Міністерство освіти і науки України
Одеський національний політехнічний університет

**О. В. Задерейко, О. В. Троянський,
Р. І. Чанишев, А. І. Дика**

КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

Монографія

2-ге видання, перероблене і доповнене

Одеса
Фенікс
2022

УДК 621.396.969.3
З 15

Рекомендовано до видання вченою радою Національного університету «Одеська політехніка» (протокол № 10 від 13.04.2022 р.)

Рецензенти:

Положаєнко С. А., доктор технічних наук, завідувач кафедри комп'ютеризованих систем управління Державного університету «Одеська Політехніка»;

Казаков А. І., доктор технічних наук, професор кафедри кібербезпеки та програмного забезпечення Державного університету «Одеська політехніка»;

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

Задерейко О. В. та ін.

З 15 Концептуальні основи захисту інформаційного суверенітету України : монографія / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика. 2-ге вид., перероб. і доп. – Одеса : Фенікс, 2022. – 220 с.

ISBN 978-966-928-812-7

У монографії розглянуто 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 чинного 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, зокрема у цифровому просторі.

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.

УДК 621.396.969.3

ISBN 978-966-928-812-7

Зміст

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 різного походження.

Матеріали монографії були апробовані упродовж тривалого часу у навчальному процесі Національного університету «Одеська юридична академія», наукових конференціях та публікаціях різного рівня.

Автори висловлюють щиру подяку рецензентам: доктору технічних наук Положаєнко С.А., доктору технічних наук Казакову А.І., доктору юридичних наук Мельничук О.С., які висловили цінні зауваження та надали пропозиції під час підготовки монографії до публікації.

УВАГА!

Повна версія монографії розташована на сайті дистанційного навчання факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

за адресою: http://cyber.onua.edu.ua

З усіх питань стосовно повної версії монографії звертатися за адресою: zadereyko@onua.edu.ua

ВИСНОВКИ

Проблема наукового осмислення та практичного використання кіберпростору держави супроводжується суттєвими термінологічними та нормативно-правовими питаннями.

Могутність провідних країн (економічна, військова, зовнішньополітична, культурна) та їх взаємозалежність робить практично неможливим відкрите протистояння, змушуючи шукати альтернативні форми суперництва, за яких кожна з країн може збільшити свою перевагу або принаймні знизити ефективність дій суперника. За таких умов кіберпростір стає одним з важливих просторів протиборства, в т.ч. через його нормативно-правову невизначеність.

Нормативно-правові проблеми є природним наслідком термінологічних, однак виводять їх із суто наукового обговорення до сфери практичних міждержавних відносин. При цьому досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростіру та всім похідним від нього поняттям сфери безпеки, принципово не визначено правовий статус кіберпростіру (існує щодо всіх інших просторів), відсутній будь-який міжнародний далекосяжний консенсус щодо правил поведінки в кіберпросторі та загальноприйняті методики оцінювання наслідків кібератак та їх «прив'язування» до міжнародних норм і правил.

Можна очікувати, що на певному етапі подібні виклики глобальному кіберпростору спричинять його сегментацію на певні «національні інтернети». Це висуває перед державою глобальне питання розбудови власного кіберсуверенітету, який розуміється як можливості національних держав самостійно і незалежно визначати внутрішні та зовнішні, політичні та геополітичні національні інтереси в кіберсфері, їх спроможність самостійно визначатися з курсом внутрішньої та зовнішньої інформаційної політики, самостійно розпоряджатися власними інформаційними ресурсами та інфраструктурою національного інформаційного простору, а, відтак, гарантувати кібернетичну та інформаційну безпеку державі, суспільству та громадянам.

Важливо сформувати загальнонаціональні міжвідомчі координаційні структури, спроможні узгоджувати та координувати діяльність різних силових відомств на час розслідування злочинів у кіберпросторі, та створити ефективну систему захисту вітчизняного кіберпростіру (зокрема у військовій сфері). Сам сектор кібербезпеки має бути на якісно новому рівні забезпечений ресурсами (фінансовими, кадровими, технічними), в тому числі через створення національної операційної системи та «антивірусу», а також через відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази. З огляду на те, що значна кількість об'єктів критичної інфраструктури наразі є у приватній власності, дуже важливим є посилення взаємодії органів державної влади з приватним сектором, а також неурядовими організаціями та громадянським суспільством у цілому.

Необхідно повсюдно впроваджувати і застосовувати розроблені авторами методи захисту від збору та витоків даних громадян і зосередити подальші наукові дослідження на проблемі кібермогутності України як здатності втілювати її волю та забезпечувати національні інтереси в кіберпросторі.

ЛІТЕРАТУРА

1. Keele B. (2018). Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law. By Radim Polčák and Dan Jerker B. Svantesson. Northampton, MA: Edward Elgar, 2017. pp. xvii, 268. International Journal of Legal Information, 46(2), 123-124. DOI:10.1017/jli.2018.28.
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. Zadorozhnia H, Mykhtunenko V, Kovalenko H, Kuryliuk Y, Yurchenko L, Maslennykova T. Protection of Information Sovereignty as an Important Component of the Political Function of the State. IJCSNS International Journal of Computer Science and Network Security, September 2021, VOL.21, No.9, pp.151-154. DOI: https://doi.org/10.22937/IJCSNS.2021.21.9.20.
4. Информационный суверенитет – iForum. URL: http://iforum.ua/docs/biz/Информационный%20суверенитет-iForum.ppt. (Дата звернення 02.07.2022).
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. Floridi, L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU // Philos. Technol. 2020, №33, pp. 369–378. DOI: https://doi.org/10.1007/s13347-020-00423-6.
7. Betz David, Stevens Tim. Cyberspace and the State: Toward a Strategy for Cyber-power. 2017. DOI: 10.4324/9781351224543. URL: https://bit.ly/3yB8pBn. (Дата звернення 02.07.2022).
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 университета. Серия: Юридичні науки, Випуск 5. – Т. II за 2013 г. – С. 23 – 26.
10. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28.06.1996 р. №254к/96-ВР. Відомості Верховної Ради України. 1996. №30. Ст. 141.

11. Про інформацію: Закон України від 02.10.1992 р. №2657-XII. Відомості Верховної Ради України. 1992. №48. Ст. 650.
12. Про забезпечення функціонування української мови як державної: Закон України від 25.04.2019 р. № 2704-VIII. Відомості Верховної Ради України. 2019. №21. Ст. 81.
13. Про науково-технічну інформацію: Закон України від 25.06.1993 р. №3322-XII. Відомості Верховної Ради України. 1993. №33. Ст. 345.
14. Про державну статистику: Закон України від 17.09.1992 р. №2614-XII. Відомості Верховної Ради України. 1992. №43. Ст. 608.
15. Податковий кодекс України: Кодекс України від 02.12.2010 р. №2755-VI. Відомості Верховної Ради України. 2011. №13. Ст. 112.
16. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України. 2011. №32. Ст. 314.
17. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. №34. Ст. 481.
18. Про державну таємницю: Закон України від 21.01.1994 р. №3855-XII. Відомості Верховної Ради України. 1994. №16. Ст. 93.
19. Про Службу безпеки України: Закон України від 25.03.1992 р. №2229-XII. Відомості Верховної Ради України. 1992. №27. Ст. 382.
20. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. №2135-XII. Відомості Верховної Ради України. 1992. №22. Ст. 303.
21. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. №3759-XII. Відомості Верховної Ради України. 1994. №10. Ст. 43.
22. Про Суспільне телебачення і радіомовлення України Закон України від 17.04.2014 р. №1227-VII. Відомості Верховної Ради України. 2014. №27. Ст. 904.
23. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23.09.1997 р. №538/97-ВР. Відомості Верховної Ради України. 1997. №48. Ст. 296.
24. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. №80/94-ВР. Відомості Верховної Ради України. 1994. №31. Ст. 286.
25. Про Національну систему конфіденційного зв'язку: Закон України від 10.01.2002 р. №2919-III. Відомості Верховної Ради України. 2002. №15. Ст. 103.
26. Про електронні комунікації: Закон України від 16.12.2020 р. №1089-IX. Голос України від 16.01.2021. №7.
27. Про підприємництво: Закон України від 07.02.1991 р. №698-XII. Відомості Верховної Ради УРСР. 1991. №14. Ст. 168.
28. Про ліцензування видів господарської діяльності: Закон України від 02.03.2015 р. №222-VIII. Відомості Верховної Ради України. 2015. №23. Ст. 158.

29. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р №2163-VIII. Відомості Верховної Ради України. 2017. №45. Ст. 403.
30. Конвенція про кіберзлочинність Ради Європи від 23.11.2001 р. Ідентифікатор: 994_575. Офіційний вісник України 2007. №65. Ст. 2535.
31. Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки»: Указ Президента України №685/2021 від 15 жовтня 2021 року. (28.12.2021) Офіційний вісник України. 2022. №3. Ст. 125.
32. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021 від 26 серпня 2021 року. Офіційний вісник України. 2021. №70. Ст. 4417.
33. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. №183/98-ВР. Відомості Верховної Ради України. 1998. №35. Ст. 237.
34. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення Ради національної безпеки і оборони України від 29.12.2016 р. №n0015525-16. Офіційний вісник України. 2017. №16. Ст. 464.
35. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. №3475-IV. Відомості Верховної Ради України. 2006. №30. Ст. 258.
36. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Постанова Кабінету Міністрів України від 03.09.2014 р. №411 Офіційний вісник України. 2014. №73. Ст. 2066.
37. Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку: Проект Закону №6055 від 14.09.2021. URL: http://surl.li/bjbsz. (Дата звернення 02.07.2022)
38. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14.01.2015 р. №2. Офіційний вісник України. 2015. №6. Ст. 124.
39. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації: Указ Президента України №1067/2011 від 23 листопада 2011 року. Офіційний вісник України. 2011. №94. Ст. 3417.
40. Новий регулятор у сфері е-комунікацій Lex Inform Юридичні новини України. URL: https://lexinform.com.ua/zakonodavstvo/novyj-regulyator-u-sferi-e-komunikatsij. (Дата звернення: 02.07.2022).
41. William Gibson, Neuromancer. New York: Ace Books, 1984. URL: https://en.wikipedia.org/wiki/Neuromancer. (Дата звернення: 02.07.2022).

42. The National Strategy to Secure Cyberspace, Washington, DC: White House, 2003. URL: https://bit.ly/3uhbvbu. (Дата звернення: 02.07.2022).
43. NATIONAL CYBER STRATEGY – Trump White House Archive. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. (Дата звернення: 02.07.2022).
44. 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, pp. 583.
45. John Matherly. Complete Guide to Shodan. Collect. Analyze. Visualize. Make Internet Intelligence Work for You. URL: https://wiki.squi.fr/images/b/b6/Shodan.pdf. (Дата звернення 02.07.2022).
46. Christopher Bennett, AbdelRahman Abdou, and Paul C. van Oorschot. Empirical Scanning Analysis of Censys and Shodan. URL: https://www.ndss-symposium.org/wp-content/uploads/madweb2021_23009_paper.pdf. (Дата звернення 02.07.2022).
47. David Clark, Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010, pp. 1-18. URL: https://bit.ly/3AqfmGS. (Дата звернення 02.07.2022).
48. ISO/IEC 2382-1:1993, Information technology – Vocabulary – Part 1: Fundamental terms. URL: https://www.iso.org/standard/7229.html. (Дата звернення 02.07.2022).
49. Klimburg, A., & Mirtl, P. (2012). Cyberspace and governance – a primer. (Working Paper / Österreichisches Institut für Internationale Politik, 65). Wien: Österreichisches Institut für Internationale Politik (oiip). URL: https://www.ssoar.info/ssoar/handle/document/43560. (Дата звернення 02.07.2022).
50. Ms. Afeera Firdous. Cyber Warfare and Global Power Politics // CISS Insight Journal. 2020, №8(1), pp.71-93.
51. 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 звернення 02.07.2022).
52. Martsenyuk , V., Sverstyuk A., Andrushchak , I., Rykovska , L., & Koshelyuk , V. (2021). Features of cybersecurity of modern information technologies during the digital transformation. COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION, (43), pp. 194-200. DOI: https://doi.org/10.36910/6775-2524-0560-2021-43-32.
53. Critical infrastructure resilience strategy. URL: http://fire-com-live-wp.s3.amazonaws.com/wp-content/uploads/EMV-CIRS_Web1.pdf. (Дата звернення 02.07.2022).

54. Integrated infrastructure: cyber resiliency in society. URL: https://www.ciosummits.com/Online_Assets_Lockheed_Martin_Integrated_Infrastructure_-_Report_Cambridge.pdf. (Дата звернення 02.07.2022).
55. Cyber Security and Resilience of Intelligent Public Transport. URL: https://www.enisa.europa.eu/publications/good-practices-recommendations/at_download/fullReport. (Дата звернення 02.07.2022).
56. Security and Resilience in Governmental Clouds. URL: https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds. (Дата звернення 02.07.2022).
57. Kovács L. National cyber security as the cornerstone of national security //Land Forces Academy Review. 2018, V.23. №2. pp. 113-120.
58. СОРМ. Система оперативно-розыскных мероприятий. URL: https://bit.ly/3ODb1Vc. (Дата звернення 02.07.2022).
59. Системы СОРМ 1,2,3. URL: https://bit.ly/3y8G83P. (Дата звернення 02.07.2022).
60. Antonyan E. A., Grishko N. A. New Technologies in Cyber Terrorism Countering. // XVII International Research-to-Practice Conference dedicated to the memory of MI Kovalyov (ICK 2020). Atlantis Press, 2020. pp. 28-31. DOI: https://dx.doi.org/10.2991/assehr.k.200321.078.
61. National security strategy. URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. (Дата звернення 02.07.2022).
62. Electromagnetic spectrum strategy. URL: http://archive.defense.gov/news/dodspectrumstrategy.pdf. (Дата звернення 02.07.2022).
63. Армия обороны Израиля и национальная кибер оборона. URL: https://bit.ly/3QXhjk9. (Дата звернення: 02.07.2022).
64. Система кибербезопасности в Китае (2021). URL: http://factmil.com/publ/strana/kitaj/sistema_kiberbezopasnosti_v_kitae_2021/59-1-0-1833. (Дата звернення: 02.07.2022).
65. The Utility of Force: The Art of War in the Modern World. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2114&context=nwc-review. (Дата звернення: 02.07.2022).
66. Гибридная Война: Хай-Тек, Информационные и Кибер Конфликты. URL: https://connections-qj.org/ru/article/gibridnaya-voyna-hay-tek-informacionnye-i-kiber-konflikty. (Дата звернення: 02.07.2022).
67. War from Ground Up: Twenty-first century Combat as Politics // Crisis in the World Politics. URL: https://www.hurstpublishers.com/book/war-from-the-ground-up-2/. (Дата звернення: 02.07.2022).
68. NETWORK CENTRIC WARFARE: Developing and Leveraging Information Superiority. URL: http://www.dodccrp.org/files/Alberts_NCW.pdf – (Дата звернення: 02.07.2022).

69. 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.
70. Electromagnetic Spectrum Superiority Strategy. URL: https://www.airforcemag.com/app/uploads/2020/10/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.pdf. Дата звернення: 12.02.2022 р.
71. Rid T. Think again: cyberwar // Foreign Policy. 2012, №192. pp. 80. URL: https://www.proquest.com/openview/1b8678744d8ad2c7376c439edd17011f/1?pq-origsite=gscholar&cbl=47510. (Дата звернення: 02.07.2022).
72. Кібербезпека України: аналіз сучасного стану / Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. // Захист інформації. – Київ: Національний авіаційний університет. – 2019. – Т. 21. – №3. – С. 150–157.
73. Моніторинг рівня кібербезпеки України у світових рейтингах / Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. // Інформаційна безпека людини, суспільства, держави. – Київ: Національна академія Служби безпеки України. – 2019. – №3(27). – С. 100–107.
74. Проблемные аспекты регулирования информационных потоков в виртуальной среде интернет и тенденции их развития. URL: https://zadereyko.info/moi_publikacii/regulation_information.htm. (Дата звернення 02.07.2022).
75. Международный пакт о гражданских и политических правах. URL: http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml. (Дата звернення 02.07.20220.
76. Европейская конвенция о правах человека. URL: http://www.echr.coe.int/Documents/Convention_RUS.pdf. (Дата звернення 02.07.2022).
77. 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.
78. Мифы о китайской Сети. URL: http://polemika.com.ua/news-123733.html. (Дата звернення 02.07.2022).
79. Xueyang Xu. Z. Morley Mao. J. Alex Halderman. Internet Censorship in China: Where Does the Filtering Occur? URL: https://link.springer.com/chapter/10.1007/978-3-642-19260-9_14. (Дата звернення 02.07.2022).
80. Li J. China: The techno-politics of the wall // Geoblocking and global video culture. 2016, pp. 110-119.
81. Gupta R., Muttoo S. K. Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA //N etw. Protoc. Algorithms. 2016, V.8. – №4, pp. 1-28.

82. Rahimi Babak. Censorship and the Islamic Republic: Two Modes of Regulatory Measures for Media in Iran // The Middle East Journal, 2015, V.69, №3, pp. 358-378. DOI: https://doi.org/10.3751/69.3.12
83. Detecting and Evading Censorship-in-Depth: A Case Study of Iran's Protocol Whitelister // URL: https://www.usenix.org/conference/foci20/presentation/bock. (Дата звернення 02.07.2022).
84. G. Aceto, A. Montieri, A. Pescape. Internet Censorship in Italy: A First Look at 3G/4G Networks. International Conference on Cryptology and Network Security, CANS 2016: Cryptology and Network Security, 2016, pp. 737–742. DOI: 10.1007/978-3-319-48965-0_53.
85. Kim, S. (2022). The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective. In: Lee, S., Kim, S. (eds) Korea's Middle Power Diplomacy. The Political Economy of the Asia Pacific. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-76012-0_6.
86. Watkin A. L. Regulating terrorist content on tech platforms: A proposed framework based on social regulation : Diss. – Swansea University, 2021. URL: https://bit.ly/3ujiUHg. (Дата звернення 02.07.2022).
87. Markus Beckedahl. The Dawning of Internet Censorship in Germany. URL: https://advox.globalvoices.org/2009/06/16/the-dawning-of-internet-censorship-in-germany/. (Дата звернення 02.07.2022).
88. Internet Censorship in France. URL: http://internetcensorshipinfrance.weebly.com/. Дата звернення 12.02.2022 р.
89. Guerrier C. Security and Privacy in the Digital Era. URL: https://bit.ly/3bBJnct. (Дата звернення 02.07.2022).
90. Faris R., Villeneuve N. Measuring global Internet filtering. URL: https://www.nartv.org/mirror/accessdenied-chapter-1.pdf. Дата звернення 02.07.2022).
91. СОРМ-3: Принципы работы должен знать каждый. URL: https://zadereyko.info/sbor_informacii_o_polzovatele/sorm_3_principu_sbora_i_hraneniya_informacii.htm. (Дата звернення 02.07.2022).
92. Масштабы глобальной слежки. Что такое СОРМ: виды и возможности. URL: https://nuz.uz/proishestvie/39877-masshtaby-globalnoy-slezhki-chto-takoe-sorm-vidy-i-vozmozhnosti.html. (Дата звернення 02.07.2022).
93. Sofio Daniel G., William A. Carter. Putting US Cybersecurity Culture in Perspective // Homeland Security Cultures: Enhancing Values While Fostering Resilience. 2018, pp. 103.
94. Мельник С. В. Концептуальні основи організації криптографічного захисту інформації // Наукові записки Українського науково-дослідного інституту зв'язку. №6(40), 2015, С. 19 – 26.
95. Blaze Matt. Key escrow from a safe distance: looking back at the clipper chip // Proceedings of the 27th Annual Computer Security Applications Conference.

2011. URL: https://www.mattblaze.org/escrow-acsac11.pdf. (Дата звернення 02.07.2022).
96. Гончар С. А. Криптографія з часовим розкриттям: минуле, теперішнє, майбутнє // Вісник Київського національного університету імені Тараса Шевченка. Серія: Фізико-математичні науки №4, 2014, С. 139-144.
97. Денісова О. О. Організація електронної звітності через Інтернет. URL: https://bit.ly/3OzHR9w. (Дата звернення 02.07.2022).
98. Семенюк Г. С. Поняття медіавірусу: виникнення й утвердження терміна // Наукові записки Інституту журналістики. №53, 2013, С. 263-267.
99. Мелешко Є. Якименко М. Інформаційні віруси в соціальних мережах як засіб інформаційно-психологічного впливу // Information, communication, society (ICS-2016), 19-21 may 2016, Lviv, С. 22 – 23.
100. Психические вирусы. Как программируют ваше сознание / Пер. с англ. Л.В. Афанасьевой. – М.: Поколение, 2007,- 304 с.
101. Д. Д. Карафано. Понимание социальных сетей и национальная безопасность. Геополитика. Информационно-аналитическое издание. Выпуск XXII, 2013, С. 22 – 35.
102. Мастикаш О., Федушко С. Автоматизація збору персональних даних з соціальних мережах // Львів: Видавництво «Редакція» УП. 2016, С. 46 – 47.
103. Пчелянський Д., Воінова, С. Штучний інтелект: перспективи та тенденції розвитку // Automation of Technological and Business Processes. №11(3), 2019, С. 59 – 64. DOI: https://doi.org/10.15673/atbp.v11i3.1500.
104. Деркаченко Я. А. Соціальні мережі, як середовище для технологій маніпулятивного впливу // Сучасний захист інформації. №1, 2016, С. 51 – 59.
105. Курбан О. В. Специфіка створення алгоритмічної системи управління інформаційними процесами в соціальних мережах // Поліграфія і видавнича справа. №2, 2016, С. 174-181.
106. Как читают пользователи интернете. F-паттерн. URL: http://www.annalevinson.com/service/reading_eye_tracking.html. (Дата звернення 02.07.2022).
107. Богуш В.М. Інформаційна безпека держави / В. Богуш. О, Юдін, – К.: «МК-пресс», 2005, – 432 с.
108. Искажение информации. Приёмы искажения информации. URL: http://starlife.kg/2013/08/20/iskazhenie-informaciipriemy-iskazheniya-informacii.html. (Дата звернення 02.07.20220.
109. Горлач Д. Феномен кліпового мислення в контексті радикалізації перетворень інформаційного середовища // Вісник Книжкової палати. №5, 2016, С. 45-46.
110. Чаплак Я. Чуйко Г. Кліпова хаотичність як маніпулятивна технологія соціально-психологічного впливу в кіберпросторі // Psychological journal. № 3(13), 2018, С. 21 – 40. DOI: https://doi.org/10.31108/2018vol12iss2.

111. Volkodav T., Semenovskikh T. Dichotomy of the ‘clip thinking’ phenomenon // Proceedings of ICEPS 2017 (International Conference on Education, Psychology, and Social Sciences). Vol. 4. 2017.
112. Riazantsev A. Necessity of essential correction of «clip thinking» // Eastern European Scientific Journal, №4, 2016. URL: http://journale.auris-verlag.de/index.php/EESJ/article/view/611. (Дата звернення 02.07.2022).
113. DAUTOV, Denis; KOROCHENTSEVA, Anna; AL HUSSINI, Mohamed Kadom Mahdi. Features of clip thinking and attention among representatives of generations X and generations Z. In: SHS Web of conferences. EDP Sciences, 2019. p. 06001. DOI: 10.1051/shsconf/20197006001.
114. Социальная дилемма. URL: https://zadereyko.info/video/sosialnaya_dilema.htm. (Дата звернення 02.07.2022).
115. Google: зловещая черта. URL: https://zadereyko.info/video/google_zloveshaya_cherta.htm. (Дата звернення 02.07.2022).
116. Корпорация монстров Google и цифровая диктатура будущего. URL: https://www.youtube.com/watch?v=azV7OHjwqdE. (Дата звернення 02.07.2022).
117. Eric Schmidt and Jared Cohen, The New Digital Age: Reshaping the Future of People, Nations and Business. London, UK: John Murray, 2013, 337 pp.
118. Расследование: «Google манипулирует общественным мнением и сознанием с помощью алгоритмов поиска». URL: https://bit.ly/3yxG4vS. (Дата звернення 02.07.2022).
119. Bar-Ilan J. Manipulating search engine algorithms: the case of Google // Journal of Information, Communication and Ethics in Society, Vol. 5 No. 2/3, pp. 155-166. DOI: https://doi.org/10.1108/14779960710837623.
120. BBC: как Facebook манипулирует мнениями пользователей. URL: https://itc.ua/blogs/vvs-kak-facebook-manipuliruet-mneniyami-polzovateley/. (Дата звернення 02.07.2022).
121. Малкольм Гладуэлл. Переломный момент. Как незначительные изменения приводят к глобальным переменам. «Альпина Паблишер». 2016. 256 с.
122. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене / [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедь, В. М. Петрика. – К.: ПАТ «ВІПОЛ», 2018. – 386 с.
123. Han Zhengbiao, et al. Risk assessment of digital library information security: a case study. The electronic library, 2016, 34.3: 471-487.
124. Zegzhda Peter D., et al. A use case analysis of heterogeneous semistructured objects in information security problems. Automatic Control and Computer Sciences, 2018, 52.8: 918-930.

125. Yang Jian-Xiong, Watada, Junzo. Accident prevention system based on semantic network. In: 2008 International Conference on Machine Learning and Cybernetics. IEEE, 2008. p. 3738-3743.
126. Stamp, Mark. Information security: principles and practice. John Wiley & Sons, 2011.
127. Психологія спілкування : навч. посіб. / [Л. О. Савенкова, В. В. Сгадова, Л. Л. Борисенко та ін.] ; за заг. ред. Л. О. Савенкової. – К. : КНЕУ, 2015. –309, [3] с.
128. Pluto loses status as a planet. URL: http://news.bbc.co.Uk/2/hi/5282440.stm. (Дата звернення 02.07.2022).
129. 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.
130. Виды цензуры в обществе. URL: https://zadereyko.info/cenzyra_v_seti/vidu_cenzyru_v_obshestve.htm. (Дата звернення 02.07.2022).
131. Марков А. Р. Індивідуально-психологічні особливості та поведінкові патерни як мішені психологічної корекції дезадаптивних станів у цивільного населення в умовах консцієнтальної війни. Науковий вісник Херсонського державного університету. Серія: Психологічні науки. 2016, №(2), С. 182-193.
132. Сенченко О. Структури, засоби і моделі застосування консцієнтальної зброї в системі соціальних комунікацій // Вісник Книжкової палати, №7, 2014, С. 44 -49.
133. Варенья Н. М. Концептуальні засади ефективного інформаційного протистояння в умовах консцієнтальної війни // Актуальні проблеми управління інформаційною безпекою держави. 2019, С. 16 – 17.
134. Kleinkrieg. URL: https://de-academic.com/dic.nsf/dewiki/775788. (Дата звернення 02.07.2022).
135. Кастельс М. Информационная эпоха: экономика, общество и культура. URL: https://bit.ly/3R1401Z. (Дата звернення 02.07.2022).
136. Литвинчук О. Соціальна та особистісна ідентичність: соціально-філософський аналіз // Наукові записки Національного університету Острозька академія. Сер.: Філософія. 2011, №8, С. 195-202.
137. Вартанова О. В. Змінення ментальних шаблонів соціуму як результат консцієнтальної війни // Вісник Східноукраїнського національного університету імені Володимира Даля. 2017, №2, С. 19-22.
138. Письменний О. О., Кашперська Д. О., Консцієнтальна війна як передтеча інформаційної війни. Рекомендовано до друку вченою радою Інституту УДО України КНУ імені Тараса Шевченка (протокол № 13 від 12 липня 2021 року) Редакційна колегія, 2021, С. 127-128. URL: http://indo.univ.kiev.

ua/media/attachments/2021/09/10/24.06.21.pdf#page=127. (Дата звернення 02.07.2022).
139. 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.
140. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/. (Дата звернення 02.07.2022).
141. Цифровізація як ключовий мегатренд мегатренд трансформації глобального економічного середовища // Вісник ОНУ імені І. І. Мечникова, 2020. Т. 25. Вип. 1(80), С. 163 – 168. DOI: https://doi.org/10.32782/2304-0920/1-80-28.
142. Панін В., Борзак О., Лалетін С. Різновиди та тенденції розвитку інформаційної зброї // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2012, №28, С. 4-6.
143. Карлов В. Д., Лукашук О. В., Шолохов С. М. До питання про суть та види інформаційної зброї в сучасних інформаційних конфліктах // Системи обробки інформації. 2016, №8, С. 111–114.
144. Трофименко О. Г., Дубовой Я. В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства // Порівняльно-аналітичне право: електронне наукове фахове видання. 2017, № 1. С. 189–192.
145. Google: зловещая черта. URL: https://eurasia.film/2019/08/google-v-tvoej-golove/. (Дата звернення 12.02.2022).
146. Esteve A. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. International Data Privacy Law, 2017, № 7(1), pp. 36–47. DOI: https://10.1093/idpl/ipw026.
147. ISO/IEC 2382:2015. URL: https://habr.com/ru/company/trinion/blog/426509/. (Дата звернення 12.02.2022).
148. Чердымова Е.И., Борисова М.О., Перемышлина Е.С., Пешнова Е.И., Щукина А.Н. Госконтроль за интернет-трафиком в XXI веке. URL: https://bit.ly/3y6x13C. (Дата звернення 02.07.2022).
149. Белявский Д. DNS: кто не спрятался, тот и виноват. Интернет в цифрах, 2015, №1(21), С. 74–77.
150. Bumanglag K., Kettani H. On the Impact of DNS Over HTTPS Paradigm on Cyber Systems // 3rd International Conference on Information and Computer Technologies (ICICT) (San Jose, CA, USA), pp. 494–499, DOI: 10.1109/ICICT50521.2020.00085.
151. How to Enable DNS Over HTTPS in Chrome, Firefox, Edge, Brave & More? Fossbytes. URL: https://fossbytes.com/how-to-enable-dns-over-https-on-chrome-firefox-edge-brave/. (Дата звернення 02.07.2022 р.
152. Т.В. Батура, Ф.А. Мурзин, А.В. Проскуряков Программный комплекс для анализа данных из социальных сетей // Программные продукты и системы. 2015. №4(112), С. 188-197.

153. Лєнков С. В. Концептуальна схема системи інтелектуальної обробки даних. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, 2014, №46, С. 181-190.
154. Сергєєва Н. П. Методичні основи побудови атрибутивних баз даних географічних інформаційних систем (на прикладі демографічних атрибутів). // Молодий вчений, 2015, №4(2), С. 104-108.
155. Разработка прогностической модели информационного образа пользователя с применением автоматизированных средств обработки данных из социальных сетей. URL: https://bit.ly/3bE8StG. (Дата звернення 02.07.2022).
156. Pal Aditya, Counts Scott. Identifying topical authorities in microblogs. // Proceedings of the fourth ACM international conference on Web search and data mining. 2011. pp. 45-54.
157. Лихачев А.Е. Разработка системы идентификации пользователей компьютерных сетей на основе анализа их поведения // Актуальные научные исследования в современном мире. № 4-3(36), 2018, С. 141-144.
158. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І. Вернадського. – К., 2021. – №2 (лютий). – 280 с.
159. Проблемные аспекты деперсонализации цифровых изображений / А. В. Задерейко, А. В. Троянский, Н. И. Логинова, Е. Г. Трофименко // Інформатика та мат. методи в моделюванні. – 2017. – Т. 7, № 1-2. – С. 37–46.
160. The implementation of depersonalization algorithm of digital images. A. Zadereyko, N. Loginova, A. Troyanskiy, E. Trofimenko. 2nd International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017), Lviv, Ukraine, July 4-7, 2017, pp. 56 – 61.
161. Algorithm of user's personal data protection against data leaks in Windows 10 OS / Olexander V. Zadereyko, Olena G. Trofymenko, Nataliia I. Loginova // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. – 2019, vol.9, – pp. 41 – 44.
162. Natesan, Shriya & Gupta, Megha & Iyer, Lakshmi & Sharma, Deepak. Detection of Data Leaks from Android Applications // Second International Conference on Inventive Research in Computing Applications (ICIRCA). 2020, pp. 326-332. DOI: 10.1109/ICIRCA48905.2020.9183066.
163. Mohammad Naseri, Nataniel Borges Jr., Andreas Zeller, Romain Rouvoy. AccessiLeaks: Investigating Privacy Leaks Exposed by the Android Accessibility Service // Proceedings on Privacy Enhancing Technologies, 2019, №2. pp. 291-305. DOI: 10.2478/popets-2019-0031.
164. Задерейко О. В. Анализ утечек данных пользователей в мобильных приложениях / Кібербезпека в сучасному світі : матеріали ІІ Всеукраїнської

науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видав ничий дім «Гельветика», 2020. – С. 108 – 114.

165. Kewate Neha. A Review on AWS – Cloud Computing Technology. International Journal for Research in Applied Science and Engineering Technology. 2022, №10. pp. 258-263. DOI: 10.22214/ijraset.2022.39802. URL: https://bit.ly/3y8Ckjd. (Дата звернення 02.07.2022).
166. Nawrocki, Marcin & Koch, Maynard & Schmidt, Thomas & Wählisch, Matthias. (2021). Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure. URL: https://bit.ly/3R4so2T. Дата звернення 12.02.2022 р.
167. Developing a platform strategy for Akamai Cloudlet applications. URL: https://bit.ly/3ug4Can. (Дата звернення 02.07.2022).
168. Omoyiola, Bayo Olushola. (2020). Strategies for Securing Cloud Services. 22. 13-19. DOI: 10.9790/0661-2201031319. URL: https://bit.ly/3y7qFkr. (Дата звернення 02.07.2022).
169. Talbi Jamal, Haqiq Abdelkrim. Towards a Cybersecurity Model for Selecting the Secured Cloud Service Provider using Security Risk Approach // International Journal of Computer Applications. 2015, V.125 – №12. pp. 1-6. DOI: 10.5120/ijca2015906146.
170. Singh, Kapil & Verma, Sanjay & Sharib, Md & Soni, Nitasha & Kumar, Krishan. Security Threats to Cloud Services // International Journal of Engineering and Advanced Technology. 2020, №9(5), pp. 40-43. DOI: 10.35940/ijeat.E9214.069520.
171. Кожомбаева А.Т., Щетилов А.В., Зотин А.Г. Анализ технологий взаимодействия мобильных приложений с веб-сервисами // Актуальные проблемы авиации и космонавтики. 2015. №1(11). С. 403-405.
172. Kizza, Joseph. (2020). Cloud Computing Technology and Security. DOI: 10.1007/978-3-030-38141-7_22. URL: https://bit.ly/3R4viVi. (Дата звернення 02.07.2022).
173. Wireshark. URL: https://www.wireshark.org/. (Дата звернення: 02.06.2022).
174. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Аналіз витоків даних у інформаційних системах. Сучасна спеціальна техніка. № 3 (66), 2021, С. 16-30.
175. No Root Firewall. URL: https://bit.ly/3OU0k0e. (Дата звернення: 02.09.2021).
176. Windows Firewall Control. URL: https://binisoft.org/wfc. (Дата звернення: 02.06.2022).
177. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Дика А.І. Захист даних користувачів в інформаційних системах. Сучасна спеціальна техніка. № 1 (68), 2022, С. 23-33.

178. What Is the Service Host Process (svchost.exe) and Why Are So Many Running? URL: https://www.howtogeek.com/howto/windows-vista/what-is-svchostexe-and-why-is-it-running/. (Дата звернення 02.07.2022).
179. What is svchost.exe? 5 ways to see if it's safe. URL: https://www.glasswire.com/process/svchost.exe.html. (Дата звернення 02.07.2022).
180. Fix svchost.exe (netsvcs) High CPU Usage or Memory Leak Issue. URL: https://whatsabyte.com/svchost-exe-netsvcs-high-cpu/. (Дата звернення 02.07.2022).
181. N. Naik and P. Jenkins, «Enhancing Windows Firewall Security Using Fuzzy Reasoning,» 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016, pp. 263-269, DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.64.
182. Bo Yu, «Based on the network sniffer implement network monitoring,» 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010, pp. V7-1-V7-3, DOI: 10.1109/ICCASM.2010.5620505.
183. Algorithm of user's personal data protection against data leaks in Windows 10 OS / Olexander V. Zadereyko, Olena G. Trofymenko, Nataliia I. Loginova // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, vol.9, – pp. 41 – 44. URL: https://bit.ly/3nrXxQd.
184. Zadereyko A. Development of algorithm to protect user communication devices against data leaks / A. Zadereyko, Y. Prokop, O. Trofymenko, N. Loginova, O. Plachinda // Eastern-European Journal of Enterprise Technologies. – V. 1/2 (109) – Technology Center, 2021. – pp. 24 – 34. URL: http://dspace.onua.edu.ua/handle/11300/14489.
185. 185. Задерейко О.В., Кухаренко С.В. Захист персональних даних від витоків в операційних системах сімейства Windows / Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 1. – С. 685 – 689.
186. Гасанова А. М. Телеграм-бот для гуртожитку на мові високого рівня програмування. – Дипломна робота на здобуття ступеня бакалавра спеціальності «Комп'ютерні науки», «Інформаційні управляючі системи та технології». – Національний авіаційний університет. – Київ, 2021. – 54 с.
187. Security Analysis of Telegram. URL: https://courses.csail.mit.edu/6.857/2017/project/19.pdf. (Дата звернення 2.07.22).
188. Ots K. Network Security. In: Azure Security Handbook. Apress, Berkeley, CA. 2021, DOI: https://doi.org/10.1007/978-1-4842-7292-3_4.

189. W. Wingerath et al. Speed Kit: A Polyglot & GDPR-Compliant Approach For Caching Personalized Content, 2020 IEEE 36th International Conference on Data Engineering (ICDE), 2020, pp. 1603-1608, DOI: 10.1109/ICDE48307.2020.00142.
190. S. Salvi, V. Geetha и S. Sowmya Kamath, » Jamura: A Conversational Smart Home Assistant Built on Telegram and Google Dialogflow», TENCON 2019 – 2019 IEEE Region 10 Conference (TENCON), 2019, стр. 1564-1571, DOI: 10.1109 / TENCON.2019.8929316.
191. Bots in libr Bots in libraries: The aries: They're coming for coming for your jobs (or is it?) our jobs (or is it?). URL: https://bit.ly/3NDWA1E. (Дата звернення 2.07.2022).
192. Cdns' dark side: identifying security problems in cdn-to-origin connections. URL: https://users.encs.concordia.ca/~mmannan/student-resources/Thesis-MASc-Shobiri-2021.pdf. (Дата звернення 2.07.2022).
193. Abegaz B. W. DNS Services, alternative ways of using DNS infrastructures. – Delft: TNO, 2011. URL: https://repository.tudelft.nl/islandora/object/uuid:1e0114b7-d907-499e-bb20-fa83753d8067/datastream/URL/download. (Дата звернення 2.07.2022).
194. 194. Задерейко О.В., Янковський О.Г., Дика А. І. Забезпечення конфіденційності месенджера Telegram / Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 1. – С. 708 – 715.

Наукове видання

Олександр Владиславович Задерейко,
Олександр Вячеславович Троянський,
Рашид Ібрагимович Чанишев
Анастасія Іванівна Дика

КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

Монографія

2-ге видання, перероблене і доповнене

Підписано до друку 08.07.2022.
Формат 60х84/16. Ум-друк. арк. 12,79.
Наклад 100 прим. Зам. № 2207-03.

Видано і віддруковано в ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
Тел. +38 050 7775901 +38 048 7959160
e-mail: fenix-izd@ukr.net
www.feniksbooks.com