

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
БІЛОЦЕРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ

Спеціальність 281 «Публічне управління та адміністрування»

Допускається до захисту

Завідувач кафедри публічного управління,
адміністрування та міжнародної економіки


назва кафедри
професор Сокольська Т.В.
підпис, вчене звання, прізвище, ініціали
« 01 » листопада 2024 року

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД ТА ПРАКТИКА УКРАЇНИ

Виконав: Ронський Антон Андрійович

прізвище, ім'я, по батькові

підпис

Керівник: доцент Панасюк Вікторія Іллівна

вчене звання, прізвище, ім'я, по батькові

підпис

Рецензент: доцент Гаврик Олеся Юріївна

вчене звання, прізвище, ім'я, по батькові

підпис

Я, Ронський Антон Андрійович, засвідчую, що кваліфікаційну роботу магістра виконано з дотриманням принципів академічної доброчесності.

Біла Церква – 2024

РЕФЕРАТ

Ронський Антон Андрійович «Державна політика у сфері забезпечення кібербезпеки: міжнародний досвід та практика України»

Досліджено теоретичні основи державної політики у сфері забезпечення кібербезпеки і розроблено практичні рекомендації для України з урахуванням міжнародного досвіду.

Виявлено сутність та складові поняття сфери кібербезпеки; узагальнено методи протидії кіберзлочинності в системі міжнародних відносин; узагальнено нормативно-правове забезпечення державної політики кібербезпеки України; проведено аналіз діяльності Державної служби спеціального зв'язку та захисту інформації України як органу реалізації державної політики кібербезпеки; з'ясовано практичні підходи до кіберзахисту критичної інфраструктури; обґрунтовано міжнародний досвід та практику України в удосконаленні державної політики забезпечення кібербезпеки.

Зроблено висновок, що для удосконалення складових національної політики кібербезпеки важливою є гармонізація національного законодавства в сфері кібербезпеки із законодавством ЄС; впровадження стандартів і рекомендацій, розроблених МСЕ, які стосуються технічних аспектів забезпечення кібербезпеки; створення на національному та регіональних рівнях спеціальних організаційних структур і команд протидії кіберзагрозам різного характеру.

Одержані результати можуть бути використані в діяльності Державної служби спеціального зв'язку та захисту інформації України в напрямі формування та реалізації державної політики кібербезпеки; а також нормативно-правового забезпечення державної політики кібербезпеки України з урахуванням пропозиції апробованих практикою міжнародних організацій.

Кваліфікаційна робота магістра містить 83 сторінки, 1 таблицю, 3 рисунки, список використаних джерел із 58 найменувань.

Ключові слова: кібербезпека, політика кібербезпеки, кіберзахист, критична інфраструктура, служба спеціального зв'язку та захисту інформації.

ANNOTATION

Ronskyi Anton Andriyovych "State policy in the sphere of ensuring cyber security: international experience and practice of Ukraine"

It has been investigated the theoretical foundations of state policy in the field of cyber security and develops practical recommendations for Ukraine, taking into account international experience.

It was revealed the essence and constituent concepts of the field of cyber security are revealed; the methods of combating cybercrime in the system of international relations are summarized; normative and legal support of the state cyber security policy of Ukraine is summarized; an analysis of the activities of the State Service for Special Communications and Information Protection of Ukraine as a body for implementing the state cyber security policy was carried out; practical approaches to cyber protection of critical infrastructure are clarified; the international experience and practice of Ukraine in improving the state policy of ensuring cyber security are substantiated.

It has been concluded that the harmonization of national legislation in the field of cyber security with EU legislation is important for improving the components of the national cyber security policy; implementation of standards and recommendations developed by the ITU, which relate to the technical aspects of ensuring cyber security; creation at the national and regional levels of special organizational structures and teams to counter cyber threats of various nature.

The results can be used in the activities of the State Service for Special Communications and Information Protection of Ukraine in the direction of the formation and implementation of the state cyber security policy; as well as regulatory and legal support of the state policy of cyber security of Ukraine, taking into account the proposals of international organizations tested by practice.

The master's thesis contains 83 pages, 1 table, 3 drawings, a list of used sources from 64 names.

Keywords: cyber security, cyber security policy, cyber defense, critical infrastructure, special communications and information protection service.

ЗМІСТ

ВСТУП.....	6
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ.....	9
1.1. Сутність та складові поняття сфери кібербезпеки	9
1.2. Методи протидії кіберзлочинності в системі міжнародних відносин	15
1.3. Нормативно-правове забезпечення державної політики у сфері кібербезпеки України	23
Висновки до розділу 1	29
РОЗДІЛ 2. ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ	30
2.1. Державна служба спеціального зв'язку та захисту інформації України як орган реалізації державної політики кібербезпеки	30
2.2. Міжнародна практика реалізації державної політики кібербезпеки..	34
2.3. Практичні підходи до кіберзахисту критичної інфраструктури	43
Висновки до розділу 2	51
РОЗДІЛ 3. МІЖНАРОДНИЙ ДОСВІД ТА ПРАКТИКА УКРАЇНИ В УДОСКОНАЛЕННІ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ	52
3.1. Міжнародна практика реалізації складових державної політики кібербезпеки	52
3.2. Ефективність та результативність забезпечення політики кіберзахисту в Україні	59
Висновки до розділу 3	65
ВИСНОВКИ	67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	71
ДОДАТОК А	78

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хоббі Ю. С. Право людини на кібербезпеку: проблеми, визначення та гарантування. *Юридичний вісник*. Одеса : Гельветика. 2020. № 2. С. 37-43. URL: <http://dspace.onua.edu.ua/handle/11300/16902>
2. Кормич Б.А. Кібербезпека: організаційно-правові основи : Навч. посібн. К. : Кондор, 2008. 382 с].
3. Кібербезпека держави: підручник. /В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.; в 2 т. Т. 2. / за заг. ред. В.В. Остроухова. К. : ДНУ «Книжкова палата України», 2016. 328 с.
4. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи кібербезпеки . За ред. проф. В.О. Хорошка. вид., доп. і перероб. К. : Вид. ДУІКТ, 2009. 292 с.
- 5.Петрик В. Щодо визначення кібербезпеки та її різновидів . Форми та методи забезпечення кібер- 261 безпеки держави : зб. матер. міжнар. наук.-практ. конф. (м. Київ, 13 березня 2008 р.). К. : Видавець Захаренко В.О., 2008. 216 с.
6. Баранов О.А. Інформаційне право України : стан, проблеми, перспективи. К. : ВД «СофтПрес», 2005. 316 с.
7. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації : організаційно-правові питання теорії і практики : підручник для студ. вищ. навч. закл. / Р.А. Калюжний, В.О. Шамрай, М.Я. Швець та ін. ; за ред. Р.А. Калюжного та В.О. Шамрая. К. : Академія державно-податкової служби України, 2002. 296 с.
8. Цимбалюк В.С. Інформаційне право (основи теорії і практики). Монографія. К. : «Освіта України», 2010. 388 с.
9. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. 272 с.
10. Про План реалізації Стратегії кібербезпеки України: рішення Ради національної безпеки і оборони України від 30 грудня 2021 року затверджене Указом Президента України №37/2022. URL: <https://www.president.gov.ua/documents/372022-41289>

11. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. URL: <https://ips.ligazakon.net/document/T172163>
12. Потій О., Семенченко А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту. *Науковий вісник: Державне управління*. 2021. № 3(9) С.136–162. URL: [https://doi.org/10.32689/2618-0065-2021-3\(9\)-136-162](https://doi.org/10.32689/2618-0065-2021-3(9)-136-162)
13. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term. URL: <http://www.infosecisland.com/blogview/23287- Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html>
14. Ponemon Institute. 2016. Cyber Security Mega Trends: Study of IT leaders in the U.S. federal government.
15. Ponemon Institute LLC. (2019). ‘Cybersecurity in Operational Technology: 7 Insights You Need to Know, March 2019’. Ponemon Institute LLC. URL: <https://lookbook.tenable.com/ee2b2c72-e552-43f6-843e-3a63a29d895c>.
16. Gorman S, Bernes JE (2011) Cyber combat: act of war. Wall Str J. 31 May 2011.
17. Lewis AJ, Neuneck G (2013) The Cyber Index. International security trends and realities. New York and Geneva, United Nations Institute for Disarmament Research
18. Dupont B (2012) L’environnement de la cybersecurite a l’horizon tendances, moteurs et implications. Note de recherche 14 Centre International de Criminology Compare. Universite de Montreal, Montreal
19. OECD (2012) Cybersecurity policy making at a turning point: analysing new generation of national cybersecurity strategies for the internet economy. OECD digital economy papers 21. OECD Publishing. URL: <http://dx.doi.org/10.1787/5k8zq92vdgtl-en>.
20. Bendiek A (2012) European cybersecurity policy. SWP website URL: www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf.
21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

22. Про внутрішнє та зовнішнє становище України у 2020 році: послання Президента України до Верховної Ради. URL: <https://www.president.gov.ua/news/poslannya-prezidenta-ukrayini-volodimira-zelenskogo-do-verho-64717> (дата звернення: 20.08.2024).

23. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія: "Юридичні науки"*. 2019. № 2. С. 23-28.

24. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Державне управління"*. 2019. № 1. С. 140-145.

25. Горун О.Ю. Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. *Інформація і Право*. 2021. № 2(37). С. 93-102. URL: <http://il.ippi.org.ua/article/view/238343>

26. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.21 р. № 179. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennya-nacionalnoyi-eko-a179> (дата звернення: 20.03.2024).

27. Концепція розвитку цифрових компетентностей: Розпорядження Кабінету Міністрів України від 03.03.21 р. № 167. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-p#Text> (дата звернення: 20.08.2024).

28. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури»: Указ Президента України від 16.01.17 р. № 8/2017. URL: <https://zakon.rada.gov.ua/laws/show/8/2017#n2> (дата звернення: 20.08.2024)

29. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 06.12.17 р. № 1009. URL: <https://zakon.rada.gov.ua/laws/show/1009-2017-p#Text> (дата звернення: 20.08.2024).

30. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518.

URL: <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> (дата звернення: 20.08.2024).

31. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 943. URL: <https://zakon.rada.gov.ua/laws/show/943-2020-п#Text> (дата звернення: 20.08.2024).

32. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : постанова Кабінету Міністрів України від 23.12.2020 р. № 1295. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text> (дата звернення : 17.05.2024).

33. UNIDIR. (2013). The cyber index, International security trends and realities. Geneva: UNIDIR, United Nations Institute for Disarmament Research

34. Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3), 9-19. Excelsior College, Albany.

35. Harknett, R., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Management. Berlin/New York: De Gruyter.

36. Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, <https://doi.org/10.1111/misr.12023>.

37. Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (pp. 3-23). Washington, D.C.: National Academy of Sciences.

38. Buzan, B., Waver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Boulder: Lynne Rienner.

39. Swiatkowska, J., et al. (2012). V4 cooperation in ensuring cyber security - Analysis and recommendations. Krakow: Kosciuszko Institute.

40. European Union Agency for Network and Information Security (ENISA). (2012). Cyber Europe 2012, key findings report, European Union Agency for Network and Information Security.

41. Saljic, E., & Bordevic, Z. (2011). Modern forms of terrorism Environmental terrorism. Retrieved from <https://dk.um.si/IzpisGradiva.php?lang=eng&id=30223> .

42. Saco, D. (1999). Colonizing cyberspace: "National security" and the Internet. In J. Weldes, M. Laffey, H. Gusterson, & R. Duvall (Eds.), Cultures of insecurity: States, communities, and the production of danger. Minneapolis: University of Minnesota Press.

43. Klimburg, A. and Healey, J. (2012) "Strategic Goals & Stakeholders" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn.

44. French Network and Information Security Agency, (2011) "Information Systems Defense and Security France's Strategy" [online] <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15>.

45. The UK Cabinet Office (2011) «The UK Cyber Security Strategy Protecting and promoting the UK in a digital world», https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

46. Bundesministerium des Innern, (2011) "Cyber-Sicherheitsstrategie für Deutschland". <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OEDVerwaltung/Informationsgesellschaft/cyber.pdf?blob=publicationFile>

47. Turkish Ministry of Transport (2013), Maritime Affairs and Communication, "National Cyber Security Strategy and Action Plan 2013-2014" Ankara [Online] http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf .

48. Наказ Адміністрації Держспецв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Site. URL: https://dut.edu.ua/ua/news-1-569-9870-metodichni--rekomendacii--schodo--pidvischennya--rivnya-kiberzahistu-kritichnoiinformaciynoi-infrastrukturi_kafedra-cistemtehnicnogo-zahistu-informacii . (дата звернення: 06.08.2024)

49. Пядишев В.Г. Кібербезпека критичних інфраструктур : закордонний досвід та українські реалії. *Південноукраїнський правничий часопис*. 2022. № 4. Ч. 3. С. 229-234. URL: <http://dspace.oduvs.edu.ua/handle/123456789/4525>

50. Cyber security Act 2018 operative from 31 August 2018 to protect critical information infrastructure against cybersecurity threats. Site. URL: <https://www.allenandgledhill.com/media/2996/ag-cybersecurityact-2018-operative-from-31-august-2018-to-protectcritical-information-infrastructure.pdf> (дата звернення: 06. 07.2024).

51. MCI response to PQ on Steps to Protect Singapore's Critical Infrastructure from Malware Threat. Parliament Sitting on 4 July 2022. Site. URL: <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/7/mci-response-to-pq-on-steps-to-protect-singaporecritical-infrastructure-from-malware-threat> . (дата звернення: 06.07.2024)

52. Leck, A., Chia, K. Singapore: New initiatives to ensure digital security and enhanced cyber resilience. Global Compliance News. March 26, 2022. Site. URL: <https://www.globalcompliancencews.com/2022/03/26/singapore-new-initiatives-toensure-digital-security-and-enhanced-cyberresilience-17032022> / (дата звернення: 06. 07.2024)

53. Security of Critical Infrastructure Act 2018, No. 29, 2018. Ausrtalia, Compilation No. 4. Compilation date: 2 April 2022. Includes amendments up to: Act No. 33, 2022. Registered: 2 May 2022. Site. URL: <https://www.legislation.gov.au/Details/C2022C00160> (дата звернення: 06. 07.2024)

54. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union territory. Site. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення: 06.08.2024)

55. Digital Agenda website: URL: http://ec.europa.eu/information_society/newsroom/cf/pillar.cfm?pillar_id=45 .

56. ITU: Committed to connecting the world. URL: <https://www.itu.int/>

57. Державна служба спеціального зв'язку та захисту інформації України.
Сайт. URL: <https://cip.gov.ua/ua>
58. Правове забезпечення кіберзахисту в Україні. URL:
<https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini>.