

О.В. Задерейко, О.В. Троянський, Р.І. Чанишев

КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАХИСТУ НОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

МОНОГРАФІЯ

КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАХИСТУ НОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

Міністерство освіти і науки України
Одеський національний політехнічний університет

О.В. Задерейко, О.В. Троянський, Р.І. Чанишев

**КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАХИСТУ
ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ**

Монографія

Одеса
Фенікс
2018

УДК 621.396.969.3

З 15

Рекомендовано до видання Вченою Радою Одеського національного
політехнічного університету. Протокол № 12 від 27.06.2017 р.

Рецензенти:

С.А. Положаєнко, доктор технічних наук, завідувач кафедри комп'ютеризованих систем управління Одеського Національного політехнічного університету;

В.Я. Чечельницький, доктор технічних наук, завідувач кафедри інформаційної безпеки Одеського національного політехнічного університету;

О.С. Мельничук, доктор юридичних наук, доцент кафедри загальнотеоретичної юриспруденції Національного університету «Одеська юридична академія».

З 15 Задерейко О.В.

Концептуальні основи захисту інформаційного суверенітету України :
монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев. – Одеса : Фенікс,
2018. – 112 с.

ISBN 978-966-928-237-8

У монографії розглянуті питання захисту інформаційного суверенітету України в умовах реалізації її стратегічного курсу на інтеграцію у світовий інформаційний простір. Проаналізовано сучасні тенденції зламу традиційного та інформаційного суверенітетів держави, які становлять приховану загрозу втрати державного суверенітету, а також правові аспекти захисту інформаційного суверенітету України з позицій діючого законодавства. Розглянуто сучасні умови та існуючі технології інформаційного впливу на громадян держави, які цілеспрямовано впроваджуються у суспільство з метою зламу інформаційного суверенітету держави. Запропоновано структуру захисту інформаційного та цифрового суверенітетів держави, впровадження якої забезпечить захист державного суверенітету України.

Монографія рекомендована для використання у вищих навчальних закладах, які готують фахівців за спеціальностями 125 - "Кібербезпека", 122 - "Комп'ютерні науки", 172 - "Телекомунікації та радіотехніка" (спеціалізація "Безпека інформаційних і комунікаційних систем"), а також фахівцям, які пов'язані зі створенням, експлуатацією та захистом інформаційних систем.

ISBN 978-966-928-237-8

© О.В. Задерейко, О.В. Троянський,
Р.І. Чанишев, 2018

ЗМІСТ

ЗМІСТ.....	3
ПЕРЕДМОВА.....	5
1. ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ.....	7
1.1. БАЗОВІ ЗАСАДИ ТРАДИЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ.....	7
1.1.1. КОНЦЕПЦІЯ ТРАДИЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ	7
1.1.2. ЗЛАМ ТРАДИЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ.....	7
1.2. ОСНОВИ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ І ЇХ ТЕНДЕНЦІЇ.....	8
1.2.1. ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ТА ЙОГО СКЛАДОВІ	8
1.2.2. МЕДІЙНА ІНФРАСТРУКТУРА ДЕРЖАВИ	9
1.2.3. ЦИФРОВИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ І ЙОГО СКЛАДОВІ.....	10
1.2.4. ПРИЗНАЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ	10
1.2.5. СКЛАДОВІ ЦИФРОВОГО СУВЕРЕНІТЕТУ.....	10
1.2.5. ЗЛАМ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ.....	11
1.2.6. РУЙНУВАННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ	11
1.3. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ	11
1.3.1. РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ (РНБО)	17
1.3.2. ДОКТРИНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ	19
1.3.3. СТРАТЕГІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ.....	20
1.3.4. ОРГАНИ, ЩО ЗАБЕЗПЕЧУЮТЬ ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ УКРАЇНИ	22
1.3.5. ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ.....	22
1.3.6. МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ	23
1.3.7. НАЦІОНАЛЬНА КОМІСІЯ, ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ (НКРЗІ).....	24
2. КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА ДЕРЖАВИ.....	26
2.1. КІБЕРПРОСТІР (ЦИФРОВИЙ ПРОСТІР) ДЕРЖАВИ	26
2.1.1. КІБЕРПРОСТІР І РЕАЛЬНА ГЕОГРАФІЯ	28
2.1.2. НАВІГАЦІЙНА ПЛАТФОРМА КІБЕРПРОСТОРУ	28
2.1.3. КАРТОГРАФУВАННЯ КІБЕРПРОСТОРУ	28
2.1.3. РІВНІ ЦИФРОВОГО ПРОСТОРУ (КІБЕРПРОСТІРУ).....	30
2.2. СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ.....	31
2.3. КІБЕРВІЙНА, КІБЕРЗБРОЯ ТА ОРГАНІЗАЦІЯ КІБЕРВІЙСЬК ДЕРЖАВИ	34
2.3.1. ВІДМІТНІ ОСОБЛИВОСТІ КІБЕЗБРОЇ	36
2.3.2. КІБЕРПРОСТІР, ЗОСЕРЕДЖЕНИЙ НА ЗВ'ЯЗКУ	37
3. ЗАХИСТ ІНФОРМАЦІЙНОГО І ЦИФРОВОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ	39
3.1. КОНТРОЛЬ І ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ У ЦИФРОВОМУ ПРОСТОРІ	39
3.2. ІНФОРМАЦІЙНИЙ "ЩИТ" ДЕРЖАВИ	44
3.2.1. ЗАСОБИ КОНТРОЛЮ "МАЛОГО ІНФОРМАЦІЙНОГО ЩИТА":.....	44
3.2.2. ЗАСОБИ ВПЛИВУ "МАЛОГО ІНФОРМАЦІЙНОГО ЩИТА":	45
3.3. ВПРОВАДЖЕННЯ СОРЗ.....	45

3.3.1. КОНТРОЛЬ ЗАШИФРОВАНИХ МЕТАДАНИХ	48
3.3.2. ДЕПОНУВАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ.....	49
4. ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ДЕРЖАВИ	51
4.1. ВІРУСНЕ ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ	51
4.2. ІНФОРМАЦІЙНІ ВІРУСИ, ЇХ ІНДУСТРІЯ І КОНВЕРСІЯ	52
4.2.2. ОСОБЛИВОСТІ УРАЖЕННЯ ГРОМАДЯН ІНФОРМАЦІЙНИМ ВІРУСОМ	52
4.2.3. ІНФОРМАЦІЙНИЙ ВІРУС І ЙОГО ВЛАСТИВОСТІ	53
4.2.4. СТРУКТУРА ІНФОРМАЦІЙНОГО ВІРУСУ	55
4.2.5. АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ВІРУСУ ВІД АНТИВІРУСУ	56
4.2.6. ІНФРАСТРУКТУРА ІНДУСТРІЇ ІНФОРМАЦІЙНИХ ВІРУСІВ.....	57
4.2.7. КОНВЕРСІЯ (МОНЕТИЗАЦІЯ) ІНФОРМАЦІЙНИХ ВІРУСІВ	60
4.3. УРАЗЛИВІСТЬ ГРОМАДЯН ПЕРЕД ІНФОРМАЦІЙНОЮ ДІЄЮ	62
5. ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ДЕРЖАВИ	63
5.1. ПЕРЕДУМОВИ ДЛЯ НАДАННЯ ІНФОРМАЦІЙНИХ ДІЙ.....	63
5.2. СПОСОБИ МАНІПУЛЮВАННЯ ІНФОРМАЦІЄЮ	65
5.2.1. ВИДИ І ПРИЙОМИ СПОТВОРЕННЯ ІНФОРМАЦІЇ.....	65
5.3. ФЕНОМЕН КЛІПОВОГО МИСЛЕННЯ	70
5.3.1. НЕГАТИВНИЙ ВПЛИВ КЛІПОВОГО МИСЛЕННЯ	72
6. ЗАХИСТ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ ТА ГРОМАДЯН	75
6.1. ЗАХИСТ ГРОМАДЯН ВІД ІНФОРМАЦІЙНОЇ ДІЇ.....	75
6.1.1. ХАРАКТЕРНІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ПОРАЗКИ	75
6.2. ЗАХИСТ ВІД ШКІДЛИВОЇ ІНФОРМАЦІЙНОЇ ДІЇ.....	76
6.3. ОРГАНІЗАЦІЯ СИСТЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВІРУСАМ	77
6.4. ЗАХИСТ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ГРОМАДЯН	78
6.4.1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТЕОРІЇ СТРУКТУРИЗАЦІЇ ЗНАНЬ	79
6.4.2. СИСТЕМА ЗНАНЬ ГРОМАДЯНИНА.....	79
6.4.3. МОДЕЛЬ ФОРМАЛІЗАЦІЇ ПІЗНАННЯ ГРОМАДЯНИНА	83
7. ЗАХИСТ СУВЕРЕНІТЕТУ ДЕРЖАВИ В ЕПОХУ КОНСЦІЄНТАЛЬНИХ ВІЙН	85
7.1. ІСТОРИЧНІ ПЕРЕДУМОВИ ДЛЯ ПРОВЕДЕННЯ КОНСЦІЄНТАЛЬНИХ ВІЙН	86
7.2. ПОНЯТТЯ ІДЕНТИЧНОСТІ ГРОМАДЯН І СУСПІЛЬСТВА	89
7.3. КОНСЦІЄНТАЛЬНА ЗБРОЯ.....	93
7.4. СПОСОБИ ПОРАЗКИ І РУЙНУВАННЯ У КОНСЦІЄНТАЛЬНІЙ ВІЙНІ	94
7.5. ВИЩЕ ДОСЯГНЕННЯ КОНСЦІЄНТАЛЬНОЇ ВІЙНИ	96
7.6. ПРИНЦИП ДІЇ КОНСЦІЄНТАЛЬНОЇ ЗБРОЇ.....	96
7.7. ЗАХИСТ СВІДОМОСТІ ГРОМАДЯН ВІД УРАЖЕННЯ ТА РУЙНУВАННЯ	97
ВИСНОВКИ.....	101
ЛІТЕРАТУРА.....	103

ПЕРЕДМОВА

XXI століття стало початком ери глобальної інформатизації та комп'ютеризації всього світу і інтеграції людства до нового інформаційного суспільства, в якому домінуючу роль в усіх сферах життя гратимуть інформаційно-телекомунікаційні ресурси та технології.

Стратегічний курс України на інтеграцію у світовий інформаційний простір викликає об'єктивну потребу у всебічному аналізі позитивних і негативних явищ, що супроводжують цей широкомасштабний процес.

Разом з традиційними загрозами, що існують у сферах формування, зберігання, поширення і керування інформаційними системами держави, зростають загрози неконтрольованого втручання в їх роботу, що несе приховану загрозу втрати державного суверенітету України.

Поява у інформаційному середовищі нових термінів і явищ, а саме: "інформаційний суверенітет", "цифровий суверенітет", "інформаційна зброя", "інформаційна війна", "інформаційне ураження", "кіберзброя" і т.д. обумовлює необхідність переосмислення фундаментальних основ подальшого існування держави як цілісного і незалежного суб'єкта. У зв'язку з цим, всебічний захист інформаційного суверенітету держави та її громадян виступає невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки України.

Монографія рекомендована для використання у вищих навчальних закладах, які готують фахівців за спеціальностями 125 - "Кібербезпека", 122 - "Комп'ютерні науки", 172 - "Телекомунікації та радіотехніка" (спеціалізація "Безпека інформаційних і комунікаційних систем"), а також може бути корисна для широких кіл фахівців, які займаються створенням, експлуатацією та захистом інформаційних систем.

Матеріали монографії були апробовані упродовж тривалого часу у навчальному процесі Національного університету "Одеська юридична академія", Одеського національного політехнічного університету, наукових конференціях та публікаціях різного рівня.

Автори висловлюють щирю подяку рецензентам: доктору технічних наук Положаєнко С.А., доктору технічних наук Чечельницькому В.Я., доктору

юридичних наук Мельничук О.С., які висловили цінні зауваження та надали пропозиції під час підготовки монографії до публікації.

ШАНОВНІ ЧИТАЧІ!
ДЛЯ ОТРИМАННЯ ПОВНОЇ ВЕРСІЇ
МОНОГРАФІЇ ПРОХАННЯ ЗВЕРТАТИСЯ ЗА
АДРЕСОЮ:
zadereyko@onua.edu.ua

ЛІТЕРАТУРА

1. Информационный суверенитет: определение, дискуссии. URL: <http://worldofscience.ru/pravovedenie/6226-informatsionnyj-suverenitet-opredelenie-diskussii.html>. (Дата звернення 30.01.2018).
2. Халецька Л. Еволюція поняття "Могутність" у політичній думці Франції кінця XX - початку XXI століття / Л. Халецька // Дослідження світової політики: зб. наукових праць. 2011. Вип. 2. С. 177-188.
3. Ашманов И. Информационный суверенитет государства и современная реальность. URL: https://zadereyko.info/vliyanie_interneta_na_cheloveka/informacionny_suverenitet.htm. (Дата звернення 30.01.2018).
4. Информационный суверенитет - iForum. URL: <http://iforum.ua/docs/biz/Информационный%20суверенитет-iForum.ppt>. (Дата звернення 30.01.2018).
5. Концептуальные основы защиты информационного суверенитета государства. Задерейко А. В., Логинова Н. И., Троянский А. В. // Гуманітарний та інноваційний ракурс професійної майстерності: пошуки молодих вчених : матер. II Міжнар. наук.-практич. конф. студ., аспір. та молод. вчених (Одеса, 27 жовтня 2016 р.). - Одеса : Фенікс, 2016. – С. 186-188.
6. Mass-media и цифровой суверенитет России. URL: www.elib.bsu.by/bitstream/123456789/110888/.../Будниченко-2015.doc.
7. Кибермогущество как базис обеспечения цифрового суверенитета в современном мире - ключевые подходы. URL: <http://riss.ru/bookstore/journal/2014-2/j25/>. (Дата звернення 30.01.2018).
8. Problem aspects of providing informative sovereignty of the state, prospects and tendencies of its defense in Ukraine / Zadereyko A. V., Troyanskiy A. V., Vlasenko E. V. // Альманах міжнародного права. Випуск 13. 2016. – С. 14 – 22.
9. Вопросы обеспечения информационного суверенитета государств в виртуальной среде интернет и тенденции их развития / А.В. Задерейко // «Науковий вестник Херсонського державного університету. Серія: Юридичні науки, Випуск 5. – Т. II за 2013 г. – С. 23 – 26.

10. Конституція України: Закон України від 28.06.1996 №254к/96-ВР//Відомості Верховної Ради України . — 1996. — №30. — С. 141.
11. Про інформацію: Закон України від 2.10.1995 №2658-XII-ВР (в редакції Закону від 13.01.2011 р.) //Офіційний вісник України. — 2011. — №10. — Ст. 445.
12. Про науково-технічну інформацію: Закон України від 25.06.1993 №3323-XII-ВР //Відомості Верховної Ради України. — 1993. — №33. — Ст. 346.
13. Про державну статистику. Закон України від 17.09.1992 р. №2614-XII //Відомості Верховної Ради України. — 1992. — №43. — Ст. 608.
14. Податковий кодекс України //Відомості Верховної Ради України. — 2011. — №13-14, №15-16, №17. — Ст. 112.
15. Про доступ до публічної інформації: Закон України від 13.01.2011 №2939-17 //Відомості Верховної Ради України. — 2011. — №32. — Ст. 314.
16. Про державну таємницю: Закон України від 21.01.1994 р. №3855-12-ВР //Відомості Верховної Ради України. —1994. — №24. — Ст. 296.
17. Про Раду національної безпеки і оборони України. Закон України від 5.03.1998 р. №183/98-ВР //Відомості Верховної Ради. — 1998. — №35. — Ст. 237.
18. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». Указ Президента України від 13 лютого 2017 року №32/2017 // Урядовий кур'єр. — 16.02.2017. — №30.
19. Міністерство інформаційної політики України: Рада національної безпеки і оборони України затвердила Доктрину інформаційної безпеки України. URL: <https://goo.gl/pLtZZK>. (Дата звернення 30.01.2018).
20. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Указ Президента України від 15.03.2016 р. №96/2016 //Урядовий кур'єр. — 18.03.2016. — №52.
21. Конвенція про кіберзлочинність Ради Європи від 23.11.2001р. ETS 185 // Офіційний вісник України. — 2007. — №65. — Ст. 2535.
22. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». Указ Президента України від 26.05.2015 р. №287/2015 //Урядовий кур'єр. — 29.05.2015. — №95.

23. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 №3475-IV-ВР // Офіційний вісник України. – 2006. – №13. – Ст. 856.
24. Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Указ Президента України від 30.06.2011 р. №717/2011 // Офіційний вісник Президента України. – 2011. – №21. – Ст. 878.
25. Питання діяльності Міністерства інформаційної політики України. Постанова Кабінету Міністрів України від 14 січня 2015 р. №2 // Урядовий кур'єр. – 22.01.2015. – №11.
26. Про систему іномовлення України: Закон від 8.12.2015р. №856-VIII // Відомості Верховної Ради України. – 2016. – №4. – Ст. 37.
27. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації. Указ Президента України від 23.11.2011 р. №1067/2011 // Офіційний вісник Президента України. – 2011. – №31. – Ст. 1195.
28. Про затвердження Положення про державне регулювання номерного ресурсу телекомунікаційної мережі загального користування України. Рішення Національної комісії з питань регулювання зв'язку України від 1.06.2007 р. №769 // Офіційний вісник України. – 2007. – №46. – Ст. 1928.
29. Міністерство інформаційної політики України: Рада національної безпеки і оборони України затвердила Доктрину інформаційної безпеки України. URL: <https://goo.gl/pLtZZK>. (Дата звернення 30.01.2018).
30. Украина: С 1 января 2017 года НКПСИ удешевит не только мобильные звонки между сетями операторов, но и звонки из-за рубежа. URL: <https://goo.gl/xRG1rh>. (Дата звернення 30.01.2018).
31. Украина: НКПСИ официально разрешила использовать смартфоны Apple iPhone 7 и iPhone 7 Plus в мобильных сетях. URL: <https://goo.gl/jn9dH2>. (Дата звернення 30.01.2018).
32. Про затвердження Правил надання та отримання телекомунікаційних послуг. Постанова Кабінету Міністрів України від 11 квітня 2012р. №295 // Офіційний вісник України. – 2012. – №29. – Ст. 1074.
33. William Gibson, Neuromancer. New York: Ace Books, 1984.
34. The National Strategy to Secure Cyberspace, Washington, DC: White House, 2003.

35. Valerie November, Eduardo Camacho-Hubner, Bruno Latour. Entering a risky territory: space in the age of digital navigation. Environment and Planning D: Society and Space 2010, volume 28, p.583.
36. Поисковая система Shodan: как хакеры подключаются к вашим веб-камерам. URL: <http://www.computerra.ru/82234/poiskovaya-sistema-shodan-kak-hakeryi-podklyuchayutsya-k-vashim-veb-kameram/>. (Дата звернения 30.01.2018).
37. Мировая карта интернет-подключений по версии Shodan. URL: <http://www.computerra.ru/105959/mirovaya-karta-podklyucheniya-po-versii-shodan/>. (Дата звернения 30.01.2018).
38. David Clark, Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010.
39. ISO/IEC 2382-1:1993, Information technology – Vocabulary – Part 1: Fundamental terms.
40. Alexander Klimburg, Philipp Mirtl. Cyberspace and Governance – A Primer. The Austrian Institute for International Affairs, Working Paper 65 / September 2012.
41. Введение в кибергеополитику. URL: https://zadereyko.info/kibervoynu/vvedenie_v_kibermir.htm . (Дата звернения 30.01.2018).
42. Олейник А. В., Соснин А. В., Шиманский Л. Е. Политико-правовые аспекты формирования информационного общества суверенного и независимого государства. URL: http://www.niss.gov.ua/book/Sosnin_2.htm. (Дата звернения 30.01.2018)..
43. От кибербезопасности к устойчивости информационных систем. URL: http://www.securitylab.ru/blog/personal/Business_without_danger/308585.php. (Дата звернения 30.01.2018).
44. Critical infrastructure resilience strategy. URL: http://fire-com-live-wp.s3.amazonaws.com/wp-content/uploads/EMV-CIRS_Web1.pdf. (Дата звернения 30.01.2018).
45. Integrated infrastructure: cyber resiliency in society. URL: https://www.ciosummits.com/Online_Assets_Lockheed_Martin_Integrated_Infrastructure_-_Report_Cambridge.pdf. (Дата звернения 30.01.2018).

46. Cyber Security and Resilience of Intelligent Public Transport. URL: https://www.enisa.europa.eu/publications/good-practices-recommendations/at_download/fullReport. (Дата звернення 30.01.2018).
47. Security and Resilience in Governmental Clouds. URL: <https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds>. (Дата звернення 30.01.2018).
48. Петренко А. А., Петренко С. А. Киберучения: методические рекомендации enisa // Вопросы кибербезопасности. – 2015. – №. 3 (11).
49. СОПМ. Система оперативно-розыскных мероприятий. URL: <http://www.tadviser.ru/index.php/>. (Дата звернення 30.01.2018).
50. Системы СОПМ 1,2,3. URL: <http://www.norsi-trans.ru/pcategory/sorm-123/>. (Дата звернення 30.01.2018).
51. СОПМ-3: формальное закрепление реализованного. URL: <http://www.securitylab.ru/analytics/446852.php>. (Дата звернення 30.01.2018).
52. National security strategy. URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. (Дата звернення 30.01.2018).
53. Electromagnetic spectrum strategy. URL: <http://archive.defense.gov/news/dodspectrumstrategy.pdf>. (Дата звернення 30.01.2018).
54. Кибервойна США против России уже началась. URL: <https://regnum.ru/news/polit/1898308.html>. (Дата звернення 30.01.2018).
55. Государственная и кадровая политика Соединенных Штатов Америки и Российской Федерации в области кибербезопасности / Е. Максименко, А. Жилин // Безпека інформації. - 2014. - Т. 20, № 2. - С. 132-142.
56. Проблемные аспекты регулирования информационных потоков в виртуальной среде интернет и тенденции их развития. URL: https://zadereyko.info/moi_publicacii/regulation_information.htm . (Дата звернення 30.01.2018).
57. Международный пакт о гражданских и политических правах. URL: http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml. (Дата звернення 30.01.2018).

- 58.Европейская конвенция о правах человека. URL: http://www.echr.coe.int/Documents/Convention_RUS.pdf. (Дата звернення 30.01.2018).
- 59.Zadereyko A. V. Problematic regulatory aspects of information flows in the virtual internet environment and the tendencies of its development / A. V. Zadereyko // Ученые записки Таврического национального университета им. В. И. Вернадского. Серия: Юридические науки. - 2013. - Т. 26 (65). № 2-1. - Ч.2.- С. 51-55.
- 60.Мифы о китайской Сети. . URL: <http://polemika.com.ua/news-123733.html>.
- 61.Интернет-цензура в КНР. URL: http://www.memoid.ru/node/Internetcenzura_v_KNR. (Дата звернення 30.01.2018).
- 62.Китай ужесточил контроль над VPN-сервисами. URL: <http://www.securitylab.ru/news/485102.php>. (Дата звернення 30.01.2018).
- 63.Индия намерена начать применение системы слежения «Нетра» за сетью Интернет. URL: <http://www.armstrade.org/includes/periodics/news/2013/1217/104521788/print.shtml>. (Дата звернення 30.01.2018).
- 64.Рунет: список запретов. URL: <http://digest.subscribe.ru/inet/inet/n1335248194.html>. (Дата звернення 30.01.2018).
- 65.Как Роскомнадзор охотится на торренты. URL: <http://digest.subscribe.ru/inet/inet/n1335221748.html>. (Дата звернення 30.01.2018).
- 66.Детей научат бояться троллей и шифровать информацию в интернете. URL: <http://www.cnews.ru/news/top/index.shtml?2013/11/27/551409>. (Дата звернення 30.01.2018).
- 67.Нам пакет: Владимир Путин подписал «законы Яровой». URL: <https://russian.rt.com/article/311295-nam-paket-vladimir-putin-podpisal-zakony-yarovoі>. (Дата звернення 30.01.2018).
- 68.Премьер-министр Великобритании предлагает блокировать экстремистские web-сайты. URL: <http://www.securitylab.ru/news/448181.php>. (Дата звернення 30.01.2018).

- 69.Германия: в сумерках рассветных забрезжила цензура в интернете. URL: <http://ru.globalvoicesonline.org/2012/08/13/17625/>.
- 70.Internet Censorship in France. URL: <http://internetcensorshipinfrance.weebly.com/>. (Дата звернення 30.01.2018).
- 71.Закон о видеонаблюдении (LOPPSI): что нового, какие изменения для Национальной комиссии по информатизации и свободам? URL: <http://www.uipdp.com/articles/2011-04/20.html>. (Дата звернення 30.01.2018).
- 72.Фильтрация и блокирование интернет-контента: мировой опыт. URL: <https://ria.ru/spravka/20120711/697151590.html>. (Дата звернення 30.01.2018).
- 73.COPM-3: формальное закрепление реализованного. URL: <http://www.securitylab.ru/analytics/446852.php>. (Дата звернення 30.01.2018).
- 74.Средство криптографической защиты информации. URL: https://www.cryptopro.ru/sites/default/files/docs/.../admin_guide_general_r3.pdf. (Дата звернення 30.01.2018).
- 75.Проект Clipper Chip. URL: <https://geektimes.ru/company/ua-hosting/blog/269494/>. (Дата звернення 30.01.2018).
- 76.Депонирование ключей. URL: <http://samoychiteli.ru/document34285.html>. (Дата звернення 30.01.2018).
- 77.От депонирования криптографических ключей к свидетельствованию против себя. URL: http://www.securitylab.ru/blog/personal/Business_without_danger/309062.php. (Дата звернення 30.01.2018).
- 78.Как читают пользователи в интернете. F-паттерн. URL: http://www.annalevinson.com/service/reading_eye_tracking.html. (Дата звернення 30.01.2018).
- 79.Богуш В.М. Інформаційна безпека держави. / В. Богуш. О, Юдін, - К.: «МК-пресс», 2005, - 432 с.
- 80.Искажение информации. Приёмы искажения информации. URL: <http://starlife.kg/2013/08/20/iskazhenie-informaciipriemy-iskazheniya-informacii.html>. (Дата звернення 30.01.2018).

81. “Клиповое мышление” — феномен современности. URL: <http://jarki.ru/wpress/2013/02/18/3208/>. (Дата звернення 30.01.2018).
82. Чем опасно клиповое мышление и как с ним бороться. URL: <http://www.lookatme.ru/mag/how-to/inspiration-howitworks/207449-clip>. (Дата звернення 30.01.2018).
83. Фрумкин К.Г. Клиповое мышление и судьба линейного текста. // Ineternum 2010. – №1. URL: http://nounivers.narod.ru/pub/kf_clip.htm. (Дата звернення 30.01.2018).
84. Люди с клиповым мышлением элитой не станут. URL: <http://www.rosbalt.ru/piter/2015/03/28/1382125.html>. (Дата звернення 30.01.2018).
85. Азаренок, Н.В. Клиповое сознание и его влияние на психологию человека в современном мире. // Материалы Всероссийской юбилейной научной конференции, посвященной 120-летию со дня рождения С.Л. Рубинштейна “Психология человека в современном мире”. Том 5. Личность и группа в условиях социальных изменений. / Отв. ред. А.Л. Журавлев. – М.: Изд-во “Институт психологии РАН”, 2009. – С. 110-112.
86. Про мозговые вирусы. URL: <http://roem.ru/2014/08/07/ashmanov104753/>. (Дата звернення 30.01.2018).
87. Григорьев В.Р. Информационные вирусы - новое оружие массового поражения. // Информационные войны. 2008, №3, С. 2-29.
88. Психические вирусы. Как программируют ваше сознание / Пер. с англ. Л.В. Афанасьевой. - М.: Поколение, 2007,- 304 с.
89. Малкольм Гладуэлл. Переломный момент. Как незначительные изменения приводят к глобальным переменам. «Альпина Пабlishер». 2016. 256с.
90. Караяни А., Зинченко Ю. Информационно-психологическое противоборство в войне: история, методология, практика. - М.: МГУ, 2007.
91. Федоров Д.Ю. Применение структуризации знаний для обеспечения информационной безопасности личности. URL: http://pycode.ru/wp-content/uploads/2011/01/fedorov_primenenie_strukturizacii_znaniy_2013.pdf. (Дата звернення 30.01.2018).
92. Федоров Д. Ю. Применение структуризации знаний в информационной безопасности // Матер. Междунар. научно-практ. конф.

- «Фундаинформационные и прикладные исследования в современном мире», 13-15 марта 2013 г.- СПб.: Информационный издательский учебно-научный центр «Стратегия будущего», 2013. - С. 40-43.
93. Розенберг В. Я. Система обучения на базе семантических сетей. Теория и практика // Матер. Междунар. научно-практ. конф. «Фундаинформационные и прикладные исследования в современном мире», 13-15 марта 2013 г.- СПб.: Информационный издательский учебно-научный центр «Стратегия будущего», 2013. - С. 184-191.
94. Федоров Д.Ю. Подходы к проектированию учебного курса «Гуманитарные аспекты информационной безопасности» // Матер. XVI Всероссийской научно-методической конференции «Фундаинформационные исследования и инновации в национальных исследовательских университетах», 17-18 мая 2012 г.- СПбГПУ, 2012.
95. Леонтьев А.А. Психология общения. 3-е изд. М., 1999. С. 274-277.
96. Pluto loses status as a planet. URL: <http://news.bbc.co.Uk/2/hi/5282440.stm>. (Дата звернення 30.01.2018).
97. Вус М. А., Кучерявый М. М., Шакин Д. Н., Юсупов Р. М.. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности // Информатизация и связь. 2012, № 9. С. 715.
98. Консциентальное оружие и консциентальные войны. Лекция Юрия Громыко. URL: <http://gtmarket.ru/laboratory/publicdoc/2007/782>. (Дата звернення 30.01.2018).
99. В.М. Макаров. Консциентальная война миф или реальность. «Наука и военная безопасность», №2, 2003 г., с. 18-22. (Дата звернення 30.01.2018).
100. Кому будет принадлежать консциентальное оружие в XXI веке?. URL: <http://www.milresource.ru/Potekhin-1.html>. (Дата звернення 30.01.2018).
101. Федоришин М.С. Особливості викладання основ японського письма у Львівській політехніці/ М. С. Федоришин // Вісн. Нац. ун-ту "Львів. політехніка". - 2007. - № 586. - С. 39-41.

Наукове видання

Олександр Владиславович Задерейко,
Олександр Вячеславович Троянський,
Рашид Ібрагимович Чанишев

Концептуальні основи захисту інформаційного суверенітету України

Монографія

Підписано до друку 27.01.2018.
Формат 60х84/16. Ум.друк. арк. 6,16. Зам. 1801-08
Наклад 100. Папір офсетний.

Видано з готового оригінал-макету ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25. Тел. (048) 7777591.