Український державний університет залізничного транспорту

Кафедра менеджменту, публічного управління та HR-технологій

ПУБЛІЧНЕ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ В УМОВАХ ЦИФРОВИХ ТА ГІБРИДНИХ ЗАГРОЗ

Пояснювальна записка і розрахунки
до кваліфікаційної роботи магістра
за освітньою програмою «Публічне управління та адміністрування»
спеціальності 281 «Публічне управління та адміністрування»

КРМ. 281.12218035 ПЗ

Розробив здобувач вищої освіти
за другим (магістерським) рівнем
(роботу виконано самостійно,
відповідно до принципів
академічної доброчесності)
групи 219-ПУА-з24
Денис КОВАЛЕВСЬКИЙ

Керівник: професор, д-р ек. наук
Олександр ДЕЙНЕКА

Рецензент: професор, д-р ек. наук
Вікторія ОВЧИННІКОВА

2026

АНОТАЦІЯ

Дана кваліфікаційна робота включає в себе 16 слайдів презентації, 89 аркушів пояснювальної записки формату А4, що включає 21 таблицю, 76 літературних джерел.

Ключові слова: ПУБЛІЧНЕ УПРАВЛІННЯ, КІБЕРБЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, ЦИФРОВІ ТА ГІБРИДНІ ЗАГРОЗИ, НАЦІОНАЛЬНА БЕЗПЕКА, КІБЕРЗАХИСТ.

Об’єктом дослідження є система публічного управління у сфері кібербезпеки держави.

Метою дослідження є є обґрунтування теоретико-методологічних засад і розроблення практичних рекомендацій щодо вдосконалення публічного управління кібербезпекою критичної інфраструктури держави в умовах цифрових та гібридних загроз.

У кваліфікаційній роботі досліджено публічне управління кібербезпекою критичної інфраструктури держави в умовах цифрових та гібридних загроз. Обґрунтовано управлінські механізми забезпечення кібербезпеки, що реалізуються на стратегічному, інституційному та операційному рівнях з урахуванням особливостей функціонування об’єктів критичної інфраструктури.

Проведено комплексний аналіз інституційно-правового забезпечення та практики публічного управління у сфері кіберзахисту, зокрема оцінено спроможність системи кібербезпеки критичної інфраструктури та визначено ключові ризики, пов’язані з гібридними загрозами.

Розроблено напрями вдосконалення публічного управління кібербезпекою, орієнтовані на підвищення стійкості держави, інтеграцію цифрових інструментів та формування стратегічних пріоритетів розвитку кібербезпеки в умовах гібридної війни.

ABSTRACT

This qualification thesis consists of 16 presentation slides and 89 A4 pages of an explanatory note, which includes 21 tables and 76 bibliographic sources.

Keywords: PUBLIC ADMINISTRATION, CYBERSECURITY, CRITICAL INFRASTRUCTURE, DIGITAL AND HYBRID THREATS, NATIONAL SECURITY, CYBER PROTECTION.

The object of the research is the system of public administration in the field of state cybersecurity.

The aim of the research is to substantiate the theoretical and methodological foundations and to develop practical recommendations for improving public administration of cybersecurity of the state’s critical infrastructure under conditions of digital and hybrid threats.

The qualification thesis examines public administration of cybersecurity of the state’s critical infrastructure under conditions of digital and hybrid threats. Management mechanisms for ensuring cybersecurity are substantiated, implemented at the strategic, institutional, and operational levels, taking into account the specific features of the functioning of critical infrastructure facilities.

A comprehensive analysis of the institutional and legal framework and public administration practices in the field of cyber protection has been conducted, including an assessment of the capacity of the critical infrastructure cybersecurity system and the identification of key risks associated with hybrid threats.

Directions for improving public administration of cybersecurity have been developed, aimed at enhancing state resilience, integrating digital tools, and forming strategic priorities for cybersecurity development in the context of hybrid warfare.

Український державний університет залізничного транспорту

Факультет економічний
Кафедра менеджменту, публічного управління та HR-технологій
Ступінь вищої освіти: магістр
Освітня програма: «Публічне управління та адміністрування»
Спеціальність: 281 «Публічне управління та адміністрування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
професор, д-р ек. наук
_____ Олена ДИКАНЬ
«28» жовтня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА
Денису Ковалевському

1 Тема «Публічне управління кібербезпекою критичної інфраструктури держави в умовах цифрових та гібридних загроз»
керівник Олександр Дейнека, д-р ек. наук, професор
затверджено розпорядженням по економічному факультету від «27» лютого 2025 року № 72/25
2 Строк подання здобувачем вищої освіти закінченої роботи «17» січня 2026 року
3 Вихідні дані закони та підзаконні нормативно-правові акти України і Європейського Союзу, що регулюють сферу кібербезпеки та захисту критичної інфраструктури держави, стратегічні документи і рекомендації міжнародних організацій, публікації провідних вітчизняних і зарубіжних учених, монографічні дослідження фахівців із проблематики публічного управління кібербезпекою, національної стійкості та управління ризиками, аналітичні звіти міжнародних інституцій, матеріали органів публічної влади, а також відкриті інформаційні ресурси мережі Інтернет.
4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Кібербезпека держави як об'єкт публічного управління та складова національної безпеки. Цифрові та гібридні загрози у системі ризиків критичної інфраструктури. Методологічні підходи до управління кіберризиками об'єктів критичної інфраструктури. Система суб'єктів публічного управління кібербезпекою та їх повноваження. Нормативно-правове забезпечення кіберзахисту критичної інфраструктури. Міжвідомча та публічно-приватна взаємодія у сфері кібербезпеки. Оцінювання спроможності системи кіберзахисту критичної інфраструктури держави. Цифрові інструменти та інноваційні механізми

публічного управління кібербезпекою. Стратегічні пріоритети розвитку публічного управління кібербезпекою в умовах гібридної війни.

5 Перелік графічного матеріалу

1 Теоретико-методологічні засади публічного управління кібербезпекою держави - шість слайдів. 2 Інституційно-правові механізми публічного управління кібербезпекою критичної інфраструктури - три слайди. 3 Напрями вдосконалення публічного управління кібербезпекою в умовах цифрових та гібридних загроз - сім слайдів.

6 Консультанти окремих розділів

Розділ	Прізвище, ініціали, посада та науковий ступінь консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 27 жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів	Строк виконання етапів роботи	Примітка
1 Теоретико-методологічні засади публічного управління кібербезпекою держави	20.11.2025	
2 Інституційно-правові механізми публічного управління кібербезпекою критичної інфраструктури	15.12.2025	
3 Напрями вдосконалення публічного управління кібербезпекою в умовах цифрових та гібридних загроз	08.01.2026	
4 Графічна частина	15.01.2026	

Здобувач вищої освіти _____ Денис КОВАЛЕВСЬКИЙ

Керівник _____ Олександр ДЕЙНЕКА

Зміст

Список використаних джерел

1 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022.

2 ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity. Geneva : International Organization for Standardization, 2012.

3 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

4 OECD. Digital Security Risk Management for Economic and Social Prosperity. Paris : OECD Publishing, 2015.

5 European Commission. EU Cybersecurity Strategy for the Digital Decade. Brussels, 2020.

6 NATO. NATO Cyber Defence Policy. Brussels : North Atlantic Treaty Organization.

7 ENISA. ENISA Threat Landscape. Heraklion : European Union Agency for Cybersecurity.

8 NIST. Cybersecurity Framework. Gaithersburg, MD : National Institute of Standards and Technology.

9 Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities. Official Journal of the European Union. 2022. L 333.

10 Kooiman J. Governing as Governance. London : Sage Publications, 2003. 280 p.

11 National Research Council. Cybersecurity and Critical Infrastructure Protection. Washington, DC : National Academies Press, 2014. 156 p.

12 ENISA. Threat Landscape for Cyber-Physical Systems. Heraklion : European Union Agency for Cybersecurity.

13 CISA. Securing Critical Infrastructure. Washington, DC : Cybersecurity and Infrastructure Security Agency.

14 NATO. Hybrid Threats and Cyber Defence. Brussels : North Atlantic Treaty Organization.

15 World Economic Forum. Global Risks Report. Geneva : World Economic Forum.

16 NIST. Cybersecurity Framework. Version 1.1. Gaithersburg, MD : National Institute of Standards and Technology.

17 ISO/IEC 27005:2018. Information security risk management. Geneva : International Organization for Standardization, 2018.

18 European Commission, Joint Research Centre. Cybersecurity of Critical Infrastructure. Luxembourg : Publications Office of the European Union.

19 European Commission. Critical Infrastructure Protection in the Digital Era. Brussels.

20 OECD. Enhancing the Digital Security of Critical Infrastructure. Paris : OECD Publishing.

21 ISO 31000:2018. Risk management – Guidelines. Geneva : International Organization for Standardization, 2018.

22 OECD. Digital Security Risk Management for Economic and Social Prosperity. Paris : OECD Publishing.

23 SO/IEC 27005:2018. Information security risk management. Geneva : International Organization for Standardization, 2018.

24 NIST. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD : National Institute of Standards and Technology.

25 Directive (EU) 2022/2555 (NIS 2) of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union. 2022. L 333.

26 ENISA. Risk Management for Cybersecurity. Heraklion : European Union Agency for Cybersecurity.

27 European Union Agency for Cybersecurity (ENISA). Scenario-based Cyber Risk Assessment. Heraklion.

28 Kjaer A. M. Governance. Cambridge : Polity Press, 2004. 192 p.

29 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 29.11.2025).

30 Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 29.11.2025).

31 Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 29.11.2025).

32 Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 29.11.2025).

33 Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 29.11.2025).

34 Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF (дата звернення: 29.11.2025).

35 Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 11.11.2020 № 1176 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF (дата звернення: 29.11.2025).

36 Деякі питання забезпечення функціонування системи виявлення вразливостей : Постанова Кабінету Міністрів України від 23.12.2020 № 1295 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF (дата звернення: 29.11.2025).

37 Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України від 29.12.2021 № 1426 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF (дата звернення: 29.11.2025).

38 Деякі питання реагування суб'єктами кібербезпеки на кіберінциденти : Постанова Кабінету Міністрів України від 04.04.2023 № 299 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF (дата звернення: 29.11.2025).

39 Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF (дата звернення: 29.11.2025).

40 Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 943 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (дата звернення: 29.11.2025).

41 Про затвердження Порядку пошуку та виявлення потенційної вразливості в інформаційно-технологічних системах : Постанова Кабінету Міністрів України від 16.05.2023 № 497 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF (дата звернення: 29.11.2025).

42 Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/z023-21 (дата звернення: 29.11.2025).

43 Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021 : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 29.11.2025).

44 Про засади державної регуляторної політики у сфері господарської діяльності : Закон України від 11.09.2003 № 1160-IV : станом на 20.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/1160-15 (дата звернення: 29.11.2025).

45 Дяченко О. П. Кібербезпека як складова національної безпеки України. Стратегічні пріоритети. 2021. № 2. С. 45–53.

46 Ситник Г. П., Абрамов В. І. Публічне управління у сфері національної безпеки: нові виклики цифрової доби. Державне управління: теорія та практика. 2020. № 1. С. 5–17.

47 Мельник А. Ф. Інституційні механізми забезпечення кібербезпеки в Україні. Публічне управління та адміністрування. 2022. № 4. С. 21–30.

48 Кравченко С. О. Критична інфраструктура як об’єкт публічного управління в умовах гібридної війни. Вісник НАДУ. Серія «Державне управління». 2023. № 1. С. 32–41.

49 Романенко Є. О. Цифрове врядування і кібербезпека: точки перетину. Економіка та держава. 2021. № 9. С. 74–79.

50 Куйбіда В. С., Петроє О. М. Стратегічне управління безпекою в умовах криз і невизначеності. Державне управління та місцеве самоврядування. 2020. № 3. С. 8–18.

51 Ліпкан В. А. Кіберпростір як поле гібридного протистояння. Право і безпека. 2019. № 4. С. 15–22.

52 Шевченко М. М. Управління ризиками у сфері кібербезпеки критичної інфраструктури. Інвестиції: практика та досвід. 2022. № 14. С. 102–108.

53 Гребенюк М. В. Публічно-приватне партнерство у сфері кібербезпеки: європейський досвід. Європейські студії. 2021. № 2. С. 59–68.

54 Ільченко О. Ю. Інформаційна стійкість держави в умовах гібридних загроз. Політичне життя. 2023. № 1. С. 44–52.

55 Dunn Cavelty M. Cybersecurity as a governance problem. Journal of Cyber Policy. 2018. Vol. 3, no. 3. P. 307–325.URL: https://doi.org/10.1080/23738871.2018.1559253 (date of access: 10.12.2025).

56 Christou G. Cybersecurity in the European Union: Resilience and Adaptability. European Security. 2020. Vol. 29, no. 4. P. 465–482.URL: https://doi.org/10.1080/09662839.2020.1789186 (date of access: 10.12.2025).

57 Boeke S. National cybersecurity strategies: The rise of resilience. International Affairs. 2021. Vol. 97, no. 3. P. 729–746.URL: https://doi.org/10.1093/ia/iiab025 (date of access: 10.12.2025).

58 Bendiek A., Porter T. The EU's cybersecurity policy: New risks, new responses. SWP Research Paper. 2019. No. 11. P. 1–32.

59 Carr M. Public–private partnerships in national cyber-security strategies. International Affairs. 2016. Vol. 92, no. 1. P. 43–62.URL: https://doi.org/10.1111/1468-2346.12504 (date of access: 10.12.2025).

60 Kostyuk N., Wayne C. Theorizing cyber escalation dynamics. Journal of Cybersecurity. 2021. Vol. 7, no. 1. P. 1–15.URL: https://doi.org/10.1093/cybsec/tyab006 (date of access: 10.12.2025).

61 Healey J. The implications of persistent cyber conflict. Survival. 2020. Vol. 62, no. 1. P. 67–86.URL: https://doi.org/10.1080/00396338.2020.1712122 (date of access: 10.12.2025).

62 Bada M., Nurse J. Developing cybersecurity education and awareness programmes. Information & Computer Security. 2019. Vol. 27, no. 3. P. 393–410.URL: https://doi.org/10.1108/ICS-07-2018-0090 (date of access: 10.12.2025).

63 Madnick S., Kafatos P. Cybersecurity, resilience and critical infrastructure. MIT Sloan Working Paper. 2020. P. 1–18.

64 Tikk E. Cyber resilience as a strategic objective. NATO Review. 2022.URL: https://www.nato.int/docu/review/articles/2022 (date of access: 10.12.2025).

65 Linkov I., Trump B. The science and practice of resilience. Environment Systems and Decisions. 2019. Vol. 39, no. 4. P. 329–331.URL: https://doi.org/10.1007/s10669-019-09732-7 (date of access: 10.12.2025).

66 Radu R. Negotiating Internet governance. Oxford: Oxford University Press, 2019. (розділи).

67 Dupont B. Cybersecurity futures: How can we regulate emerging risks? Technology in Society. 2021. Vol. 67. P. 101761.URL: https://doi.org/10.1016/j.techsoc.2021.101761 (date of access: 10.12.2025).

68 van Eeten M., Mueller M. Where is the governance in Internet governance? New Media & Society. 2019. Vol. 21, no. 6. P. 1364–1383.URL: https://doi.org/10.1177/1461444818813634 (date of access: 10.12.2025).

69 Buchanan B. The cybersecurity dilemma. Survival. 2017. Vol. 59, no. 4. P. 7–36.URL: https://doi.org/10.1080/00396338.2017.1349751 (date of access: 10.12.2025).

70 Schneider F. Cybersecurity governance in critical infrastructures. IEEE Security & Privacy. 2020. Vol. 18, no. 2. P. 65–71.

71 Shackelford S. Governing cybersecurity. Cambridge: Cambridge University Press, 2020. (окремі статті).

72 Björck F. et al. Cyber resilience fundamentals for a digital society. Computers & Security. 2019. Vol. 87. P. 101610.URL: https://doi.org/10.1016/j.cose.2019.101610 (date of access: 10.12.2025).

73 Pursiainen C. Critical infrastructure resilience. Security Dialogue. 2018. Vol. 49, no. 4. P. 295–309.

74 Deibert R. Toward a human-centric approach to cybersecurity. Journal of Cyber Policy. 2023. Vol. 8, no. 1. P. 1–18.URL: https://doi.org/10.1080/23738871.2023.2174821 (date of access: 10.12.2025).

75 Студентська навчальна звітність. Текстова частина (пояснювальна записка). Загальні вимоги до побудови, викладення та оформлення : методичний посібник з додержання вимог нормоконтролю у студентській навчальній звітності / уклад. Л. М. Козар, Є. В. Коновалов, А. О. Лапко, О. Е. Наумова, Г. В. Шаповал,

Д. В. Шумик, В. М. Петухов, С. В. Панарін. Харків : УкрДУЗТ, 2014. 46 с.

76 Методичні вказівки до виконання кваліфікаційної роботи для здобувачів другого (магістерського) рівня спеціальності 281 «Публічне управління і адміністрування» / уклад. О. В. Дикань, Ю. О. Крихтіна, Л. С. Коновалов ; кафедра менеджменту і адміністрування. Харків : УкрДУЗТ, 2022. 40 с.

77 Ковалевський Д. Організаційні засади публічного управління кібербезпекою держави // Тези 85-ї студентської науково-технічної конференції (10–11 грудня 2025 р.). Харків : Український державний університет залізничного транспорту, 2025. С. 569–570.