варезной группой, то оригинальные патчи не устанавливаются из-за несовпадения версий программного обеспечения.

FLAC (от англ. *Free Lossless Audio Codec,* свободный аудиокодек без потерь). Популярный бесплатный кодек для сжатия аудио. В отличие от кодеков с потерями (lossy), таких как OGG и MP3, FLAC не удаляет какую-либо информацию из аудиопотока и подходит для прослушивания музыкальных композиций на высококачественной аппаратуре.

Flash Video. См. FLV.

Flash. Интерактивная технология, разработанная компанией Macromedia и впоследствии перешедшая к корпорации Adobe. Инструменты Flash позволяют создавать мультипликации и интерактивное содержимое для веб-сайтов, игр, презентаций и т. п. Для просмотра Flash-содержимого в браузере необходимо специальное программное обеспечение, дистрибутив которого можно загрузить из Всемирной паутины.

Flash-накопитель, USB-накопитель, флешка. Запоминающее устройство, использующее в качестве носителя **Flash-память** и подключаемое к компьютеру или иному считывающему устройству через интерфейс USB.

Flash-память. Разновидность полупроводниковой технологии электрически перепрограммируемой памяти. Также это словосочетание закрепилось за классом твердотельных устройств хранения информации. Серьезным недостатком этой технологии является ограниченный срок эксплуатации носителей, а также их чувствительность к электростатическому разряду.

FLV (Flash Video). Формат файлов, применяемый для передачи видео через Интернет. Используется такими сервисами, как YouTube, Google Video, RuTube и др.

FoxyProxy. Дополнение для браузеров Mozilla Firefox, Google Chrome и Internet Explorer, предназначенное для управления настройками прокси-сервера.

Freenet. Одноранговая сеть, созданная с целью предоставить пользователям возможность анонимного общения и обмена файлами.

Freeware (от англ. *Free* (free of charge), бесплатный и *Software,* программное обеспечение). Программное обеспечение, лицензионное соглашение которого не требует каких-либо выплат разработчику или правообладателю.

Frenchelon (от англ. *French Echelon).* Французская глобальная система радиоэлектронной разведки, аналог системы Эшелон.

FTP (от англ. *File Transfer Protocol,* протокол передачи файлов). Протокол FTP используется в сетях, в частности в Интернете, и позволяет передавать и получать различные файлы. Передача файлов при помощи FTP напоминает копирование файла с одного диска компьютера на другой.

FTP-сервер. Сервер, обеспечивающий обмен файлами по протоколу FTP. Может допускать как анонимное (без указания логина и пароля), так и подключение с авторизацией.

FTTx (от англ. *Fiber To The X,* оптическое волокно до точки *X).* Технология организации кабельной инфраструктуры сети передачи данных, в которой от узла связи до определенной точки (X) подходит оптоволоконный кабель, а далее, до абонента — медный. В семейство FTTx входят различные виды архитектур: FTTN (Fiber to the Node) — волокно до сетевого узла, FTTC (Fiber to the Curb) — волокно до микрорайона, квартала или группы домов, FTTB (Fiber to the Building) — волокно до здания, FTTH (Fiber to the Home) — волокно до жилища (квартиры или отдельного коттеджа).

G

Gamez. Дистрибутивы игр, распространяемые нелегально (варезные игры).

GIF (от англ. *Graphics Interchange Format,* формат для обмена изображениями). Формат хранения графических изображений, в том числе и анимированных.

Gmail. Бесплатная электронная почта с веб-интерфейсом. Также является провайдером для всех служб Google.

GNOME (от англ. *GNU Network Object Model Environment,* сетевая среда объектной модели GNU). Свободная среда рабочего стола для UNIX-подобных операционных систем. GNOME является частью проекта GNU.

GnuPG, GPG (от англ. *GNU Privacy Guard,* защита объектной модели GNU). Свободная программа для шифрования информации и создания электронных цифровых подписей. Разработана в качестве альтернативы PGP. Текущие версии GnuPG могут взаимодействовать с PGP и другими OpenPGP-совместимыми системами.

Gnutella. Полностью децентрализованная файлообменная сеть, отличающаяся отсутствием центрального сервера. Сеть формируется, когда один пользователь Gnutella соединяется с другим, после чего они могут обмениваться сообщениями и файлами. В результате полной децентрализации сеть практически невозможно уничтожить, т. к. для этого потребуется вывести из строя каждый узел сети.

Gold (от англ. *Gold,* золото). Используется для обозначения, что игра (программа) имеет окончательную (финальную) версию и готова для отгрузки потребителям. Пример: «игра ушла на золото».

Google (Гугл). Крупнейшая поисковая система во Всемирной паутине, принадлежащая корпорации Google Inc.

Google+. Социальная сеть корпорации Google.

Google AdSense. Сервис контекстной рекламы, позволяющий заработать владельцам веб-сайтов.

Google AdWords. Сервис контекстной рекламы, работающий с ключевыми словами.

Google Analytics. Бесплатный сервис, предоставляющий детальную статистику по трафику веб-сайта.

Google Chrome. Браузер, разрабатываемый корпорацией Google на основе свободного браузера Chromium.

Google Drive. Облачное хранилище с возможностью просмотра в браузере множества различных типов файлов. Документы также можно редактировать и создавать, как ранее в Google Docs.

Google Groups. Архив конференций Usenet.

Google Hangouts. Служба обмена мгновенными сообщениями, а также видео- и голосовой связи.

Google Maps. Бесплатный картографический сервис с возможностью построения маршрутов.

Google Play. Интернет-магазин корпорации Google, позволяющий владельцам устройств с операционной системой Android устанавливать и приобретать различные приложения, книги, музыку и фильмы.

Google Планета Земля (англ. Google Earth). Программа и веб-сервис одноименного проекта компании Google, в рамках которого в Интернете были размещены спутниковые изображения всей земной поверхности.

GPG. См. GnuPG.

GPRS (от англ. *General Packet Radio Service,* пакетная радиосвязь общего пользования). Надстройка над технологией мобильной связи GSM, позволяющая пользователю сети сотовой связи осуществлять обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе с Интернетом. Максимальная скорость передачи данных в GPRS-сети составляет 171.2 Кбит/с. В реальности скорость ниже, т. к. зависит от нагрузки на базовую станцию, к которой подключился абонент, и от используемой схемы кодирования.

GPS (от англ. *Global Positioning System,* система глобального позиционирования). Спутниковая система навигации, реализованная и эксплуатируемая Министерством обороны США. Позволяет в любом месте Земли определять местоположение и скорость объектов. В настоящее время доступна также и для гражданских целей — нужен только навигатор или другой аппарат (например, смартфон) с GPS-модулем.

Guestbook. *См.* **Гостевая книга.**

H

H.264. Стандарт сжатия видео, позволяющий при высокой степени сжатия видеопотока сохранить высокое качество изображения. Также называется MPEG-4 Part 10 и AVC (Advanced Video Coding, расширенное кодирование видео).

HDD (от англ. *Hard (Magnetic) Disk Drive,* накопитель на жестких магнитных дисках (НЖМД)), жесткий диск, в компьютерном сленге «винчестер». Устройство хранения информации произвольного доступа, основанное на принципе магнитной записи. Является основным накопителем данных в большинстве компьютеров. Информация в HDD

записывается на алюминиевые или стеклянные пластины, покрытые слоем ферримагнитного материала, — магнитные диски. Данные считываются специальными головками.

HDTV (от англ. *High Definition Television,* телевидение высокой четкости). Стандарт вещания цифровых телевизионных сигналов с высококачественным видеоизображением и объемным звуком.

HDV (от англ. *High Definition Video,* видео высокой четкости). Стандарт видеоизображения. Используются два формата HDV: 720p (разрешение 1280x720 пикселов со скоростью 25p или 50p кадров в секунду в странах с системой PAL и 30p или 60p кадров в секунду в странах с системой NTSC), а также 1080i (1440x1080 пикселов со скоростью 50i кадров в секунду в странах с системой PAL и 60i кадров в секунду в странах с системой NTSC). Символы p и i означают, соответственно, progressive, прогрессивную развертку и interlaced, чересстрочную развертку.

HFS (от англ. *Hierarchical File System,* иерархическая файловая система). Файловая система, разработанная компанией Apple Computer для компьютеров с установленной операционной системой Mac OS. К настоящему моменту устарела и заменена HFS+.

HFS+ (HFS Plus). Усовершенствованная файловая система, разработанная для замены ранее использовавшейся HFS, основной файловой системы на компьютерах Mac. Еще с этой файловой системой может работать плеер iPod.

HSDPA (от англ. *High-Speed Downlink Packet Access,* высокоскоростная пакетная передача данных от базовой станции к мобильному телефону). Протокол передачи данных мобильной связи 3G. Позволяет сетям, основанным на UMTS, передавать данные на более высоких скоростях — вплоть до 42 Мбит/с.

HTML (от англ. *HyperText Markup Language,* язык разметки гипертекста). Язык HTML предназначен для разметки документов Всемирной паутины, которые могут быть просмотрены при помощи браузера. Большинство веб-страниц создано при помощи языка HTML. Основой языка HTML являются теги.

HTML5 (англ. *HyperText Markup Language, version* 5, язык разметки гипертекста версии 5). Пятая версия языка HTML (на замену HTML 4.01, XHTML 1.0 и XHTML 1.1), предназначенная для улучшения уровня поддержки мультимедийных технологий с одновременным сохранением обратной совместимости, удобочитаемости кода для человека и простоты анализа. Консорциум W3C начал разработку следующей версии стандарта 5.1, в которой описываются такие технологии, как вывод титров в видеороликах, заполнение электронных форм с автозавершением, а также проверка правописания.

HTML-документ. Документ, созданный при помощи языка разметки гипертекста (HTML).

HTTP (от англ. *HyperText Transfer Protocol,* протокол передачи гипертекста). Прикладной протокол передачи данных в Интернете.

HTTPS (от англ. *HyperText Transfer Protocol Secure,* безопасный протокол передачи гипертекста). Расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS.

Hulu. Веб-сайт, предлагающий доступ (как бесплатно, так и по подписке) к потоковым видеозаписям телевизионных шоу, фильмов, сериалов и прочих материалов многих телевизионных студий и телеканалов. В настоящее время разрешен доступ только пользователям из США, для остальных посещение сайта блокируется по IP-адресу.

I

I2P (от англ. *Invisible Internet Project, IIP, I^2P,* проект «Невидимый интернет»). Анонимная компьютерная сеть, работающая поверх Интернета. Внутри сети I2P можно разместить HTTP-серверы, адреса сайтов находятся в псевдодоменном пространстве **.i2p.** Поверх сети I2P можно строить одноранговые сети (P2P), например, BitTorrent, eDonkey, Kad, Gnutella и т. д.

12P-сайт (eepsite, ипсайт). Сайт (или служба) (форум, блог, файлообменник, электронная почта, чат и т. д.) с сохранением анонимности, размещенный и доступный только в сети **I2P.**

Icedove. Переименованная версия программы Mozilla Thunderbird, установленная в операционной системе Tails.

ICloud. Интернет-сервис облачного хранения данных с поддержкой push-технологий, созданный компанией Apple. Каждому пользователю бесплатно предоставляется 5 Гбайт дискового пространства для хранения электронной почты, документов и резервных копий файлов. Также сервис предоставляет возможность автоматической синхронизации музыки, книг и приложений с портативными устройствами.

ICMP (от англ. *Internet Control Message Protocol,* протокол межсетевых управляющих сообщений). Сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, — например, запрашиваемая услуга недоступна, или хост или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

ICQ (от англ. *I seekyou* (читается как «ай сик ю»), я ищу тебя). Служба, а также программа, предназначенная для обмена мгновенными сообщениями через Интернет.

Ш (от англ. *IDentifler,* идентификатор). Уникальный набор символов, присвоенный пользователю на определенном веб-сайте во Всемирной паутине для его идентификации.

ШБ. *См.* **Интегрированная среда разработки.**

IEEE 1394. Последовательная высокоскоростная шина, предназначенная для обмена цифровыми данными между компьютером и другими электронными устройствами. Различные компании продвигают стандарт под своими торговыми марками: Apple — FireWire, Sony— i.LINK, Yamaha— mLAN, TI— Lynx, Creative— SB1394. Передача данных поддерживается на расстояние до 4,5 м со скоростью 400-3200 Мбит/с.

IEEE 802.11. Набор стандартов беспроводной связи более известный по названию **Wi-Fi.** Получил широкое распространение благодаря развитию мобильных электронно-вычислительных устройств: планшетов и ноутбуков. Существует множество стандартов, распространенными из которых являются: 802.11a (скорость передачи данных 54 Мбит/с в частотном диапазоне 5 ГГц), 802.11b (5,5-11 Мбит/с), 802.11g (54 Мбит/с, 2,4 ГТц), 802.1 In (600 Мбит/с, 2,4-2,5 или 5 ГГц), 802.11ac (до 6,77 Гбит/с для устройств, имеющих 8 антенн) и 802.1 lad (до 7 Гбит/с, 60 ГГц).

IGMP (англ. *Internet Group Management Protocol,* протокол управления группами Интернета). Протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

IMAP (от англ. *Internet Message Access Protocol,* протокол доступа к сообщениям в Интернете). Протокол прикладного уровня для доступа к электронной почте.

IMEI (от англ. *International Mobile Equipment Identity,* международный идентификатор мобильного оборудования). Число (обычно 15-разрядное в десятичном представлении), уникальное для каждого использующего его аппарата. Применяется в сотовых телефонах сетей GSM, WCDMA и IDEN, а также в некоторых спутниковых телефонах. IMEI служит для идентификации устройства в сети и хранится в прошивке аппарата. Как правило, IMEI указывается в самом аппарате (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре), под аккумуляторной батареей, на упаковке и в гарантийном талоне. IMEI играет роль серийного номера аппарата при авторизации в сети и передается в эфир при авторизации в сети. Также IMEI используется для слежения за аппаратами и блокирования краденых телефонов на уровне оператора сотовой связи.

IMSI (от англ. *International Mobile Subscriber Identity,* международный идентификатор мобильного абонента). Индивидуальный номер, ассоциированный с каждым пользователем мобильной связи стандарта GSM, UMTS или CDMA. При регистрации в сети аппарат абонента передает IMSI, по которому происходит его идентификация. Во избежание перехвата этот номер посылается через сеть очень редко (только при аутентификации пользователя). В системе GSM идентификатор содержится на SIM-карте. Длина IMSI, как правило, составляет 15 цифр, первые три из них составляют мобильный код страны, за ним следует двузначный код мобильной сети, а все последующие цифры составляют непосредственно сам номер (идентификатор) пользователя с кодом оператора сотовой связи.

IMSI-ловушка (IMSI-catcher). Специальное устройство, маскирующее себя под базовую станцию сотовой телефонной сети для организации перехвата и мониторинга сотовых коммуникаций без ведома компаний-операторов и пользователей мобильной связи.

Internet Explorer. *См.* **Microsoft Internet Explorer.**

iOS. Операционная система, разработанная корпорацией Apple Inc. и предназначенная для мобильных устройств Apple.

IP (от англ. *Internet Protocol*, протокол Интернета). Протокол, предназначенный для обмена данными в Интернете и локальных сетях. Протокол IP описывает формат пакета данных, передаваемых в сети, а также порядок присвоения и поддержки адресов абонентов сети. Существует в версиях IPv4 и IPv6.

iPad (Айпад). Планшет с возможностью подключения к Интернету и сотовым сетям (зависит от модели), выпускаемый корпорацией Apple.

iPhone (Айфон). Серия смартфонов, разработанных корпорацией Apple.

iPod (Айпод). Серия портативных мультимедийных проигрывателей компании Apple, в качестве носителя данных использующих Flash-память или, в ряде моделей, жесткий диск.

IPsec (сокращение от IP Security). Набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. В основном, применяется для организации VPN-соединений.

IPv4 (от англ. *Internet Protocol version 4,* четвертая версия протокола Интернета). Протокол, предназначенный для обмена данными в Интернете и локальных сетях. Протокол IPv4 использует 32-битные адреса, ограничивающие адресное пространство 4,22 миллиардами возможных уникальных адресов, которые практически исчерпаны. Для решения проблемы был реализован протокол IPv6. Также *см.* **IP.**

IPv6 (от англ. *Internet Protocol version 6,* шестая версия протокола Интернета). Новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая вер-

сия (IPv4) при ее использовании в Интернете, за счет использования длины адреса 128 битов вместо 32.

IP-адрес. Уникальный идентификатор (адрес) устройства (обычно компьютера), подключенного к локальной сети или к Интернету. IP-адрес обычно состоит из четырех групп цифр, разделенных точкой, например, 192.168.0.1. Любому компьютеру, осуществляющему сеанс связи с Интернетом, обязательно выделяется статический или динамический IP-адрес. Динамический IP-адрес выделяется провайдером Интернета компьютеру пользователя лишь на текущий сеанс связи. При следующем подключении может быть выделен другой IP-адрес. Это связано с тем обстоятельством, что количество пользователей провайдера может превышать фиксированное количество IP-адресов, выделенных ему системой DNS. Статический IP-адрес неизменяем при каждом сеансе связи.

IP-пакет. Фрагмент данных в формате протокола IP. Помимо передаваемой информации, пакет может содержать дополнительные сведения, которые следуют непосредственно за заголовком пакета.

IP-телефония. См. VoIP.

IRC (от англ. *Internet Relay Chat,* ретранслируемый интернет-чат). Сервисная система, при помощи которой пользователи могут общаться через Интернет в режиме реального времени. Как правило, для этого используется специальное программное обеспечение, например, mIRC. Также позволяет передавать файлы.

ISO (от англ. *International Organization for Standardization,* Международная организация по стандартизации). Точная копия (называемая также «образом диска») оригинального диска CD (DVD, HD-DVD, Blu-ray), содержащего файловую систему стандарта ISO 9660 в виде одного файла с расширением iso. Все данные в этом стандарте находятся в несжатом виде, что делает файл очень большим. Может быть записан на чистый диск соответствующими программами или эмулирован в виртуальном приводе (к примеру, программой Daemon Tools Lite).

ISO 9660. Стандарт, описывающий файловую систему для дисков CD-ROM. Также известен как CDFS (*Compact Disc File System,* файловая система компакт-дисков). Целью стандарта является обеспечение совместимости носителей под разными операционными системами — такими как Linux, OS X и Windows. Расширение стандарта, называемое **Joliet,** добавляет поддержку длинных имен файлов и не-ASCII символов в именах. На DVD также можно использовать ISO 9660, но файловая система UDF является более подходящей для них, т. к. имеет поддержку объемных носителей и лучше подходит для современных операционных систем. На дисках Blu-ray (BD) используется raibKq файловая система UDF.

ISP. *См.* **Провайдер.**

J

Jabber. *См.* **XMPP.**

JAP. См. Java Anonymous Proxy.

Java. Язык программирования, предназначенный для разработки клиентских приложений и серверного программного обеспечения.

Java Anonymous Proxy (JAP), он же AN.ON и JonDonym. Система прокси, предназначенная для анонимизации только HTTP, т. е. веб-трафика. Пересылка трафика производится в зашифрованном виде через фиксированный каскад микс-серверов, при этом пользова-

тель не имеет возможности составить произвольную цепочку серверов. Компрометация анонимности клиента JAP невозможна без перехвата всего входящего и исходящего трафика всех узлов каскада и их содействия с целью расшифровывания пакетов. Также JAP умеет использовать узлы сети Tor в качестве каскада для анонимизации HTTP-трафика.

Java Runtime Environment (в пер. с англ. «среда выполнения для Java»), Виртуальная машина, необходимая для исполнения Java-приложений без компилятора и других средств разработки. Состоит из виртуальной машины — Java Virtual Machine — и библиотеки Java-классов.

JavaScript. Язык сценариев, использующийся для придания интерактивности веб-страницам.

Joliet. См. ISO 9660.

JonDonym. См. Java Anonymous Proxy.

JPEG (от англ. *Joint Photographie Experts Group,* объединенная группа экспертов в области фотографии). Один из популярных графических форматов, применяемый для хранения изображений. Алгоритм JPEG позволяет сжимать изображение как с потерями, так и без потерь. Поддерживаются изображения с линейным размером не более 65535^65535 пикселов.

K

KDE (сокращение от K Desktop Environment). Свободная среда рабочего стола и набор программ, преимущественно используемых в UNIX-системах.

Key Generator (от англ. «генератор ключей»). Небольшое приложение, способное сгенерировать на основе введенных данных (имени пользователя и наименования компании) или же без таковых допустимый ключ для установки и/или активации приложения, игры и т. п. Поскольку генераторы ключей создаются только под конкретную программу (и, как правило, определенной версии), это приложение способно сгенерировать правильный ключ исключительно для конкретной программы.

L

LAN (от англ. *Local Area Network,* локальная сеть). Локальная сеть, объединяющая несколько компьютеров, — например, для обмена данными или совместной работы.

Leeching, личинг. Использование чужих (украденных) прямых ссылок для скачивания файлов, а также распространение этих файлов (или прямых ссылок на них) без предварительного разрешения владельца.

Li-Fi (от англ. *Light Fidelity,* оптическая точность). Двунаправленная высокоскоростная беспроводная коммуникационная технология. Этот вид передачи данных использует видимый свет в качестве канала связи (в отличие от радиоволн в Wi-Fi). При тестировании, скорость в сети Li-Fi достигла 224 Гбит/с.

Linux. Общее название UNIX-подобных операционных систем, в большинстве случаев распространяемых бесплатно. Наиболее известны следующие дистрибутивы Linux: ASP Linux, Mandriva, Fedora, Ubuntu, Red Hat, openSUSE, Slackware, Debian, ALT Linux.

Log-файл (файл регистрации, протокол, журнал или лог). Файл с записями о событиях системы в хронологическом порядке.

LOL (от англ. *Laughing Out Loud* или *Lots Of Laughing,* громко смеюсь). Аббревиатура, часто используемая в чатах и на форумах для выражения комплимента к чувству юмора у собеседника. Нередко используется в спорах, как выражение неуважения к аргументам оппонента. Также существует понятие lulz (лулз), обозначающее радость от нарушения чьего-либо душевного равновесия. Лулзы — основа троллинга во Всемирной паутине, они означают развлечение за счет страданий других людей.

Lossless. *См.* **Сжатие данных без потерь.**

Lossy. *См.* **Сжатие с потерями.**

LTE (от англ. *Long-Term Evolution,* долговременное развитие) (часто обозначается как 4G LTE). Стандарт беспроводной высокоскоростной передачи данных для мобильных телефонов и других устройств, работающих с данными. В разных странах используются различные частоты и полосы для LTE.

LUKS (от англ. *the Linux Unified Key Setup).* Спецификация шифрования дисков, первоначально предназначавшаяся для операционной системы Linux.

Lulz. См. LOL.

M

Mac. См. Macintosh.

Macintosh. Линейка персональных компьютеров, спроектированных, разработанных, производимых и продаваемых корпорацией Apple Inc. и функционирующих под управлением операционной системы OS X.

MAC-адрес (от англ. *Media Access Control,* управление доступом к носителю). Уникальный идентификатор, назначаемый оборудованию для его функционирования в компьютерных сетях Ethernet, в том числе и в Интернете.

MAC-спуфинг (от англ. *spoof* мистификация). Метод изменения MAC-адреса сетевого устройства, позволяющий обойти список контроля доступа к серверам, маршрутизаторам, либо скрыть сетевое устройство.

Matroska (Матрешка). Проект, нацеленный на создание открытого, гибкого, кроссплатформенного (включая аппаратные платформы) формата мультимедийного контейнера и набора инструментов и библиотек для работы с данными в этом формате.

Malware (от англ. *Malicious software,* вредоносное программное обеспечение). Обозначение любого приложения, специально разработанного для выполнения несанкционированных, часто вредоносных действий.

MAN (от англ. *Metropolitan Area Network,* городская вычислительная сеть). Проводная или беспроводная локальная сеть, объединяющая компьютеры в пределах города.

Mesh-сеть. *См.* **Ячеистая топология.**

Microsoft Corporation. Одна из крупнейших транснациональных компаний по производству проприетарного программного обеспечения для различного рода вычислительной техники: персональных компьютеров, игровых приставок, планшетов, смартфонов и пр., разработчик семейства операционных систем Windows. Подразделения компании производят смартфоны, планшеты, игровые консоли Xbox, а также аксессуары для персональных компьютеров (клавиатуры, мыши и т. д.).

Microsoft, Edge. Браузер корпорации Microsoft, призванный заменить Internet Explorer и предустановленный в операционной системе Windows 10 наряду с Internet Explorer.

Microsoft Internet Explorer. Программа-браузер, разработанная корпорацией Microsoft. Входит в состав операционных систем семейства Windows вплоть до версии Windows 10.

MIDI (от англ. *Music Instrument Digital Interface*, цифровой интерфейс музыкальных инструментов). Стандарт представления звуков различных инструментов. В отличие от звуковых файлов, MIDI-файлы содержат не аудиоданные, а команды, которые сообщают аппаратуре, у какого инструмента, на какой октаве и какая нота должна звучать.

MIME (от англ. *Multipurpose Internet Mail Extensions,* многоцелевые расширения интернет-почты). Стандарт, описывающий передачу различных типов данных по электронной почте, а также, в общем случае, спецификация для кодирования информации и форматирования сообщений таким образом, чтобы их можно было пересылать через Интернет.

mIRC. Условно-бесплатный IRC-клиент для операционной системы Windows. *См. также* **IRC.**

Miredo. Клиент, сервер и маршрутизатор для передачи IPv6 пакетов через сети IPv4, предназначенные для операционных систем Linux, BSD и OS X.

Mirror (от англ. *Mirror Server,* зеркало). Сайт-клон, дублирующий основной сайт, например, на случай его неработоспособности. Может существовать несколько зеркал одного сайта, например, в доменных зонах разных стран: **us, ru, ua** и т. п.

MitM-атака *См.* **Атака посредника.**

MKV. См. Matroska.

Monkey's Audio. Популярный формат кодирования звука без потерь. Формат использует расширение ape для хранения аудио и api для хранения метаданных.

Mozilla Firefox. Свободный браузер, разработкой которого занимается корпорация Mozilla. Программа официально выпускается для операционных систем Windows, OS X, GNU/Linux и Android.

Mozilla Thunderbird. Бесплатная кроссплатформенная программа для работы с электронной почтой и группами новостей. В Tails носит название Icedove.

MMS (от англ. *Multimedia Messaging Service,* служба мультимедийных сообщений) — система передачи мультимедийных сообщений (изображений, аудиозаписей, видеороликов) в сетях сотовой связи. Размер каждого MMS-сообщения ограничен 999 Кбайт. При пересылке MMS-сообщения на телефон, который не поддерживает MMS, получателю придет веб-ссылка, воспользовавшись которой, он сможет просмотреть это сообщение онлайн.

MP3 Pro. См. MPEG-1 audio layer 3 Pro.

MP3. См. MPEG-1 audio layer 3.

MPEG (от англ. *Motion Picture Expert Group,* экспертная группа по вопросам движущегося изображения). Группа специалистов, разрабатывающих стандарты сжатия цифровых видео- и аудиоданных.

MPEG-1 audio layer 3 **Pro.** «Продвинутая» версия файла стандарта MP3, обеспечивающая лучшее сжатие, но менее распространенная.

MPEG-1 audio layer 3. Популярнейший потоковый формат хранения и передачи аудиосигнала в цифровой форме. Используется главным образом для передачи звука в реальном времени по сетевым каналам и для кодирования звуковых дорожек Audio CD. Также носит названия MP3 и MPEG Layer3.

MPEG-1. Стандарт кодирования видеоизображения с низким разрешением и битрейтом. Использовался для создания дисков Video CD, по качеству видеоизображения схожих с кассетами VHS.

MPEG-2. Стандарт для высококачественной передачи и хранения видеоизображения с разрешением вплоть до HD (High Definition). Используется для передачи сигнала в цифровом телевидении (в том числе спутниковом и кабельном), а также для хранения информации на дисках DVD.

MPEG-4. Стандарт кодирования видео- и аудиоданных, разработанный для передачи по каналам с низкой пропускной способностью. Применение более сложных алгоритмов компрессии позволило размещать полнометражные фильмы длительностью полтора-два часа в приемлемом качестве всего на одном компакт-диске.

MS-DOS (от англ. *MicroSoft Disk Operating System*, дисковая операционная система компании Microsoft). Дисковая операционная система для компьютеров на базе архитектуры ***x86.*** MS-DOS — самая известная среди семейства DOS-совместимых операционных систем и самая используемая среди IBM PC-совместимых компьютеров на протяжении 1980-х и до середины 1990-х годов, пока ее не вытеснили операционные системы с графическим пользовательским интерфейсом, в основном из семейства Microsoft Windows.

MTProto. Криптографический протокол, используемый для шифрования коммуникаций в мессенджере Telegram.

N

Naruslnsight. Компьютерная система шпионажа кластерного класса, предназначенная для прослушивания и анализа данных сетевого трафика в Интернете. Система представляет собой большое количество объединенных в кластер компьютеров, которые установлены в центрах обработки данных провайдеров Интернета в США и ряде других стран. В качестве вспомогательных узлов поставки данных используется система **Carnivore.** Оператором системы в США является ФБР, пользователями — все федеральные агентства США.

NAT (от англ. *Network Address Translation,* преобразование сетевых адресов). Механизм в сетях TCP/IP, предназначенный для преобразования IP-адресов транзитных пакетов. NAT позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в меньшее число или даже в один внешний публичный IP-адрес.

NetBIOS (от англ. *Network Basic Input/Output System,* сетевая базовая система ввода/вывода). Протокол для работы в локальных сетях на компьютерах типа IBM/PC, разработанный в виде программного интерфейса. Включает в себя интерфейс сеансового уровня, а в качестве транспортных протоколов использует **TCP** и **UDP.**

NFO. Расширение файла, в котором содержится информация по варезному дистрибутиву программы (игры). Файл содержит все необходимые сведения, относящиеся к релизу: количество файлов, дату релиза, систему защиты от копирования, тип взлома, инструкцию по установке, наименование группы-релизера, ASCII-изображение и т. п.

NTFS (от англ. *New Technology File System,* файловая система новой технологии). Стандартная файловая система для семейства операционных систем Windows NT компании Microsoft.

O

OEM (от англ. *Original Equipment Manufacturer,* производитель изначальной комплектации). Версия (вариант поставки) продукта (как правило, комплектующих и программного обеспечения), не предназначенная для розничной продажи. OEM-продукты приобретаются другой компанией с целью продажи вместе с каким-либо товаром. Например, на большинстве ноутбуков устанавливаются OEM-версии операционной системы Windows, ограниченные условиями лицензионного и гарантийного соглашения в отличие от коробочных (retail) версий. Несомненный плюс OEM-версий для конечного пользователя — низкая (обычно на 10-40% дешевле retail-версии) цена.

Offline. Автономный режим работы, при котором компьютер не подключен к локальной сети и/или Интернету. При автономном режиме работы есть возможность просматривать ранее сохраненные файлы веб-страниц.

OGG. Открытый стандарт мультимедийного контейнера. В контейнере OGG можно хранить видео- и аудиоданные в различных форматах, — например, FLAC, MPEG-4 или MP3.

Onion-сайт. Ресурс с псевдодоменом верхнего уровня .onion, доступный только внутри сети Tor. Адрес onion-сайта состоит из набора символов и домена .onion — например: http://zerobinqmdqd236y.onion (анонимный сервис сообщений ZeroBin).

Online. Неавтономный режим работы, при котором установлено подключение к локальной сети и/или Интернету.

Опух. Система радиоэлектронной разведки, оператором которой является Федеральная разведывательная служба Швейцарии. Аналог систем Эшелон и Frenchelon, но имеет гораздо меньшие масштабы.

Opera. Веб-браузер и пакет прикладных программ для работы во Всемирной паутине, выпускаемый компанией Opera Software.

OS X. Операционная система, разработанная корпорацией Apple Inc., устанавливаемая на компьютеры Mac.

OSI, сетевая модель (от англ. *Open Systems Interconnection basic reference model,* базовая эталонная модель взаимодействия открытых систем). Модель стека сетевых протоколов. В связи с затянувшейся разработкой протоколов OSI, в настоящее время основным используемым стеком протоколов является TCP/IP, разработанный еще до принятия модели OSI и вне связи с ней. В модели OSI используются семь уровней, как показано в табл. П5.1.

Таблица П5.1. Модель OSI

Уровень		Тип данных	Функции	Примеры
Система	7. Прикладной		Доступ к сетевым службам	HTTP, FTP, SMTP
	6. Представления		Представление и шифрование данных	ASCII, EBCDIC, JPEG
	5. Сеансовый		Управление сеансом связи	RPC, PAP
	4. Транспортный	Сегменты/ Дейтаграммы	Прямая связь между конечными пунктами и надежность	TCP, UDP, SCTP

Таблица'П5.1 *(окончание)*

Уровень		Тип данных	Функции	Примеры
Сеть	3. Сетевой	Пакеты	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk
	2. Канальный	Биты/ Кадры	Физическая адресация	PPP, IEEE 802.2, Ethernet, DSL, L2TP, ARP
	1. Физический	Биты	Работа со средой передачи, сигналами и двоичными данными	USB, витая пара, коаксиальный кабель, оптический кабель

OST (от англ. *Original SoundTrack,* оригинальный саундтрек). Альбом/сборник музыкальных композиций, представляющих саундтрек к фильму (игре).

OTR (от англ. *Off-The-Record messaging,* неофициальный обмен сообщениями). Криптографический протокол для систем мгновенного обмена сообщениями.

P

P2P. *См.* **Одноранговая сеть.**

Pandora.com. Потоковая радиостанция во Всемирной паутине, основанная на рекомендательной системе. Пользователь сайта выбирает музыкального исполнителя, после чего система ищет похожие композиции, используя около 400 музыкальных характеристик (например, синкоп, тональность, гармония и т. д.). Используя функции «нравится»/«не нравится», слушатель может настроить радиостанцию по своему вкусу. В базе данных системы свыше 1,5 млн композиций различных исполнителей. Из-за лицензионных ограничений сервис не предоставляется за пределами США, Австралии и Новой Зеландии.

PARADOX. Датско-французская варезная группа, занимавшаяся взломом программного обеспечения в 1989-2012 гг.

Passkey. *См.* **Пасскей.**

Patch, патч. Официально — исполняемый файл (имеет расширение com, exe или msi), который исправляет определенный набор багов или усовершенствует программу (игру) на определенную дату. В варезных кругах — небольшой исполняемый файл (с расширениями com, exe или **bat),** который используется для «модификации» оригинального программного обеспечения, —, например, «отвязки» от компакт-диска, отмены ограничения по времени использования или функциональности и т. п.

PayPal. Крупнейшая дебетовая электронная платежная система. Позволяет оплачивать счета и покупки, отправлять и принимать денежные переводы. В случае оплаты покупок важнейшей особенностью PayPal является предоставление гарантий безопасности как покупателю, так и продавцу.

Perfect Dark. Клиент для анонимной файлообменной сети SKad (OpenKAD), по своей структуре схожей с Freenet, но использующей DHT с большим распределением. Данные хранятся в виде зашифрованных блоков и передаются отдельно от ключей. Для шифрования используются алгоритмы RSA и AES, причем ключи кэшируются для ускорения файлообмена.

PGP (от англ. *Pretty Good Privacy,* «вполне хорошая приватность»). Компьютерная программа, а также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе шифрование данных на запоминающих устройствах, например на жестком диске.

PHP (от англ. *Hypertext PreProcessor,* препроцессор гипертекста). Простой и надежный язык сценариев, выполняемых на стороне сервера, созданный для генерирования HTML-страниц и работы с базами данных.

Pidgin (ранее назывался Gaim). Бесплатный модульный клиент мгновенного обмена сообщениями, который поддерживает наиболее популярные протоколы.

PING (от англ. *Packet InterNet Grouper,* отправитель пакетов в Интернет). Инструментальное средство, отправляющее запросы и фиксирующее полученные ответы. Позволяет, например, проверить доступность сервера в сети. Для этого в командной строке отдается команда вида ping *yandex.ru,* где вместо значения *yandex.ru* может быть вписан адрес (в том числе и IP-адрес) любого компьютера в сети.

PirateBrowser. Веб-браузер трекера The Pirate Bay, используемый для обхода интернет-цензуры. Представляет собой комплект из программы Firefox Portable и клиента Tok с надстройкой Vidalia, обеспечивающей конфигурацию прокси для ускорения загрузки.

Plug-in. Независимый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения и/или использования ее возможностей. Плагины в операционной системе Windows обычно представлены в виде файлов библиотек с расширением dll.

Plug and Play (PnP). Технология, предназначенная для быстрого определения и конфигурирования устройств в компьютере и других технических устройствах.

POP (от англ. *Post Office Protocol,* протокол почтового отделения). Протокол, используемый для загрузки электронных сообщений из почтового ящика на сервере в почтовую программу, запущенную на компьютере пользователя. Применяется в сетях, построенных на базе стека протоколов TCPЛP.

Pop-up. Открываемые (всплывающие) новые окна (вкладки) в браузере с рекламными сообщениями.

PPP (англ. *Point-to-Point Protocol,* двухточечный протокол). Двухточечный протокол канального уровня сетевой модели OSI. Обычно используется для установления прямой связи между двумя узлами сети, при этом он может обеспечить аутентификацию соединения, шифрование и сжатие данных. Используется во многих типах физических сетей: нуль-модемный кабель, телефонная линия, сотовая связь и т. д.

PPPoE (от англ. *Point-to-Point Protocol over Ethernet,* двухточечный протокол через Ethernet). Сетевой протокол канального уровня передачи кадров PPP через Ethernet. В основном используется xDSL-сервисами. Предоставляет дополнительные возможности (аутентификацию, сжатие данных, шифрование).

Pre-Alpha. Статус программного обеспечения от начала разработки до выхода версии **Alpha** и начала тестирования.

PRISM (от англ. *Program for Robotics, Intelligents Sensing and Mechatronics).* Комплекс мероприятий в США, осуществляемых с целью массового негласного сбора информации, передаваемой по сетям электросвязи, принятый АНБ в 2007 году и формально классифицированный как совершенно секретный. Системы сбора информации АНБ (в том чис-

ле PRISM) перехватывают и записывают телефонные разговоры и электронные сообщения, а также данные о местонахождении и передвижениях владельцев мобильных телефонов по всему миру.

Proxy-сервер. *См.* **Прокси-сервер.**

Psiphon. Программное обеспечение, разработанное с целью обеспечить граждан разных стран доступом к интернет-ресурсам, заблокированным сетевой цензурой. В сети Psiphon жители стран со свободным Интернетом предоставляют свои компьютеры для хостинга прокси-серверов с зашифрованным соединением, используемых гражданами стран с интернет-цензурой.

Pub. FTP-сервер со свободным доступом для всех.

Push, технология (в пер. с англ. — «проталкивание»). Один из способов распространения информации (контента) в Интернете, когда данные поступают от поставщика к пользователю на основе установленных параметров. Пользователь же в свою очередь либо отвергает, либо принимает данные. Противоположностью Push-технологии является технология Pull, где запрос инициирует клиентское программное обеспечение. Уведомления могут содержать различные поля, такие как кнопки ответа, изображение, числовое значение, звук и др.

Q

QuickTime. Технология корпорации Apple Inc., разработанная для воспроизведения цифрового видео, звука, текста, анимации и статичных изображений в различных форматах.

R

Radium. Варезная группа, специализировавшаяся на взломе аудиософта.

Ransomware (от англ. *Ransom,* выкуп и *software,* программное обеспечение). Вредоносное программное обеспечение, предназначенное для вымогательства.

Raspberry Pi. Одноплатный компьютер размером с банковскую карту, изначально разработанный как бюджетная система для обучения информатике, впоследствии получивший широкое применение. Основан на процессоре ARM.

Ratio. *См.* **Рейтинг.**

Razor 1911 (сокр. RZR). Известная норвежская варезная и демогруппа, основанная в 1985 году и функционирующая до сих пор.

RC (от англ. *Release Candidate,* релиз-кандидат). Версия программного обеспечения, собираемая разработчиками незадолго для финального релиза программы и прошедшая комплексное тестирование (с исправлением критических ошибок). Как правило, собирается несколько версий RC (с некоторыми отличиями) программы, с целью выбора кандидата в RTM-версию.

README-файл (от англ. *read me,* «прочти меня»). Текстовый файл, содержащий информацию о других файлах в том же каталоге или архиве. Такой файл обычно сопровождает дистрибутив программы при ее распространении.

RealMedia. Стандарт потокового вещания и формат аудио- и видеофайлов. Файлы RealMedia обычно имеют расширение rm, ram или rmvb.

RegFile. Файл реестра (с расширением reg), который вносит необходимые дополнения в реестр Windows. Обычно с целью нелегальной регистрации приложения (игры).

Release Group. Группа людей, которые занимаются взломом (или риппингом) программ (игр), с последующей их переупаковкой.

Release. См. RTM.

Remux. Копия HD DVD или Blu-ray-диска, когда производится перепаковка из одного контейнера в другой без перекодировки. Обязательное условие — сохранение оригинальной видеодорожки. При этом несущественные звуковые дорожки, меню и рекламные/дополнительные ролики обычно удаляются. Пример: копия содержимого Blu-ray-диска в видеофайл формата MKV.

Resume (в пер. с англ. — «восстановление»). Возобновление скачивания/закачки файлов с момента, когда подключение к Интернету было потеряно.

Retail. Продукт, приобретенный в системе розничной торговли, не подлежащий дальнейшей перепродаже, а предназначенный для непосредственного использования.

RetroShare. Анонимная сеть, топология которой подразумевает осуществление соединений и обмен данными лишь с доверенными участниками сети и исключает как внешние контакты, так и непосредственные контакты с другими участниками, не являющимися доверенными. Позволяет в зашифрованном и анонимном режиме обмениваться сообщениями и файлами.

Rip. Программа, из которой были удалены все несущественные для работы файлы, с целью уменьшить конечный размер дистрибутива софта (игры). В отношении видеофайлов, термин Rip применяется чаще и обозначает копию с определенного носителя (например, DVDRip или HDRip) с занижением качества видеоизображения (сжатием кодеками, уменьшением разрешения и скорости потока и т. п.) и звука (сжатием, удалением несущественных звуковых дорожек, преобразованием объемного звука в стереофонический или монофонический и т. п.) для уменьшения размера. Чаще всего сжатие видеофайлов производится таким образом, чтобы достичь определенного размера итогового файла. К примеру: 700 Мбайт (для записи на CD), 1,36 Гбайт (1/3 DVD), 2,18 Гбайт (1/2 DVD), 4,36 Гбайт (DVD) и т. п.

RLOGIN (от англ. *Remote LOGIN,* удаленный вход в систему). Протокол прикладного уровня модели OSI, часть стека TCP/IP. Позволяет пользователям UNIX подключаться к системам UNIX на других компьютерах и работать так же, как при прямом подключении терминала к машине. Этот протокол обеспечивает такой же сервис, как протокол TELNET.

Rootkit. *См.* **Руткит.**

Root (в пер. с англ. — «корень», читается «рут»), суперпользователь. Специальный аккаунт в UNIX-подобных системах с идентификатором 0, владелец которого имеет право на выполнение всех без исключения операций.

RSA (аббревиатура от фамилий создателей *Rivest, Shamir* и *Adlemari).* Криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и др.

RSS-каналы. RSS-каналы, также известные как XML-каналы, веб-каналы шит каналы свободного содержимого, предоставляют пользователю возможность быстрого просмотра содержимого, обновившегося на той или иной странице в Интернете. Чаще всего RSS-содержимое доступно на новостных сайтах, где информация обновляется достаточно часто. С помощью браузера, — например, Internet Explorer, вы можете подписываться на

RSS-каналы, автоматически обновлять их содержимое и просматривать их позднее. Для каждого веб-сайта, предоставляющего RSS-содержимое, подписка оформляется отдельно.

RTM, Release (от англ. *Release To Manufacturing,* релиз в производство). Версия программного обеспечения (финальная), готовая к применению.

S

Safari. См. Apple Safari

SD-карта (от англ. *Secure Digital memory card,* безопасная цифровая карта памяти). Формат карт памяти (Flash-память), разработанный для использования в основном в портативных устройствах. На сегодняшний день широко используется в цифровых фотоаппаратах и видеокамерах, мобильных телефонах, КПК, коммуникаторах и смартфонах, электронных книгах, GPS-навигаторах и в некоторых игровых приставках. Существуют четыре поколения карт памяти этого формата, различающиеся возможным объемом данных: SD 1.0 — от 8 МБайт до 2 ГБайт, SD 1.1 — до 4 ГБайт, SDHC — до 32 ГБайт и SDXC — до 2 ТБайт. Также *см.* **Карта памяти.**

Serial, серийный номер. Допустимое имя пользователя, пароль и/или цифровой код, который позволяет снять все ограничения для коммерческого программного обеспечения. Часто это легальные данные, украденные или специально купленные для распространения вареза.

Service Pack, SP. Пакет обновлений, устанавливаемый на программное обеспечение с целью исправления ошибок и/или улучшения функциональности. Как правило, имеет порядковый номер, к примеру: Windows XP Service Pack 3 или Windows 7 Service Pack 1.

SFV. Расширение файла, который генерируется специальными программами, проверяющими соответствие закачанного файла оригиналу методом подсчета сумм CRC.

Shareware. Условно-бесплатное программное обеспечение. Тип, способ или метод распространения программного обеспечения, при котором пользователю предлагается версия, ограниченная по возможностям (неполнофункциональная или демонстрационная), сроку действия (trial-версия) или периодически напоминающая о необходимости оплатить программу. В некоторых случаях незарегистрированная программа спустя некоторое время (например, 30 дней) после установки прекращает запускаться.

Signal. Бесплатная программа с открытым кодом для устройств под управлением операционных систем iOS и Android, позволяющая общаться с собеседником в зашифрованном режиме.

Silk Road (в пер. с англ. «Шелковый путь»). Торговая интернет-площадка, находившаяся в зоне **.onion** анонимной сети Tor и работавшая с 2011 по 2013 год. Сайт был наиболее известен, как площадка по торговле запрещенными психоактивными веществами, которые составляли 70% товаров.

SIM-карта (от англ. *Subscriber Identification Module,* модуль идентификации абонента). Идентификационный модуль абонента, применяемый в мобильной связи. Основная функция SIM-карты — хранение идентификационной информации об аккаунте, что позволяет абоненту легко и быстро менять сотовые аппараты, не меняя при этом свой аккаунт, а просто переставив свою SIM-карту в другой телефон. Для этого SIM-карта включает в себя микропроцессор с ПО и данные с ключами идентификации карты (IMSI и т. д.), записываемые в карту на этапе ее производства и используемые на этапе идентификации карты (и абонента) сетью GSM. Также SIM-карта может хранить дополни-

тельную информацию — например, телефонную книжку абонента, списки входящих/исходящих телефонных номеров, текст SMS-сообщений. В современных телефонах чаще всего эти данные не записываются на SIM-карту, а хранятся в памяти телефона, поскольку SIM-карта имеет достаточно жесткие ограничения на формат и объем хранимых на ней данных. В настоящее время распространены три формата SIM-карт, различающиеся по размеру: привычная mini-SIM— используется в большинстве телефонов, micro-SIM — миниатюрная альтернатива SIM-карты (она меньше, чем mini-SIM, однако контактная пластина и интерфейс обмена у них, как правило, идентичны — в большинстве случаев можно получить micro-SIM из mini-SIM путем обрезки пластикового корпуса), nano-SIM — еще меньше предыдущих форматов и используются в таких устройствах, как iPhone 5.

Skype. Бесплатное программное обеспечение для IP-телефонии, обеспечивающее бесплатную голосовую связь через Интернет между компьютерами, а также платные услуги для связи с абонентами обычной телефонной сети.

SMS, СМС (от англ. *Short Message Service,* служба коротких сообщений). Технология, позволяющая осуществлять прием и передачу коротких текстовых сообщений с помощью сотового телефона. Входит в стандарты сотовой связи.

SMTP (от англ. *Simple Mail Transfer Protocol,* простой протокол передачи почты). Протокол передачи электронной почты в сетях, основанных на протоколе TCP/IP. Предназначен для отправки электронных сообщений из почтовой программы (установленной на компьютере пользователя) на почтовый сервер.

SOCKS (от англ. *SOCKet Secure,* безопасный разъем). Сетевой протокол, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер незаметно для них и таким образом использовать сервисы за межсетевыми экранами (брандмауэрами). Более поздняя версия SOCKS5 предполагает аутентификацию, так что только авторизованные пользователи получают доступ к серверу.

SP. *См.* **Service Pack.**

Spam. *См.* **Спам.**

SpeedTest. Веб-сервис и программное обеспечение для проверки и анализа характеристик соединения с Интернетом.

Spyware (шпионское программное обеспечение). Программы, устанавливающиеся скрытным образом на компьютер пользователя с целью наблюдения за работой компьютера без согласия пользователя. Подобные программы могут собирать информацию о посещаемых сайтах во Всемирной паутине, запоминать нажатия клавиш и записывать скриншоты экрана (screen scraper), несанкционированно и удаленно управлять компьютером, устанавливать на компьютер пользователя дополнительные приложения, изменять параметры операционной системы. Вся собранная информация может быть позднее автоматически отправлена Создателю шпионского программного обеспечения.

SSD. *См.* **Твердотельный накопитель.**

SSH (от англ. *Secure SHell,* безопасная оболочка). Сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами TELNET и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли.

SSID (от англ. *Service Set IDentißer,* идентификатор беспроводной сети). Идентификатор беспроводной сети (Wi-Fi). По умолчанию в качестве идентификатора SSID использует-

ся наименование сетевого устройства. Позволяет подключаться к сети Wi-Fi путем выбора названия сети (SSID) из списка доступных сетей.

SSL (от англ. *Secure Sockets Layer,* уровень защищенных сокетов). Криптографический протокол, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP (VoIP) в таких приложениях, как электронная почта, интернет-факс и др. В настоящее время известно, что протокол не является безопасным и планируется к исключению из работы в пользу TLS.

SSTP (от англ. *Secure Socket Tunneling Protocol,* протокол безопасного туннелирования сокетов). Протокол прикладного уровня, спроектированный для создания синхронного взаимодействия при совместном обмене двух программ. Благодаря ему возможно несколько подключений приложения по одному соединению между узлами, в результате чего достигается эффективное использование сетевых ресурсов, которые доступны в этой сети.

T

T9 (от англ. *Text on 9 keys,* набор текста на 9 кнопках). Предиктивная (предугадывающая) система набора текстов для мобильных телефонов. При наборе текста система T9 пытается предугадать, какое слово вы пытаетесь набрать, используя встроенный словарь, при этом наиболее часто употребляющиеся слова подставляются первыми. Такой способ набора намного быстрее обычного, потому что позволяет избежать повторных нажатий.

Tails (от англ. *The Amnesic Incognito Live System,* амнестическая анонимная «лайв»-система). Дистрибутив Linux на основе Debian, созданный для обеспечения приватности и анонимности. Система предназначена для загрузки с диска, Flash-накопителя или SD-карты, и не оставляет следов на компьютере, на котором запускалась. Операционная система использовалась Эдвардом Сноуденом для разоблачения PRISM.

TCP (от англ. *Transmission Control Protocol,* протокол управления передачей). Протокол, предназначенный для управления передачей данных в сетях TCPЯP. Протокол TCP определяет порядок разделения данных на дискретные пакеты и контролирует передачу и целостность данных.

TCPЯP (от англ. *Transmission Control Protocol/Internet Protocol,* протокол управления передачей/протокол Интернета). Стек основных сетевых протоколов, которые позволяют разнородным компьютерам совместно использовать информацию в сети.

Telegram. Бесплатный кроссплатформенный мессенджер для смартфонов и других устройств, позволяющий обмениваться текстовыми сообщениями и мультимедийными файлами различных форматов, в том числе и в конфиденциальном режиме.

TELNET (от англ. *TErminaL NETwork,* терминальная сеть). Сетевой протокол для реализации текстового интерфейса по сети (в современной форме — при помощи транспорта TCP). Выполняет функции протокола прикладного уровня модели OSI. Название telnet имеют также некоторые утилиты, реализующие клиентскую часть протокола.

Tempora. Секретная программа компьютерного слежения, созданная в 2011 году и используемая Центром правительственной связи Великобритании (GCHQ) совместно с Агентством национальной безопасности США. Факт существования программы стал известен от бывшего сотрудника АНБ Эдварда Сноудена. По данным Сноудена, Tempora ведет

сбор данных из перехватов телефонных разговоров, сообщений электронной почты, записей в Facebook и прочего интернет-трафика в максимально возможных объемах. Перехват коммуникаций, в том числе частных, ведется, невзирая на то, идет ли речь о подозреваемых в преступлениях или невинных людях.

Teredo. Сетевой протокол, предназначенный для передачи IPv6-пакетов через сети IPv4, в частности через устройства, работающие по технологии NAT, путем их инкапсуляции в UDP-дейтаграммы.

The Pirate Bay (в пер. с англ. «Пиратская бухта»). Крупнейший в мире BitTorrent-индексатор и каталог для поиска torrent-файлов.

The Scene. *См.* **Сцена.**

THG (от англ. *The Humble Guys,* «робкие ребята»). Легендарная американская варезная группа. Примечательна тем, что первой в свои релизы включила NFO-файл.

Thnx!, THX (от англ. *thanks, thankyou,* спасибо). Выражение благодарности, как правило, на форуме или в чате.

Thunderbird. *См.* **Mozilla Thunderbird.**

Thunderbolt. Аппаратный интерфейс, разработанный компанией Intel, для подключения периферийных устройств к компьютеру с максимальной скоростью передачи данных до 10 Гбит/с по медному проводу и до 20 Гбит/с при использовании оптического кабеля. Допускается подключение к одному порту до шести периферийных устройств путем их объединения в цепочку.

TLS (от англ. *Transport Layer Security,* безопасность транспортного уровня). Криптографический протокол, пришедший на смену SSL и обеспечивающий защищенную передачу данных между узлами в Интернете. Протокол TLS использует асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Этот протокол широко используется в приложениях, работающих с Интернетом, таких как веб-браузеры, клиенты электронной почты, обмена мгновенными сообщениями и IP-телефонии (VoIP).

TMSI (от англ. *Temporary Mobile Subscriber Identity,* временный идентификатор мобильного абонента). Идентификатор TMSI назначается после успешной аутентификации и используется в процессе установки вызова, регистрации в сети и т. д. TMSI используется из соображений безопасности для сокрытия других идентификаторов абонента, а именно во избежание передачи IMSI через радиоэфир.

Tor (от англ. *The Onion Router,* луковая маршрутизация). Система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания.

Tor Browser. Бесплатный браузер, обеспечивающий анонимность в сети за счет использования распределенной сети серверов Tor.

Tox. Протокол и программное обеспечение для защищенной текстовой, голосовой и видеосвязи в Интернете.

Trainer, трейнер. Небольшая исполняемая программу, позволяющая назначить «горячие» клавиши для чит-команд (cheat) в игре или же автоматически активирующая определенные читы.

Trialware. См. Shareware.

и

UDF (от англ. *Universal Disk Format,* универсальный дисковый формат). Спецификация формата файловой системы, не зависящей от операционной системы, для хранения файлов на оптических носителях. Универсальность и поддержка в разных операционных системах позволяет использовать UDF как файловую систему не только для оптических дисков, но и для других сменных носителей, таких как Flash-накопители и внешние жесткие диски.

UDP (от англ. *User Datagram Protocol,* протокол пользовательских дейтаграмм). Один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые дейтаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.

UEFI. См. EFI.

UHDTV. *См.* **4К UHDTV и 8К UHDTV.**

UMTS (от англ. *Universal Mobile Telecommunications System,* универсальная мобильная телекоммуникационная система). Технология сотовой связи, разработанная для внедрения передачи данных 3G в Европе. С целью отличия от конкурирующих решений, UMTS также часто называют 3GSM.

UNIX. Группа многозадачных и многопользовательских операционных систем. Также *см.* **Linux.**

Upload, аплоад. Копирование файлов с вашего компьютера на сервер в Интернете (например, на файлообменный хостинг).

UPnP (Universal Plug and Play). Набор сетевых протоколов, созданных с целью универсальной автоматической настройки сетевых устройств, как дома, так и в корпоративной среде.

URL (от англ. *Uniform Resource Locator,* единообразный определитель местонахождения ресурса). Способ записи адреса ресурса в Интернете. Например, HTTP — протокол передачи гипертекста, HTTPS — протокол передачи гипертекста с шифрованием, FTP — протокол передачи файлов, MAILTO — адрес электронной почты и др.

USB (от англ. *Universal Serial Bus,* универсальная последовательная шина). Последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств в вычислительной технике. Существует несколько модификаций USB, в основном отличающихся максимальной поддерживаемой скоростью: USB 1.0/1.1 (до 12 Мбит/с), USB 2.0 (до 480 Мбит/с), USB 3.0 (до 5Тбит/с) и USB 3.1 (до 10 Гбит/с).

Usenet (от англ. *User network, пользовательская сеть),* юзнет. Компьютерная сеть, используемая для общения и публикации файлов и состоящая из новостных групп, в которые пользователи могут посылать сообщения. Usenet оказал большое влияние на развитие современной веб-культуры, дав начало таким широко известным понятиям, как «ник», «смайл», «модератор», «троллинг», «флуд», «флейм», «бан», «FAQ (ЧаВо)» и «спам».

V

Viber. VoIP-приложение для смартфонов, работающих на платформах Android, BlackBerry OS, iOS, Symbian, Windows Phone, Bada и компьютеров под управлением Windows, OS X и Linux. Позволяет совершать бесплатные звонки через Wi-Fi и сотовые сети передачи

данных между смартфонами с установленным Viber, а также передавать текстовые сообщения, изображения, видео- и аудиосообщения.

Vidalia. Графический интерфейс для системы Tor. Позволяет просматривать карту сети и изменять цепочку узлов.

VirtualBox. Программный продукт компании Oracle для виртуализации операционных систем Microsoft Windows, Linux, FreeBSD, OS X, Solaris/OpenSolaris, ReactOS, DOS и других.

VMware Workstation Player. Бесплатный для некоммерческого использования программный продукт на основе виртуальной машины VMware Workstation, но с ограниченной функциональностью, предназначенный для создания и запуска образов виртуальных машин.

VOB (от англ. *Video OBject,* видеообъект). Формат файлов, используемый для хранения мультимедийных файлов на DVD. Представляет собой контейнер, основанный на стандарте MPEG-2 и способный содержать в себе несколько потоков видео- и аудиоданных, субтитры, а также меню диска. Может содержать не более 9 различных аудиопотоков и 32 потока субтитров.

VoIP (от англ. *Voice-over-Internet Protocol,* голос посредством протокола Интернета). Система связи, также называемая IP-, или интернет-телефонией, которая обеспечивает передачу речи в цифровом виде по протоколу IP. Наиболее распространенным приложением для ведения переговоров посредством IP-телефонии является Skype.

VPN (от англ. *Virtual Private Network,* виртуальная частная сеть). Сеть, создаваемая поверх другой сети, например, Интернета. Способ предполагает объединение, например, нескольких офисов организации в единую защищенную сеть для обмена данными.

Vuvuzela. Проектируемая анонимная сеть, призванная обеспечить большую защиту и анонимность, чем Tor.

W

Wallpaper. Фоновое изображение, размещаемое на рабочем столе в операционной системе Windows.

WAN (от англ. *Wide Area Network,* глобальная вычислительная сеть). Сеть, охватывающая большие территории, — например, Интернет.

Warez, варез (от англ. ***Software,*** программное обеспечение). Полные рабочие версии (взломанные) коммерческих программ (игр), которые свободно распространяются среди пользователей.

WAV (от англ. *waveform,* «в форме волны»). Формат файла-контейнера для хранения несжатых цифровых аудиоданных.

WebMoney («Вебмани»). Электронная платежная система, основанная в 1998 году.

Web-камера. *См.* **Веб-камера.**

Web-сайт. Совокупность веб-страниц, объединенных общей темой, дизайном, а также связанных между собой ссылками и обычно находящихся на одном и том же веб-сервере, позволяющая пользователям Интернета интерактивно взаимодействовать с ними при помощи протокола HTTP. Помимо текстовой информации на веб-сайтах можно размещать графические изображения, аудио- и видеофайлы, а также использовать различные языки программирования для создания эффектов и расширения функциональных возможностей веб-сайта.

Web-сервер. Компьютер, подключенный к Интернету, который принимает по протоколу HTTP запросы, в большинстве случаев от программ-браузеров, и выдает ответы, обычно вместе с веб-страницей, изображением, файлом или другими данными. Веб-серверы — основа Глобальной паутины.

WEP (от англ. *Wired Equivalent Privacy,* защита, эквивалентная проводной сети). Алгоритм для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей в беспроводных сетях Wi-Fi. В настоящее время эта технология является устаревшей, т. к. ее взлом может быть осуществлен всего за несколько минут. Для безопасности в сетях Wi-Fi рекомендуется использовать WPA.

What.cd («вата»). Крупнейший музыкальный закрытый торрент-трекер. Попасть на трекер можно, только получив инвайт у друга или пройдя тестирование.

WhatsApp. Бесплатный мессенджер для смартфонов (также существует веб-версия). Позволяет пересылать текстовые сообщения, изображения, видео- и аудиозаписи через Интернет. Под держиваются платформы Android, BlackBerry OS, iOS и Windows Phone.

Wi-Fi (от англ. *Wireless Fidelity,* беспроводная точность). Стандарт беспроводной сети для передачи данных. Также *см.* **IEEE 802.11**

WiMAX (от англ. *Worldwide Interoperability for Microwave Access,* всемирная совместимость для микроволнового доступа). Технология универсальной беспроводной связи на больших расстояниях (в настоящее время до 10 км) для передачи данных (до 1 Гбит/с). Основана на стандарте IEEE 802.16.

Windows Media Audio. Формат звуковых файлов, разработанный корпорацией Microsoft для хранения и трансляции аудиоданных. Формат WMA характеризуется хорошей степенью сжатия при сохранении отличного качества в сравнении с форматом MP3. Основным недостатком формата WMA является низкая стойкость к ошибкам. Если при кодировании/передаче часть файла WMA повреждается, то воспроизведение файла становится практически невозможным.

Windows Media Video. Система кодирования видеоизображения, разработанная корпорацией Microsoft для хранения и трансляции видеоданных в собственных форматах с расширением WMV.

Windows. Семейство операционных систем корпорации Microsoft.

Windows Mobile. См. Windows Phone.

Windows Phone. Мобильная операционная система, разработанная Microsoft и выпущенная в октябре 2010 года. Операционная система является преемником устаревшей Windows Mobile, хотя и несовместима с ней. Новая операционная система Windows 10 для мобильных устройств получила название Windows 10 Mobile, вместо Windows Phone 10.

WLAN (от англ. *Wireless Local Area Network,* беспроводная локальная сеть). Разновидность локальной сети, для связи и передачи данных между узлами которой используются радиоволны, а не кабельные соединения. Примерами таких сетей являются Wi-Fi и WiMAX.

WPA (от англ. *Wi-Fi Protected Access,* защищенный доступ к Wi-Fi). Представляет собой обновленную программу сертификации устройств беспроводной связи. Технология WPA пришла на замену технологии WEP. Плюсами WPA являются усиленная безопасность данных и ужесточенный контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств как на аппаратном уровне, так и на программном.

WPS (от англ. *Wi-Fi Protected Setup,* защищенная настройка Wi-Fi). Стандарт (и одноименный протокол) для полуавтоматического создания беспроводной сети Wi-Fi. WPS автоматически обозначает имя (SSID) сети и задает шифрование для защиты беспроводной сети Wi-Fi от несанкционированного доступа в нее, при этом нет необходимости вручную задавать все параметры.

WWW. Расшифровывается как *World Wide Web.* Другие названия: Всемирная паутина, Глобальная паутина. Система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к Интернету. Глобальную паутину образуют миллионы веб-серверов.

X

X-Keyscore. Программа компьютерного слежения, используемая совместно Агентством национальной безопасности США, Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии. Предназначена для слежения за иностранными гражданами во всем мире с помощью серверов, расположенных в США и на территории стран-союзников США, а также в посольствах и консульствах США в нескольких десятках стран.

XML (от англ. *extensible Markup Language,* расширяемый язык разметки гипертекста). Текстовый формат, предназначенный для хранения структурированных данных, для обмена информацией между программами и для создания специализированных языков разметки.

XMPP (от англ. *extensible Messaging and Presence Protocol,* расширяемый протокол обмена сообщениями и информацией о присутствии). Открытый, основанный на XML, свободный для использования протокол для мгновенного обмена сообщениями и информацией о присутствии в режиме, близком к реальному времени. Ранее назывался Jabber. Изначально спроектированный легко расширяемым, протокол, помимо передачи текстовых сообщений, поддерживает передачу голоса, видео и файлов по сети. В отличие от коммерческих систем мгновенного обмена сообщениями, таких как AIM, ICQ, WLM и Yahoo, XMPP является децентрализованной, расширяемой и открытой системой. На основе протокола XMPP уже открыто множество частных и корпоративных серверов XMPP. Среди них есть достаточно крупные проекты — такие как Facebook, Google Talk, WhatsApp, Одноклассники.ги, QIP, LiveJournal, Juick и др.

Xvid. Библиотека сжатия видео стандарта MPEG-4 Part 2, являющаяся основным конкурентом кодека DivX Pro (Xvid — это DivX наоборот). В противоположность кодеку DivX, Xvid бесплатный и допустим к использованию на всех платформах и операционных системах, для которых можно скомпилировать исходный код кодека.

А

Аватар. Небольшое изображение, логотип, олицетворяющий пользователя. Иногда называется «юзерпик».

Авторинг. Процесс сборки исходного материала: изображений, видео- и аудиодорожек (и т. п.) — в структуру оптического диска (как правило, DVD или Blu-ray).

Администратор. Специалист, отвечающий за функционирование локальных и иных сетей, как правило, в пределах какого-либо учреждения.

Аккаунт. *См.* **Account.**

Альфа. См. Alpha.

Анализатор трафика, или **сниффер** (от англ. *sniffer).* Программа или программно-аппаратное устройство, способное осуществлять перехват и последующий анализ либо только анализ сетевого трафика, предназначенного для других узлов.

АНБ, Агентство национальной безопасности Соединенных Штатов (National Security Agency, NSA). Подразделение радиотехнической и электронной разведки Министерства обороны США, сформированное в ноябре 1952 года. АНБ США отвечает за сбор и анализ информации средствами радиоэлектронной разведки, контроль электронных коммуникационных сетей, учет электронного трафика, решает высокоспециализированные задачи радиотехнической разведки и радиоразведки по получению информации из коммуникационных сетей зарубежных государств путем электронного и радиоперехвата и ее дешифровки с применением компьютерной техники. АНБ также несет ответственность за закрытие электронных коммуникационных сетей госучреждений США от несанкционированного доступа служб радиоэлектронной других государств.

Анлим (от англ. *Unlimited,* неограниченный). Доступ в Интернет с неограниченным трафиком и временем.

Анонимайзер. Средство для скрытия информации о компьютере или пользователе в сети от удаленного сервера. Необходимо отметить, что использование анонимайзера не только не обеспечивает конфиденциальности передаваемых данных между пользователем и целевым веб-сервером, но и является дополнительным звеном возможности утечки персональной информации. Не рекомендуется при работе через анонимайзер использовать сколько-нибудь значимые учетные записи, т. к. они могут быть легко скомпрометированы на сервере-анонимайзере.

Антивирус. Программа, предназначенная для обнаружения и удаления компьютерных вирусов.

Апгрейд (от англ. *Up,* повышение и *grade,* качество). Увеличение производительности компьютера путем замены модулей или добавления дополнительных элементов.

Апдейт (от англ. *Update,* обновление). Обновление программного обеспечения или вебсайта.

Аплоад. См. Upload.

Апплет. См. Applet.

Архиватор. Программа, предназначенная для сжатия файлов для с целью освобождения места на дисках. Заархивированный файл, как правило, уменьшается в размере за счет использования различных математических алгоритмов сжатия без потери данных. Для распаковки архивов необходима установка программы, поддерживающей формат архива, за исключением случаев, когда создается самораспаковывающийся архив.

Аська. См. ICQ.

Атака методом холодной перезагрузки (от англ. *Cold boot attack).* В криптографии — класс атак по сторонним каналам, при которых злоумышленник, имеющий физический доступ к компьютеру, может извлечь из него ключи шифрования или ценные данные. Атака требует полной перезагрузки компьютера либо выключения и изъятия из него модулей памяти. В атаке используется эффект сохранения данных в ОЗУ типа DRAM и SRAM после выключения питания (данные частично сохраняются в памяти в течение периода от нескольких секунд до минут).

Атака посредника (от англ. *Man in the middle,* MITM). Вид атаки в криптографии, когда злоумышленник перехватывает и подменяет сообщения, которыми обмениваются собеседники, причем ни один из них не догадывается о его присутствии в канале.

Б

Баг. *См.* **Уязвимость.**

База данных. Совокупность структурированных данных в какой-либо предметной области. Например, база данных городских телефонов.

Базовая станция в радиосвязи. Системный комплекс приемопередающей аппаратуры, осуществляющей централизованное обслуживание группы конечных абонентских устройств.

Байт (от англ. *byte).* Единица измерения количества информации, равная 8 битам.

Бан, банить. Один из принятых во Всемирной паутине способов контроля над действиями пользователей. Как правило, бан заключается в лишении или ограничении каких-либо прав пользователя (на создание/отправление новых сообщений или создание новых тем на веб-форуме, на отправление сообщений в чате, на комментирование в блогах и др.). Возможность введена в целях оградить интернет-сайт от троллей, спамеров и прочих лиц, чьи сообщения вредят продуктивной работе ресурса.

Баниер (от англ. *banner,* флаг, транспарант). Изображение (в том числе и анимационное) рекламного характера, при щелчке мышью на котором происходит открытие веб-страницы, содержащей рекламируемый продукт или услугу.

Бернерс-Ли, Тим. Британский ученый, изобретатель URI, URL, HTTP, HTML, создатель Всемирной паутины и действующий глава Консорциума Всемирной паутины. Автор концепции семантической паутины. Автор множества других разработок в области информационных технологий.

Бета. См. Beta.

Билд. См. Build.

Биометрическая защита. Система распознавания людей по одной или нескольким чертам, состоящая, как правило, из аппаратного и программного обеспечения. В отношении компьютеров, Flash-накопителей, внешних жестких дисков и прочих устройств в качестве черты распознавания используется отпечаток пальца.

Бит (от англ. *binary digit,* двоичное число). Минимальная единица измерения информации, простое двоичное число, принимающее значения 1 или 0 и служащее для записи и хранения данных в компьютерной технике. Определенное количество битов составляет размер других единиц: байта, килобайта, мегабайта и т. д.

Бит в секунду, бит/с (от англ. *bits per second, bps).* Базовая единица измерения скорости передачи информации, используемая на физическом уровне сетевой модели OSI или

TCP/IP. На более высоких уровнях сетевых моделей, как правило, используется более крупная единица — байт в секунду (Б/с, или Bps, от англ. *bytes per second),* равная 8 бит/с.

Для обозначения больших скоростей передачи применяют более крупные единицы, образованные с помощью приставок кило-, мега-, гига- и т. п. системы СИ: килобиты в секунду — кбит/с (Kbps, Kbit/s или kb/s), мегабиты в секунду — Мбит/с (Mbps, Mbit/s или Mb/s), гигабиты в секунду — Гбит/с (Gbps, Gbit/s или Gb/s) и т. д. Часто путают мегабайты и мегабиты в секунду: Mb/s и MB/s (1 MB/s = 8 Mb/s), поэтому рекомендуется использовать сокращение Mbit/s. А так как объем данных принято измерять в байтах, начинающие часто путают килобиты с килобайтами, ожидая скорости 256 КБ/с от канала 256 кбит/с.

Нужно помнить, что 1 байт содержит 8 битов. Для того чтобы узнать скорость передачи данных в единицах, обычно используемых для определения объема хранимой информации (байт, килобайт, мегабайт и т. д.), нужно разделить скорость канала на 8 и получить скорость в (кило-, мега- или гига-) байтах — в зависимости от исходной единицы измерения. Например, если скорость равна 16 Мбит/с, то 16/8 = 2 МБ/с.

Также часто путают бит/с и бод. *См.* **Бод.**

Биткоин (от англ. *Bitcoin: bit,* «бит» и *coin,* «монета»). Пиринговая платежная система, использующая одноименную расчетную единицу — биткоин.

Битрейт (от англ. *bitrate,* скорость передачи данных). Количество битов, используемых для хранения одной секунды мультимедийного контента. Битрейт выражается битами в секунду (бит/с, bps), а также производными величинами. В форматах потокового видео и аудиосигналов (например, MPEG и MP3) битрейт определяет степень сжатия потока. Существуют три режима сжатия потоковых данных: постоянный битрейт (Constant bitrate, CBR), переменный битрейт (Variable bitrate, VBR) и усредненный битрейт (Average bitrate, ABR). Все они используются для достижения оптимального коэффициента сжатие/качество.

Бод (от англ. *baud).* Единица измерения скорости передачи данных с учетом служебных битов (стартовые/стоповые/четность, избыточность). Зачастую ошибочно считают, что бод — это количество битов, переданное в секунду. В действительности же это верно лишь для двоичного кодирования, которое используется не всегда. Например, в современных модемах одним изменением уровня сигнала может кодироваться несколько (до 16) битов информации. Например, при символьной скорости 2400 бод скорость передачи может составлять 9600 бит/с благодаря тому, что в каждом временном интервале передается 4 бита. Кроме этого, бодами выражают полную емкость канала, включая служебные символы (биты), если они есть. Эффективная же скорость канала выражается другими единицами — например, битами в секунду. *См.* **Бит в секунду**

Бот, сокращение от робот (англ. *bot).* Специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь (имитируя его).

Ботнет (англ. *botnet,* сокращение от слов *robot* и *network).* Компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера: рассылки спама, перебора паролей на удаленной системе, DoS-атак.

Брандмауэр. *См.* **Сетевой экран.**

Браузер или веб-обозреватель (от англ. *Web browser).* Прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач. В глобальной сети браузеры используют для запроса, обработки и отображения содержания веб-сайтов, а также манипулирования им. Многие современные браузеры могут использоваться и для обмена файлами с FTP-серверами, и для непосредственного просмотра файлов многих графических форматов (GIF, JPEG, PNG, SVG), аудио- и видеоформатов (MP3, MPEG), текстовых форматов (PDF, DJVU) и других файлов.

Буфер обмена. Буфер обмена представляет собой временную область хранения данных. В эту область могут быть помещены файлы, папки, фрагменты текста, рисунки и другие данные для дальнейшей вставки в другое место. В один момент времени буфер обмена может содержать только один набор данных, при копировании в него новой информации старая стирается.

Бэкдор (от англ. *back door,* задняя дверь или «черный ход»). Дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить тайный доступ к данным или удаленное управление компьютером. Основное назначение бэкдора — скрытное и быстрое получение доступа к данным, чаще всего зашифрованным. Например, бэкдор может быть встроен в алгоритм шифрования для последующей прослушки защищенного канала злоумышленником.

В

Вардрайвинг (от англ. *Wardriving,* «боевое вождение»). Процесс поиска и взлома уязвимых точек доступа беспроводных сетей Wi-Fi злоумышленником, оснащенным переносным компьютером с адаптером Wi-Fi.

Варез. См. Warez

Варезная группа (также называемая *ремизной группой).* Сообщество людей-энтузиастов, объединенных идеей свободы информации. Выпускает нелегальные электронные копии дисков с видеофильмами, музыкой, программами и играми для компьютеров и игровых приставок, руководствуясь правилами релизов и соревнуясь со своими коллегами-конкурентами в скорости и качестве выпуска таких копий (релизов). Сообщество релизных групп, объединенных одной темой (музыка определенного жанра, кинофильмы или варез), называется *Сценой (см.* **Сцена).** Деятельность варезных групп является высокопрофессиональной, некоммерческой и, как правило, незаконной. С ними ведут борьбу правоохранительные органы, а также неправительственные организации, спонсируемые компаниями грамзаписи и киноиндустрии. Внутри варезной группы существует жесткая иерархия, а общение ее участников между собой происходит только через закрытые каналы связи. Варезные группы существуют также на демосцене.

Веб-камера (Web-камера). Цифровая камера, способная в реальном времени производить видеосъемку, оцифровку, сжатие и передачу по компьютерной сети видеоизображения. Веб-камеры могут загружать изображения на веб-сервер по запросу, непрерывно либо через определенные промежутки времени. Каждая сетевая веб-камера имеет собственный IP-адрес и встроенное программное обеспечение, что позволяет ей функционировать как веб-сервер, FTP-сервер, FTP-клиент и почтовый клиент.

Веб-мастер (веб-разработчик). Человек, занимающийся разработкой веб-сайтов или веб-приложений для Всемирной паутины.

Веб-портал. *См.* **Портал.**

Векторное изображение. Файл, представляющий собой изображение из геометрических примитивов, таких как точки, линии, сплайны и многоугольники. При масштабировании качество изображения не изменяется.

Взлом. Действия, направленные на устранение защиты программного обеспечения, встроенной разработчиками для ограничения его функциональных возможностей. При этом, взломщик — это человек, взламывающий программное обеспечение при помощи уже готового крэка или без такового.

Виджет. *См.* **Гаджет**

Винлокер (Trojan.Winlock). Семейство вредоносных программ, блокирующих или затрудняющих работу с операционной системой и требующих перечисления денег злоумышленникам за восстановление работоспособности компьютера. Относятся к программам-вымогателям (см. **Ransomware).**

Виртуальная машина (ВМ). Программная и/или аппаратная система (*хостовая*), эмулирующая аппаратное обеспечение другой или той же платформы (*гостевой*) в изолированной среде *(см.* **Песочница).** Помимо процессора, виртуальная машина может эмулировать работу как отдельных компонентов аппаратного обеспечения, так и целого реального компьютера (включая BIOS, оперативную память, жесткий диск и другие периферийные устройства). В этом случае в виртуальную машину, как и на реальный компьютер, можно устанавливать операционные системы (например, Windows можно запускать в виртуальной машине под Linux или наоборот). На одном компьютере может функционировать несколько виртуальных машин (такая структура организуется для имитации нескольких серверов на одном реальном сервере с целью оптимизации использования ресурсов сервера).

Также этим словосочетанием обозначается спецификация некоторой вычислительной среды (например: «виртуальная машина Java»).

Виртуальный сервер. Виртуальная машина, эмулирующая отдельный физический сервер. На одном компьютере может быть запущено множество виртуальных серверов. Каждый виртуальный сервер имеет свои процессы, ресурсы, конфигурацию и отдельное администрирование. Аренда виртуального сервера — популярный вид хостинга, т. к. предоставляет разумный баланс между ценой и возможностями для большинства владельцев интернет-сайтов и приложений.

Вирус. Самовоспроизводящаяся программа, способная внедрять свои копии в файлы, системные области, вычислительные сети и т. д. и своими действиями приводить к нарушению нормального функционирования компьютера. Существует множество разновидностей вирусов. *Файловые* вирусы внедряются в файлы, обычно в текстовые документы и электронные таблицы. *Загрузочные* вирусы внедряются в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. *Сетевые* вирусы распространяются по компьютерной сети. Существуют также *файлово-загрузочные* вирусы, которые заражают и файлы, и загрузочные секторы. По способу активации вирусы подразделяют на резидентные и нерезидентные. *Резидентный* вирус при заражении оставляет в оперативной памяти резидентную часть своего кода, которая затем перехватывает обращения операционной системы к файлам и внедряется в них. *Нерезидентные* вирусы являются активными ограниченное время и активизируются в определенные моменты — например, при открытии зараженных файлов. Деятельность одних вирусов может быть вполне безобидна и проявляться в уменьшении пространства на диске в результате своего распространения или порождать графические, звуковые и другие эффекты. Опасные вирусы,

помимо нарушения нормальной работы компьютера, могут привести к уничтожению программ и данных, стиранию информации в системных областях памяти и даже вывести из строя жесткий диск.

Вирус загрузочного сеiсrора. *См.* **Загрузочный вирус.**

Всемирная паутина (от англ. *World Wide Web).* Распределенная система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к Интернету. Для обозначения Всемирной паутины также используют слово веб (от англ. *web* — «паутина») и аббревиатуру WWW.

Выделенный сервер (англ. *Dedicated Server).* Вид хостинга, при котором клиенту целиком предоставляется отдельный компьютер (в противоположность виртуальному хостингу). Обычно используется для запуска приложений, которые не могут сосуществовать на одном сервере с другими проектами или имеют повышенные требования к ресурсам.

Г

Гаджет (англ. *gadget,* устройство). Небольшое устройство, предназначенное для облегчения и усовершенствования жизни человека: смартфоны, планшеты, музыкальные плееры, игровые приставки, очки для дополненной и виртуальной реальности, фитнес-трекеры и многое другое. В программном обеспечении гаджет (виджет) — небольшое приложение, предоставляющее дополнительную информацию, — например, прогноз погоды или курс валют.

Гигабайт (Гбайт, Гб). Единица измерения количества информации, равная 1024 Мбайт, или 2^{30} байт.

ГЛОНАСС (сокр. от *ГЛОбальная НАвигационная Спутниковая Система).* Советская/российская спутниковая система навигации, состоящая из 24 спутников и предназначенная для оперативного навигационно-временного обеспечения неограниченного числа пользователей наземного, морского, воздушного и космического базирования. Доступ к гражданским сигналам ГЛОНАСС в любой точке земного шара предоставляется российским и иностранным потребителям на безвозмездной основе и без ограничений.

Глубинная паутина (также известна как *глубокая паутина* и *невидимая сеть).* Множество веб-страниц Всемирной паутины (включая ресурсы Даркнета), не индексируемых поисковыми системами. В глубинной паутине находятся веб-страницы, не связанные с другими страницами гиперссылками, — например, страницы, динамически создаваемые по запросам к базам данных, а также сайты, доступ к которым открыт только для зарегистрированных пользователей (например, ресурс **What.cd** или персональная часть контента на Facebook) или с помощью специального программного обеспечения (например, сайты в домене **.onion).** Глубинная паутина превышает по своей информационной емкости доступную Всемирную паутину как минимум в 500 раз.

Глюк (от слова «галлюцинация»). Сбой в программе, вызванный ошибкой в коде или сторонними программами. Проявляется случайно и редко, в отличие от бага, который появляется неоднократно. Соответственно, выражения: программа «заглючила» или «глючит».

Гостевая книга (от англ. *guestbook).* Скрипт (сценарий) на веб-сайте, позволяющий посетителям оставлять пожелания, комментарии и т. п.

Графический объект. Рисунок, картинка или другое изображение, такое как схема или диаграмма, предназначенные для визуального представления информации.

Д

Даркнет (от англ. *Dark Network,* «темная сеть»). Часть Интернета, в которой люди могут оставаться анонимными. В отличие от привычной Всемирной паутины, или так называемого *чистого Интернета,* сайты в котором индексируются поисковыми системами типа Яндекс или Google, ресурсы в Даркнете не индексируются, а для доступа к ним необходимо специальное программное обеспечение, зачастую оснащенное механизмами обеспечения анонимности, такими как Tor, но есть и другие способы попасть в эту сеть, — например, через форумы, защищенные паролями и требующие авторизации по приглашениям.

Дата-центр (от англ. *data center).* Специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам Интернета.

Движок. Определенная часть программного кода для реализации конкретной задачи. Как правило, один и тот же движок может быть использован при разработке нескольких программ, игр, веб-сайтов или других продуктов, что сокращает время разработки.

Девайс (от англ. *device,* устройство). По сути, любое техническое устройство.

Дейтаграмма (англ. *datagram,* датаграмма). Блок информации, передаваемый протоколом без предварительного установления соединения и создания виртуального канала. Любой протокол, не устанавливающий предварительное соединение (а также обычно не контролирующий порядок приемопередачи и дублирование пакетов), называется *дейтаграммным протоколом.* Таковы, например, протоколы Ethernet, IP, UDP и др. Название «датаграмма» было выбрано по аналогии со словом «телеграмма».

Демо, демка (от англ. *demonstration,* демонстрация). Жанр компьютерного искусства, представляющий собой мультимедийную презентацию. Демки создаются в целях демонстрации возможностей и знаний в области программирования, компьютерной графики, 3D-моделирования и написания музыки. Основным отличием демки от компьютерной анимации является то, что демо рендерится в режиме реального времени, а не заранее. Чаще всего демки являются результатом рендеринга 3D-анимации в реальном времени в сочетании с двумерными эффектами.

Демомейкер (от англ. *demo* и *maker).* Создатель демо.

Демонстрационная версия. *См.* **Demoware.**

Демосцена. Субкультура и направление компьютерного искусства, главной особенностью которого является выстраивание сюжетного видеоряда по принципу работы компьютерных игр, создаваемого компьютером в реальном времени. Иногда такие демо, называемые *интро,* в виде исполняемых файлов небольшого размера поставляются в архивах с варезом или инструментами взлома.

Демотиватор. Жанр графического баннера (интернет-плаката), выполненный по определенному канону: изображение в толстой черной рамке с коротким текстом в нижней части. Содержание демотиватора обычно антиреклама, сатира, юмор.

Дентро (от англ. *dentro).* Презентация готовящегося демо (обычно большого и долгожданного). Может быть оформлено в виде текстового превью с несколькими картинками и фоновой музыкой.

Диалап. *См.* **Коммутируемый доступ.**

Динамический IP-адрес. Существует тенденция путать понятия частного **IP**-адреса и динамического, ошибочно полагая, что все адреса, выделяемые провайдером динами-

чески — частные, а фиксированные адреса (закрепленные статически) — внешние. Под динамическим выделением адреса узлу сети понимается присвоение нового адреса для каждой сессии соединения (аренда адреса, отсутствие постоянно закрепленного за узлом адреса), таким образом присваиваться могут как частные, так и внешние адреса.

Дистрибутив программы. Комплект файлов программы, предназначенных для ручного или автоматического копирования на компьютер пользователя с внедрением (или без такового) определенных ключей в системный реестр. Чаще всего дистрибутивы программ для операционной системы Windows распространяются в виде инсталляторов с расширением mse или exe.

Дйффи-Хеллмана, протокол. Криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена данными с помощью алгоритмов симметричного шифрования. В чистом виде алгоритм Диффи-Хеллмана уязвим для модификации данных в канале связи, поэтому схемы с его использованием применяют дополнительные методы односторонней или двусторонней аутентификации. По последним данным алгоритм Диффи-Хеллмана мог быть скомпрометирован АНБ.

Доджкоин (от англ. *Dogecoin: doge,* «собака» и *coin,* «монета»). Криптовалюта наподобие биткоина, придуманная в Австралии.

Домен (от англ. *domain*). Область пространства доменных имен в Интернете, которая обозначается уникальным доменным именем. А также группа компьютеров, работающих в сети, объединенных одним именем домена.

Доменное имя. Символьное имя домена, как правило, состоящее из нескольких доменов. Например, доменное имя **warez.ucoz.com** состоит из домена третьего уровня **warez,** домена второго уровня **ucoz,** домена первого уровня **com,** который входит в корневой домен. Корневой домен в системе DNS отделяется, как правило, неотображаемой точкой от домена первого уровня и не обозначается никакими символами.

Драйвер (от англ. *driver).* Программа, расширяющая возможности операционной системы и предназначенная для управления устройствами ввода/вывода (например, клавиатурой, мышью, принтером, модемом), оперативной памятью и др., а также для подключения к компьютеру дополнительных внешних устройств. С помощью драйверов операционная система и программное обеспечение получают доступ к аппаратному обеспечению. В большинстве случаев в составе операционной системы имеются драйверы для большинства стандартных устройств. Для некоторых специфичных устройств, а также в случае обновления версии драйвера (с целью исправления ошибок и/или расширения возможностей по управлению устройством), может потребоваться загрузка драйвера с вебстраницы производителя устройства (или с прилагаемого оптического диска).

Дроппер (от англ. *Dropper).* Вредоносная программа (как правило, троянская), предназначенная для несанкционированной и скрытой от пользователя установки на компьютер других вредоносных программ, содержащихся в самом теле дроппера или загружаемых по сети.

З

Зависание. Нерегламентированное состояние операционной системы или прикладного программного обеспечения, при котором эта операционная система и/или программа не реагирует на действия пользователя. В том числе и **BSOD.**

Загрузочный вирус (от англ. *Boot virus).* Компьютерный вирус, записывающийся в первый сектор жесткого диска и выполняющийся при загрузке компьютера. При включении или перезагрузке компьютера такой вирус заменяет собой загрузочный код и получает управление еще до непосредственного запуска операционной системы.

Закладка. Скрытно внедренная в защищенную систему программа либо намеренно измененный фрагмент программы, которые позволяют злоумышленнику осуществить несанкционированный доступ к ресурсам системы. Закладка может быть внедрена самим разработчиком программного обеспечения. Часто программные закладки выполняют роль перехватчиков паролей и трафика, а также служат в качестве проводников для компьютерных вирусов. Программные закладки невозможно обнаружить при помощи стандартных антивирусных средств.

Зеркало сайта. См. Mirror.

Зеттабайт (Збайт, 36). Единица измерения количества информации, равная 1024 Эбайт, или 2^{70} байт.

Золото. См. Gold.

И

ИМХО (от англ. *IMHO, In My Humble Opinion*, по моему скромному мнению). Обычное выражение на форумах и в чатах.

Инвайт (в пер. с англ. приглашение). Приглашение «по рекомендации» (от уже действующего участника сообщества). Инвайты применяются для доступа (регистрации) на некоторых интернет-сервисах (закрытых форумах, сайтах и т. п.) — например, на трекере **What.cd.**

Инкапсуляция (в компьютерных сетях). Метод построения модульных сетевых протоколов, при котором логически независимые функции сети отделяются от нижележащих механизмов путем включения (инкапсулирования) этих механизмов в более высокоуровневые объекты.

Инсталлятор. *См.* **Дистрибутив программы.**

Инсталляция программы. Процесс переноса файлов устанавливаемой программы в соответствующие системные папки и внедрение информации о программе в системный реестр.

Интегрированная среда разработки (от англ. *Integrated Development Environment, IDE).* Комплекс программных средств, используемый для разработки программного обеспечения. Среда разработки, как правило, включает в себя: текстовый редактор, компилятор и/или интерпретатор, средства автоматизации сборки и отладчик.

Интернет (от англ. *Interconnected Networks,* объединенные сети). Всемирная система объединенных компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. Построена на базе стека протоколов TCP/IP. На основе Интернета работает Всемирная паутина и множество других систем передачи данных. Не следует путать с понятием **Всемирная паутина.**

Интернет-банкинг. Технология дистанционного банковского обслуживания, а также доступ к счетам и операциям (по ним), предоставляющийся в любое время и с любого компьютера, имеющего доступ в Интернет. В большинстве случаев для выполнения операций используется браузер, т. е. отсутствует необходимость установки клиентской части программного обеспечения системы.

Интернет-мем (от англ. *Internet meme).* Информация в той или иной форме (мультимедийный объект, фраза, концепция или занятие), как правило, остроумная и ироническая, спонтанно приобретшая популярность в интернет-среде посредством распространения в Интернете разнообразными способами (в социальных сетях, на форумах, в блогах, в мессенджерах и др.). Также обозначает явление спонтанного распространения такой информации или фразы. К примеру, в настоящее время популярен мем про мальчика Карла из постапокалиптического сериала «Ходячие мертвецы». Сюжет, из-за которого появился мем, состоит в следующем: главный герой сериала осознает, что его жена умерла при родах, после чего начинает плакать, кричать и падает на землю. Его сын Карл все это время просто стоит и молчит. Пока сын молчит, отец что-то ему эмоционально рассказывает, после чего с надрывом повторяет фрагмент своей последней фразы, добавляя к нему слово «Карл». Пример мема в рунете: «игра GTA V продается на семи дисках!!! На семи, Карл!!»

Интернет-провайдер. *См.* **Провайдер.**

Интернет-шлюз. Программное обеспечение, призванное организовать передачу трафика между разными сетями. Программа является рабочим инструментом системного администратора, позволяя ему контролировать трафик и действия сотрудников. Также под шлюзом часто понимается IP-адрес компьютера, через который организован доступ в Интернет.

Интро (от англ. *intro).* Короткое и зацикленное демо очень малого размера (64 Кбайт, 16 Кбайт, 4 Кбайт и 512 Байт). Также интро могут называться демо любого размера, посвященные некоему событию (например, приглашение на демопати).

Й

Йоттабайт (Йбайт, Йб). Единица измерения количества информации, равная 1024 Збайт, или 2^{80} байт.

К

Кардридер (от англ. *Card reader,* устройство чтения карт). Устройство для чтения карт памяти, а также иных электронных карт самого различного назначения.

Карта памяти. Компактное электронное запоминающее устройство, используемое для хранения цифровой информации. Современные карты памяти изготавливаются на основе Flash-памяти, хотя принципиально могут использоваться и другие технологии. Карты памяти широко используются в электронных устройствах, включая цифровые фотоаппараты, сотовые телефоны, ноутбуки, аудиоплееры и т. п. Наиболее распространены карты типов Compact Flash, Secure Digital, microSD и Memory Stick.

Кейлогер (от англ. *keylogger: key,* ключ и *logger,* регистрирующее устройство). Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя: нажатия клавиш на клавиатуре компьютера, движения и нажатия кнопок мыши и т. д. Дополнительно могут создаваться периодические снимки экрана (а в некоторых случаях — даже видеозапись экрана) и копироваться данные из буфера обмена. Существуют как программные, так и аппаратные кейлогеры. Аппаратные кейлогеры представляют собой миниатюрные приспособления, которые могут быть прикреплены между клавиатурой и компьютером или встроены в саму клавиатуру. Акустические кейлогеры представляют собой аппаратные устройства, которые вначале записывают звуки,

создаваемые пользователем при нажатии на клавиши клавиатуры компьютера, а затем анализируют эти звуки и преобразовывают их в текстовый формат.

Киберсквоттинг (от англ. *cybersquatting: cyber,* кибер и *squatting,* самовольное заселение). Регистрация доменных имен, содержащих торговую марку, принадлежащую другому липу с целью их дальнейшей перепродажи или недобросовестного использования. Люди, практикующие такие действия, называются киберсквоттерами.

Килобайт (Кбайт, Кб). Единица измерения количества информации, равная 1024 байт, или 2^{10} байт.

Ключ шифрования. Секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности.

Кодек (от англ. *codec: coder/decoder,* кодировщик/декодировщик). Устройство или программа, способные выполнять преобразование данных или сигнала. Например, преобразование кодеком MP3 звукового файла формата WAV в формат MP3. Большинство кодеков для звуковых и визуальных данных использует сжатие с потерями, чтобы получить на выходе небольшой размер готового (сжатого) файла. Существуют также кодеки, сжимающие без потерь (lossless codecs), при использовании которых размер готового файла больше, но и качество (изображения или звука) лучше.

Коллизии. *См.* Сетевой концентратор.

Коммутация IP-пакетов. Технология, использующаяся для оптимизации работы маршрутизаторов при использовании неизменных или редко меняющихся маршрутов.

Коммутируемый доступ (от англ. *dial-up,* набор номера, дозвониться). Сервис, позволяющий компьютеру, используя модем и телефонную сеть общего пользования, подключаться к другому компьютеру (серверу доступа) для инициализации сеанса передачи данных (например, для доступа в Интернет).

Компрометация. Факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа.

Консорциум Всемирной паутины, Консорциум W3C (англ. *World Wide Web Consortium,* W3C) — организация, разрабатывающая и внедряющая технологические стандарты для Всемирной паутины. Консорциум возглавляет Тимоти Бернерс-Ли, автор множества разработок в области информационных технологий и создатель Всемирной паутины.

Контейнер. Мультимедийный контейнер представляет собой файл с определенным расширением, видео- и аудиоданные которого сжаты различными кодеками. Например, в файле 1 .avi видеоизображение может быть сжато кодеком DivX, а звук — PCM, в файле 2.avi видео сжато кодеком Indeo, а звук — MP3. Оба файла имеют одно и то же расширение, а содержимое этих файлов совершенно разное. Поэтому некоторые файлы с одним и тем же расширением могут воспроизводиться на вашем компьютере, а другие — нет (требуется установка кодека, которым сжато содержимое контейнера). В настоящее время для HD-видео в основном используются три типа контейнеров: MKV, TS или M2TS.

Контент. Содержимое (обычно веб-сайта: статьи, файлы).

Криптовалюта. Электронный механизм обмена, цифровое платежное средство, эмиссия и учет которого децентрализованы. Функционирование системы происходит в рамках распределенной компьютерной сети. Общее число криптовалют превышает 2 тыс. Среди них самые популярные — это биткоин, лайткоин и доджкоин.

Крэктро (от англ. *cracktro).* Интро, вставленное во взломанную игру. Характерными элементами крэктро являются чит-меню и прокручивающийся текст с приветствиями другим группам.

Крэк (от англ. *crack,* взлом). Программа, позволяющая осуществить взлом программного обеспечения. Как правило, крэк пригоден для массового использования. По сути, крэк является воплощением одного из видов взлома и зачастую это обычный патч. Для слова крэк используются следующие эвфемизмы: «лекарство», «таблетка», «аспирин» и т. п.

Крэкер (от англ. *cracker).* Человек, взламывающий компьютерные игры, программное обеспечение и системы защит, а также занимающийся созданием или доработкой крэков. В практике также применяется общий термин «компьютерный взломщик» или «хакер», что не является правильным. Результатом работы крэкера целенаправленно являются так называемые *крэки.* В абсолютном большинстве случаев крэкер не располагает исходным кодом программы, поэтому программа изучается с помощью дизассемблера и отладчика с применением специальных утилит.

Курсор. Небольшой мигающий прямоугольник (или линия), показывающий текущую позицию ввода текста на экране. Не путайте с указателем — изображением позиции мыши (или иного устройства управления).

Кэш (кэш-память) (от англ. *cache,* наличная память). Память ноутбука или настольного компьютера с быстрым доступом, предназначенная для размещения копии информации, которая хранится в памяти с менее быстрым доступом, но которая с наибольшей вероятностью может быть запрошена.

Л

Лайткоин. Пиринговая электронная платежная система, использующая одноименную криптовалюту.

Лэмер. Неумелый пользователь компьютера с завышенной самооценкой.

Линк (от англ. *link,* ссылка). Гиперссылка.

Личер (от англ. *leecher, leech,* «пиявка»). Человек, пользующийся ресурсами Интернета, предоставляемыми другими, но не предлагающий ничего взамен. Понятие распространено в пиринговых сетях.

Логин (от англ. *log in,* вход в систему). Процедура идентификации ранее зарегистрированного пользователя в каком-либо программном обеспечении или на сервере. А также имя пользователя, которое требуется для его идентификации (в большинстве случаев вместе с паролем).

Логическая бомба (англ. *Logic bomb).* Программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных). Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определенное время или при выполнении определенных условий, — например, в пятницу, 13-го, или при запуске какого-либо файла.

Лол. См. LOL.

Луковая маршрутизация (от англ. *Onion routing).* Технология анонимного обмена информацией через компьютерную сеть (в частности, Tor). Сообщения неоднократно шифру-

ются и потом отсылаются через несколько сетевых узлов, называемых *луковыми маршрутизаторами* (узлами). Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторяется. Таким образом, промежуточные узлы не знают источник, пункт назначения и содержание сообщения.

M

Макровирус (от англ. *macro virus).* Вредоносная программа, написанная на макроязыках, встроенных во многие системы обработки данных (текстовые редакторы, электронные таблицы и т. д.), — например, в пакет Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие.

Макрос (от англ. *macros).* Программный объект, состоящий из последовательности команд.

Маркет (в Даркнете) (от англ. *market).* Торговая интернет-площадка, доступная в Tor и других анонимных сетях, а также после получения доступа к закрытому сообществу. Как правило, на таких площадках предлагаются незаконные услуги и товары. Оплата обычно осуществляется в криптовалютах, имена участников анонимизированы и используется PGP для шифрования сообщений.

Маршрутизатор (роутер) (от англ. *router).* Сетевое устройство, определяющее оптимальный путь (исходя из информации о топологии сети и определенных правил) для пересылки пакетов между различными сегментами сети. Маршрутизатор может связывать разнородные сети различных архитектур. Маршрутизаторы работают на более высоком — сетевом — уровне модели OSI, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают соответственно на втором и первом уровнях модели OSI.

Маска подсети. Битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети (при этом, в отличие от IP-адреса, маска подсети не является частью IP-пакета).

Мастер-пароль. Кодовое слово для доступа к базам данных паролей и другим системам для удобства работы и обеспечения защиты данных.

Мегабайт (Мбайт, Мб). Единица измерения количества информации, равная 1024 Кбайт, или 2^{20} байт.

Мегадемо (от англ. *megademo).* Сборник эффектов, как правило, не связанных общей темой, и обладающий такой отличительной особенностью, как интерактивность. Интерактивность проявляется в том, что части демо (эффекты) длятся до прерывания пользователем и, кроме того, могут содержать управляемые элементы. В каждой части обычно присутствует какого-либо рода бегущая строка (или несколько бегущих строк) с длинным текстом — например, об авторах демо. Мегадемо были распространены в начале 1990-х, но постепенно вытеснились *трекмо* — жанром, более пригодным для демонстрации на публике.

Межсетевой экран, сетевой экран. Комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита сети или отдельных ее узлов от несанкционированного доступа. Сетевые экраны часто называют *фильтрами,* т. к. их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определенные в конфигурации,

в том числе и с целью блокировки определенных ресурсов. Также межсетевой экран называют **брандмауэром** (от нем. *Brandmauer: Brand,* пожар и *Mauer,* стена) и **файрволлом** (от англ .*firewall: fire,* огонь и *wall,* стена).

Метаданные. Сведения о некоем контенте. Например, при съемке цифровых фотографий в графический файл изображения добавляются метаданные о месте и времени съемки, характеристиках камеры и объектива, геолокационные сведения и т. п.

Многофакторная аутентификация (от англ. *Multi-factor authentication).* Расширенная аутентификация, метод контроля доступа к компьютеру (системе, веб-сайту и т. п.), в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства механизма аутентификации». Например, ПИН-код, отправленный по SMS, электронный токен, биометрические данные (отпечаток сетчатки или пальца) и т. д.

Модем (производное от сочетания «модулятор/демодулятор»). Устройство, преобразующее (модулирующее) цифровые данные для передачи по телефонным линиям, а затем демодулирующее полученные модулированные данные обратно в цифровой формат. Предназначено для подключения компьютера к сети (в том числе к Интернету), а также для приема/передачи факсимильных сообщений.

Модератор (от лат. *moderor,* умеряю, сдерживаю). Пользователь, имеющий более широкие права по сравнению с обыкновенными пользователями на общественных сетевых ресурсах (чатах, форумах, эхоконференциях, трекерах и т. п.) и обладающий правом редактировать и удалять чужие сообщения, удалять страницы пользователей, ограничивать пользователей в правах редактирования и просмотра сайта (банить). Точный перечень полномочий и обязанностей модератора на каждом сайте свой. Чаще всего модератор отвечает за соблюдение пользователями правил сайта.

Мэйнфрейм (от англ. *mainframe,* главная вычислительная машина). Большой универсальный высокопроизводительный отказоустойчивый сервер со значительными ресурсами ввода/вывода, большим объемом оперативной и внешней памяти, предназначенный для использования в критически важных системах с интенсивной пакетной и оперативной транзакционной обработкой.

Н

Ник, никнейм (от англ. *nickname,* «другое имя»). Псевдоним, используемый пользователем в Интернете, обычно в местах общения (в блогах, форумах, чатах).

Нюк (от англ. nuke, «убить» файл) — запрет распространения релиза за нарушение правил Сцены или за то, что релиз является повтором уже существующего. Нюкнутые релизы публикуются на специальных сайтах повторов dupecheck, но не попадают на топ-сайты.

О

Облачное хранилище данных (от англ. *cloud storage).* Модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один боль-

шой виртуальный сервер. Физически же такие серверы могут располагаться удаленно друг от друга географически, вплоть до расположения на разных континентах. К самым известным облачным хранилищам данных относятся: Dropbox, Облако Mail.Ru, Яндекс.Диск, Microsoft OneDrive, Google Drive, iCloud и др.

Обратная разработка, реверс-инжиниринг (от англ. *reverse engineering).* Исследование некоторого готового устройства или программы, а также документации на него, с целью понять принцип его работы — например, чтобы обнаружить недокументированные возможности, изменить или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без копирования как такового.

Оверпостинг. Несколько сообщений подряд от одного пользователя на форуме. Во избежание оверпостинга рекомендуется редактировать исходное сообщение, а не создавать новые.

Одноранговая (децентрализованная, пиринговая) **сеть** (от англ. *peer-to-peer, P2P,* «равный к равному»). Сеть, все участники которой обладают равными правами. В одноранговой сети отсутствуют серверы, и каждый компьютер пользователя (так называемый **Пир)** является как клиентом, так и сервером. Одноранговые сети, как правило, позволяют пользователям обмениваться звуковыми, видео- и иными файлами, находящимися на их компьютерах, поэтому их часто называют *файлообменными.* Популярными приложениями для обмена файлами являются eMule, mTorrent, Shareaza и др.

Олдскул (в пер. с англ. «Старая школа»). Уровень предпочтений и даже образ жизни, идеалом которого является поклонение старому «порядку вещей» и присущим ему феноменам и артефактам (музыка, фильмы, компьютерные игры и пр.).

Операционная система. Комплекс программного обеспечения, который загружается при каждом включении компьютера. Операционная система предназначена для обеспечения пользовательского интерфейса, распределения ресурсов компьютера, запуска прикладных программ, работы с файлами и обработки операций ввода/вывода. Существуют как клиентские, так и сетевые операционные системы, представляющие собой комплекс программ, обеспечивающий обработку, передачу и хранение данных в сети.

Оптоволоконная сеть. См. FTTx

Оффтоп (от англ. *off topic,* вне темы). Любое сетевое сообщение, выходящее за рамки заранее установленной темы общения, — например, запись на веб-форуме, не соответствующая либо общему направлению форума, либо той теме, в рамках которой запись оставлена. Во Всемирной паутине оффтоп обычно наказуем модераторами ресурса.

П

Пасскей. Уникальный идентификатор участника пиринговой сети, необходимый для учета рейтинга.

Патч. См. Patch.

Песочница (от англ. *sandbox).* Специально выделенная среда для безопасного исполнения компьютерных программ. Обычно представляет собой контролируемый набор ресурсов для исполнения гостевой программы — например, место на диске или в памяти. Доступ к сети, возможность сообщаться с главной операционной системой или считывать информацию с устройств ввода обычно либо частично эмулируют, либо сильно ограничивают. К примеру песочницы можно отнести виртуальную машину.

Петабайт (Пбайт, Пб). Единица измерения количества информации, равная 1024 Тбайт, или 2^{50} байт.

Пиксел. Минимальный элемент изображения на экране, который может быть сгенерирован компьютером.

ПИН-код (от англ. *Personal Identification Number*, личный опознавательный номер). Аналог пароля. ПИН-код предусматривается для банковских и других карт (например, SIM-карт) — с его помощью производится авторизация держателя карты. Обычно предусмотрено ограничение попыток правильного ввода ПИН-кода (в основном, не больше трех раз), после чего карта блокируется для использования. В мобильных телефонах для разблокирования забытого PIN-кода требуется ввести так называемый PUK-код.

Пир. Общее название участника файлообмена в пиринговой сети.

Пиринговая сеть. *См.* **Одноранговая сеть.**

Плагин. См. Plug-in.

Подсеть. Логическое разделение компьютерной сети IP. Компьютеры, входящие в одну подсеть, принадлежат одному диапазону IP-адресов. Преимущества подсетей заключается в более эффективном использовании доступных адресов.

Полиморфизм компьютерного вируса (от греч. *nolv,* много и *[хорщ,* форма). Специальная техника, используемая разработчиками вредоносного программного обеспечения для снижения уровня обнаружения вредоносной программы классическими антивирусными продуктами. Полиморфизм заключается в формировании программного кода вредоносной программы «на лету» — уже во время исполнения, при этом сама процедура, формирующая код, также не должна быть постоянной и видоизменяется при каждом новом заражении.

Порт (от англ. *port).* Число, записываемое в заголовках протоколов транспортного уровня модели OSI (TCP, UDP, SCTP, DCCP). Используется для определения процесса-получателя пакета в пределах одного хоста.

Портал (от англ. *portal).* Крупный сайт с большим количеством информации, объединяющий в себе несколько тем и учитывающий интересы широкой аудитории.

Пост. Сообщение на форуме или блоге.

Почтовая рассылка (от англ. *mailing list).* Рассылка идентичных электронных писем, как правило, новостных, на почтовые ящики нескольких адресатов.

Приватный режим браузера. Режим работы браузера, при котором данные о сеансе — информация о том, какие сайты и страницы посещались, cookie-файлы и т. п. — не сохраняются.

Провайдер (от англ. *ISP, Internet Service Provider,* поставщик интернет-услуги). Организация, предоставляющая зарегистрированным пользователям и другим организациям доступ в Интернет. Провайдер также может выделить часть пространства на жестком диске сервера для размещения на нем файлов пользователя.

Программное обеспечение (ПО). Совокупность программ, обеспечивающих функционирование компьютера и выполнение на нем различных задач. По функциональным задачам программное обеспечение делится на системное и прикладное. *Системное* программное обеспечение используется, в первую очередь, для управления всеми ресурсами компьютера, выполнения и разработки различных программ, а также для предоставления пользователю определенных услуг. Оно включает в себя операционные системы, се-

тевое программное обеспечение, инструменты расширения функций операционной системы, средства тестирования и диагностики компьютера, а также средства разработки программ. *Прикладные* программы призваны решать самые разные задачи, и обладают дружественным интерфейсом. К прикладным относят текстовые редакторы, электронные таблицы, графические редакторы, системы управления базами данных, программы математических расчетов и моделирования, аудио- и видеоредакторы и т. д.

Прокси-сервер (от англ. *proxy server,* сервер полномочий). Компьютер и/или программное обеспечение, играющие роль шлюза, через который пользователи согласно персонально назначенным правам доступа могут получать данные из локальной сети и/или Интернета.

Протокол (от англ. *protocol).* Совокупность правил, определяющих формат и процедуру обмена данными между двумя или несколькими независимыми устройствами или процессами.

Прошивка. Программный код, записанный в энергонезависимой памяти устройства (например, в материнской плате компьютера, сотового телефона или маршрутизатора). В качестве действия обозначает процесс загрузки программного кода в энергонезависимую память устройства.

Р

Радиорелейная связь. Один из видов наземной радиосвязи, основанный на многократной ретрансляции радиосигналов. Радиорелейная связь осуществляется, как правило, между стационарными объектами.

Развертка. Режим вывода видеоизображения на экран, который может быть чересстрочным или прогрессивным. При *чересстрочной* развертке: в HD обозначается как i — interlaced, например, 1080i (1920x1280, чересстрочная развертка) — видеоизображение передается со скоростью 50 или 60 полукадров в секунду (т. е. 25 или 30 кадров в секунду). При *прогрессивной* развертке: в HD обозначается как p— progressive, например, 1080p (1920x1280, прогрессивная развертка) и 720p (1280x720, прогрессивная развертка) — видеоизображение передается со скоростью 24, 25, 30 или 60 полных кадров в секунду.

Разрешение. Описывает уровень детализации изображения или процесса его создания. Разрешение изображения выражается в двух числах — например, значение 1920x1080 обозначает, что ширина изображения равна 1920 пикселам, а высота— 1080 пикселам. Разрешение печатающих и сканирующих устройств указывается в dpi (dots per inches, точках на дюйм) — например, 600 dpi или 1200 dpi.

Рапида. Вариация названия закрытого в 2015 году файлообменного сервиса Rapidshare.

Растровое изображение. Файл, представляющий собой сетку пикселов или точек разных цветов и отображенный на экране компьютера, бумаге и других устройствах и материалах. Основной недостаток растровых изображений— невозможность идеального масштабирования.

Расширение файла. *См.* **Тип файла.**

Реавторинг. Пересборка структуры оптического диска (как правило, DVD или Blu-ray), например, с целью добавления аудиодорожки.

Реестр. Системный реестр операционной системы Windows представляет собой сложную базу данных, которая представлена в операционной системе Windows в виде нескольких

файлов и содержит все параметры и настройки компьютера. После повреждения реестра компьютер, как правило, становится неработоспособным, но пользовательские файлы остаются в сохранности.

Резидентная программа, TSR-программа (от англ. *Terminate and Stay Resident,* «завершиться и остаться резидентной»). В операционной системе MS-DOS программа, вернувшая управление оболочке операционной системы либо надстройке над операционной системой и т. п., но оставшаяся в оперативной памяти персонального компьютера. Резидентная программа активизируется каждый раз при возникновении прерывания, вектор которого эта программа изменила на адрес одной из своих процедур. В эпоху многозадачных операционных систем резидентными иногда называют программы, загруженные постоянно и работающие в фоновом режиме. Но применение этого термина некорректно по отношению к многозадачным операционным системам.

Рейтинг. На трекерах — соотношение отданного пользователем к скачанному.

Релиз. На трекере — уникальная раздача. Официально — выпуск финальной версии программы на продажу. В варезных кругах — готовая к распространению во Всемирной паутине пиратская версия программного обеспечения или мультимедийного контента.

Релизная группа. *См.* **Варезная группа.**

Рип. См. Rip.

Роуминг (от англ. *roaming, roam,* бродить, странствовать). Процедура предоставления услуг (сотовой связи, Wi-Fi) абоненту вне зоны обслуживания «домашней» сети абонента с использованием ресурсов другой (гостевой) сети. При телефонном роуминге у абонента сохраняется его телефонный номер. Существуют **внутрисетевой (региональный) роуминг,** позволяющий сохранять номер при перемещении из одного региона в другой внутри покрытия одного оператора, **национальный межсетевой роуминг,** позволяющий при перемещении использовать сеть другого мобильного оператора внутри той же страны, и **международный роуминг,** позволяющий использовать сотовую связь в других странах.

Роутер. *См.* **Маршрутизатор.**

Рунет (от англ. *Russian Internet,* российский Интернет). Российский сегмент Всемирной паутины.

Руткит (от англ. *rootkit,* т. е. «набор root-пользователя»). Набор программных средств, с помощью которых хакеры пытаются получить несанкционированный доступ к компьютерам пользователей, оставаясь при этом незамеченными. Также руткитами называют технологии, используемые для сокрытия действий троянских программ в среде Windows.

С

Сабж. Тема разговора, обычно на форуме (тема сообщения).

Сайт. *См.* **Web-сайт.**

Свитч. *См.* **Сетевой коммутатор.**

Секвенсор (от англ. *sequence,* последовательность). Аппаратное или программное устройство для записи в реальном времени и воспроизведения музыки, как совокупности нот и характеристик их исполнения, представляемых в различных формах, — например, MIDI-сообщений. *См.* **MIDI.**

Сервер (от англ. *server, to serve,* служить). Компьютер или программное обеспечение, подключенное к сети и/или Интернету и предназначенное для обработки запросов сетевых пользователей.

Серийный номер. См. Serial.

Сетевая плата (сетевая карта, сетевой адаптер, Ethernet-адаптер). Устройство, позволяющее компьютеру взаимодействовать с другими устройствами в сети.

Сетевой адрес. Идентификатор устройства, работающего в компьютерной сети.

Сетевой интерфейс. Сетевая карта в компьютере, а также точка соединения компьютера и сети (или двух сетей между собой).

Сетевой коммутатор, свитч (от англ. *switch,* переключатель). Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (третий уровень OSI). В отличие от концентратора (первый уровень OSI), который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались. *См.* **Сетевой концентратор.**

Сетевой концентратор, хаб (от англ. *hub,* центр). Устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа «витая пара». В настоящее время вытеснены сетевыми коммутаторами. Концентратор работает на первом (физическом) уровне сетевой модели OSI, ретранслируя входящий сигнал, с одного из портов в сигнал на все остальные (подключенные) порты, реализуя, таким образом, свойственную Ethernet топологию «общая шина», с разделением пропускной способности сети между всеми устройствами. Коллизии (т. е. попытка двух и более устройств начать передачу одновременно) обрабатываются аналогично сети Ethernet на других носителях — устройства самостоятельно прекращают передачу и возобновляют попытку через случайный промежуток времени. Сетевой концентратор также обеспечивает бесперебойную работу сети при отключении устройства от одного из портов или повреждении кабеля, в отличие, например, от сети на коаксиальном кабеле, которая в таком случае прекращает работу целиком. *См.* **Сетевой коммутатор.**

Сетевой маршрутизатор. *См.* **Маршрутизатор.**

Сетевой мост, бридж (от англ. *bridge).* Сетевое устройство, предназначенное для объединения сегментов (подсети) компьютерной сети в единую сеть. Сетевой мост работает на канальном (втором) уровне сетевой модели OSI — при получении из сети кадра он сверяет MAC-адрес последнего и, если он не принадлежит этой подсети, передает (транслирует) кадр дальше в тот сегмент, которому предназначался этот кадр. Если кадр принадлежит этой подсети, мост ничего не делает.

Сетевой повторитель, репитер (от англ. *repeater).* Сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения путем повторения электрического сигнала (который рано или поздно затухает) «один в один». Повторитель работает на физическом уровне модели OSI. Хотя концентратор выполняет похожие функции, повтори-

тель обладает гораздо меньшим временем задержки, ввиду того что он, как правило, обладает двумя разъемами для подключения кабеля. Ему нет необходимости где-то, концентрировать сигнал и распространять на остальные выходы. *См.* **Сетевой концентратор.**

Сетевой сканер. Устройство для поиска и сбора информации по доступным сетям Wi-Fi.

Сетевой шлюз (от англ. *gateway).* Аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной). Сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды (сети). Например, при соединении локального компьютера с сетью Интернет обычно используется сетевой шлюз. Маршрутизатор является одним из примеров аппаратных сетевых шлюзов.

Сжатие без потерь (от англ. *lossless data compression).* Метод сжатия данных (видео, аудио, графики, документов, представленных в цифровом виде), при использовании которого закодированные данные однозначно могут быть восстановлены с точностью до бита. При этом оригинальные данные полностью восстанавливаются из сжатого состояния. Этот тип сжатия принципиально отличается от сжатия с потерями. Для каждого из типов цифровой информации, как правило, существуют свои оптимальные алгоритмы сжатия без потерь. Примеры форматов файлов, использующих сжатие без потерь: Zip, 7-Zip, RAR, FLAC (аудиофайлы), APE (аудиофайлы), BMP (графика), PNG (графика) и др. Релизы мультимедийного контента часто обозначаются словом Lossless, если записаны с применением сжатия без потерь.

Сжатие с потерями (от англ. *lossy data compression).* Метод сжатия данных, при использовании которого распакованные данные отличаются от исходных, но степень отличия не существенна с точки зрения их дальнейшего использования. Этот тип компрессии часто применяется для сжатия аудио- и видеоданных, статических изображений, в Интернете (особенно в потоковой передаче данных) и цифровой телефонии. Примеры форматов файлов, использующих сжатие с потерями: JPEG (графика), MP3 (музыка), H.264 (видео) и др. Релизы мультимедийного контента часто обозначаются словом Lossy, если записаны с применением сжатия с потерями.

Сидер. Участник пиринговой сети, имеющий раздачу полностью.

Синий экран смерти. См. BSOD.

Синхронизация. Процедура согласования времени обработки или передачи данных. А также процедура сверки и обновления данных на различных устройствах.

Система управления базами данных (СУБД). Программное обеспечение, предназначенное для организации и ведения базы данных.

Сканер портов. Программное средство, разработанное для поиска хостов сети, в которых открыты нужные порты. Эти программы обычно используются, системными администраторами для проверки безопасности их сетей и злоумышленниками для взлома сети. Может производиться поиск как ряда открытых портов на одном хосте, так и одного определенного порта на многих хостах. Последнее характерно для деятельности ряда сетевых червей.

Сквозное шифрование. Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения.

Скриншот, скрин (от англ. *Screenshot).* «Снимок» содержимого экрана компьютера, помещенный в буфер обмена или сохраненный в виде графического файла. Для получения

скриншотов в операционной системе Windows используется клавиша <PrtSc>, а в OS X — сочетания клавиш <1}>+<§§>+<3> (весь экран) и <1}>+<§§>+<4>.

Скрипт (от англ. *script,* сценарий). Программа, выполняющая последовательный, заранее написанный, набор действий. Например, форум или гостевая книга во Всемирной паутине представляют собой сложные скрипты.

Смайлик (от англ. *smile,* улыбающийся). Стилизованное графическое изображение улыбающегося человеческого лица. Традиционно изображается в виде желтого круга с двумя черными точками, представляющими глаза, и черной дугой, символизирующей рот. Слово «смайлик» также часто применяется как общий термин для любого эмотикона. *См.* **Эмотикон.**

Смешанные сети (от англ. *mix networks).* Протоколы маршрутизации, запутывающие пути следования трафика с помощью цепочек прокси-серверов, известных как микс-серверы. Прокси-серверы принимают данные от разных отправителей, перемешивают их и отправляют в случайном порядке к следующему узлу (например, другому микс-серверу). Таким образом, разрушается связь между источником запроса и сервером назначения, что затрудняет отслеживание и перехват трафика. Кроме того, микс-серверу известны только два узла в цепочке: от которого переданы данные и к которому их нужно отправить.

Данные шифруются отдельным публичным ключом для каждого прокси-сервера, и в результате они напоминают «матрешку» с непосредственными данными под слоями шифров. Каждый прокси-сервер удаляет собственный слой шифрования, чтобы узнать, куда отсылать данные далее. Последний узел передает данные в открытом виде серверу назначения. Этот принцип используется в сети Tor.

Сниффер. *См.* **Анализатор трафика.**

Сноуден Эдвард (Edward Joseph Snowden). Американский технический специалист, бывший сотрудник ЦРУ и АНБ США. В 2013 году Сноуден передал газетам The Guardian и The Washington Post секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру при помощи существующих информационных сетей и сетей связи, включая сведения о проектах PRISM, а также X-Keyscore и Tempora. По данным закрытого доклада Пентагона, Сноуден похитил 1,7 млн секретных файлов. В настоящее время проживает в России, но его точное местонахождение не разглашается по соображениям безопасности.

СОРМ, «Система технических средств для обеспечения функций Оперативно-Розыскных Мероприятий». Комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи. Аппаратура СОРМ устанавливается у российских операторов услуг связи, а пульты дистанционного управления, серверы и системы хранения данных располагаются у спецслужб. В своем развитии СОРМ прошел три этапа: СОРМ-1: анализ телефонных разговоров, СОРМ-2: анализ интернет-трафика, СОРМ-3: комплексный анализ информации.

Софт (от англ. *Software).* Программное обеспечение.

Спам (от англ. *Spam, Stupid Person's Annoying Message,* тупые надоедливые сообщения). Массовая рассылка сообщений рекламного характера без согласия пользователя.

Сплиттер. Устройство, которое разделяет ADSL-сигнал на компоненты «голос» и «передача данных» и позволяет одновременно по одной линии получать доступ в Интернет и вести телефонные разговоры.

Спонсор. Во Всемирной паутине — организация, которая платит за то, что владельцы веб-сайтов размещают баннерную рекламу на своих сайтах. Посетители веб-сайтов, щелкая по баннерам, приносят владельцу сайта доход, который и выплачивается спонсором.

Спуфинг MAC-адресов. *См.* **MAC-спуфинг.**

Стек протоколов. Набор взаимодействующих сетевых протоколов— например, TCP/IP, состоящий из двух протоколов: TCP и IP. Протоколы работают в сети одновременно, чтобы не возникало конфликтов или незавершенных операций.

СУБД. *См.* **Система управления базами данных.**

Сцена. Закрытое, законспирированное онлайн-сообщество, развившееся из подпольной группы людей «по интересам». Распространено по всему миру. Сцена в основном ориентирована на выпуск нелегальных или взломанных копий программного обеспечения (0-day) и мультимедийного контента (новых фильмов, музыкальных альбомов и т. п.).

Сценарий. *См.* **Скрипт.**

Сырой. Исходный код или программное обеспечение, содержащее недоработки, ошибки.

Т

Твердотельный накопитель (от англ. *solid-state drive, SSD).* Запоминающее устройство на основе микросхем памяти с управляющим контроллером. В настоящее время твердотельные накопители используются в стационарных компьютерах и ноутбуках, а также смартфонах, планшетах и других устройствах. По сравнению с традиционными жесткими дисками (HDD) твердотельные накопители имеют меньший размер и вес, более высокую скорость, но в несколько раз большую стоимость и значительно меньшую износостойкость (ресурс записи). Кроме того, для SSD характерна невозможность восстановить информацию при электрических повреждениях. Так как контроллер и носители информации в SSD находятся на одной плате, то при превышении или значительном перепаде напряжения чаще всего сгорает весь SSD-носитель с безвозвратной потерей информации. Напротив, в жестких дисках чаще сгорает только плата контроллера, что делает возможным восстановление информации с приемлемой трудоемкостью.

Тег (от англ. *tag,* именованная метка). Элемент языка HTML, предназначенный для разметки веб-страниц. Например, запись <±>яблоко</1> позволяет вывести на веб-странице слово *Яблоко* курсивом. Важно отличать *теги* и *элементы* разметки — к примеру, элемент body состоит из открывающего тега <body> и закрывающего тега </body>. Элементом называется все содержимое между открывающим и закрывающим тегами, включая сами теги.

Текстро (от англ. *textro).* Интро, объявляющее о каком-либо событии (например, о готовящемся мероприятии). Отличается большим количеством текста и простеньким эффектом.

Терабайт (Тбайт, Тб). Единица измерения количества информации, равная 1024 Гбайт, или 2^{40} байт.

Суперпользователь. См. Root.

Тип файла. Тип файла определяется его *расширением* — набором символов, добавляемых в конце названия файла, после точки. Чаще всего расширение состоит из трех символов и позволяет системе определять, какие данные содержатся в файле и какая программа предназначена для чтения такого файла. При настройках по умолчанию в операционной

системе Windows расширение файла скрывается и отображается только его название. Например, текстовый файл **Записка.M,** расширением которого является **txt,** по умолчанию будет выглядеть как **Записка.**

Токен. Компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, используемое также для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам и т. д. Этот термин может относиться и к программным токенам, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам.

Топик. Тема на форуме.

Топ-сайт. Скрытый, высокозащшценный, высокоскоростной FTP-сервер, используемый варезными группами и курьерами для распространения, хранения и архивирования релизов.

Торрент (идентификатор). Файл, который содержит в себе информацию о запрошенных файлах: размере и количестве фрагментов, контрольной сумме CRC, трекере.

Трафик (от англ. *traffic,* движение, грузооборот). Объем данных, передаваемых через компьютерную сеть за определенный период времени. Количество трафика измеряется как в пакетах, так и в битах, байтах и их производных: килобайтах, мегабайтах и т. д.

Трекер. В пиринговых сетях — специализированный сервер, работающий по протоколу HTTP. Трекер нужен для того, чтобы клиенты могли найти друг друга. Трекер часто, помимо своей основной функции, выполняет и функцию небольшого веб-сервера. Такой сервер хранит файлы метаданных и описания распространяемых файлов, предоставляет статистику закачек по разным файлам, показывает текущее количество подключенных пиров и др. В музыке — общий термин для класса программных музыкальных секвенсоров, которые в их простейшем виде позволяют пользователю расставлять звуковые сэмплы (звуковые фрагменты, как правило, зацикленные) последовательно во времени на нескольких монофонических каналах.

Трекерная музыка, MOD-музыка. Музыка, созданная на компьютере при помощи программы-трекера.

Трекмо (от англ. *trackmo).* Демо, синхронизированное под музыкальное сопровождение. Ритм музыки может соответствовать ритму смены эффектов и ритму движения объектов на экране.

Троллинг. Форма социальной провокации в сетевой коммуникации, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.

Троянская программа (от англ. *trojari).* Неспособная самостоятельно распространяться (чем и отличается от вирусов и червей) программа, предназначенная для выполнения вредоносных действий на зараженном компьютере. Как правило, троянские программы устанавливаются на компьютере скрытно и без ведома пользователя. Существует множество разновидностей троянских программ, каждая из которых предназначена для выполнения конкретных вредоносных действий, но, в большинстве случаев, троянские программы служат для сбора информации (в том числе и конфиденциальной) на компьютере пользователя и отправки ее разработчику вредоносного приложения. Основными симптомами действий троянской программы на компьютере являются: появление в автозагрузке новых неизвестных приложений, демонстрация рекламы или открытие рекламных веб-сайтов, создание снимков экрана, открывание и закрывание оптического привода, воспроизведение звуков, демонстрация изображений, непредвиденная переза-

грузка или отключение питания компьютера. Термин произошел от троянского коня — деревянной фигуры, с помощью которой, согласно легенде, греки обманным путем проникли в город Трою и захватили его.

Туннелирование (от англ. *tunnelling,* прокладка туннеля). Процесс в компьютерных сетях, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Туннелирование представляет собой метод построения сетей, при котором один сетевой протокол инкапсулируется в другой. Комбинация туннелирования и шифрования позволяет реализовать закрытые виртуальные частные сети (VPN).

Туннельный брокер. Специальный сервис, позволяющий получить доступ к IPv6-ресурсам посредством туннелирования через существующую IPv4-сеть.

У

Узел сети (от англ. *node).* Устройство, соединенное с другими устройствами как часть компьютерной сети. Узлами могут быть компьютеры, смартфоны, планшеты, а также специальные сетевые устройства, такие как маршрутизатор, коммутатор или концентратор.

Утилита. Программа, служащая для выполнения вспомогательных операций обработки данных или обслуживания компьютера.

Учетная запись пользователя. Комплекс параметров и пользовательских файлов, характерных для той или иной учетной записи. Таких записей на компьютере может быть несколько, и все они могут содержать различные настройки интерфейса операционной системы.

Уязвимость. Ошибка или недоработка в защите приложения или операционной системы, позволяющая злоумышленнику получить несанкционированный доступ к компьютеру пользователя. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты. Обычно уязвимость позволяет злоумышленнику «обмануть» приложение — заставить его совершить действие, на которое у того не должно быть прав. С целью ликвидации обнаруженных уязвимостей, производители программного обеспечения выпускают обновления (патчи). Неликвидированные недоработки называются уязвимостями нулевого дня (0-Day).

Ф

Файловая система (от англ *file system).* Порядок, определяющий способ организации, хранения и именования данных на носителях информации в компьютерах, а также в другом электронном оборудовании: цифровых фотоаппаратах, мобильных телефонах и т. п. Файловая система определяет формат содержимого и способ физического хранения информации, которую принято группировать в виде файлов. Конкретная файловая система определяет размер имен файлов (и каталогов), максимальный возможный размер файла и раздела, набор атрибутов файла. Некоторые файловые системы предоставляют сервисные возможности — например, разграничение доступа или шифрование файлов.

Файловый вирус. Компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой операционной

системы. Объектом вирусного поражения могут выступать исполняемые двоичные файлы (EXE, COM), файлы динамических библиотек (DLL), драйверы (SYS), командные файлы (BAT, CMD) и др.

Файлообменная сеть. *См.* **Одноранговая сеть.**

Файрволл. См. Firewall.

Фишинг (от англ. *phishing,* рыбная ловля, выуживание). Вид преступлений, связанный с получением персональных (например, личных или банковских) данных пользователей обманным путем. Для этих целей создается подложный веб-сайт, идентичный по внешнему виду сайту, через который пользователь проводит финансовые взаиморасчеты. Затем злоумышленники обманным путем, как правило, рассылкой спама, добиваются, чтобы пользователи посетили этот сайт и ввели на нем свои конфиденциальные данные.

Флейм (от англ. *flame,* огонь, пламя). Оскорбления или малоинформативные сообщения, безрезультативные споры, словесные войны. Флейм-сообщения могут содержать личные оскорбления и зачастую направлены на дальнейшее разжигание ссоры. Иногда флейм применяется в контексте троллинга, но чаще флейм вспыхивает просто из-за обиды на виртуального собеседника. Во Всемирной паутине флейм обычно наказуем модераторами ресурса.

Флуд (от англ. *flood,* поток). Многократное повторение одинаковых сообщений. Технический флуд представляет собой хакерскую атаку с большим количеством запросов, приводящую к отказу в обслуживании. Во Всемирной паутине флуд обычно наказуем модераторами ресурса.

Форум (от англ. *forum).* Веб-сайт, предназначенный для общения зарегистрированных участников посредством размещения; сообщений.

Фотожаба. Разновидность фотомонтажа, сленговое название результата творческой переработки участниками форума, блога или другого ресурса некоего изображения с помощью растрового или векторного графического редактора. Название происходит от наиболее часто использующегося для создания подобных изображений редактора Adobe Photoshop, хотя для этого может быть использован любой другой графический редактор. Обычно создаваемые изображения носят карикатурный характер.

Фрисайт. Сайт, опубликованный в анонимной сети Freenet.

X

Хаб. *См.* **Сетевой концентратор.**

Хакер (от англ. *hacker, to hack,* рубить, кромсать). Человек, досконально изучивший компьютерные системы и программы. Практическое использование этих знаний зависит от моральных качеств хакера. Часто хакеров классифицируют на разные виды, из которых двумя основными являются «белая шляпа» (*White hat)* и «черная шляпа» *(Black hat).* Черными шляпами называют киберпреступников, тогда как белыми шляпами — прочих специалистов по информационной безопасности (в частности, работающих в крупных IT-компаниях) или исследователей IT-систем, не нарушающих закон. В случаях, например, мелких нарушений законодательства или отсутствия нарушений законодательства, но нарушения внутренних правил какого-либо интернет-сервиса может использоваться термин «серая шляпа» *(Grey hat).* Термин «скрипт-кидди» *(Script kiddie)* означает взломщика или киберпреступника, использующего чужие наработки (например, покупающего их), но не понимающего механизма их реализации и которого к хакерам, как правило, не относят.

Хакинг. Получение доступа к удаленному компьютеру без разрешения владельца. Обычно используется для воровства кражи конфиденциальных данных или их уничтожения.

Холивар (от англ. *holy war,* священная война). Обмен сообщениями в интернет-форумах и чатах, представляющий собой бессмысленные дискуссии, в которых участники яростно пытаются навязать друг другу свои точки зрения.

Хост (от англ. *host,* хозяин, принимающий гостей). Любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определенное на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключенный к локальной или глобальной сети. В случае использования виртуальных машин, хостом называется система, в которой производится запуск гостевой операционной системы в виртуальной машине.

Хостинг. Услуга по предоставлению пространства на сервере в Интернете для размещения веб-сайта пользователя. Услуга может быть как платной, так и бесплатной, включает регистрацию уникального адреса сайта для его идентификации в Интернете и обеспечивает доступ к веб-сайту других пользователей по протоколу HTTP.

Ч

ЧаВо. *См.* **FAQ.**

Чат (от англ. *chatter,* болтать). Веб-сайт, предназначенный для общения зарегистрированных и/или авторизованных участников посредством размещения сообщений в реальном времени.

Червь (от англ. *worm).* Компьютерная программа, самостоятельно распространяющая свой код, но, в отличие от вирусов, не способная к заражению других файлов. Также в отличие от вирусов, черви создают единственную копию своего кода на каждой машине, а не дописывают себя в файлы, размещенные на жестком диске.

Чесночная маршрутизация (от англ. *Garlic Routing).* Технология анонимного зашифрованного обмена информацией через компьютерную сеть, используемая в анонимной сети I2P. Чесночная технология является расширением луковой маршрутизации, на которой основан проект Tor. Чесночная технология, используя многослойное шифрование, позволяет единственному сообщению (так называемому «чесноку») содержать в себе множество «зубчиков» — полностью сформированных сообщений рядом с инструкциями для их доставки. В один «чеснок» в момент его формирования перед отправкой закладываются множество «зубчиков», являющихся зашифрованными сообщениями как нашего узла, так и чужими — транзитными. Является ли тот или иной «зубчик» в «чесноке» нашим сообщением или это чужое транзитное сообщение, которое просто проходит через нас, знает только тот, кто создал «чеснок», никто иной узнать эту информацию не может. Чесночная технология применяется тогда, когда нужно отправить зашифрованное сообщение через промежуточные узлы, у которых не должно быть доступа к этой информации. Также *см.* **Луковая маршрутизация.**

Чиптюн (от англ. *chiptune).* Электронная музыка, синтезируемая в реальном времени аудиочипом компьютера или игровой приставки (обычно ранних поколений), а не набором музыкальных сэмплов, записанных с аудиоустройств.

Читер. На трекере — участник, использующий средства обхода системы учета рейтинга. В играх — геймер, использующий читы для прохождения игры.

Ш

Шапка. Первое сообщение в теме на форуме.

Шифрование. Обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Шлют. *См.* **Интернет-шлюз и Сетевой шлюз.**

Шпионская программа. *См.* **Spyware.**

Э

Экзабайт (Эбайт, Эб). Единица измерения количества информации, равная 1024 Пбайт, или 2^{60} байт.

Эксплойт (от англ. *exploit,* эксплуатировать). Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования (DoS-атака).

Электронная почта (от англ. *e-mail, electronic mait).* Система передачи электронных сообщений между компьютерами с помощью локальной сети и/или Интернета.

Эмотикон (от англ. *emoticon).* Пиктограмма, изображающая эмоцию, чаще всего составляется из типографских знаков. Особое распространение получила во Всемирной паутине и SMS (и прочих текстовых сообщениях). В повседневной русской речи обычно называется «смайликом» — независимо от выражения (хотя фактически слово «смайлик» имеет иное значение). Примеры эмотиконов: ^_^ — радость, v_v — грусть, o_o — удивление, *_* — восхищение и др.

Эмулятор (от англ. *emulator*). Приложение, которое симулирует (эмулирует) работу другой компьютерной среды на компьютере. Например, эмуляция Linux в среде Windows.

Эшелон (Echelon). Общепринятое название глобальной системы радиоэлектронной разведки, работающей в рамках соглашения о радиотехнической и разведывательной безопасности Великобритании и США (Австралия, Канада, Новая Зеландия, Великобритания, Соединенные Штаты Америки). Система имеет возможность перехвата и анализа телефонных переговоров, факсов, электронных писем и других информационных потоков по всему миру путем подключения к каналам связи — таким как спутниковая связь, телефонная сеть общего пользования, радиорелейная связь.

Ю

Юникод (от англ. *Unicode*). Стандарт кодирования символов всех национальных алфавитов.

Яндекс.Деньги. Сервис электронных платежей в Рунете, который позволяет принимать оплату электронными деньгами, наличными, с банковских карт. Валюта расчетов — российский рубль.

Яндекс.Диск. Облачный сервис, принадлежащий компании Яндекс и позволяющий пользователям хранить свои данные на серверах в «облаке» и передавать их другим пользователям в Интернете.

Ячеистая топология (от англ. *Mesh Topology*). Сетевая топология компьютерной сети, построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников. Эта организация сети является достаточно сложной в настройке, однако при такой топологии реализуется высокая отказоустойчивость. Как правило, узлы соединяются по принципу «каждый с каждым». Таким образом, большое количество связей обеспечивает широкий выбор маршрута следования трафика внутри сети — следовательно, обрыв одного соединения не нарушит функционирования сети в целом.

Источники

1. Wikipedia: **https://www.wikipedia.org/**
2. Безопасность Wi-Fi в публичных сетях: **http://www.ci2b.info/o-proekte/texnologii/11-texnicheskie-voprosy/vzlom-wi-fi-c-kpk-soft-dlya-vardrajvinga/bezopasnost-wi-fi-v-publichnyx-setyax/**
3. Вирусология: **http://w-security.ru**
4. Как правильно защищать сети Wi-Fi: **http://www.osp.ru/nets/2011/0S/13011S47/**
5. Проект Electronic Frontier Foundation: **https://ssd.eff.org/ru/**
6. Сайт компании BatBlue The Cloud Security Company: **http://www.batblue.com/**
7. Сайт компании Kaspersky lab: **http://www.kaspersky.ru/internet-security-center/**
8. Проект Vuvuzela: **https://people.csail.mit.edu/nickolai/papers/vandenhooff-vuvuzela.pdf**
9. Проект cMix: **https://eprint.iacr.org/2016/008.pdf**
10. Анонимные сети: **https://ru.wikipedia**.0rg/**wiki**/AH0HHMHbie_**ceTH**
11. Настройка IPv6/Teredo в Windows 7, 8: **http://blog.cherepovets.ru/serovds/2011/ll/lS/teredo-win7/**
12. IPv6: здесь и сейчас: **https://xakep.ru/2012/01/09/S8121/**
13. IPv64epe3tunnelbroker.net: **https://version6.ru/he.net/howto**
14. «Отец» криптографии представил «убийцу» Tor: **https://piratemedia.net/otec-kriptografli-predstavil-ubiycu-tor**
15. **Атака посредника: https://ru.wikipedia.org/wiki/ATaKa_nocpeflHHKa**
16. Какова цена анонимности в Сети: **http://samag.ru/archive/article/631**
17. Choose IMAP or POP: **https://help.riseup.net/en/email/clients#choose-imap-or-pop**
18. Удаление файлов в NTFS: **http://interesu.ru/index.php/poleznye-sovety/36S-udalenie-fajlov-v-ntfs**
19. Удаление данных с жестких дисков: **http://www.etegro.ru/articles/secure-disk-erasing**
20. **Утилита восстановления данных с диска: http://www.r-studio.com/ru/**
21. Как стереть данные так, чтобы их не смогли восстановить спецслужбы?: **https://habrahabr.ru/company/storelab/blog/151SS4/**
22. Runtex — система гарантированного уничтожения данных: **http://www.runtex.ru/**

Предметный указатель

o

Oday 456
O-Day 525
O-Hour 525
O-Sec 492, 525

2

2IP, 182

3

3D 525
3О-кинематофаф 525
3О-печать 525
3G 525, 537
ЗвЛЮ-модем 257
3GP 525

4

4G 526, 542
4K UHDTV 526

5

5G 526

6

6to4 526
О механизм 237

8

802.1 la 538
802.1 lac 538
802.1 lad 538
802.11b 538
802.1 In 538
8K UHDTV 526

H

(iTorrent: настройка IPv6/Teredo 237
pTox 147

A

AC3 532
ActiveX 526
AdBlock Plus: блокировщик рекламы 320
Adium 126,166,526
0 добавление аккаунта 168
0 защищенный чат 168
0 настройка 170
0 проверка ключей 169
0 установка 167
Adobe Flash 526
Adobe Reader 526
0 уязвимости 78
Adobe Systems 526
ADSL 526
Adware 71,527
AES 153, 546
AES-шифрование 527
AIM 166
AirDrop 527
Alpha 527
Amazon Web Services 215,527
0 настройка подключения 224
0 регистрация аккаунта 215
0 создание виртуального сервера 218

AN.ON См. Java Anonymous Proxy
Android 527, 536
0 использование PAC-файла 205
0 настройка прокси 194
0 настройка точки доступа 253
0 подмена IP-адресов DNS-сервера 231
0 приватный режим браузера 30
0 уязвимости 78
Anonymous 451
ANSI-графика 527
ANts P2P 262, 527
API 527
App Store 140,149, 527
Apple 527
Apple Safari 527
Apple TV 528
Apple Watch 528
Applet 528
Appz528
apt-get: команда 421
Arduino 528
ARM 528
ARP 546
0 протокол 18,528
ARPANET 528
ARP-спуфинг 18, 528
ASCII 545
ASCII-Art 528
ASCII-графика 466
ASF: формат 528
Atari 528
Audacity 415
AUTHORS: файл 467
Autodesk 529
AVCHD: формат 529
AVI: формат 529

B

BBS 458, 529
Beta 529
BIOS 529
0 модификация 322
0 настройка 343
0 приоритет загрузочных устройств 344
Bitmask 269
Bitmessage 263,529
0 каналы 265
BitTorrent 529
Blackberry 529
0 настройка прокси 195
0 настройка точки доступа 256
0 приватный режим браузера 30
0 удаление cookie-файлов 42
Blackphone 143
BleachBit 85, 86
0 интерфейс 86
0 установка в Linux 86
0 установка в Windows 86
Bluetooth 129,529
0 отслеживание 129
Blu-ray 529
Blu-ray диск: удаление данных 89
bootleg 475
Boundless Informant 529
Brasero 416
Brosix 125
BSOD 530
Buccaneer: операция 495
BUGS: файл 467
Build 530

C

CamRip 462
CAPTCHA 530
CAPTCHA-код 298
C are ware 530
Carnivore 530
CD Key 530
CD-диск: удаление данных 89
Cellcrypt 125
CGI 197, 530
ChangeLog: файл 467
Chaos Constructions 530
ChatSecure 126, 148,530
0 настройка 149
0 общение 151
0 проверка отпечатков 152
0 создание сертификата 150
0 установка 149
Cheat 530
Chrome
0 использование PAC-файла 201
0 настройка I2P 289
0 настройка прокси 189
0 приватный режим 28
0 удаление cookie-файлов 38
Cjdns 268, 530
0 протокол 268
cMix 530
0 протокол 171
Compact Flash 567

Cookie 24, 531
O просмотр 34
O удаление 32
COPYING/LICENSE: файл 467
CORE
O FILEJD.DIZ 465
O NFO-файл 466
CO-TRAVELER 531
Crack 477, 531
CRC Error 531
CRC32 467
CVV: код на карте 25
CVV2 531

D

DCSNet 531
dd: команда 337,338
DDoS-атака 74,531
Debian 552
O операционная система 319
demo 475
Demoware 531
DHCP 532
DHT 532, 546
DiHalt 532
DiskCryptor 9
O установка 10
0 шифрование диска 10
diskpart: утилита 373
diskutil: команда 337
displaydns: команда 179
DIZ 464, 532
DMG: формат 532
DMG-образ 110
DNS 532
DNS-провайдер 226
DNS-сервер 221, 532
0 Google 226, 240
0 подмена IP-адресов в OS X 229
0 подмена IP-адресов в Windows 227
0 подмена IP-адресов на маршрутизаторе 232
Dolby Digital 532
Donationware 532
DOS 532
DoS-атака 532
driver 565
Dropbox 62, 532
Dropmire 532
DSL 546
DTS 533
dubplate 475
DVD-диск: удаление данных 89

E

eBay 533
Echelon 584
Edge: удаление cookie-фашюв 34
Edge 533
eepsite 311, 538
EFI 533
Electron: тип банковской карты 216
Emulator 478
Enigmail
0 в Tails 386
0 настройка 100, 118, 122, 123
0 отзыв ключей 109
0 управление ключами 103
0 установка 117
0 установка в Linux 122
0 установка в Windows 99
EP 474
Ethernet 533,546

F

Facebook 149, 166, 533
0 альтернативные адреса 177
FAQ 533
Fastlink: операция 495
FAT 533
Fedora Core 120
FIDO U2F: стандарт токенов 52
FILEJD.DIZ 464, 534
FileVault 534
Firefox
0 выборочное удаление cookie-фашюв 36
0 использование PAC-файла 200
0 настройка I2P 286
0 настройка прокси 186,188
0 приватный режим 28
0 просмотр cookie-фашюв 35
0 удаление cookie-фашюв 35
Fire Wire 538
Fix 534
FLAC 534
Flash 534
Flash-накопитель 534
0 с биометрической защитой 16
0 с клавиатурой 16
0 с шифрованием 16
0 шифрование данных 16

Flash-память 534
Florence: клавиатура 354
FLV 534
FoxyProxy 534
O настройка 313
Freenet 276, 534
O настройка 276
O принцип работы 275
O просмотр фрисайтов 277
O установка клиента 276
Freeware 535
Frenchelon 535
friGate: расширение для браузера 251
FTP 535, 545
FTP- и HTTP-архивы 486
FTP-сервер 535
O копирование файлов 488
O скомпрометированный 459
FTTx 535

G

Gamez 535
GetDiz: редактор NFO-файлов 465
GIF: формат 535
GIMP 412
Gmail 535
GNOME 353
GnuPG 97, 535
O установка в Linux 120
Gnutella 535
Gold 535
Google 535
0 AdSense 536
0 AdWords 536
0 Analytics 536
0 Chrome 536
0 Docs 62, 536
0 Drive 62, 78, 536
0 Groups 536
0 Hangouts 160,166,536
0 Maps 536
0 Play 140,149, 536
0 Talk 149
0 Переводчик 251
0 Планета Земля 536
Google+ 535
0 альтернативные адреса 177
GPG 535
GPG4Win 97
GPGTools 110
GPRS 536
GPS 130,132, 536
GranitePhone 144
GSM 129, 539
GtkHash 408

H

H.264 536
HDD 536
HDD-диск: удаление данных 88
HDTV 537
HDV 537
HFS 537
HFS+ 537
Hidden Wiki 448
Hide My Phone: приложение 139
hosts: файл 178
Hotspot Shield 18,208
0 настройка 210
0 установка 209
HSDPA 537
HTML 537
HTML5 537
HTML-документ 537
HTTP 537, 545
HTTPS 18, 25, 126,166, 183, 197,380, 537
0 протокол 31
HTTPS Everywhere 20, 31, 320, 381
0 установка 31
Hulu 537
0 обход ограничения 175
Hyperboria 268

I

1 .LINK 538
I2P 267, 538
0 использование в Tails 387
0 консоль управления 283
0 настройка Chrome 288
0 настройка Firefox 286
0 настройка Internet Explorer 285
0 настройка Opera 287
0 настройка Safari 290
0 принцип работы 279
0 проверка работоспособности 291
0 установка клиента 282
12P-сайт 311,538
Icedove 538
0 настройка учетной записи 385
0 программа электронной почты 385
iCloud 15

ICloud 538
ICMP 538
O ошибка доступа 245
ICQ 166, 538
ID 538
IDE 566
IEEE 1394 538
IEEE 802.11 538
IGMP: протокол 538
IMAP: протокол 386, 538
IMEI 129, 539
IMHO 566
IMSI 539
IMSI-кетчер 128
IMSI-ловушка 133, 539
IMSI-ловушки 128
Inkscape 413
INSTALL: файл 467
Internet Explorer
0 InPrivate, режим 27
0 использование PAC-файла 199
0 настройка I2P 285
0 настройка прокси 185
0 приватный режим 27
0 просмотр cookie-файлов 34
0 удаление cookie-файлов 32
0 удаление cookie-фашюв в Windows Phone 41
0 эксплойты 78
iOS 539
0 использование PAC-файла 204
0 настройка прокси 192
0 настройка точки доступа 255
0 подмена IP-адресов DNS-сервера 230
0 приватный режим браузера 29
0 установка пароля 14
0 шифрование данных 14
IP: протокол 539
iPad 539
0 использование PAC-файла 204
0 настройка прокси 192
0 шифрование данных 14
ipconfig: команда 179
iPhone 539,551
0 использование PAC-файла 204
0 настройка прокси 192
0 шифрование данных 14
iPod 539
iPodTouch
0 шифрование данных 14
0 использование PAC-файла 204
0 настройка прокси 192
IPsec 546
0 протокол 539
IPv4 546
0 адресное пространство 235
0 протокол 234, 539
IPv6 546
0 адресное пространство 235
0 настройка 237
0 проверка протокола 247
0 протокол 234, 539
IPv6, протокол 234
IPv6/Teredo
0 настройка 238
0 отключение 244
IP-адрес 540
0 определение 181
0 подмена 184, 234
0 приватный 234
0 публичный 234
IP-пакет 540
IRC 540
0 бот 460
ISO
0 файлы 475
0 формат 540
ISO 9660 540

J

Jabber 152, 540
JAP 540
Java 540
0 виртуальная машина 262,271,282
0 уязвимости 78
Java Anonymous Proxy 270,540
0 JonDoFox 273
0 сравнение аккаунтов 271
0 установка клиента 271
Java Runtime Environment 541
JavaScript 541
JonDoFox: профиль JAP 273
JonDonym 541. См. Java Anonymous Proxy
JPEG 545
0 формат 541
JPG-файл: вредоносный 77

K

Kaspersky Internet Security 25,79
KDE 541

KeePassX 49,405
0 блокировка базы паролей 50
0 группы паролей 49
0 добавление записей 48
0 использование 407
0 использование паролей 50
0 мастер-пароль 47
0 создание базы паролей 405
0 установка 47
Key Emulator 477
Key Generator 541
Keygen 476
Keymaker 476

L

LAN 541
Leeching 541
LibreOffice 41
Li-Fi 541
Linux 541
0 PGP-щифрование 119
0 запись дисков 334
0 создание загрузочного накопителя 338
0 удаление данных 86
Linux Mint 120
live 475
Loader 477
Log-файл 181,541
LOL 542
LP 474
LTE 542
LUKS 542
0 шифрование 365
lulz 542
Lulzsec 451

M

Macintosh 542
MAC-адрес 23,130, 542
0 спуфинг348
MAC-спуфинг 542
Mailnesia.com: сайт 134
Mal ware 542
MAN 542
Matroska 542
Memory Stick 567
microSD 567
Micro-SIM 551
Microsoft Corporation 542
Microsoft Edge 542
Microsoft Internet Explorer 543
MIDI: формат 543
MIME 543
Mini-SIM 551
mIRC 520, 543
Miredo 543
0 протокол 237
Mirror 543
MitM-атака 543
Mixed 475
MKV 543, 549
MMS 543
MMS-сообщения: обеспечение безопасности 125
Monkey's Audio 543
Mozilla Firefox 543
Mozilla Thunderbird 543
MP3 543
MPEG 543
MPEG-1 544
MPEG-4 544
MS-DOS 544
MTProto 544
0 протокол 153
My Space: альтернативные адреса 177

N

Nano-SIM 551
Naruslnsight 544
NAT 544
0 механизм 234
nautilus: команда 366
Nautilus
0 затирание свободного места 404
0 файловый менеджер 357
NetBIOS
0 протокол 544
NFO 464
0 формат 544
NFO-файл 465, 467
NoCD 478
NoDVD 478
NoScript: дополнение 320, 383
nslookup: команда 178
NTFS 544
Nukenet: сеть пре-релизов 492

O

OEM 545
Offline: режим 545

OGG: формат 545
Onion-сайт 311, 545,563
Online 545
Опух 545
OpenPGP
O апплет 354,396
O шифрование и подпись сообщения с помощью открытого ключа 398
O шифрование сообщения с помощью пароля 396
Opera 545
O использование PAC-файла 202
0 настройка I2P 287
0 настройка прокси 188,201
0 приватный режим 28
0 режим Turbo 248
0 удаление cookie-файлов 37
OS X 545
0 PGP-шифрование 110
0 запись дисков 334
0 подмена IP-адресов DNS-сервера 229
0 создание загрузочного накопителя 336
0 удаление данных 85
0 управление паролями 47
OSI: сетевая модель 545
OST 546
Ostel 125
OTR 546
0 модуль 164
0 настройка модуля 164
0 протокол 151,159, 167, 384

P

Pandora.com 546
O получение доступа 213,311
PARADOX: варезная группа 546
Patch 477, 546
PayPal 25, 546.
PDF-файл: вредоносный 77
Perfect Dark 265, 546
PGP 547
PGP/MIME 101,123
PGP-шифрование 92
O в Linux 119
0 **B**OSXIIO
O в Windows 97
O метаданные 95
O отзыв ключей 109
O поиск ключей 105
O расшифровка 109
O резервные копии ключей 114
O создание ключей 111
O шифрование сообщений 107,114
PHP 547
Pidgin 126,159, 547
O добавление контактов 163
O запуск в Tails 383
O общение в защищенном режиме 165
O создание учетной записи 162
O установка в Linux 161
O установка в Windows 160
O уязвимости 160,167
ping: команда 243
PING 547
Pinger: сайт 138
PirateBrowser 311,313,547
O настройка 313
Pitivi 417
Plug and Play 547
Plug-in 547
POP: протокол 386,547
Porn ware 71
PPP 546
O протокол 547
PPPoE: протокол 547
P re-Alpha 547
PRISM 547
Private Wave 125
promo 475
Psiphon 269, 548
Pub 548
Push: технология 548
PuTTY 221
PuTTY Key Generator 221
O генерация ключей 221

Q

qTox 146
0 Tox ID 148
O добавление,друзей 148
O интерфейс 147
O локализация 148
QuickTime 548

R

Radium: варезная группа 548
Ransomware 548
RAR-архив: вредоносный 77
Raspberry Pi 548

Razor 1911
O варезная группа 548
RC548
README: файл 467, 548
RealMedia 548
Red Hat 120
Red Onion: браузер для iOS 310
Regfile 477
RegFile 548
Release Group 549
Remux 549
Resume 549
Retail 549
RetroShare 267, 549
0 добавление друзей 297
0 настройка подключения 295
0 обмен файлами 294
0 общение 293
0 поиск файлов 3, 303,315,329, 374, 389, 409,419,444,455, 511,519, 524, 586
0 принцип работы 292
0 создание личности 301
0 чаты 301
rfkill: команда 437
Rip 549
Riskware 72
RLOGIN 549
Root 549
RSA 153, 546, 549
RSS-канал 549
RTM 550

S

Safari
0 использование PAC-файла 203
0 настройка I2P 290
0 настройка прокси 191
0 приватный режим 29
0 удаление cookie-файлов 40
0 удаление cookie-фаШюв в iOS 41
Safehaven: операция 495
Score 475
Scribus 413
0 поддержка кириллицы 414
SD-карта 550
0 удаление данных 90
Secure Digital 567
Serial 476,550
Service Pack 550
SFV: формат 550
SFV-файл 467
Shareaza: клиент 266
Shareware 550
Signal 125, 140, 550
0 зашифрованная голосовая связь 141
0 зашифрованные сообщения 141
0 установка 140
Silent Phone 125, 171
Silk Road 451,550
SIM-карта 539, 550
Single 475
Site Down: операция 495
SKad 546
Skype 551
SMP-ATJIAC/2: смартфон 146
SMS 551
SMS-сообщения
0 анонимные 136
0 для подтверждения аутентификации 53
0 обеспечение безопасности 125
0 платные 75
SMTP 545
0 протокол 551
SOCKS 197
0 протокол 551
SP475
SpeedTest 551
0 сайт 521
SpiderOak: облачное хранилище 145
Spyware 551
SSD 579
SSD-диск: удаление данных 90
SSH
0 протокол 551
0 настройка туннеля 218
SSID 23,551
SSL 20
0 протокол 552
0 соединение 19
SSTP: протокол 213,214, 552
Stealthphone 142
sudo: Тция команды 337

T9 552
Tails 319, 330, 375, 390,410,420, 543, 552
0 Pidgin 383
0 Tails Installer 339
0 Tor Browser 379

O автономный режим 352
O активация Bluetooth 437
O безопасное стирание 371
O бесследное удаление файлов 403
0 виртуальная клавиатура 354,391
0 включение I2P 346
0 выбор носителя 331
0 доступ к FTP-серверу 436
0 доступ к жесткому диску 391
0 доступ к локальным сетям 436
0 завершение работы 370
0 запись носителя 332
0 запуск 343
0 запуск в виртуальной машине 422
0 запуск терминала суперпользователя 356
0 зашифрованное хранилище 357
0 защита пользователя 327
0 значки рабочего стола 356
0 интерфейс 352
0 использование I2P 327
0 использование зашифрованного хранилища 363
0 использование мостов Tor 351
0 использование сети I2P 388
0 меню Места 353
0 меню Приложения 353
0 меню специальных возможностей 354
0 меню управления компьютером 355
0 навигационная панель 352
0 настройки зашифрованного хранилища 359
0 настройки подключения к сети 351
0 Небезопасный браузер 376
0 обновление 340
0 обработка графических файлов 412
0 основа 319
0 отображение Flash-анимации 442
0 параметры загрузки 346
0 перенос зашифрованного хранилища 365
0 печать 418
0 подключение беспроводных устройств 436
0 подключение к сети 375
0 проблемы безопасности 322
0 работа с документами 410
0 регистрация на порталах перехвата 376
0 решение проблем 438
0 решение проблем запуска 369
0 сканирование 418
0 скачивание дистрибутива 330
0 скачивание торрентов 443
0 скачивание файлов с локального веб-сайта 436
0 смена загрузчика 440
0 создание зашифрованного хранилища 358
0 сокрытие использования 323,328
0 состав 320
0 спуфинг MAC-адресов 349
0 удаление зашифрованного хранилища 369
0 управление мультимедийными данными 415
0 управление файлами и папками 356
0 установка пароля администратора 348
0 шифрование текста 396
Tails Greeter: окно 347
Tails Installer
0 инструмент 342
0 обновление Tails 342
Tails Upgrader: инструмент 341
TCP 545
0 протокол 552
TCP/IP
0 протокол 544
0 стек протоколов 552
Telegram 152,552
0 общение 155
0 самоуничтожение сообщений 158
0 секретный чат 157
0 удаление аккаунта 159
0 установка русского языка 153
TELNET 552
Tempora 552
Teredo
0 настройка 237
0 протокол 236,553
THANKS: файл 467
The Pirate Bay 553
THG: варезная группа 553
Thunderbird
0 настройка 120
0 настройка PGP 101,123
0 настройка аккаунта электронной почты 98,116,121
0 установка в Linux 120
0 установка в OS X 115
0 установка в Windows 97
0 установка дополнений 100
0 шифрование сообщений 119

Thunderbolt 553
THX 553
TLS 553
TMSI 128, 553
TopSec Mobile 143
Tor 3, 270, 553
0 изменение маршрута 315
0 использование мостов 351
0 карта сети 378
0 луковая маршрутизация 270, 305
0 принцип работы 270, 304,306
0 проблемы производительности 388
0 смена личности 382
0 сокрытие использования 323
0 структура пакета 305
0 управление с помощью Vidalia 377
0 установка 309
Tor Browser 320,379,553
0 AppArmor 379
0 смена личности 310
0 установка 309
Tor Messenger 172
TorBirdy: дополнение 387
Torbutton 320,381
torrent-файл: вредоносный 77
Tox 146, 553
Trainer 478, 553
Traverso 417
Trialware 553
tribute 475
Tunlr: сайт 226
Tunnelbroker.net: сайт 245

Ubuntu 120
UDF 554
UDP 545
0 протокол 554
UDP-дейтаграмма 237
UEFI 554
UltraSurf 184
UMTS 537, 539, 554
Universal USB Installer 336
UNIX 554
Upload 554
UPnP 554
USB 78, 546, 554
USB-адаптер Bluetooth 252
USB-адаптер Wi-Fi 252
Usenet 536, 554

V

VA475
Various Artists См. VA
Viber 153, 554
Vidalia 377, 555
0 смена личности 379
VirtualBox 422,555
0 запуск виртуальной машины 425
0 настройка виртуальной машины 424
0 создание виртуальной машины 423
0 установка 423
VMware Workstation Player 423,555
0 запуск виртуальной машины 429
0 настройка BIOS виртуальной машины 429
0 настройка виртуальной машины 427
0 подключение USB-накопителя 428
0 создание виртуальной машины 426
0 установка 425
VOB: формат 555
VoGSM 142
VoIP 555
VoIP-сервис 146
VPN 18, 555
0 сети 207
VPN-туннель 19
0 настройка 213
VPN-шлюз 207
Vuvuzela 172, 555

UW

Wallpaper 555
WAN 555
Warez 555. См. Варез
0 Oday 460
0 apps460
0 crack 477
0 cracks 460
0 dox 461
0 eBooks 461
0 emulator 478
0 FILEJD.DIZ 464
0 FixedExe 461
0 games 461
0 INSTALL 467
0 key emulator 477
0 keygen 476
0 key gens 461

O кеутакег47б
O loader 477
O movies 461
O тр3 461
O MVids 461
O NFO-файл 465
O NoCD 461,478
O NoDVD 461,478
O Nuke 468,492
O patch 477
O portables 461
O PROPER 492
O README 467
O regfile 477
O REPACK 492
O RIP 461
O scripts 461
O serial 461,476
O SFV-файл 467
O subs 461
O templates 461
O trainer 478
O TV-Rip 461
O XXX 461
O архивация 464
O имена файлов 464
O обозначения 463
O пре-релиз492
O преследование по закону 479
O релизы софта 475
O русификатор 478
O создание релизов 492
O форматы 463
wkV: формат 555
WebMoney 555
O кража 75
Web-сайт 555
Web-сервер 556
WEP556
Whatcd 520, 556
O получение инвайта 520
What's new: файл 467
WhatsApp 17,153
Wi-Fi 556, 561
O SSID23
O безопасность использования 17
O вардрайвинг 20
O. дефолтные пин-коды WPS 20
O настройка алгоритма шифрования 22
O отслеживание 129
O перехват трафика 18
O подмена точки доступа 19
WiMAX 556
Windows
O PGP-шифрование 97
O запись дисков 332
O подмена IP-адресов DNS-сервера 228
O создание загрузочного накопителя 335
O удаление данных 86
O управление паролями 47
Windows 10 Mobile 556
Windows Live Messenger 166
Windows Media Audio
O формат 556
Windows Media Video: формат 556
Windows Mobile 556
Windows Phone 556
O настройка прокси 193
O настройка точки доступа 254
WMA: формат 556
WMV: формат 556
WPA556
O WPA2 22
WPS 557
O пин-коды 20
WWW 557

X

X-Keyscore 557
XML: формат 557
XMPP 152,160,166
O протокол 557
Xvid: формат 557

Y

Yahoo! Messenger 166
YouTube: альтернативные адреса 177

Z

ZenMate, расширение для браузера 211
O смена страны 213
O установка 211,213
Zyxel Keenetic
O настройка ICMP 246
O подмена IP-адресов DNS-сервера 232
O шифрование Wi-Fi-сети 23

А

Аватар 558
Авторинг 558
Администратор 558
Аккаунт 526, 558
Альфа 558
Анализатор трафика 558
АНБ 558
Анлим 558
Анонимайзер 180, 181, 199, 558
0 использование 182
0 цепочка 197
Анонимная сеть 261
0 ANts P2P 262
0 Bitmessage 263
0 Cjdns 268
0 Freenet 265,275
O Gnutella 265
O I2P 267, 278
O Java Anonymous Proxy 270
0 Perfect Dark 265
0 Psiphon 269
0 RetroShare 267,292
0 Tor 304
O гибридная 267
O децентрализованная 262
Антивирус 558
Антивирусная программа 79
O бесплатные программы 81
0 сравнение цен 80
Апгрейд 558
Апдейт 558
Апплет 558
Атака методом холодной перезагрузки 559
0 предотвращение 409
Атака посредника 95,323,559
0 схема 324
Атаки целевые 76
Аутентификация
O двухфакторная 43, 51, 60
O многофакторная 43, 51, 60
0 электронной почты 63

Б

Баг 77, 559
База данных 559
Базовая станция 559
Байт 559
Бан 559
Банковские данные: кража 75
Баннер 559
Безопасность
0 личные данные 134
0 фильтрация трафика 24
Бернерс-Ли, Тим 559
Бесплатный Wi-Fi 17
Бета 559
Билд 559
Биометрическая защита 559
Бит 559
0 в секунду 559
Биткоин 453, 560
0 обмен 387
Битрейт 560
Блокировка сайта: определение типа блокировки 269
Бод 560
Боксы
0 настройка виртуальной машины 430
0 программа виртуализации 423
0 создание виртуальной машины 429
0 установка 429
Ботнет 74, 560
Брандмауэр 561,571
0 включение в OS X 19
0 включение в Windows 19
Браузер 561
0 приватный режим 26
Буфер обмена 561
Бэкдор 561

В

Вардрайвинг 20, 561
Варез 456, 561,555
0 NFO-файлы 465
0 инструменты взлома 476
Варезная группа 495,561
0 aPOCALYPSE PRODUCTION cREW 496
O C.O.R.E. 496
0 Centropy 495,497
0 CLASS 497
0 DEViANCE 498
0 DrinkOrDie 498
0 Echelon 500
0 FaiRLiGHT 500
O HYBRID 501
0 INC501

O Kalisto 501
0 LineZerO 502
O MYTH 502
O PARADOX 503
O Rabid Neurosis 504
O Radium 504
O Razor 1911 504,512
O Reloaded 505
O RiSCiSO 506
O SKIDROW 506
O SKIDROW 494
O Superior Art Creations 506
O THG 465, 508, 512
O Tristar and Red Sector Incorporated 509
0 United Software Association 510
O курьеры 495
O релизеры495
Варезные сайты 482
O аккумулирующие ссылки 483
O инструменты взлома 483
O опасности 479
O форумы 485
Веб-камера 561
Веб-обозреватель 561
Векторное изображение 562
Взлом 562
Виджет 562, 563
Винлокер 562
Виртуальная машина 562
Виртуальный сервер 562
Вирус 64, 562
0 загрузочного сектора 65,563
0 загрузочный 566
0 макровирус 65
0 онлайн-проверка 63
0 скрипт 65
ВКонтакте
0 фишинговый сайт 55
0 альтернативные адреса 177
Вредоносные программы
0 вирусы 64
0 действия при обнаружении 84
0 защита 77
0 индикатор взлома 83
0 проверка онлайн 82
0 программы-вымогатели 76,457
0 троянские программы 66
0 черви 65
Всемирная паутина 557,563,566
Выделенный сервер 563

Г

Гаджет 563
Гигабайт 563
ГЛОНАСС 132, 563
Глубинная паутина 447, 563
Глюк 563
Голосовая связь: шифрование 140
Голосовые вызовы: обеспечение безопасности 125
Гостевая книга 563
Графический объект 563

Д

Данные
0 надежное удаление 401
0 удаление с жесткого диска 85
Даркнет 447,564
0 Black Death 452
0 Silk Road 451
0 анонимная мобильность 448
0 аудитория 447,449
0 Биткоин 453
0 Доджкоин 453,565
0 криптовалюты 453
0 Лайткоин453
0 получение доступа 448
0 реакция властей 447,454
0 черные рынки (маркеты) 451
Дата-центр 564
Движок 564
Двухфакторная аутентификация
См. Многофакторная аутентификация
0 в Thunderbird 99,117,122
Девайс 564
Дейтаграмма 564
Демо 564
Демомейкер 564
Демонстрационная версия 564
Демосцена 564
0 Aces of ANSI Art 513
0 ANSI-графика 514
0 ASCII-Art 512
0 ASCII-игры 513
0 Chaos Constructions 516
0 chiptune 517
0 DiHalt 516
0 Farbrausch 519
0 Razor 1911 516
0 Roguelike 513

Демосцена *(прод.)*
O United Force & Digital Dynamite 519
O демо 517, 518
O Звездные войны 513
O интро 517
O мегадемо518
O трекерная музыка 514
O трекеры 515
Демотиватор 564
Дентро 564
Диалап 564
Динамический IP-адрес 564
Дистрибутив программы 565
Диффи-Хеллмана
O метод 153
O протокол 157,565
Доджкоин 453, 565
Домен 565
Доменное имя 565
Драйвер 565
Дроппер 565

Ж

Жесткий диск
O с биометрической защитой 17
O с клавиатурой 17
O с шифрованием 17

З

Зависание 565
Закладка 566
Зеркало сайта 543
Зеттабайт 566

И

Идентификатор 538
ИМХ0 566
Инвайт 566
Инкапсуляция 566
Инсталляция: программы 566
Интегрированная среда разработки 566
Интернет 566
Интернет-банкинг 75, 566
Интернет-мем 567
Интернет-шлюз 567
Интро 567

И

Йотгабайт 567

К

Кардридер 567
Карта памяти 567
Кейлогер 567
Киберпреступность 73
Киберсквотгинг 568
Кибершантаж 75
Килобайт 568
Ключ
O восстановления в ОБ X 13
O закрытый 91
O открытый 91
O шифрования 568
° длина 112
Кодек 568
Коллизии 568
Коммуникации: обеспечение безопасности 124
Коммутация 1P-пакетов 568
Коммутируемый доступ 568
Компрометация 568
Консорциум Всемирной паутины 568
Контейнер 568
Контент 568
Криптовалюта 447,453, 568
O Биткоин453
O Доджкоин 453,565
O Лайткоин453
Крэк 569
Крэкер 569
Крэктро 569
Курсор 569
Кэш 569

Л

Лайткоин 453,569
Ламер 569
Логин 569
Логическая бомба 569
Луковая маршрутизация 305, 569

М

Макровирус 570
Макрос 570
Маркет 570
Маршрутизатор 570
Маршрутизация
0 луковая 305, 569
0 чесночная 281, 583

Маска подсети 570
Мастер-пароль 570
Мгновенные сообщения: обеспечение безопасности 126
Мегабайт 570
Мегадемо 570
Межсетевой экран 570
Менеджер виртуальных машин 423,431
0 настройка виртуальной машины 434
0 создание виртуальной машины 432
0 установка 432
Метаданные 95,127,571
0 в Tails 411
0 документов 325,411
Многофакторная аутентификация 43, 51, 60,571
0 настройка 51
Модем 571
Модератор 571
Мой мир: альтернативные адреса 177
Мошенничество 56
Мультики by ArjLover 486
0 подмена расширений файлов 486
Мультфильмы: просмотр в Интернете 486
Мэйнфрейм 571

Н

Найти iPhone: функция 15, 133
Накопитель
0 размагничивание 402
0 уничтожение 402
Небезопасный браузер 436
Ник 571
Нюк релизов 571

О

Облачное хранилище данных 571
Обмен сообщениями: шифрование 146
Обратная разработка 572
Обход ограничений 181
Обход сети: метод 266
Общий доступ к файлам: отключение 19
Оверпостинг 572
Одноклассники.ги: альтернативные адреса 178
Одноранговая сеть 572
Окно всплывающее 547
Олдскул 572
Операционная система 572
Определение IP-адреса 181
Определение местонахождения 128
Оффтоп 572

П

Пароль
0 выбор надежного 43
0 мастер-пароль 45
0 наиболее распространенные 21
0 синхронизация 46
0 установка в iOS 14
Пасскей 572
Патч 546
Персональные данные: защита 24
Песочница 572
Петабайт 573
Пиксел 573
ПИН-код 217, 573
Пир 572, 573
Подпись электронная 93
Подсеть 573
Полиморфизм компьютерного вируса 573
Порт 573
Портал 573
Пост 573
Приватный режим браузера 573
Провайдер 573
Программа троянская 580
Программное обеспечение 573
0 история пиратства 458
0 фейковый релиз 458
Программы-вымогатели 75
Прокси-сервер 574
Протокол 574
Прошивка 574

Р

Радиорелейная связь 574
Развертка 574
Размагничивание накопителя 402
Разрешение 574
Распределенные сетевые атаки 74
Рассылка почтовая 573
Растровое изображение 574
Реавторинг 574
Редактор локальной групповой политики 239
0 настройка 241
Реестр 574
0 Windows: редактирование 239

Резидентная программа 575
Рейтинг 575
Релиз 575
О сырой 579
Рип 549
Роуминг 575
О внутрисетевой 575
О международный 575
О национальный межсетевой 575
Рунет 575
Русификатор 478
Руткит 70, 575

С

Сабж575
Сайт: зеркало 566
Свободное пространство: очистка 88
Секвенсор 575
Сервер 576
0 открытых ключей 96
серийный номер 550
Сертификат отзыва 109,114
Сетевая плата 576
Сетевой
0 адрес 576
0 интерфейс 576
0 коммутатор 576
0 концентратор 576
0 маршрутизатор 576
0 мост 576
0 повторитель 576
0 сканер 17, 577
0 шлюз 577
Сеть
0 смешанная 578
0 туннелирование 208
Сжатие
0 без потерь 577
0 с потерями 577
Сидер 577
Синий экран смерти 530,565
Синхронизация 577
Система управления базами данных 577
Сканер портов 577
Скриншот 577
Скрипт 578
Смайлик 578
Сниффер 558, 578
Сноуден Эдвард 578
СОРМ 578
Сотовая связь
0 обеспечение безопасности 124, 127
0 прослушивание 132
Сотовый телефон
0 анализ данных 133
0 заражение 133
0 одноразовый 131
0 прослушивание защищенных моделей 146
Софт 578
Социальные сети: IP-адреса 176
Спам 73, 75, 578
0 борьба со спамом 59
Сплиттер 578
Спонсор 579
Спуфинг MAC-адресов 348
Стек протоколов 579
СУБД 577
Суперпользователь 549
Сцена 490
0 crack 477
0 emulator 478
0 FILEJD.DIZ 464
0 INSTALL 467
0 key emulator 477
0 keygen 476
0 keymaker476
0 loader 477
0 NFO-файл 465
0 NoCD 478
0 NoDVD 478
0 Nuke 468,492
0 patch 477
0 PROPER 492
0 README 467
0 regfile 477
0 REPACK 492
0 serial 476
0 SFV-файл 467
0 trainer 478
0 warez463
0 архивация 464
0 варезная 579
0 демопати512
0 демосцена512
0 имена файлов 464
0 интро 512
0 курьеры 495
0 обозначения вареза 463
0 пре-релиз492

O развитие 491
O релизная группа 495
O релизы софта 475
O сайт 491
O система кредитов 494
O создание релизов 492
O стандарты 463
O топ-сайты 494
O трекерная музыка 512
O форматы 463
Сырой релиз 579

Т

Твердотельный накопитель 579
Тег 579
Текстро 579
Терабайт 579
Терминал в Linux 120
Тип файла 579
Токен 580
O безопасности 51
Топик 580
Топ-сайт 580
Торрент 580
Трафик 580
Трейнер 553
Трекер 580
Трекерная музыка 580
Трекмо 580
Троллинг 580
Троянская программа 66,580
Туннельный брокер 244, 581
0 настройка 244

У

Уведомление о недоверенном соединении 324
Удаление данных 86
0 ограничения 88
0 с Flash-накопителей 90
0 с SD-карт 90
0 с SSD-накопителей 90
0 с оптических дисков 89
Узел сети 581
Утилита 581
Учетная запись пользователя 581
Уязвимость 77, 581

Ф

Файл
0 безвозвратное удаление 87
0 бесследное удаление 403
Файловая система 581
Файловый вирус 581
Файрволл 571
Фишинг 54, 75,180,582
0 защита 62
0 классический 55
0 примеры 55
0 советы 58
Фишинговые сайты 180
Флейм 582
Флуд 582
Форум 582
0 варез 485
Фотожаба 5 82
Фрисайт 582
Функция File Vault 11
0 включение 12
0 отключение 13

Х

Хаб 582
Хакер 582
O белая шляпа 582
0 классификация по шляпам 449
0 серая шляпа 582
0 скрипт-кидди 582
O черная шляпа 582

Хакинг 583
Холивар 583
Хост 583
Хостинг 583

Ч

ЧАВО 533
Чат 583
Червь 583
Чесночная маршрутизация 281, 583
Чиптюн 583
Чит 530
Читер 583

Ш

Шапка 584
Шифрование 8,91,584
0 AES 16
0 DiskCryptor 9
0 FileVault 11
O Flash-накопитель 16
O PGP92
O в iOS 14
O в OS X I I
O в Tails 325
O в Windows 9
O документов 325'
O закрытый ключ 91
O метаданные 95
O открытый ключ 91
O отпечатки ключей 92
O раздела диска 391
O с открытым ключом 92
O сертификат безопасности 91
O сквозное 124,577
O электронная подпись 93

Э

Экзабайт 584
Экранка 462
Эксплойт 68,584
Электронная подпись 93
Электронная почта 584
O анонимная 134
O аутентификация 63
O временная 134
O обеспечение безопасности 126
Электронные библиотеки 488
Эмотикон 584
Эмулятор 584
Эшелон: система разведки 584

Ю

Юникод 584

Я

Яндекс: Переводчик 251
Яндекс.Браузер: Турбо-режим 249
Яндекс. Деньги 584
O кража 75
Яндекс.Диск 62, 104,585
Ячеистая сеть: топология 268
Ячеистая топология 585

ИСКУССТВО ЛЕГАЛЬНОГО, АНОНИМНОГО И БЕЗОПАСНОГО ДОСТУПА К РЕСУРСАМ ИНТЕРНЕТА



Райтман Михаил Анатольевич, журналист и системный администратор, в прошлом главный редактор издательства компьютерной литературы. Имеет богатый опыт эксплуатации и настройки операционных систем Windows, OS X, Linux, Android, iOS, Windows Phone, а также различного программного обеспечения. Автор и переводчик множества книг и статей по программному обеспечению.

- Защита персональных данных в Интернете
- Создание надежных паролей и защита от злоумышленников
- Бесследное удаление данных с носителей
- Приватный обмен информацией
- Основы шифрования и прочих методов конспирации
- Работа в анонимных сетях I2P, RetroShare, Tor и других
- Доступ к onion-ресурсам
- Полная анонимность и защита с помощью Tails
- Способы доступа к заблокированным ресурсам, таким как Pandora и Hulu
- Получение инвайтов в закрытые сообщества, такие как What.cd
- Даркнет: скрытые ресурсы Интернета
- «Варезная» сцена: все, что вы хотели знать о ней
- Демосцена: компьютерное искусство
- Краткий словарь компьютерного сленга и терминов

В ваших руках уникальная книга, аналогов которой нет! Прочитав ее, вы научитесь защищать свои персональные данные от попадания в руки злоумышленников. Вы разберетесь, почему важны надежные пароли и двухфакторная аутентификация, а также зачем рядовому пользователю использовать шифрование. Вы освоите приемы конспиративного общения по защищенным каналам связи и погрузитесь в анонимные сети, такие как I2P RetroShare, Tor и др., о существовании которых могли и не подозревать. Поймете, чем плох или хорош Даркнет — подводная часть Интернета, научитесь анонимно и не оставляя следов работать на любом компьютере с помощью операционной системы Tails.

В качестве бонуса познакомитесь с андеграундом Интернета — «варезной» сценой и узнаете, что хакеры могут не только взламывать, но и творить — этому посвящено приложение о компьютерном искусстве (демосцене). На примере музыкального комьюнити What.cd разберетесь, как получать инвайты в закрытые сообщества. Если же какой-то из терминов покажется непонятным, в конце книги вы найдете краткий глоссарий не только компьют менных сленгов

SCAN IT!
1073795718
в приложении OZON.ru

bhv®

БХВ-ПЕТЕРБУРГ
191036, Санкт-Петербург, Гончарная ул., 20
Тел.: (812) 717-10-50, 339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

ISBN 978-5-9775-3745-2