МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ
ФАКУЛЬТЕТ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ
КАФЕДРА ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

МАГІСТЕРСЬКА РОБОТА ЗА ФАХОМ

«ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ СТРАТЕГІЧНИХ ОБ'ЄКТІВ УКРАЇНИ»

здобувача вищої освіти другого (магістерського) рівня вищої освіти освітньо-професійної програми 251 «Державна безпека»
Спеціалізація – Організація забезпечення державної безпеки підрозділами Національної гвардії України
Подоляка Дмитра Сергійовича
Науковий керівник:
Комісарова Наталя Олександрівна
доцент кафедри забезпечення державної безпеки, кандидат юридичних наук, доцент, полковник

Магістерська робота захищена з оцінкою
«___» 20__ р.

Київ – 2026

АНОТАЦІЯ

Подоляк Дмитро Сергійович "Організаційно-правовий механізм захисту стратегічних об'єктів України".– Рукопис.

Магістерська робота за спеціальністю 251 Державна безпека – Київський інститут Національної гвардії України, Київ, 2025.

Магістерська робота присвячена комплексному дослідженню організаційно-правового механізму захисту стратегічних об'єктів України в контексті забезпечення національної безпеки. Актуальність дослідження обумовлена критичною важливістю захисту об'єктів критичної інфраструктури в умовах зростаючих кіберзагроз, техногенних та природних ризиків, внутрішніх загроз суспільного характеру та воєнно-стратегічних викликів, особливо в умовах повномасштабної збройної агресії Російської Федерації проти України.

У роботі проаналізовано концепції критичної інфраструктури та її роль у забезпеченні національної безпеки, досліджено міжнародний досвід визначення критичної інфраструктури (США, Німеччина, Великобританія, Нідерланди) та запропоновано визначення для України. Систематизовано основні види критичної інфраструктури: енергетична, транспортна, інформаційна, медична та фінансова інфраструктура.

Здійснено комплексну оцінку сучасних викликів та вразливостей життєво важливих систем. Проаналізовано кібернетичні виклики, досліджено основні методи кібератак, технологічні та природні ризики.

Досліджено внутрішні загрози суспільного характеру, зокрема вплив економічних криз 2008-2009, 2014-2015 та 2022-2025 років на енергетичний, транспортний, комунальний сектори та охорону здоров'я. Проаналізовано вплив соціальних протестів 2021-2025 років на критичну інфраструктуру через фізичне пошкодження об'єктів та блокування доступу. Окрему увагу приділено воєнно-стратегічним викликам: масовані атаки на енергетичну

інфраструктуру, що вплинуло на медичні заклади, освітню сферу та побутові умови населення.

Детально розглянуто досвід застосування сил Національної гвардії України для забезпечення безпеки стратегічних об'єктів за умов особливого правового режиму. Проаналізовано організацію охорони об'єктів критичної інфраструктури, включаючи визначення критичних об'єктів, встановлення захисних заходів (фізичні бар'єри, системи контролю доступу, відеоспостереження). Досліджено системи ситуаційного моніторингу та раннього попередження з використанням БПЛА, датчиків та аналітичних систем.

Розроблено рекомендації щодо вдосконалення системи захисту критичної інфраструктури: впровадження інтегрованої системи моніторингу, створення резервних систем, забезпечення стабільного фінансування, посилення міжвідомчої координації, регулярне проведення тренувань та симуляцій, розширення міжнародного співробітництва.

Наукова новизна дослідження полягає в комплексному обґрунтуванні організаційно-правового механізму захисту стратегічних об'єктів України в умовах воєнного стану, удосконаленні понятійно-категоріального апарату у сфері захисту критичної інфраструктури, розробці науково обґрунтованих рекомендацій щодо інтеграції фізичних та кіберзахисних систем, визначенні ролі Національної гвардії України у системі захисту за умов особливого правового режиму.

Практичне значення результатів полягає в можливості їх використання органами державної влади при розробці нормативно-правових актів у сфері захисту критичної інфраструктури, командуванням Національної гвардії при плануванні та організації заходів щодо забезпечення безпеки стратегічних об'єктів, у навчальному процесі вищих військових навчальних закладів.

Результати роботи були апробовані у фахових виданнях:

Комiссарова Н.О., Комiссаров М.Л., Подоляк Д. С. Захист об’єктів критичної інфраструктури як складова забезпечення національної безпеки.

Національні інтереси України. Серія «Право». Видавнича група «Наукові перспективи». № 9 (14) 2025. С.248-257 (фахове видання категорії В, спеціальність 251 «Воєнні науки, національна безпека, безпека державного кордону»)

Комісарова Н.О., Комісаров М.Л., Подоляк Д. С. Внутрішні загрози суспільного характеру: правові та організаційні аспекти протидії. Наукові інновації та передові технології. Серія «Право». Видавнича група «Наукові перспективи». № 10 (50) 2025. С.923-931 (фахове видання категорії В, спеціальність 081 «Право»)

Ключові слова: критична інфраструктура, національна безпека, кіберзагрози, організаційно-правовий механізм, стратегічні об'єкти, Національна гвардія України, воєнно-стратегічні виклики, системи захисту.

ABSTRACT

Podolyak Dmytro Serhiyovych "Organizational and Legal Mechanism for Protecting Strategic Objects of Ukraine". – Manuscript.

Master's thesis in specialty 251 State Security – Kyiv Institute of the National Guard of Ukraine, Kyiv, 2025.

The master's thesis is devoted to a comprehensive study of the organizational and legal mechanism for protecting strategic objects of Ukraine in the context of ensuring national security. The relevance of the study is determined by the critical importance of protecting critical infrastructure objects in conditions of growing cyber threats, man-made and natural risks, internal societal threats, and military-strategic challenges, especially during the full-scale armed aggression of the Russian Federation against Ukraine.

The work analyzes the concepts of critical infrastructure and its role in ensuring national security, examines international experience in defining critical infrastructure (USA, Germany, Great Britain, Netherlands), and proposes a definition for Ukraine. The main types of critical infrastructure are systematized: energy, transport, information, medical and financial infrastructure.

A comprehensive assessment of modern challenges and vulnerabilities of vital systems has been carried out. Cyber challenges are analyzed, the main methods of cyber attacks, technological and natural risks are studied.

Internal societal threats are examined, particularly the impact of economic crises of 2008-2009, 2014-2015, and 2022-2025 on the energy, transport, utilities sectors, and healthcare. The impact of social protests of 2021-2025 on critical infrastructure through physical damage to objects and blocking access is analyzed. Special attention is paid to military-strategic challenges: massive attacks on energy infrastructure that affected medical institutions, education, and living conditions of the population.

The experience of using the forces of the National Guard of Ukraine to ensure the security of strategic objects under special legal regime conditions is examined in detail. The organization of protection of critical infrastructure objects is analyzed, including the identification of critical objects, establishment of protective measures (physical barriers, access control systems, video surveillance). Situational monitoring and early warning systems using UAVs, sensors, and analytical systems are studied.

Recommendations for improving the critical infrastructure protection system have been developed: implementation of an integrated monitoring system, creation of backup systems, ensuring stable funding, strengthening inter-agency coordination, regular training and simulations, expansion of international cooperation.

The scientific novelty of the study lies in the comprehensive justification of the organizational and legal mechanism for protecting strategic objects of Ukraine under martial law conditions, improvement of the conceptual apparatus in the field of critical infrastructure protection, development of scientifically grounded recommendations for the integration of physical and cyber defense systems, definition of the role of the National Guard of Ukraine in the protection system under special legal regime conditions.

The practical significance of the results lies in the possibility of their use by state authorities in developing regulatory acts in the field of critical infrastructure protection, by the National Guard command in planning and organizing measures to ensure the security of strategic objects, and in the educational process of higher military educational institutions.

The results of the study have been tested in professional publications:

Komissarova N.O., Komissarov M.L., Podolyak D.S. Protection of critical infrastructure objects as a component of national security assurance. National Interests of Ukraine. Series 'Law'. Publishing Group 'Scientific Prospects'. No. 9 (14) 2025. Pp. 248-257 (specialized publication category B, specialty 251 'Military Sciences, National Security, State Border Security').

Komissarova N.O., Komissarov M.L., Podolyak D.S. Internal societal threats: legal and organizational aspects of counteraction. Scientific Innovations and Advanced Technologies. Series 'Law'. Publishing Group 'Scientific Prospects'. No. 10 (50) 2025. Pp. 923-931 (specialized publication category B, specialty 081 'Law').

Keywords: critical infrastructure, national security, cyber threats, organizational and legal mechanism, strategic objects, National Guard of Ukraine, military-strategic challenges, protection systems.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В сучасних умовах критична інфраструктура є основним елементом забезпечення стабільності та безпеки держави. До її складу входять об'єкти та системи, що забезпечують життєво важливі функції суспільства: енергетичні комплекси, транспортні вузли, об'єкти хімічної промисловості, оборонно-промисловий комплекс, системи інформаційно-комунікаційних технологій, банківський та фінансовий сектори.

Ці об'єкти є не лише ключовими для економічного та соціального розвитку країни, але й найбільш уразливими перед різноманітними загрозами: природними катастрофами, техногенними аваріями, терористичними актами, кібератаками та агресивними діями на міжнародній арені. У воєнний період загроза для національної безпеки набуває критичного характеру, оскільки пошкодження або знищення стратегічних об'єктів може спричинити серйозні наслідки для економіки, безпеки та стабільності держави, а також значне зниження життєвого рівня населення.

Організаційно-правовий механізм захисту стратегічних об'єктів України характеризується низкою системних протиріч, що потребують наукового осмислення та практичного розв'язання.

Протиріччя між централізованим та децентралізованим управлінням. Ефективний захист об'єктів критичної інфраструктури потребує як загальнодержавного контролю, так і гнучкого підходу на місцевому рівні. Централізована модель управління часто супроводжується надмірною бюрократією, що уповільнює прийняття рішень, тоді як децентралізована система може страждати від браку координації, створюючи слабкі місця у загальній системі безпеки.

Протиріччя між швидким впровадженням стандартів і реальними можливостями інфраструктури. Запровадження сучасних стандартів безпеки стикається з обмеженнями застарілої інфраструктури. Багато об'єктів

технічно не готові відповідати новим вимогам, що створює напруженість між необхідністю оперативного оновлення безпекових систем та труднощами, пов'язаними з високими витратами на модернізацію. Негайне впровадження нових стандартів є критично важливим для протидії сучасним загрозам, проте технічні та фінансові можливості часто виявляються недостатніми.

Протиріччя між фізичним захистом і кібербезпекою. Захист об'єктів інфраструктури традиційно орієнтувався на фізичні заходи: охорону, системи відеоспостереження та контроль доступу. Однак сучасні загрози все частіше проявляються в кіберпросторі у вигляді хакерських атак та саботажу інформаційних систем. Недостатня інтеграція фізичних і цифрових систем безпеки створює критичні вразливості, дозволяючи зловмисникам використовувати прогалини як у фізичному, так і в кіберзахисті.

Наявність зазначених протиріч підтверджує актуальність теми магістерської роботи та необхідність комплексного дослідження організаційно-правових механізмів захисту стратегічних об'єктів України.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконано відповідно до наукових пріоритетів Київського інституту Національної гвардії України та узгоджується з Концепцією створення державної системи захисту критичної інфраструктури, затвердженою розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р, а також Законом України "Про критичну інфраструктуру" від 16 листопада 2021 року № 1882-IX.

Мета дослідження полягає у комплексному аналізі та науковому обґрунтуванні вдосконалення організаційно-правового механізму захисту стратегічних об'єктів України в контексті забезпечення національної безпеки.

Об'єкт дослідження – система захисту об'єктів критичної інфраструктури в контексті національної безпеки, яка охоплює механізми, структури та політики забезпечення функціонування критично важливих об'єктів в умовах зростаючих фізичних, техногенних та кібернетичних загроз,

а також взаємодію між державними інституціями, приватними компаніями та міжнародними партнерами.

Предмет дослідження – організаційно-правові засади захисту об'єктів критичної інфраструктури України, включаючи оцінку потенційних загроз, аналіз існуючих заходів безпеки, визначення їхньої ефективності та розробку рекомендацій щодо вдосконалення системи захисту.

Завдання дослідження:

1. Проаналізувати концепції критичної інфраструктури та її роль у забезпеченні національної безпеки.
2. Дослідити типологію об'єктів критичної інфраструктури та визначити їх значення для стабільного функціонування суспільства.
3. Здійснити оцінку потенційних загроз для об'єктів критичної інфраструктури, включаючи кібератаки, терористичні акти та природні катастрофи.
4. Вивчити існуючі стратегії та методи захисту критичної інфраструктури від сучасних загроз.
5. Розглянути технічні засоби захисту, зокрема системи кібербезпеки, інтелектуальні системи захисту та фізичного забезпечення.
6. Проаналізувати організаційні аспекти захисту критичної інфраструктури, включаючи розробку політик безпеки, підготовку персоналу та планування антикризових заходів.
7. Дослідити стратегічні аспекти захисту критичної інфраструктури на національному та міжнародному рівнях, включаючи міжнародне співробітництво та обмін найкращими практиками.
8. Розробити науково обґрунтовані рекомендації щодо вдосконалення системи захисту критичної інфраструктури з метою забезпечення національної безпеки України.

Методи дослідження. У процесі виконання роботи використовувалися такі методи дослідження:

Теоретичний аналіз – вивчення наукових праць, монографій, статей, нормативно-правових актів та міжнародних документів з питань захисту критичної інфраструктури; аналіз концепцій і підходів до забезпечення національної безпеки у контексті захисту критично важливих об'єктів.

Порівняльний аналіз – зіставлення підходів до захисту критичної інфраструктури в Україні та інших країнах; оцінка сильних і слабких сторін різних моделей управління безпекою на основі міжнародного досвіду.

Практичний метод – збір і аналіз даних про інциденти на об'єктах критичної інфраструктури, а також оцінка ефективності заходів, вжитих для їх попередження чи усунення наслідків; використання статистичних даних для оцінки загроз і ризиків.

Метод сценарного підходу – побудова сценаріїв потенційних загроз для критичної інфраструктури та оцінка можливих наслідків їх реалізації; розробка рекомендацій на основі змодельованих ситуацій та варіантів реагування.

Наукова новизна одержаних результатів полягає в тому, що в дослідженні:

1. Вперше комплексно обґрунтовано організаційно-правовий механізм захисту стратегічних об'єктів України в умовах воєнного стану;
2. Удосконалено понятійно-категоріальний апарат у сфері захисту критичної інфраструктури;
3. Розроблено науково обґрунтовані рекомендації щодо інтеграції фізичних та кіберзахисних систем забезпечення безпеки стратегічних об'єктів;
4. Визначено роль Національної гвардії України у системі захисту критичної інфраструктури за умов особливого правового режиму.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані:

1. Органами державної влади при розробці нормативно-правових актів у сфері захисту критичної інфраструктури;

2. Командуванням Національної гвардії України при плануванні та організації заходів щодо забезпечення безпеки стратегічних об'єктів;

3. У навчальному процесі вищих військових навчальних закладів при підготовці фахівців у галузі національної безпеки.

Теоретична основа дослідження. Дослідження базується на аналізі законодавства України про захист критичної інфраструктури, постанов уряду, аналітичних звітів національних та міжнародних організацій, наукових статей у фахових журналах, досліджень аналітичних агентств, монографій з кібербезпеки та фізичної безпеки, матеріалів міжнародних конференцій, а також інтерв'ю з експертами у галузі безпеки.

Апробація результатів дослідження. За результатами дослідження опубліковано дві наукових фахових статті, а саме:

1. Комісарова Н.О., Комісаров М.Л., Подоляк Д. С. Захист об’єктів критичної інфраструктури як складова забезпечення національної безпеки.. Національні інтереси України. Серія «Право». Видавнича група «Наукові перспективи». № 9 (14) 2025. С.248-257 (фахове видання категорії В, спеціальність 251 «Воєнні науки, національна безпека, безпека державного кордону»)

2. Комісарова Н.О., Комісаров М.Л., Подоляк Д. С. Внутрішні загрози суспільного характеру: правові та організаційні аспекти протидії. Наукові інновації та передові технології. Серія «Право». Видавнича група «Наукові перспективи». № 10 (50) 2025. С.923-231 (фахове видання категорії В, спеціальність 251 «Воєнні науки, національна безпека, безпека державного кордону»)

Структура та обсяг роботи. Магістерська робота складається зі вступу, двох розділів, що містять 8 підрозділів, висновку, списку використаних джерел (182 найменування). Загальний обсяг роботи становить 83 сторінки.

Розділ 1. КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ БЕЗПЕКИ ЖИТТЄВО ВАЖЛИВИХ СИСТЕМ

1.1 Сутність та дефініція поняття "критична інфраструктура"

В Україні, як і в інших країнах світу, функціонують системи, об'єкти та ресурси, знищення або пошкодження яких може мати істотний негативний вплив на громадян, суспільство та державні інституції. Сьогодні в країні діє низка законодавчих і нормативних актів, що визначають повноваження та компетенцію державних органів у сфері захисту критичної інфраструктури, встановлюють особливості забезпечення охорони та безпечного функціонування таких об'єктів [1, 2].

Критична інфраструктура охоплює широкий спектр ресурсів та об'єктів, які є життєво важливими для сучасного суспільства та відображають різні аспекти його функціонування та розвитку. Безпека цих об'єктів як у нормальних умовах, так і в умовах надзвичайних ситуацій, зокрема воєнного стану, є одним із пріоритетів держави [3].

Визначення терміна "критична інфраструктура" в українському законодавстві має відповідати загальновизнаним у світі підходам і повною мірою відображати специфіку безпекових умов, у яких перебуває країна. Це особливо важливо для забезпечення відповідності законодавства міжнародним стандартам і нормам безпеки [4]. Чітке і узгоджене визначення терміна дозволяє уникнути розбіжностей у міжнародних відносинах та забезпечує ефективне застосування законів у сфері національної безпеки.

В Україні термін "критична інфраструктура" неодноразово використовувався в нормативно-правових документах, проте його законодавче визначення тривалий час було відсутнім. Уперше в офіційних документах цей термін з'явився у 2006 році в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства [5].

У Стратегії національної безпеки "Україна у світі, що змінюється" (2012 р.) термін згадувався при визначенні способів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки [6]. У новій Стратегії національної безпеки України (2015 р.) термін "критична інфраструктура" було деталізовано й розширено, що дозволило краще розуміти його суть та значення в контексті національної безпеки [7].

Уперше серед "актуальних загроз національній безпеці" було виокремлено загрози критичній інфраструктурі. Окремо в підрозділі "Загрози кібербезпеці і безпеці інформаційних ресурсів" зазначалася вразливість об'єктів критичної інфраструктури та державних інформаційних ресурсів до кібератак [7]. Також уперше одним із "основних напрямів державної політики в сфері національної безпеки" було названо забезпечення безпеки критичної інфраструктури та визначено пріоритети цього напряму.

Відсутність чіткого визначення терміна "критична інфраструктура" в українському законодавстві та, як наслідок, переліку об'єктів, які необхідно віднести до цієї інфраструктури, неодноразово перешкоджали ефективному виконанню першочергових безпекових завдань. Зокрема, це стосувалося виконання п. 6 Рішення Ради національної безпеки і оборони України "Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України" від 01 березня 2014 р. (введено в дію Указом Президента України №189/2014 від 02 березня 2014 р.) [8].

Енергетичний сектор у всіх країнах та у міжнародних об'єднаннях, таких як ЄС і НАТО, відносять до критичної інфраструктури [9, 10]. Основна його функція полягає в забезпеченні потреб населення, суспільства й держави в енергії. Як свідчить світовий досвід, найтяжчі наслідки для забезпечення електроенергією суспільства виникають унаслідок аварій у системах передачі та розподілення електроенергії, а не у випадку виходу з ладу окремих об'єктів генерації [11].

Сучасне життя людини, суспільства та держави нерозривно пов'язане з різноманітними системами, мережами та об'єктами, які забезпечують

критично важливі послуги та виконують необхідні функції. У різних країнах та міжнародних організаціях термін "критична інфраструктура" має подібне визначення, але існують відмінності, що відображають особливості національних специфікацій.

У США критична інфраструктура охоплює системи та ресурси, які є настільки важливими, що їхня недієздатність може загрожувати національній безпеці, економіці, здоров'ю та безпеці населення [12]. У Німеччині під критичною інфраструктурою розуміють організаційні та фізичні структури, які є життєво важливими для суспільства та економіки країни [13]. Англія та Нідерланди також мають власні визначення критичної інфраструктури, зосереджуючись на системах та мережах, які забезпечують нормальне функціонування країни та життя її громадян [14, 15].

У різних національних законодавствах акцент може бути розміщений не лише на фізичних об'єктах, але й на функціях та послугах, які вони забезпечують [16]. Це дозволяє краще розуміти важливість кожного елементу для суспільства та держави.

З огляду на міжнародний досвід провідних країн світу з розроблення підходів до забезпечення національної безпеки на основі застосування концепції "критична інфраструктура", пропонуємо використовувати в Україні наступне визначення [17]:

Критична інфраструктура – це сукупність об'єктів, систем та ресурсів, фізичних або в кіберпросторі, які є вирішальними для стабільного функціонування суспільства та економіки країни. Вона включає різноманітні види інфраструктури, що забезпечують життєво важливі послуги, безпеку та ефективність функціонування суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.

До складових частин критичної інфраструктури належать: енергетичні мережі, системи водопостачання та водовідведення, транспортні мережі (автомобільні дороги, залізниця, морські та повітряні шляхи),

телекомунікаційні мережі, банківські системи, медичні установи, системи захисту та безпеки, об'єкти оборони та інші [18].

Важливо враховувати взаємозв'язок і взаємовплив між окремими елементами критичної інфраструктури, оскільки ця особливість впливає на масштаб наслідків у разі виникнення загроз або інцидентів [19]. Управління безпекою кожного окремого об'єкта має здійснюватися з урахуванням його взаємодії з іншими елементами системи критичної інфраструктури. Це передбачає не лише захист окремих об'єктів, але й розуміння їхнього впливу на функціонування всієї системи [20].

Захист критичної інфраструктури України – це комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [21].

Нормативно-правові інструменти визначають правила, стандарти та вимоги до захисту критичної інфраструктури, встановлюють відповідальність за порушення цих вимог і регулюють процеси планування та реагування на потенційні загрози [22]. Організаційні заходи включають створення спеціалізованих організацій, комітетів або центрів управління кризовими ситуаціями, а також розробку планів та процедур реагування на різні види загроз [23]. Технологічні інструменти охоплюють впровадження сучасних технологій і систем захисту, включаючи системи контролю доступу, відеоспостереження, кіберзахисту та інші технічні засоби, спрямовані на запобігання та виявлення можливих загроз [24].

Безпека критичної інфраструктури – це комплексний підхід до забезпечення захищеності об'єктів та систем, які є невід'ємною складовою суспільства, що має на меті забезпечення їхньої функціональності, безперервності роботи, відновлюваності, цілісності та стійкості у будь-яких умовах та обставинах [25]. Поняття "безпека" містить фізичну (фізичний захист), експлуатаційну та операційну безпеку.

Стійкість критичної інфраструктури – це її спроможність надійно функціонувати в нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти й швидко відновлюватися після аварій і технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ [26]. Стійкість передбачає здатність продовжувати надавати послуги навіть після виникнення надзвичайних подій.

Функціональність означає здатність об'єктів критичної інфраструктури виконувати свої функції згідно з призначенням у звичайних умовах та під час надзвичайних ситуацій [27].

Безперервність роботи передбачає, що навіть у разі виникнення перешкод, помилок або атак системи критичної інфраструктури мають забезпечити безперебійне функціонування або мінімізувати час простою [28].

Відновлюваність означає здатність систем відновлювати свою працездатність після виникнення негативних подій, включаючи відновлення даних, працездатності обладнання та можливості повернення до нормального режиму роботи [29].

Цілісність стосується здатності системи зберігати свою функціональність і дані в повноті, не допускаючи їх неправомірного доступу, змін або пошкоджень [30].

Об'єкти критичної інфраструктури – об'єкти інфраструктури, їх частини та їх сукупність, важливі компоненти і системи, які є ключовими для економічного розвитку, національної безпеки та оборони країни, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [31]. Вони включають атомні, теплові, гідроелектростанції, залізничні мережі, станції, аеропорти, телекомунікаційні компанії, водозабірні станції та водосховища, лікарні та медичні центри, які забезпечують нормальне функціонування суспільства.

Порушення функціонування цих об'єктів може призвести до серйозних наслідків, що загрожують життям і здоров'ю громадян, стабільності економіки та національній безпеці [32]. Тому важливо забезпечити надійний захист цих

об'єктів, розвинути системи попередження та реагування на можливі загрози, а також вдосконалити механізми співпраці між різними секторами, урядовими та приватними структурами для ефективного управління ризиками [33].

Сектор критичної інфраструктури – це сукупність об'єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість [34]. Визначення секторів критичної інфраструктури допомагає управляти ризиками та виробляти стратегії захисту, спрямовані на забезпечення стійкості та надійності важливих галузей економіки, а також сприяє координації дій між різними урядовими та приватними структурами у сфері захисту критичної інфраструктури [35].

1.2 Типологія та систематизація життєво важливих систем

Визначення видів критичної інфраструктури передбачає складання переліку конкретних об'єктів, систем і ресурсів (елементів) критичної інфраструктури. У нормативно-правовому полі України існують категорії об'єктів, близькі за змістом до об'єктів критичної інфраструктури [36]. Українське законодавство щодо захисту таких об'єктів є досить розгалуженим і включає численні нормативно-правові акти, які, проте, мають переважно відомчий характер.

Історично склалося, що в Україні різні категорії стратегічно важливих об'єктів регулювалися окремими нормативними актами, що призводило до фрагментарності підходів до їх захисту. Прийняття Закону України "Про критичну інфраструктуру" у 2021 році стало важливим кроком до уніфікації підходів та створення комплексної системи захисту [1].

Чинне законодавство визначає наступні категорії об'єктів, для яких встановлюються особливі умови забезпечення їх захисту й функціонування [37]:

Стратегічні об'єкти економіки: підприємства, які мають стратегічне значення для економіки та безпеки держави. До цієї категорії належать великі промислові комплекси, підприємства оборонно-промислового комплексу, металургійні комбінати, машинобудівні заводи, які забезпечують значну частку ВВП країни та зайнятості населення.

Енергетичні об'єкти: особливо важливі об'єкти електроенергетики, включаючи атомні, теплові та гідроелектростанції, магістральні електромережі, системні підстанції; особливо важливі об'єкти нафтогазової галузі, що охоплюють газотранспортну систему, нафтопроводи, газосховища, компресорні станції.

*Об'єкти державного управління: в*ажливі державні об'єкти, зокрема пункти управління органів державної влади та органів місцевого

самоврядування, які забезпечують безперервність функціонування системи державного управління.

Об'єкти антитерористичної спрямованості: об'єкти можливих терористичних посягань, визначені на основі оцінки ризиків та вразливостей; об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період.

Об'єкти з особливим режимом охорони: об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами; органи державної влади, що підлягають безоплатній охороні Національною гвардією України.

Об'єкти підвищеної небезпеки: об'єкти підвищеної небезпеки відповідно до класифікації за ступенем ризику; об'єкти, включені до Державного реєстру потенційно небезпечних об'єктів; радіаційно небезпечні об'єкти, включаючи атомні електростанції, сховища радіоактивних відходів, науково-дослідні ядерні установки.

Об'єкти цивільного захисту: об'єкти, віднесені до категорій із цивільного захисту; чергово-диспетчерська система екстреної допомоги населенню за єдиним номером 112; аварійно-рятувальні служби та їх матеріально-технічна база.

Комунікаційні системи: національна система конфіденційного зв'язку, що забезпечує захищений обмін інформацією між державними органами; державна система урядового зв'язку України, яка гарантує безперебійний зв'язок органів державної влади.

Фінансові системи: платіжні системи, включаючи системи електронних платежів, міжбанківського розрахунку, функціонування банкоматів.

Об'єкти культурної спадщини: нерухомі об'єкти культурної спадщини національного та місцевого значення.

Деякі із зазначених категорій об'єктів частково або повністю після виконання відповідного аналізу можуть бути віднесені до об'єктів критичної інфраструктури [38]. Критерії віднесення включають оцінку масштабу

можливих наслідків від порушення функціонування об'єкта, кількість населення, яке може постраждати, та вплив на інші об'єкти критичної інфраструктури.

Енергетична інфраструктура є найважливішою складовою критичної інфраструктури будь-якої держави, оскільки від неї залежить функціонування всіх інших секторів економіки та життєдіяльності суспільства.

Атомні електростанції генерують електроенергію за допомогою ядерних реакцій поділу атомів урану [39]. В Україні функціонують чотири атомні електростанції: Запорізька (найбільша в Європі з шістьма енергоблоками), Південноукраїнська, Рівненська та Хмельницька АЕС. Атомні електростанції відомі своєю високою потужністю та стабільністю постачання електроенергії, проте потребують високих заходів безпеки, багаторівневих систем захисту та постійного моніторингу радіаційної обстановки. Особлива увага приділяється захисту від внутрішніх і зовнішніх загроз, включаючи фізичний захист периметра, системи контролю доступу, кіберзахист автоматизованих систем управління технологічними процесами.

Теплові електростанції працюють на спалюванні вугілля, газу або нафти для генерації електроенергії [40]. Вони є одними з найпоширеніших і забезпечують значну частину енергії в багатьох країнах. В Україні теплові електростанції розташовані переважно на сході країни, поблизу вугільних басейнів. До найбільших належать Бурштинська ТЕС, Ладижинська ТЕС, Трипільська ТЕС. Теплові електростанції характеризуються високою маневреністю, здатністю швидко змінювати рівень генерації відповідно до споживчого навантаження. Однак вони мають значний вплив на довкілля через викиди парникових газів та потребують постійного постачання палива.

Гідроелектростанції використовують потік води для приводу турбін, які генерують електроенергію [41]. Вони є екологічно чистими і мають великий потенціал для виробництва стабільної електроенергії. Найбільшими ГЕС України є Дніпровський каскад гідроелектростанцій, що включає Київську, Канівську, Кременчуцьку, Середньодніпровську, Дніпровську та Каховську

ГЕС. Гідроелектростанції також виконують важливі функції регулювання частоти в енергосистемі, можуть швидко збільшувати або зменшувати потужність. Крім того, водосховища ГЕС використовуються для регулювання стоку річок, водопостачання, зрошення, рибного господарства та рекреації.

Вітроелектростанції використовують енергію вітру для приводу вітротурбін [42]. Вони є одними з найшвидше розвиваючихся джерел виробництва енергії і мають низький вуглецевий відбиток. В Україні найбільший потенціал для розвитку вітроенергетики мають південні регіони – Одеська, Миколаївська, Херсонська, Запорізька області. Розвиток вітроенергетики сприяє диверсифікації енергетичного балансу країни та зменшенню залежності від імпортованих енергоносіїв. Сучасні вітрові турбіни мають потужність від 2 до 8 МВт, висоту башти до 150 метрів та діаметр ротора до 180 метрів.

Сонячні електростанції перетворюють енергію сонячного випромінювання в електричну енергію за допомогою фотоелектричних панелей. Україна має значний потенціал для розвитку сонячної енергетики, особливо в південних регіонах, де кількість сонячних днів на рік сягає 230-280. Сонячні електростанції можуть бути наземними (великі промислові станції потужністю десятки і сотні мегават) або дахові (малі домогосподарські установки потужністю до 30 кВт).

Електромережі – це система проводів і трансформаторів, яка транспортує електроенергію від електростанцій до споживачів [43]. Вони працюють на різних рівнях напруги відповідно до потреб споживачів: магістральні мережі 750 кВ і 330 кВ для передачі великих обсягів електроенергії на значні відстані; розподільні мережі 110 кВ і 35 кВ для передачі електроенергії в межах регіонів; мережі низької напруги 10 кВ, 6 кВ і 0,4 кВ для безпосереднього живлення споживачів.

Загальна протяжність електричних мереж України становить понад 1 млн кілометрів. Ці мережі забезпечують електропостачання населених пунктів, промислових підприємств, об'єктів соціальної інфраструктури.

Критично важливими є міждержавні електричні зв'язки, які дозволяють Україні інтегруватися в європейську енергосистему ENTSO-E та здійснювати експорт-імпорт електроенергії.

Підстанції – це споруди, які забезпечують перетворення напруги та розподіл електроенергії в електромережі [44]. Вони відіграють ключову роль у забезпеченні стабільності електропостачання. Підстанції поділяються на трансформаторні (які змінюють рівень напруги) та розподільні (які розподіляють електроенергію між різними споживачами). Сучасні підстанції оснащуються цифровими системами управління, автоматикою швидкодіючого захисту, системами моніторингу технічного стану обладнання. Особливо важливими є системні підстанції, від яких залежить електропостачання великих регіонів або міст.

Газопроводи транспортують природний газ з місць видобутку до місць споживання [45]. Газотранспортна система України є однією з найбільших у Європі та включає: магістральні газопроводи загальною протяжністю близько 38 тис. км; 72 компресорні станції з загальною потужністю понад 5,7 тис. МВт; 13 підземних сховищ газу загальною місткістю 31 млрд куб. м; газорозподільні станції, які знижують тиск газу для подачі споживачам.

Газотранспортна система забезпечує не лише внутрішні потреби України, але й транзит російського та центральноазіатського газу до країн Європи. Компресорні станції підтримують необхідний тиск газу в трубопроводах, забезпечуючи його транспортування на великі відстані. Регуляторні станції здійснюють автоматичне регулювання тиску та витрати газу відповідно до потреб споживачів.

Нафтопроводи транспортують нафту та нафтопродукти від місць видобутку до різних пунктів споживання [46]. Система нафтопроводів України включає магістральні нафтопроводи загальною протяжністю близько 4,8 тис. км; нафтопродуктопроводи протяжністю близько 4,5 тис. км; 51 нафтоперекачувальну станцію; резервуарні парки для зберігання нафти та нафтопродуктів. Нафтопроводи складаються з трубопроводів великого

діаметра (до 1220 мм), насосних станцій для підтримки потоку рідини, регуляторних станцій для контролю та розподілу нафти.

Система нафтопроводів забезпечує постачання нафти на нафтопереробні заводи України та транзит нафти з країн Каспійського регіону до країн Центральної Європи. Нафтопродуктопроводи транспортують готові нафтопродукти (бензин, дизельне паливо, авіаційний гас) від НПЗ до нафтобаз та пунктів споживання.

Системи теплопостачання включають теплоелектроцентралі (ТЕЦ), котельні та тепломережі, що забезпечують опалення та гаряче водопостачання населених пунктів. В Україні централізоване теплопостачання отримують близько 60% міського населення. Тепломережі включають магістральні теплопроводи, розподільні мережі, теплові пункти. Загальна протяжність теплових мереж в Україні становить понад 27 тис. км, однак значна їх частина має високий рівень зносу (понад 60%), що призводить до значних втрат тепла при транспортуванні.

Транспортна інфраструктура забезпечує мобільність населення, перевезення вантажів, інтеграцію України в світову транспортну систему та є критично важливою для економічного розвитку країни.

Автомагістралі та шосе складають мережу доріг для автотранспорту, яка забезпечує швидке та ефективне переміщення між містами та регіонами [47]. Мережа автомобільних доріг України включає: дороги державного значення загальною протяжністю 51,7 тис. км (у тому числі дороги міжнародного значення – 8,5 тис. км, дороги національного значення – 5,4 тис. км, дороги регіонального значення – 23,4 тис. км, дороги територіального значення – 14,4 тис. км); дороги місцевого значення протяжністю близько 120 тис. км.

Через територію України проходять важливі міжнародні транспортні коридори: Критський коридор №3 (Берлін – Дрезден – Вроцлав – Львів – Київ); Критський коридор №5 (Трієст – Любляна – Будапешт – Ужгород – Львів); Критський коридор №9 (Гельсінкі – Санкт-Петербург – Москва – Київ –

Кишинів – Бухарест). Ці коридори мають стратегічне значення для транзиту вантажів між Європою та Азією.

Автомобільні дороги також включають мостові споруди (близько 25 тис. мостів), тунелі, естакади, шляхопроводи. Особливо важливими є мости через великі річки (Дніпро, Дунай, Дністер), пошкодження яких може критично вплинути на транспортне сполучення між регіонами.

Залізничні мережі та станції забезпечують перевезення пасажирів та вантажів за допомогою залізничного транспорту [48]. Залізнична мережа України є однією з найгустіших у Європі та включає: колії загальною експлуатаційною довжиною близько 21 тис. км; електрифіковані колії – 9,9 тис. км; залізничні станції – понад 1,5 тис.; вантажні станції та термінали; локомотивне депо та вагонні депо; ремонтні центри та майстерні.

АТ "Укрзалізниця" є одним з найбільших працедавців в Україні, забезпечує понад 80% вантажних перевезень у країні. Залізничний транспорт має критичне значення для перевезення експортних вантажів (зерно, металопродукція, руда), вугілля для електростанцій, будівельних матеріалів, нафтопродуктів. Пасажирські перевезення включають міжрегіональне, приміське та міжнародне сполучення.

Залізнична інфраструктура також включає системи електропостачання (контактна мережа, тягові підстанції), системи зв'язку та сигналізації, автоматизовані системи управління рухом поїздів. Критично важливим є технічний стан залізничних мостів, тунелів, шляхопроводів, від яких залежить безпека руху поїздів.

Аеропорти та повітряні шляхи забезпечують пасажирські та вантажні перевезення за допомогою літаків [49]. До початку повномасштабного вторгнення в Україні функціонували 18 аеропортів з регулярним пасажирським сполученням, найбільшими з яких були: міжнародний аеропорт "Бориспіль" (обслуговував близько 70% пасажиропотоку країни); міжнародний аеропорт "Київ" (Жуляни); аеропорти Львова, Одеси, Харкова, Дніпра, Запоріжжя.

Аеропортова інфраструктура включає: злітно-посадкові смуги з відповідним обладнанням (світлосигнальне обладнання, системи посадки); пасажирські термінали з системами реєстрації, контролю безпеки, обробки багажу; вантажні термінали для обробки авіаційних вантажів; системи забезпечення авіаційної безпеки; системи аеронавігаційного обслуговування; пункти заправки авіаційним паливом; ангари для технічного обслуговування літаків.

Повітряний простір України контролюється Державною авіаційною службою та забезпечує пролітання міжнародних авіарейсів між Європою та Азією. Аеронавігаційне обслуговування включає диспетчерське управління повітряним рухом, радіотехнічне забезпечення польотів, метеорологічне забезпечення, аеронавігаційну інформацію.

Порти та морські термінали забезпечують морські та річкові перевезення вантажів та пасажирів [50]. Україна має вихід до Чорного та Азовського морів, що надає можливість здійснювати міжнародні морські перевезення. Морська портова інфраструктура включає: 18 морських портів загальною потужністю близько 230 млн тонн вантажів на рік; найбільші порти: Південний, Чорноморськ (Іллічівськ), Миколаїв, Одеса, Маріуполь, Бердянськ; спеціалізовані термінали для різних типів вантажів (зерно, руда, вугілля, метал, контейнери, нафтопродукти).

Річкові порти розташовані на Дніпрі, Дунаї, Південному Бузі та включають вантажні термінали, пасажирські станції, судноремонтні підприємства. Дніпро-Бузький водний шлях з'єднує річкові порти з морськими та має важливе значення для транспортування вантажів.

Портова інфраструктура включає: причали та пристані для швартування суден; портальні крани та навантажувальні пристрої; складські комплекси та елеватори; залізничні під'їзні колії та автомобільні під'їзди; системи навігаційного обладнання; об'єкти портового флоту (буксири, кат ери, плавкрани).

Інформаційна інфраструктура в сучасному цифровому суспільстві є критично важливою для функціонування всіх інших секторів економіки, державного управління, фінансової системи, охорони здоров'я, освіти.

Інтернет-провайдери та телекомунікаційні компанії забезпечують доступ до Інтернету та інших телекомунікаційних послуг [51]. В Україні функціонують близько 3 тис. провайдерів телекомунікаційних послуг, найбільшими з яких є "Київстар", "Vodafone Україна", "lifecell". Телекомунікаційна інфраструктура включає: волоконно-оптичні магістральні мережі; базові станції мобільного зв'язку (понад 60 тис. базових станцій 4G LTE); вузли зв'язку та комутації; супутникові станції; кабельні лінії міжнародного з'єднання.

Україна має розгалужену систему міжнародних каналів зв'язку, які з'єднують країну з європейськими та світовими телекомунікаційними мережами. Це включає наземні волоконно-оптичні лінії через сусідні країни та підводні кабельні системи в Чорному морі. Критично важливим є забезпечення резервування каналів зв'язку для підтримання безперебійного функціонування телекомунікаційної системи.

Розвивається мережа 5G мобільного зв'язку, яка має забезпечити високошвидкісний доступ до Інтернету, підтримку Інтернету речей (IoT), розвиток "розумних міст". Впровадження 5G технологій критично важливе для цифровізації економіки, розвитку дистанційної медицини, автономного транспорту, промислового Інтернету речей.

Центри та серверні установки забезпечують зберігання, обробку та розподіл даних [52]. В Україні функціонують як великі комерційні дата-центри міжнародного рівня, так і корпоративні дата-центри окремих організацій. Дата-центри включають: серверне обладнання для обробки даних; системи зберігання даних (SAN, NAS); комутаційне та мережеве обладнання; системи безперебійного живлення (UPS); системи резервного електропостачання (дизель-генератори); системи кондиціонування та

вентиляції; системи пожежогасіння; системи фізичної охорони та контролю доступу; системи моніторингу та управління інфраструктурою.

Сучасні дата-центри будуються відповідно до міжнародних стандартів (Tier III, Tier IV), що передбачає високу надійність, резервування всіх критичних систем, можливість проведення технічного обслуговування без зупинки роботи. Критично важливим є забезпечення кібербезпеки дата-центрів, захист від несанкціонованого доступу, регулярне резервне копіювання даних, плани відновлення після аварій (Disaster Recovery).

Критичні інформаційні системи державного та комерційного значення забезпечують роботу державних та комерційних організацій [53]. До них належать: системи електронного урядування (Єдиний державний веб-портал електронних послуг, системи електронного документообігу); системи державних реєстрів (Державний реєстр речових прав на нерухоме майно, Державний реєстр актів цивільного стану, Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців); автоматизовані системи управління технологічними процесами (SCADA) на об'єктах критичної інфраструктури; банківські інформаційні системи; системи електронної комерції; медичні інформаційні системи; системи диспетчерського управління транспортом.

Ці системи потребують особливого захисту, оскільки їх порушення може призвести до серйозних наслідків для національної безпеки, економіки, життя та здоров'я громадян. Критично важливим є впровадження багаторівневих систем захисту, регулярне оновлення програмного забезпечення, моніторинг кіберзагроз, навчання персоналу основам кібербезпеки.

Системи водопостачання та водовідведення забезпечують життєво важливі потреби населення та промисловості, їх безперебійне функціонування критично важливе для здоров'я населення та санітарно-епідеміологічного благополуччя.

Водозабірні станції та водосховища забезпечують постачання прісної води для населення та промисловості [54]. Джерелами водопостачання в Україні є поверхневі води (річки, водосховища, озера) та підземні води. Найбільші водозабірні споруди розташовані на річках Дніпро, Дністер, Південний Буг, Сіверський Донець.

Водозабірні споруди включають: водозабори з річок та водосховищ (берегові захоплювальні споруди, плавучі насосні станції); свердловини та водозабірні колодязі для підземних вод; станції водопідготовки для очищення та знезараження води; резервуари чистої води; насосні станції першого підйому.

Процес водопідготовки включає механічне очищення (видалення завислих частинок), освітлення та знебарвлення води (коагуляція, відстоювання, фільтрування), знезараження (хлорування, озонування, ультрафіолетове опромінення). Якість питної води контролюється відповідно до державних стандартів та санітарних норм.

Водопровідні мережі та насосні станції транспортують очищену прісну воду з водозабірних станцій до споживачів [55]. Системи водопостачання України включають: магістральні водоводи; розподільні водопровідні мережі в населених пунктах; насосні станції для підтримки необхідного тиску; резервуари та водонапірні башти; водопровідні вводи в будівлі.

Загальна протяжність водопровідних мереж в Україні становить понад 130 тис. км. Значна частина водопровідних мереж має високий рівень зносу (понад 70% в деяких містах), що призводить до значних втрат води через витоки (до 30-50% від загального обсягу води, що подається в мережу). Це створює потребу в модернізації та реконструкції водопровідних систем.

Каналізаційні системи та очисні споруди забезпечують відведення та очищення стічних вод для запобігання забрудненню довкілля [56]. Системи водовідведення включають: каналізаційні мережі для збору та відведення господарсько-побутових та виробничих стічних вод; каналізаційні насосні

станції; каналізаційні колектори; каналізаційні очисні споруди; споруди для обробки та утилізації осаду.

Каналізаційні очисні споруди здійснюють механічне (видалення великих забруднень, відстоювання), біологічне (очищення за допомогою активного мулу або біофільтрів) та хімічне очищення стічних вод перед їх випуском у водойми. Сучасні очисні споруди також включають споруди доочищення та знезараження стічних вод для забезпечення відповідності нормативам якості.

Критично важливим є забезпечення безперебійної роботи систем водовідведення, оскільки їх порушення може призвести до санітарно-епідеміологічних проблем, забруднення довкілля, затоплення територій стічними водами.

Медична інфраструктура забезпечує охорону здоров'я населення, надання екстреної та планової медичної допомоги, профілактику та лікування захворювань.

Лікарні та медичні центри надають екстрену та планову медичну допомогу, госпіталізацію хворих, проведення складних медичних процедур та операцій [57]. Система медичних закладів України включає: багатопрофільні обласні лікарні; спеціалізовані лікарні (кардіологічні, онкологічні, інфекційні, психіатричні, туберкульозні); центральні районні лікарні; міські лікарні; дільничні лікарні в сільській місцевості; пологові будинки; дитячі лікарні.

Лікарні оснащуються діагностичним обладнанням (комп'ютерні томографи, магнітно-резонансні томографи, ультразвукові апарати, рентгенівські апарати), лабораторіями, операційними блоками, відділеннями інтенсивної терапії, реанімаційними відділеннями. Критично важливим є забезпечення безперебійного електропостачання медичних закладів (резервні генератори), постачання медичного кисню, функціонування систем життєзабезпечення.

В умовах надзвичайних ситуацій медичні заклади повинні бути готові до прийому великої кількості постраждалих, що вимагає наявності планів

реагування, достатніх запасів медикаментів та медичного обладнання, навченого персоналу.

Аптечні мережі та лабораторії забезпечують населення медикаментами та лікарськими засобами, проведення лабораторних досліджень та аналізів. Аптечна мережа України включає понад 17 тис. аптечних закладів. Критично важливим є забезпечення доступності лікарських засобів для населення, особливо життєво необхідних медикаментів, зберігання достатніх резервів медикаментів для надзвичайних ситуацій.

Медичні лабораторії здійснюють клінічні, біохімічні, мікробіологічні, імунологічні, генетичні дослідження. Вони обладнані сучасними аналітичними приладами, системами контролю якості досліджень. Особливе значення мають лабораторії, які здійснюють діагностику особливо небезпечних інфекцій, радіологічний контроль, токсикологічні дослідження.

Амбулаторії та інші медичні установи надають первинну медичну допомогу, консультування пацієнтів, ведення медичної документації. Система первинної медичної допомоги включає: амбулаторії сімейної медицини; центри первинної медико-санітарної допомоги; фельдшерсько-акушерські пункти в сільській місцевості; поліклініки; медичні пункти на підприємствах та в навчальних закладах.

Первинна медична допомога є першим рівнем контакту населення з системою охорони здоров'я, забезпечує профілактичні огляди, вакцинацію, лікування найпоширеніших захворювань, направлення до спеціалістів. Критично важливим є забезпечення доступності первинної медичної допомоги для всього населення, особливо в сільській місцевості.

Швидка медична допомога забезпечує екстрену медичну допомогу населенню, транспортування хворих до медичних закладів. Система швидкої медичної допомоги включає станції та відділення швидкої допомоги, спеціалізовані бригади (кардіологічні, неврологічні, педіатричні, реанімаційні), медичні автомобілі та медичні гелікоптери для санітарної авіації.

Фінансова інфраструктура забезпечує функціонування фінансової системи країни, проведення платежів, кредитування економіки, інвестиційну діяльність.

Банки та фінансові установки надають фінансові послуги, такі як зберігання грошових коштів, видача кредитів, обслуговування платіжних операцій, інвестиційні послуги. Банківська система України включає: Національний банк України (центральний банк); банки (станом на 2024 рік функціонує близько 60 банків); небанківські фінансові установи (кредитні спілки, ломбарди, лізингові компанії).

Банки забезпечують функціонування платіжної системи країни, проведення готівкових та безготівкових розрахунків, міжнародних платежів. Банківська інфраструктура включає: відділення банків; банкомати та термінали самообслуговування; процесингові центри для обробки платіжних карток; системи дистанційного банківського обслуговування (інтернет-банкінг, мобільний банкінг).

Критично важливим є забезпечення стійкості банківської системи, захист від кіберзагроз, запобігання легалізації доходів, отриманих злочинним шляхом, фінансуванню тероризму. Національний банк України здійснює нагляд за банківською системою, встановлює нормативи діяльності банків, здійснює регулювання грошово-кредитної політики.

Платіжні системи забезпечують переказ коштів між учасниками. В Україні функціонують: Системно важлива платіжна система (СЕП) НБУ для міжбанківських розрахунків; міжнародні платіжні системи (Visa, Mastercard, American Express); локальні платіжні системи (PROSTIR – національна платіжна система України); системи електронних грошей; системи переказу коштів.

Фондові ринки та біржі є місцем торгівлі цінними паперами, такими як акції, облігації, фьючерси, опціони та інші фінансові інструменти. Інфраструктура фондового ринку України включає: Національну комісію з цінних паперів та фондового ринку (регулятор); фондові біржі (Українська

біржа, Перспектива); торговельно-інформаційні системи; депозитарії цінних паперів; клірингові установи; реєстратори власників іменних цінних паперів.

Фондовий ринок забезпечує залучення інвестицій в економіку, можливість для підприємств залучати капітал шляхом випуску цінних паперів, для інвесторів – можливість інвестувати кошти та отримувати дохід. Критично важливим є забезпечення прозорості фондового ринку, захист прав інвесторів, запобігання маніпулюванню цінами, використанню інсайдерської інформації.

Об'єкти критичної інфраструктури формують різні сектори, які представляють собою певні групи об'єктів зі схожими характеристиками, функціональною спрямованістю або галузевою приналежністю. Класифікація об'єктів у сектори допомагає уряду та організаціям краще розуміти специфіку загроз та ризиків і визначати ефективні стратегії захисту.

Для забезпечення безпеки критичної інфраструктури визначаються окремі сектори, у кожному з яких розробляються специфічні підходи до захисту, що відповідають державній політиці у сфері безпеки. Перелік секторів критичної інфраструктури та відповідальних за них суб'єктів управління формує Кабінет Міністрів України.

Серед життєво важливих функцій і послуг, порушення яких може негативно вплинути на національну безпеку, виділяють:

1. *Надання важливих адміністративних послуг* – забезпечення функціонування органів державної влади, надання послуг населенню (реєстрація актів цивільного стану, видача документів, надання соціальних послуг).

2. *Енергозабезпечення, включаючи постачання тепла* – виробництво, передача та розподіл електричної та теплової енергії, забезпечення паливом.

3. *Водопостачання та водовідведення* – забезпечення населення та промисловості питною водою, відведення та очищення стічних вод.

4. *Продовольче забезпечення* – виробництво, зберігання, переробка та розподіл продуктів харчування, забезпечення продовольчої безпеки.

5. *Охорона здоров'я та фармацевтична промисловість* – надання медичної допомоги, виробництво та постачання лікарських засобів.

6. *Інформаційні та електронні комунікації* – функціонування телекомунікаційних мереж, забезпечення доступу до Інтернету, трансляція теле- та радіопрограм.

7. *Фінансові послуги* – функціонування банківської системи, платіжних систем, страхових компаній, фондового ринку.

8. *Транспорт* – перевезення пасажирів та вантажів автомобільним, залізничним, повітряним, водним транспортом.

9. *Оборона та безпека держави* – забезпечення обороноздатності країни, охорона державного кордону, протидія тероризму.

10. *Правопорядок та судочинство* – діяльність правоохоронних органів, судової системи, прокуратури, забезпечення правопорядку.

11. *Цивільний захист та рятувальні служби* – запобігання надзвичайним ситуаціям, реагування на них, ліквідація наслідків.

12. *Космічна діяльність* – функціонування космічних систем зв'язку, навігації, дистанційного зондування Землі.

13. *Хімічна промисловість* – виробництво хімічних речовин, добрив, фармацевтичних препаратів, забезпечення безпеки хімічних виробництв.

14. *Наукові дослідження* – проведення фундаментальних та прикладних досліджень, забезпечення інноваційного розвитку країни.

Кожен з цих секторів має свою специфіку загроз, вразливостей, вимог до захисту. Секторальний підхід дозволяє визначити відповідальні органи державної влади за кожен сектор, розробити галузеві стандарти безпеки, плани реагування на інциденти, здійснювати моніторинг стану критичної інфраструктури в кожному секторі.

Взаємозв'язок між секторами критичної інфраструктури означає, що порушення функціонування об'єктів в одному секторі може каскадно вплинути на інші сектори. Наприклад, порушення електропостачання впливає на телекомунікації, водопостачання, транспорт, медичні заклади. Тому

критично важливим є комплексний підхід до захисту критичної інфраструктури, врахування міжсекторальних залежностей, координація дій різних відповідальних органів.

1.3 Роль захисту об'єктів критичної інфраструктури в системі забезпечення державної безпеки

За період з 2022 по 2024 рік Україна зазнала численних атак на свою критичну інфраструктуру, що включають енергетичні об'єкти, державні мережі, транспортні системи та громадські місця. Ці атаки включають ракетні удари, кібератаки, дронові атаки та терористичні акти.

У жовтні 2022 року вся країна зазнала масованих ракетних ударів, спрямованих на електростанції, що призвело до масштабних пошкоджень електромереж та перерв у постачанні електроенергії. У листопаді Київ постраждав від кібератаки на державні мережі, яка спричинила перебої у роботі урядових систем. У грудні ракетні удари по Києву, Харкову та Львову пошкодили енергетичну інфраструктуру та системи водопостачання.

У лютому Дніпропетровська та Запорізька області зазнали ракетних ударів по електростанціях. У квітні Харків зазнав кібератаки на банківські системи. У травні Харків знову став ціллю ракетних ударів по енергетичній та транспортній інфраструктурі. У серпні Одеська область постраждала від атак дронів, які завдали шкоди портам та енергетичним мережам.

28 січня Полтавська, Донецька, Запорізька та Дніпропетровська області зазнали атак дронів і ракет на критичну інфраструктуру. 22 березня Запоріжжя зазнало масованого ракетного обстрілу, який призвів до руйнування Дніпровської ГЕС та загибелі трьох осіб, понад 20 осіб отримали поранення. 8 травня атаки на Київську та Львівську області крилатими ракетами пошкодили енергетичну інфраструктуру, було поранено двох осіб. 1 червня різні регіони України зазнали масованих атак дронами і ракетами на енергетичну інфраструктуру.

Захист критичної інфраструктури є ключовим елементом забезпечення національної безпеки з кількох причин.

Ефективне функціонування різних галузей економіки має тісний зв'язок з критичною інфраструктурою.

Енергетичні системи є основою економіки, оскільки забезпечують електроенергією підприємства та домогосподарства. Пошкодження або перебої в енергопостачанні можуть призвести до зупинки виробництва, втрати прибутку, зростання вартості продукції через додаткові витрати на енергію, збільшення інфляції та безробіття. Електроенергія необхідна для задоволення побутових потреб населення, і перебої в енергопостачанні призводять до дискомфорту та погіршення якості життя громадян.

Транспортний сектор відіграє критичну роль у глобальній економіці, забезпечуючи рух товарів, послуг та людей. Пошкодження транспортної інфраструктури може спричинити перерви у постачанні, затримки в поставках та підвищення вартості транспортування [47]. Транспорт дозволяє пересувати товари від виробника до споживача, і без ефективного транспортного сектору постачання товарів може бути ускладненим або зовсім зупинитися, що призведе до нестачі товарів на ринку та втрати прибутку для підприємств.

Транспортний сектор забезпечує можливість подорожей для людей як для особистих, так і для професійних цілей. Будь-які обмеження в роботі транспортної інфраструктури можуть призвести до незручностей для пасажирів, збоїв у графіку та втрати часу. Для багатьох галузей промисловості важлива постійна доступність сировини та матеріалів, і транспортний сектор забезпечує їх перевезення від постачальників до виробників [48]. Пошкодження транспортної інфраструктури може призвести до зупинки виробництва через нестачу сировини.

Перерви у роботі транспортної інфраструктури можуть призвести до затримок у поставках, що збільшує вартість транспортування та може призвести до зростання цін на товари і послуги для споживачів [49]. Це також впливає на конкурентоспроможність компаній і загальну економічну стабільність.

Інформаційні мережі є основою сучасної економіки, вони забезпечують зв'язок між бізнесом, клієнтами та партнерами. Пошкодження комунікаційної

інфраструктури може призвести до збоїв у виробництві, втрати контактів із клієнтами, а також погіршення комунікації в екстрених ситуаціях [51].

Інформаційні мережі дозволяють бізнесу підтримувати зв'язок зі своїми клієнтами та партнерами через електронну пошту, телефонні дзвінки, відеоконференції та інші засоби комунікації. Пошкодження комунікаційної інфраструктури може призвести до перерв у спілкуванні, втрати замовлень та партнерів, а також порушення ділових відносин.

Багато підприємств використовують інформаційні технології для автоматизації та оптимізації процесів виробництва, включаючи системи автоматизації виробництва, системи управління ланцюгами постачання, моніторингу якості та інвентаризації [52]. Виробництво часто залежить від вчасного отримання необхідних матеріалів, компонентів та інформації. Збої в комунікаційній інфраструктурі можуть призвести до затримок у поставках матеріалів, що впливає на вчасність виробництва та виконання замовлень.

Якщо виробничі процеси зупиняються через збої в комунікаційній інфраструктурі, це призводить до втрати продуктивності, часу, ресурсів та грошей, що негативно впливає на фінансові результати підприємства [53].

Важливим аспектом інфраструктури комунікацій є її використання в екстрених ситуаціях, таких як природні катастрофи, терористичні атаки чи інші надзвичайні події. Комунікаційні засоби дозволяють органам управління та рятувальним службам координувати дії та надавати необхідну інформацію громадськості для забезпечення безпеки та реагування на небезпеку.

Інформаційні технології стимулюють інновації у багатьох галузях економіки, дозволяючи швидко обмінюватися ідеями, розробляти нові продукти та послуги, впроваджувати нові методи виробництва та управління [52]. Збої у комунікаційній інфраструктурі можуть ускладнити співпрацю між компаніями, затримати впровадження нових технологій та уповільнити темпи розвитку, що може призвести до втрати конкурентоспроможності.

Збої у роботі комунікаційної інфраструктури можуть призвести до перерв у роботі команд, які працюють над новими технологіями та

інноваціями, що спричиняє затримки у випуску нових продуктів на ринок та втрату можливостей для вдосконалення і розширення бізнесу.

У сучасному світі швидкість впровадження нових технологій і інновацій є ключовим фактором для успіху компаній та економік. Проблеми в комунікаційній інфраструктурі можуть уповільнити цей процес та підірвати конкурентоспроможність країни або регіону на міжнародному ринку [53].

Фінансовий сектор грає ключову роль у розвитку економіки, забезпечуючи капітал для інвестицій та функціонування бізнесу. Фінансові установи, такі як банки та інвестиційні компанії, надають кредити та інвестиції для розвитку бізнесу, створення нових підприємств та реалізації інноваційних проектів.

Пошкодження фінансової інфраструктури може призвести до скорочення кредитування та інвестицій, що ускладнює розвиток підприємств та економіки в цілому, до зупинки роботи банків та інших фінансових установ, що спричинить фінансові труднощі для підприємств та населення [54]. Люди можуть мати проблеми з доступом до своїх банківських рахунків або отриманням кредитів, що може призвести до втрати вкладів для банківських клієнтів.

Якщо банк, де зберігаються гроші, стає неспроможним виконувати свої функції через технічні або інші проблеми, це може призвести до втрати заощаджень для клієнтів, спричинити паніку на ринках, втрату довіри до фінансових установ та загрозу фінансовій стабільності [55].

Багато об'єктів критичної інфраструктури надають послуги, які є життєво важливими для населення, такі як електропостачання, водопостачання, медичні послуги. Об'єкти критичної інфраструктури, такі як системи електропостачання, водопостачання та медичні заклади, надають послуги, без неперервної роботи яких може загрожувати безпека та здоров'я громадян, а також порушуватися звичний порядок життя [54, 55, 57].

Надійна робота критичної інфраструктури сприяє збереженню соціального порядку, оскільки вона забезпечує громадянам доступ до

необхідних ресурсів та послуг, що сприяє зменшенню напруги та конфліктів у суспільстві.

Пошкодження або перебої в роботі критичної інфраструктури можуть призвести до виникнення гуманітарних криз, таких як перерви в електропостачанні, відключення водопостачання чи недоступність медичних послуг, що може спричинити екстрені ситуації та загострення соціальних проблем [56].

Багато об'єктів критичної інфраструктури мають стратегічне значення для оборони країни, оскільки вони можуть використовуватися для забезпечення військової мобілізації, комунікації та ведення оборонних операцій.

Об'єкти, такі як енергетичні мережі, транспортна інфраструктура, комунікаційні системи та водопостачання, мають велике стратегічне значення для оборони країни [39, 43, 47, 51]. Вони є основою функціонування військових структур, забезпечують важливі ресурси та послуги для військових задач та операцій.

Критична інфраструктура грає ключову роль у забезпеченні військової мобілізації. Транспортні мережі важливі для переміщення військ та обладнання до місць концентрації, а енергетичні системи – для забезпечення роботи військово-промислових об'єктів [47, 43].

Інформаційні системи та комунікаційна інфраструктура дозволяють забезпечити зв'язок між військовими підрозділами, координувати дії та передавати важливі команди та інформацію, є невід'ємною частиною ведення оборонних операцій [51].

Пошкодження чи зупинка роботи критичної інфраструктури може серйозно ускладнити здатність країни відстоювати себе в разі військової агресії. Недоступність ключових ресурсів та послуг може значно обмежити можливості оборони та вразити ефективність військової складової.

Об'єкти критичної інфраструктури можуть бути об'єктом терористичних атак або кібератак, спрямованих на національну безпеку. Енергетичні мережі, транспортні вузли чи водопостачання можуть стати потенційними цілями для терористичних груп.

Крім традиційних терористичних атак, критична інфраструктура також піддається кіберзагрозам. Кібератаки можуть спрямовуватися на інформаційні системи, електронні мережі та критичні технологічні системи, що може призвести до порушення роботи об'єктів інфраструктури та втрати конфіденційної інформації [51, 52, 53].

Захист критичної інфраструктури від терористичних атак та кіберзагроз включає різноманітні заходи, такі як підвищення фізичної охорони об'єктів, застосування сучасних технологій кібербезпеки, розвиток імунітету до кібератак та підвищення обізнаності персоналу щодо можливих загроз [24].

Ефективна боротьба з тероризмом та кіберзагрозами передбачає не лише запобігання можливим атакам, але й швидке реагування у разі їхнього виникнення. Це включає вчасне виявлення потенційних загроз, швидке реагування на інциденти та відновлення роботи інфраструктури після атаки [23, 24].

Країни, які мають ефективно захищену критичну інфраструктуру, є більш привабливими для інвесторів та міжнародних партнерів. Інвестори шукають країни з надійною та стабільною інфраструктурою, оскільки це забезпечує їм високий рівень впевненості у безпеці їхніх інвестицій [10, 16]. Країни з ефективно захищеною критичною інфраструктурою вважаються більш привабливими для інвесторів, що може призвести до збільшення обсягів інвестицій та розвитку бізнесу.

Країни, які демонструють високий рівень захисту критичної інфраструктури, зазвичай мають більшу ймовірність налагодження міжнародних партнерств та співпраці [35]. Це може включати торговельні угоди, науково-технічну співпрацю, обмін технологіями та інші форми співробітництва.

Ефективний захист критичної інфраструктури сприяє стабільному функціонуванню економіки, стимулює підприємництво, збільшує рівень виробництва та залучає нові інвестиції. В результаті економіка країни зростає, а її позиції на міжнародній арені підвищуються [16, 35].

Країни з ефективно захищеною критичною інфраструктурою відомі своєю надійністю та стабільністю, що підвищує їхній престиж на міжнародній арені та сприяє покращенню їхнього міжнародного образу [10].

Висновки до розділу 1

Захист критичної інфраструктури є важливим завданням для забезпечення національної безпеки, оскільки він допомагає забезпечити економічну та соціальну стабільність, зберегти оборонну готовність та запобігти різноманітним загрозам.

Критична інфраструктура становить основу функціонування сучасного суспільства та держави, охоплюючи системи енергопостачання, транспорту, комунікацій, водопостачання, фінансові установи, медичні заклади та інші життєво важливі об'єкти [1, 3, 18]. Її захист є пріоритетним напрямом державної політики у сфері національної безпеки [7, 21].

Аналіз міжнародного досвіду показує, що ефективна система захисту критичної інфраструктури базується на комплексному підході, який поєднує нормативно-правові, організаційні та технологічні інструменти [12, 13, 14, 15, 16]. Секторальний принцип організації захисту дозволяє враховувати специфіку кожної галузі та розробляти адаптовані стратегії безпеки [34, 35].

Події 2022-2024 років продемонстрували критичну важливість надійного захисту об'єктів критичної інфраструктури для забезпечення життєдіяльності держави в умовах збройної агресії. Масовані атаки на енергетичну, транспортну та комунікаційну інфраструктуру підтвердили необхідність посилення заходів фізичного та кіберзахисту стратегічних об'єктів.

Захист критичної інфраструктури безпосередньо впливає на всі ключові сфери національної безпеки: економічну стабільність, соціальний порядок, оборонну спроможність, протидію терористичним та кіберзагрозам, а також на міжнародну репутацію держави [32, 33, 35]. Це робить розвиток ефективної системи захисту критичної інфраструктури одним із найважливіших завдань сучасної безпекової політики України.

Розділ 2. ОЦІНКА СУЧАСНИХ ВИКЛИКІВ ТА ВРАЗЛИВОСТЕЙ ЖИТТЄВО ВАЖЛИВИХ СИСТЕМ

2.1 Кібернетичні виклики

Проблема інформаційної безпеки та комп'ютерної злочинності в Україні

Наразі в Україні гостро постає проблема інформаційної безпеки та комп'ютерної злочинності, тоді як правова база та судова практика не повністю відповідають вимогам сучасності. Комп'ютерні злочини – це незаконні дії, в яких інформаційно-обчислювальні системи стають об'єктом або інструментом злочинних посягань [58]. Усі відомі у світі види таких злочинів, як комп'ютерне шахрайство, саботаж, шпигунство та крадіжки програм, вже реєструються в Україні.

1 вересня 2001 року набув чинності Кримінальний кодекс України, який містить розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж" [59]. У ньому вперше визначені та юридично оформлені існуючі суспільно небезпечні діяння у цій сфері. Однак методичні рекомендації щодо їх розслідування є недостатніми, а судова практика потребує розвитку.

Слід зазначити, що закони самі по собі, а також організаційно-технічні заходи, не можуть системно захистити інформаційні системи від злочинних посягань [60]. Тому державі необхідно не лише реагувати на існуючі суспільно небезпечні дії у сфері інформатизації, але й формувати адекватну політику кібербезпеки, враховуючи реалії та прогнозовані тенденції розвитку в кібернетичній сфері [61].

За останні десятиліття інформаційні технології стали невід'ємною частиною повсякденного життя. Активний розвиток цих технологій пов'язаний не лише з розробкою новітніх рішень, але й із створенням найбільш

досконалого програмного забезпечення [62]. На жаль, ці технології також використовуються у незаконній діяльності, зокрема в кібершпигунстві.

Кібершпигунство або ***комп'ютерний шпіонаж*** означає несанкціоноване отримання інформації з метою здобуття особистої, економічної, політичної чи військової переваги [63]. Це досягається шляхом зламу систем комп'ютерної безпеки, використання шкідливого програмного забезпечення, зокрема "троянських коней" та шпигунських програм. Кібершпигунство може проводитися дистанційно через Інтернет або шляхом фізичного проникнення в комп'ютери та мережі підприємств.

У Кримінальному кодексі України шпигунство визначено як передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії здійснені іноземцем або особою без громадянства (ст. 114 КК України) [59].

Основним об'єктом кібершпигунства є кібернетична загроза зовнішній безпеці України, її суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці [64]. Кібернетична загроза включає наявні та потенційні явища і фактори, які створюють небезпеку для інтересів людини, суспільства і держави через порушення доступності, цілісності, достовірності та автентичності інформації, що циркулює в критичних об'єктах національної інформаційної інфраструктури.

Згідно з аналізом Державної служби спеціального зв'язку та захисту інформації України, у 2022 році було зафіксовано 2194 кіберінциденти, з яких 1048 мали високий або критичний рівень [65]. У 2023 році загальна кількість кіберінцидентів становила 2554, з яких 367 були серйозними [65].

Перші місяці 2024 року демонструють збільшення кількості кібератак, які здійснюють російські хакери на українські інформаційні системи. У першому кварталі 2024 року Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA вжито заходів з недопущення реалізації

зловмисного задуму щодо деструктивного впливу на три українські організації урядового та енергетичного сектору [66].

Однією з найактивніших загроз є угруповання найманців UAC-0050, пов'язане з російськими правоохоронними органами [66]. Станом на 22 лютого 2024 року було виявлено щонайменше 15 кампаній, під час яких зловмисники використовували п'ять видів шкідливих програм: REMCOS RAT, QUASAR RAT, VENOM RAT, REMOTE UTILITIES та LUMMASTEALER.

Команда CERT-UA також виявила, що однією з найбільших кіберзагроз є UAC-0010 (Armageddon), яка походить від колишніх співробітників органів безпеки, які у 2014 році перейшли на бік РФ [66]. Головною метою цієї групи є кібершпигунство щодо безпеки та оборони України. Кількість одночасно інфікованих комп'ютерів, переважно у системах державних органів, може сягати кількох тисяч.

Під кібератакою розуміють атаку на інформаційну інфраструктуру, яка є сукупністю пов'язаних між собою дій зловмисника, що приводять до реалізації загроз для інформаційних ресурсів шляхом використання вразливостей певної інформаційної системи [67].

Умовно можна розрізняти два типи кібератак залежно від місця знаходження зловмисника:

1. *Локальне проникнення* (local penetration) – зловмисник знаходиться всередині об'єкта та використовує прямий доступ до інформаційної системи.

2. *Віддалене проникнення* (remote penetration) – зловмисник знаходиться поза системою та використовує віддалений доступ для здійснення атаки [68].

Фішинг – це вид кіберзлочину, в якому зловмисники намагаються отримати конфіденційну інформацію, таку як логіни, паролі, дані кредитних карток або інші персональні дані, обманним шляхом [69]. Зазвичай це робиться шляхом маскування під надійне джерело через електронну пошту, повідомлення в соцмережах, телефонні дзвінки або вебсайти.

Систематичні фішинг-атаки почалися в мережі America Online (AOL) у 1995 році [70]. Термін "фішинг" з'явився в групі новин Usenet. У 2001 році відбулася одна з перших великих спроб, коли зловмисники, скориставшись хаосом від терористичних атак 9/11, розіслали потерпілим електронну розсилку нібито для перевірки посвідчення особи.

У 2005 році за допомогою фішингу кіберзлочинці викрали у користувачів США понад 900 мільйонів доларів [71]. У 2016 році спостерігалося понад 250 тисяч унікальних фішингових атак, під час яких використовувалось рекордне число доменних імен, що перевищило позначку в 95 тисяч [72].

Смішинг (від "SMS" і "фішинг") – це вид фішингу, який здійснюється через SMS [73]. Шахраї надсилають жертві повідомлення з посиланням на фішинговий сайт. Через особливості мобільних браузерів URL-адреси можуть відображатися не повністю, що ускладнює ідентифікацію підробленої сторінки входу.

Вішинг (від "voice" і "fishing") – це вид телефонного шахрайства, який полягає у виманюванні реквізитів банківських карток або іншої конфіденційної інформації [74]. Схема проста: шахраї телефонують із незнайомого номера і під різними приводами намагаються вивідати дані платіжної картки або змусити перерахувати кошти.

Основні сценарії вішингу включають: залякування – представляються співробітниками правоохоронних органів і повідомляють про нібито скоєний злочин родичем жертви; виграш – повідомляють про виграші, перерахунки пенсій чи соціальних виплат.

Кетфішинг – це вид шахрайства, коли людина створює вигаданий неспр авжній акаунт у соціальних мережах або на сайтах знайомств, зазвичай націлюючись на конкретну жертву [75].

Атака "злий двійник" (Evil twin) – різновид фішингу у бездротових комп'ютерних мережах [76]. Зловмисник створює копію бездротової точки

доступу, що знаходиться в зоні досяжності користувача, замінюючи справжню точку доступу своєю підробкою.

У 2024-2025 роках фішинг залишається однією з головних загроз кібербезпеці в Україні [77]. За даними звіту Cybersecurity Ventures, у 2024 році було виявлено значне зростання кількості шкідливих URL-адрес на 61%, що відповідає 255 млн фішингових атак за рік [77].

Україна також стикається зі збільшенням кількості кібератак через геополітичну нестабільність. Близько третини глобального потоку шкідливих email-розсилок надходить з Росії, і ці атаки часто спрямовані на українські організації та інфраструктуру [78].

SQL-ін'єкція – один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду [79]. Впровадження SQL може дати можливість зловмиснику виконати довільний запит до бази даних, отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері.

Види SQL-ін'єкцій:

1. *SQL Injection в параметрах запитів* – найбільш поширений вид, коли зловмисник вводить SQL-код безпосередньо в параметри запиту до веб-додатка через форми вводу, URL-параметри або інші вхідні дані [80].

2. *Blind SQL Injection* – зловмисник використовує техніки тестування на "сліпоту" для визначення наявності і структури даних без прямого витягування їх [80].

3. *Time-Based SQL Injection* – використовується для створення затримок у відповіді сервера, які дозволяють виявити наявність і експлуатувати вразливість [80].

4. *Second-Order SQL Injection* – виникає, коли введені дані не відразу використовуються у SQL-запитах, але зберігаються в базі даних і використовуються пізніше [80].

Схема атаки SQL-ін'єкції включає: збір інформації про структуру бази даних; створення SQL-ін'єкційного виразу; експлуатацію вразливості; приховування слідів атаки.

XSS (Cross-Site Scripting) є типом кібератаки, яка полягає у впровадженні на веб-сторінку зловмисного JavaScript-коду, який виконується у веб-браузері іншого користувача [81]. Основна ідея XSS-атак полягає в тому, що зловмисник використовує недостатньо фільтровані або оброблені вхідні дані для впровадження коду.

Види XSS-атак:

1. *Stored XSS* (збережені XSS) – найпоширеніший тип, коли зловмисний код зберігається на сервері і виконується у браузерах користувачів, які переглядають вразливу сторінку [81].

2. *Reflected XSS* (відображені XSS) – зловмисний код вставляється у відповідь веб-сервера і потрапляє до браузера користувача як частина URL-адреси або форми [81].

3. *DOM-based XSS* – відбувається на стороні клієнта і викликається через модифікацію DOM (Document Object Model) [81].

Наслідки XSS-атак: крадіжка сесійних ідентифікаторів; видалення або модифікація вмісту сторінки; перенаправлення на зловмисний сайт

Заходи захисту від XSS-атак: екранування вхідних даних; валідація і фільтрація вхідних даних; використання безпечних API для вставки HTML-коду; використання HTTP заголовків, таких як Content Security Policy (CSP); регулярне оновлення програмного забезпечення [82].

Аналізатори протоколів є потужними інструментами для отримання і аналізу мережевого трафіку в реальному часі [83]. Вони працюють на рівні мережевого інтерфейсу, дозволяючи отримувати доступ до всіх пакетів даних, що проходять через мережеву карту.

Основні функції аналізаторів протоколів: захоплення трафіку; аналіз протоколів; фільтрація і сортування трафіку; детальний аналіз і візуалізація; виявлення вразливостей і атак.

Однією з найбільш небезпечних аспектів використання аналізаторів протоколів є можливість отримання конфіденційної інформації, такої як логіни, паролі, сесійні токени і інші чутливі дані [83]. Якщо мережевий трафік не зашифрований, зловмисники можуть захоплювати ці дані і використовувати для незаконного доступу.

MITM-атака – це серйозна кібератака, в якій зловмисник вставляється між двома спілкуючимися сторонами і перехоплює весь або частину їхнього комунікаційного потоку [84].

Як працює MITM атака: перехоплення трафіку між двома легітимними сторонами; аналіз і модифікація даних, що передаються; вставлення фальшивих даних у комунікаційний потік.

Потенційні наслідки: крадіжка конфіденційної інформації; маніпуляція з комунікацією; атаки на безпеку мережі.

DoS-атака має на меті зробити певний ресурс недоступним для користувачів шляхом перевантаження його ресурсів або експлуатації слабких місць у системі [85].

Основні типи DoS атак: UDP Flood – надсилання великого обсягу UDP-пакетів; ICMP Flood – використання ICMP-пакетів для перевантаження; SYN Flood – надсилання величезної кількості SYN-пакетів; HTTP Flood – велика кількість HTTP-запитів до веб-сервера [86].

DDoS атака (Distributed Denial of Service) – це підтип DoS, що відрізняється тим, що атака проводиться з множини комп'ютерів, розташованих у різних частинах світу [87].

Особливості DDoS атак: розподілене джерело через ботнет; складність виявлення через різні IP-адреси; великі обсяги трафіку.

Приклади DDoS атак: атака на компанію GitHub у 2018 році перевищила 1,3 Tbps [88]; атака на українські банки у 2016 році паралізувала банківські системи [89].

Спам e-mail вважається найстарішим методом атак: велика кількість поштових повідомлень роблять неможливою роботу з поштовими скриньками та цілими поштовими серверами [90].

Основні характеристики: масове відправлення повідомлень; цільовість на конкретного користувача або домен; використання анонімних поштових серверів; приховування ідентичності

Потенційні наслідки: перевантаження поштових серверів; втрата робочого часу; зниження продуктивності.

2.2 Технологічні та природні ризики

Фізичні загрози для об'єктів критичної інфраструктури є серйозною проблемою, що може мати далекосяжні наслідки для суспільства [91]. Ці загрози можуть бути викликані різними факторами: терористичними актами, природними катастрофами, техногенними аваріями та іншими небезпечними подіями.

Терористичні акти є одним із найбільш серйозних типів загроз для критичної інфраструктури [92]. Терористи можуть впроваджувати вибухові пристрої на об'єкти інфраструктури, такі як залізничні колії, аеропорти, електростанції та водозабірні споруди.

Мінування об'єктів критичної інфраструктури:

1. Транспортні мережі (залізничні, авіаційні, водний і автомобільний транспорт).
2. Залізничні колії та автомобільні дороги.
3. Автомобіль-фугас на об'єктах критичної інфраструктури [93].

Застосування вибухових пристроїв:

1. У поштових посилках або бандеролях.
2. Хімічна зброя масового ураження.
3. Вибухові пристрої на стратегічних об'єктах.

Збройне захоплення заручників на об'єктах критичної інфраструктури є однією з найбільш серйозних загроз безпеці [94]. Такий вид нападу часто використовується для досягнення політичних, фінансових або ідеологічних цілей.

Сценарії збройного захоплення:

- *політичні мотиви* – привернення уваги до політичних проблем або вимагання політичних змін [94].

- *фінансові вимоги* – вимагання викупу або інших матеріальних вигод.

- *ідеологічні мотиви* – відстоювання певних політичних, релігійних або етнічних поглядів.

Наслідки захоплення заручників: серйозна загроза для життя та здоров'я людей; припинення нормальної роботи об'єкта; паніка серед населення та психологічні травми; значний рівень страху і непевності в суспільстві [95].

Природні катастрофи, такі як землетруси, урагани, повені та лісові пожежі, можуть призвести до значних руйнувань інфраструктури [96].

Види загроз природного характеру:

- *Метеорологічні:* снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, засухи [97].
- *Гідрологічні:* повені, селі, паводки, підтоплення [97].
- *Геологічні:* небезпечні екзогенні геологічні процеси - зсуви, просідання та карст [97].
- *Геліофізичні:* пожежі [97].

Листопад 2000 року – значні обледеніння спричинили серйозні матеріальні збитки і проблеми з інфраструктурою [98]: понад 20 тисяч ліній електропередач було пошкоджено; 307 тисяч залізобетонних опор стали непридатними; 34 тисяч тонн дроту стали непридатними; 2000 сільських телефонних станцій було відключено.

Січень 2014 року – сильний снігопад і обледеніння значно ускладнили життя населення [99]: пошкоджено повітряні лінії електропередач; знеструмлено 1605 населених пунктів; ускладнено або припинено рух автотранспорту.

Найбільш масштабний паводок спричинив [100]: пошкодження понад 500 автомобільних мостів; розмивання 1660 км автомобільних доріг різного значення.

До 20% залізничних колій знаходяться під впливом регіонального підтоплення земель, близько 40% перебувають у зонах карстових загроз, до 11% – на територіях можливої активізації зсувних процесів [101].

До 59% магістральних газопроводів перебувають в умовах можливого прояву карсту, до 21% – у зонах прояву регіонального підтоплення земель [101].

Техногенні аварії, такі як вибухи на промислових об'єктах, аварії на ядерних електростанціях або хімічні розливи, становлять серйозну загрозу [102]. Ці події можуть мати далекосяжні наслідки для оточуючого середовища, здоров'я людей і навколишнього регіону.

Вибухи на заводах, складах хімічних речовин або нафтопереробних підприємствах можуть призвести до [103]: руйнування будівель та інфраструктури; випуску хімічних речовин в атмосферу; забруднення навколишнього середовища.

Аварії на атомних електростанціях, а саме випуск радіоактивних матеріалів може призвести до [104]: серйозного забруднення атмосфери і ґрунтів; необхідності евакуації територій; значного соціального і економічного впливу.

Аварії на хімічних виробництвах, а саме випуск хімічних речовин може спричинити [105]: серйозні наслідки для здоров'я людей; пожежі і вибухи; забруднення навколишнього середовища.

Техногенні аварії на об'єктах критичної інфраструктури вимагають комплексного підходу до моніторингу, запобігання та реагування [106], а саме:

1. Належне функціонування систем моніторингу для вчасного виявлення відхилень.
2. Системи виявлення викидів, радіаційні монітори.
3. Системи моніторингу хімічних речовин.
4. Збір даних в реальному часі.

Фізичні загрози для об'єктів критичної інфраструктури не лише призводять до значних матеріальних збитків і втрат людських життів, але й порушують звичний ритм функціонування суспільства [107]. Вони можуть спричиняти паніку, великі соціальні та економічні втрати, а також призводити до значних викликів для систем здоров'я, правопорядку і громадської безпеки.

У зв'язку з цим важливо розвивати та впроваджувати ефективні стратегії захисту інфраструктури, включаючи підвищення обізнаності про загрози, розробку планів надзвичайних ситуацій і вдосконалення технологічних

засобів безпеки [108]. Тільки комплексний підхід може забезпечити ефективний захист від фізичних загроз для об'єктів критичної інфраструктури і зберегти стабільність суспільства в умовах надзвичайних подій.

2.3 Внутрішні загрози суспільного характеру

Соціально-економічні загрози, такі як економічні кризи та соціальні протести, можуть мати значний вплив на об'єкти критичної інфраструктури, що включає системи, необхідні для підтримки основних функцій суспільства [109].

Енергетичний сектор часто стає жертвою бюджетних скорочень під час економічних криз [110]. Зменшення інвестицій у модернізацію та обслуговування енергетичних об'єктів призводить до зниження якості послуг та збільшення частоти аварій. Ці наслідки відчутно позначаються на всіх аспектах економічного та соціального життя країни.

Наслідки недостатнього фінансування: зниження якості обслуговування енергетичних об'єктів; перебої в постачанні електроенергії; підвищення ризику аварій та технічних збоїв; значні економічні втрати для підприємств; соціальне напруження та незадоволення населення [111].

Світова фінансова криза 2008-2009 років суттєво вплинула на економіку України [112]. Значне падіння ВВП, скорочення промислового виробництва та дефіцит бюджету призвели до скорочення інвестицій у енергетичний сектор. Багато енергетичних компаній зіткнулися з браком фінансування для модернізації та ремонту обладнання, що призвело до частих аварій та перебоїв у постачанні електроенергії.

Економічна криза, спричинена політичною нестабільністю та військовими діями на сході України у 2014-2015 роках, ще більше загострила проблеми енергетичного сектору [113]. Багато електростанцій, підстанцій та ліній електропередач було зруйновано або пошкоджено. У 2014 році Україна зіткнулася з серією масштабних відключень електроенергії, викликаних дефіцитом вугілля для електростанцій та зниженням виробничих потужностей.

Під час економічної кризи 2008-2009 років Іспанія зіткнулася зі значними фінансовими труднощами [114]. Зниження інвестицій у

електромережі та генераційні потужності спричинило часті збої у постачанні електроенергії. У 2007 році у Барселоні відбувся масштабний блекаут, який тривав понад 24 години і вплинув на життя сотень тисяч людей.

Греція зазнала серйозних економічних труднощів під час фінансової кризи, що почалася у 2009 році [115]. Скорочення державного фінансування енергетичних об'єктів призвело до дефіциту ресурсів для їх обслуговування та модернізації. Влітку 2011 року Греція зіткнулася з серією відключень електроенергії через неспроможність енергетичних компаній забезпечити належний рівень обслуговування.

Економічні кризи, особливо ті, що супроводжуються військовими конфліктами, призводять до значного зниження інвестицій у критичні сектори економіки [116]. З 2022 року країна зіткнулася з гострою нестачею інвестицій через бюджетний дефіцит, спричинений військовими діями та економічною нестабільністю.

За останні два роки значно скоротилися капітальні інвестиції в ремонт та будівництво доріг, модернізацію залізничної інфраструктури, а також оновлення парку громадського транспорту [117]. Відсутність належного ремонту призводить до утворення ям та інших дефектів на дорогах, що збільшує ризик дорожньо-транспортних пригод [118]. Застаріла інфраструктура та недостатній рівень обслуговування рухомого складу спричиняють часті поломки та затримки у графіку руху поїздів [119]. Багато ділянок залізничних колій потребують капітального ремонту, що призвело до збільшення кількості аварій. Недостатня технічна підтримка призводить до затримок у обслуговуванні літаків та суден [120]. Обмеження фінансування спричинило зниження якості обслуговування пасажирів та вантажів.

В умовах економічних криз та військових конфліктів багато місцевих бюджетів стикаються з серйозними проблемами у фінансуванні критичних комунальних інфраструктур [121]. Відсутність достатнього фінансування призводить до недостатньої модернізації та обслуговування водопровідних систем, що спричиняє зниження якості води та часті пориви труб [122]. Багато

комунальних підприємств не мають достатніх ресурсів для ефективного обслуговування та модернізації систем каналізації [123]. Старі котельні та тепломережі не модернізуються, що призводить до підвищення витрат на енергію і частих аварій [124].

Нестача фінансування веде до зниження якості обслugovування комунальних послуг. У багатьох містах України під час кризи 2022-2025 років стали частими випадки перебоїв у водопостачанні, збоїв у системах водовідведення і проблеми з теплопостачанням [125].

З початком військового конфлікту та економічної нестабільності система охорони здоров'я зазнала значних труднощів через дефіцит ресурсів [126]. Обмежені бюджетні кошти призводять до дефіциту фінансування для медичних установ, що обмежує можливості для закупівлі медикаментів, медичного обладнання та оплати праці медичних працівників [127]. У 2022-2025 роках спостерігалося зниження якості медичного обслуговування через застаріле або недостатньо забезпечене обладнання в лікарнях [128].

В умовах економічної кризи багато медичних закладів, особливо у менш населених або економічно слабших регіонах, стикаються з необхідністю закриття через фінансові труднощі [129]. У 2024 році в ряді малих міст і сіл України було закрито кілька лікарень через зниження фінансування.

Соціальні протести можуть суттєво вплинути на об'єкти критичної інфраструктури, зокрема на енергетичну інфраструктуру [130]. У Києві протести призвели до атак на енергетичні об'єкти. Протестувальники пошкодили підстанцію, що спричинило значні перебої в електропостачанні в центральних районах міста [131]. Під час масових протестів на сході України відбулися напади на енергетичну інфраструктуру в зонах конфлікту. Були пошкоджені лінії електропередач і трансформаторні підстанції, що призвело до тривалих відключень електроенергії [132].

Соціальні протести можуть спричинити збої у постачанні енергії, блокуючи доступ до ключових енергетичних об'єктів або перешкоджаючи нормальному функціонуванню енергетичних систем [133]. В Одесі

протестувальники блокували дороги, що ведуть до важливих енергетичних об'єктів, таких як електростанції і підстанції, що ускладнило доставку необхідних ресурсів та обслуговування обладнання [134]. Протестувальники перекрили основні транспортні артерії для доставки пального на електростанції, що призвело до дефіциту пального для генераторів [135].

Акції протесту можуть значно порушити стабільність надання комунальних послуг через блокування транспортних шляхів, перекриття доступу до об'єктів інфраструктури та затримки у виконанні обслуговувальних робіт [136]. Протестувальники можуть завдати шкоди водопровідним і каналізаційним системам, котельням і насосним станціям, газовим мережам [137]. Пошкодження такого обладнання може спричинити тимчасове припинення постачання тепла або води.

2.4 Воєнно-стратегічні виклики та їх вплив на інфраструктуру

З 2022 року Україна зіткнулася з одночасною економічною та військовою кризою, спричиненою повномасштабним вторгненням Росії [138]. Ці події мали руйнівний вплив на всі аспекти критичної інфраструктури, зокрема на енергетичний сектор.

З початку вторгнення у лютому 2022 року російські війська здійснили численні атаки на енергетичні об'єкти України, включаючи електростанції, підстанції, трансформатори та лінії електропередач [139].

Російські війська здійснили ракетний обстріл Київської області, що призвело до знищення однієї з великих підстанцій і масових відключень електроенергії у столиці та прилеглих районах [140]. Відбулася атака на Запорізьку атомну електростанцію, найбільшу в Європі. В результаті пошкодження критичних компонентів станції було знижено її потужність [141].

Економічна криза, викликана війною, ще більше загострила ситуацію [142]. Зменшення бюджетних надходжень, інфляція, дефіцит ресурсів та збільшення витрат на військові потреби призвели до скорочення фінансування на модернізацію та обслуговування енергетичних об'єктів.

У 2023 році Україна втратила понад 10 мільярдів доларів через пошкодження енергетичної інфраструктури та перебої в постачанні електроенергії [143]. Ці втрати включають не лише прямі витрати на відновлення об'єктів, але й економічні збитки від зупинки промислових підприємств.

Постійні перебої в постачанні електроенергії вплинули на всі аспекти життя, включаючи медичні послуги, освіту, комунальні послуги та побутові умови [144].

Зимовий період 2022-2023, 2024-2025 років став особливо важким. Часті відключення електроенергії змусили людей шукати альтернативні джерела опалення та освітлення [145].

Лікарні були змушені використовувати резервні генератори, які не завжди могли забезпечити стабільне постачання електроенергії для всіх необхідних пристроїв [146]. Школи та університети були змушені переходити на дистанційне навчання або скорочувати заняття через неможливість забезпечити необхідні умови [147].

В Україні воєнні загрози виявляються у численних формах, включаючи прямі атаки на інфраструктуру, руйнування об'єктів і дестабілізацію життєво важливих систем [148].

В умовах воєнного конфлікту енергетичні об'єкти стають цільовими для атак [149]. Знищення або пошкодження електростанцій, підстанцій і ліній електропередач призводить до перебоїв у постачанні електроенергії.

Під час військових дій на сході України, зокрема в Донецькій і Луганській областях, спостерігались численні атаки на енергетичну інфраструктуру [150]. Внаслідок обстрілів були зруйновані або пошкоджені високовольтні лінії та трансформаторні підстанції.

Воєнні дії часто призводять до блокування транспортних шляхів і зниження постачання пального та інших необхідних матеріалів для енергетичних об'єктів [151]. В умовах війни постачання пального для електростанцій може бути ускладнене, що призводить до зменшення виробництва електроенергії. Вони часто супроводжуються атаками на дороги, мости, залізниці та аеропорти [152]. Під час військового конфлікту на сході України багато мостів і залізничних шляхів були зруйновані або пошкоджені, що призвело до затримок у перевезенні гуманітарної допомоги і товарів.

Обстріли і бойові дії можуть ускладнити проведення ремонту та обслуговування транспортної інфраструктури [153]. У зонах бойових дій ремонтні роботи на дорогах і залізницях часто припиняються через небезпеку для працівників. Таки атаки на об'єкти водопостачання, теплопостачання та газопостачання можуть призвести до їх фізичного пошкодження [154]. Військові дії в Україні призводили до пошкодження водозабірних станцій,

насосних станцій і котелень, що спричинило перебої в водопостачанні і опаленні.

В умовах воєнного конфлікту можуть виникати затримки у ремонті і обслуговуванні комунальних об'єктів через безпекові ризики [155]. Під час активних бойових дій обслуговування і ремонт комунальних служб може бути ускладнене або зовсім припинене.

Атаки на медичні заклади можуть призвести до їх руйнування або пошкодження, що обмежує доступ до медичних послуг [156]. У зонах бойових дій в Україні були зафіксовані випадки обстрілу лікарень і медичних центрів, що призводило до тимчасового закриття медичних установ.

Воєнні дії можуть призвести до затримок у постачанні медичних товарів і обладнання [157]. Під час воєнного конфлікту постачання медичних матеріалів може бути ускладнене через порушення логістичних ланцюгів.

2.5 Досвід застосування сил Національної гвардії України для забезпечення безпеки стратегічних об'єктів за умов особливого правового режиму

В умовах воєнного стану захист критичної інфраструктури стає надзвичайно важливим завданням для забезпечення національної безпеки і стабільності [158]. Національна гвардія України, як один з основних складових частин системи національної безпеки, грає ключову роль у забезпеченні охорони критичних об'єктів.

В умовах збройного конфлікту та підвищених загроз підрозділи Національної гвардії виконують ряд важливих завдань, включаючи охорону стратегічних об'єктів, реагування на загрози і забезпечення стабільності [159].

Захист критичної інфраструктури є життєво важливим для забезпечення стабільності та безпеки держави [160]. Першим етапом у процесі охорони є точне визначення критичних об'єктів. Для ефективного визначення таких об'єктів проводять комплексний аналіз їхньої важливості, уразливості та потенційного впливу на національну безпеку у разі атаки.

Під час військового конфлікту Національна гвардія взяла на себе охорону стратегічних об'єктів енергетичної інфраструктури в Києві [161]. Включення підстанцій і електростанцій до переліку критичних об'єктів дозволило своєчасно забезпечити їхню охорону. Це було обумовлено тим, що збої в електропостачанні можуть мати серйозні наслідки для життєдіяльності міста.

Для цього були розроблені конкретні заходи захисту, такі як встановлення фізичних бар'єрів, організація постійного патрулювання та моніторинг ситуації [162].

Після визначення критичних об'єктів важливо встановити відповідні заходи захисту, які можуть включати фізичні бар'єри, системи контролю доступу, моніторинг і оперативну підтримку [163].

На великих транспортних вузлах проводиться комплексне впровадження захисних заходів:

1. *Фізичні бар'єри:* Встановлення спеціальних огорож, блокпостів і контрольно-пропускних пунктів.

2. *Системи контролю доступу:* Використання електронних систем з RFID-технологією, біометричні зчитувачі.

3. *Моніторинг:* Установка камер відеоспостереження, інтеграція з системами раннього попередження [164].

В умовах воєнного стану ефективний ситуаційний моніторинг та раннє попередження є критично важливими для забезпечення безпеки об'єктів критичної інфраструктури [165].

Ситуаційний моніторинг включає використання різноманітних технологій і систем для відстеження і аналізу ситуації на об'єкті:

Відеоспостереження: системи відеоспостереження забезпечують цілодобовий моніторинг території. Сучасні камери можуть бути оснащені високою роздільною здатністю, функціями нічного бачення і можливістю розпізнавання облич [166].

Безпілотні літальні апарати (БПЛА): БПЛА використовуються для патрулювання великих територій і виконання моніторингу з висоти [167]. Вони дозволяють здійснювати огляд території, який важко забезпечити з допомогою стаціонарних камер.

Системи раннього попередження забезпечують оперативну і точну інформацію про потенційні загрози [168]. Це включає інтеграцію даних з різних джерел, аналіз інформації та прийняття рішень для забезпечення безпеки.

Використання аналітичних інструментів на критичних об'єктах дозволяє прогнозувати можливі загрози на основі аналізу патернів поведінки та історичних даних [169].

Регулярні тренування і симуляції є критично важливими для підрозділів, що відповідають за охорону критичної інфраструктури [170]. Вони

дозволяють відпрацювати дії в умовах надзвичайних ситуацій, що може значно підвищити готовність та ефективність реагування на реальні загрози.

До основних типів тренувань належать:

- *навчання з евакуації персоналу:* головною метою є забезпечення безпечного і організованого виходу з небезпечної зони у випадку надзвичайної ситуації [171].
- *протидія атакам:* тренування зосереджені на відпрацюванні дій у разі фізичних атак, таких як проникнення зловмисників або терористичні акти [172].
- *реакція на критичні ситуації:* фокусуються на оперативному реагуванні в умовах, коли вже сталися надзвичайні ситуації [173].
- *навчання з евакуації під час терористичних атак:* на комунальному підприємстві, що постачає воду для великого міста, проводяться регулярні тренування з евакуації у разі терористичного нападу [174].
- *симуляції протидії саботажу:* на великому виробничому підприємстві проводяться симуляції, де відпрацьовуються сценарії саботажу [175].
- *тренування з реагування на загрози:* під час навчань на стратегічних об'єктах, таких як атомні електростанції, персонал відпрацьовує сценарії аварій з викидом радіоактивних матеріалів [176].

Національна гвардія активно співпрацює з іншими правоохоронними органами та місцевими адміністраціями для забезпечення комплексного захисту критичної інфраструктури [177]. Це включає обмін інформацією, координацію дій та спільні навчання.

У разі підвищеної загрози Національна гвардія спільно з поліцією організовує посилені патрулі і контрольні пункти [178]. На прикладі спільної операції під час великих державних свят такі заходи дозволяють забезпечити додатковий рівень безпеки.

Національна гвардія регулярно проводить спільні тренування з місцевими службами цивільного захисту [179]. Це включає симуляції різних надзвичайних ситуацій, таких як природні катастрофи, техногенні аварії та терористичні атаки.

Національна гвардія активно співпрацює з міжнародними організаціями, такими як Європейський Союз і НАТО, для підвищення рівня безпеки критичної інфраструктури [180]. Це включає обмін передовим досвідом, навчання за міжнародними програмами та участь у спільних навчаннях.

У рамках програми НАТО з управління кризовими ситуаціями Національна гвардія бере участь у міжнародних навчаннях, що дозволяє відпрацьовувати дії у випадках масштабних кризових ситуацій і отримувати досвід від партнерів [181].

Під час виконання міжнародних операцій з підтримання миру або в рамках міжнародних антитерористичних коаліцій Національна гвардія взаємодіє з іноземними військовими та безпековими службами [182]. Спільна робота з міжнародними партнерами дозволяє забезпечити високий рівень безпеки і стабільності в зонах конфлікту.

Висновки до розділу 2

Аналіз сучасних викликів та вразливостей життєво важливих систем України демонструє комплексний характер загроз для критичної інфраструктури. Кібернетичні виклики, технологічні та природні ризики, внутрішні загрози суспільного характеру та воєнно-стратегічні фактори створюють багаторівневу систему небезпек, що потребує інтегрованого підходу до захисту.

Кібернетична безпека залишається одним із найбільш динамічних напрямів загроз. Статистика свідчить про постійне зростання кількості кіберінцидентів: у 2022-2023 роках було зафіксовано 2194 кіберінциденти (з яких 1048 високого або критичного рівня), у 2024-2025 роках – 2554 інциденти (367 серйозних). Аналіз показує, що основними джерелами кіберзагроз для України є угруповання UAC-0050 та UAC-0010 (Armageddon), пов'язані з російськими спецслужбами.

Дослідження виявило широкий спектр методів кібератак: фішинг (включаючи смішинг, вішинг, кетфішинг), SQL-ін'єкції, XSS-атаки, використання аналізаторів протоколів, MITM-атаки, DoS/DDoS-атаки та спам-атаки. У 2024 році зафіксовано зростання шкідливих URL-адрес на 61%, що відповідає 255 млн фішингових атак. Близько третини глобального потоку шкідливих email-розсилок надходить з Росії, причому ці атаки часто спрямовані саме на українські організації та критичну інфраструктуру.

Аналіз технологічних та природних загроз виявив їх значний вплив на критичну інфраструктуру. Терористичні загрози включають мінування об'єктів, застосування вибухових пристроїв, хімічної зброї та збройне захоплення заручників. Природні катастрофи (метеорологічні, гідрологічні, геологічні та геліофізичні явища) також становлять серйозну небезпеку.

Історичний аналіз показав масштаб впливу природних катастроф на українську інфраструктуру: обледеніння листопада 2000 року пошкодило понад 20 тисяч ліній електропередач та 307 тисяч опор; снігопад січня 2014

року призвів до знеструмлення 1605 населених пунктів; паводок 2008 року пошкодив понад 500 мостів та 1660 км доріг. До 20% залізничних колій знаходяться під впливом підтоплення, 40% – у зонах карстових загроз, 11% – у зонах можливих зсувів.

Техногенні аварії (вибухи на промислових об'єктах, аварії на АЕС, хімічні розливи) потребують комплексного підходу до моніторингу, запобігання та реагування. Критично важливим є належне функціонування систем раннього попередження та моніторингу.

Дослідження виявило значний вплив соціально-економічних факторів на стан критичної інфраструктури. Економічні кризи 2008-2009 та 2014-2015 років продемонстрували руйнівний вплив на енергетичний, транспортний, комунальний сектори та охорону здоров'я через скорочення інвестицій, зниження якості обслуговування та закриття об'єктів.

Під час кризи 2022-2024 років ситуація значно загострилася. Транспортний сектор зазнав критичного зменшення капітальних інвестицій у ремонт доріг та модернізацію залізничної інфраструктури. Комунальні послуги постраждали від недостатнього фінансування водопостачання, водовідведення та теплопостачання. Система охорони здоров'я зіткнулася з дефіцитом фінансових і матеріальних ресурсів, що призвело до закриття медичних закладів у малих містах.

Соціальні протести також створюють загрози для критичної інфраструктури через фізичне пошкодження об'єктів (протести 2021-2022 років), блокування доступу до енергетичних об'єктів (протести 2023-2024 років) та порушення стабільності надання комунальних послуг.

Повномасштабне вторгнення Росії у 2022 році створило безпрецедентні виклики для критичної інфраструктури України. Масовані атаки на енергетичну інфраструктуру (жовтень-листопад 2022 року) призвели до знищення підстанцій і пошкодження Запорізької АЕС. Економічні втрати від пошкодження енергетичної інфраструктури у 2023 році перевищили 10 мільярдів доларів.

Соціальні наслідки воєнних дій виявилися особливо відчутними: зимовий період 2022-2023, 2024-2025 років характеризувався частими відключеннями електроенергії, проблемами в роботі медичних закладів через необхідність використання резервних генераторів, та труднощами в освітній сфері. Воєнні дії призвели до руйнування транспортних артерій, пошкодження комунальних об'єктів та руйнування медичних закладів.

Аналіз досвіду застосування сил Національної гвардії для забезпечення безпеки стратегічних об'єктів виявив ефективність комплексного підходу до організації охорони. Визначення критичних об'єктів та встановлення захисних заходів (фізичні бар'єри, системи контролю доступу, відеоспостереження) дозволило забезпечити належний рівень захисту енергетичних об'єктів, транспортних вузлів та об'єктів водопостачання.

Впровадження систем ситуаційного моніторингу та раннього попередження (включаючи відеоспостереження, БПЛА, датчики та аналітичні системи) підвищило ефективність виявлення загроз. Регулярні тренування та симуляції (навчання з евакуації, протидії атакам, реагування на критичні ситуації) значно покращили готовність підрозділів до надзвичайних ситуацій.

Інтеграція з іншими структурами показала свою ефективність: співпраця з правоохоронними органами дозволяє проводити спільні операції; взаємодія з місцевими адміністраціями забезпечує координацію дій; участь у програмах НАТО та ЄС сприяє обміну передовим досвідом та підвищенню рівня підготовки.

Проведений аналіз підтверджує необхідність комплексного підходу до захисту критичної інфраструктури, який має включати:

1. Постійне вдосконалення систем кібербезпеки та підвищення кваліфікації фахівців.
2. Розробку ефективних систем моніторингу та раннього попередження природних і техногенних загроз.
3. Забезпечення стабільного фінансування критичної інфраструктури навіть в умовах економічних криз.

4. Створення резервних систем та планів реагування на воєнно-стратегічні виклики.

5. Інтеграцію зусиль різних державних структур, приватного сектору та міжнародних партнерів.

Досвід України 2022-2024 років демонструє критичну важливість стійкості критичної інфраструктури для забезпечення національної безпеки, економічної стабільності та життєдіяльності населення в умовах збройної агресії. Це робить подальше вдосконалення організаційно-правового механізму захисту стратегічних об'єктів одним із найважливіших пріоритетів державної політики.

ВИСНОВКИ

Магістерська робота "Організаційно-правовий механізм захисту стратегічних об'єктів України" присвячена комплексному аналізу та науковому обґрунтуванню вдосконалення системи захисту критичної інфраструктури в контексті забезпечення національної безпеки. Виконання поставлених завдань дозволило отримати наступні результати:

1. Проаналізовано концепції критичної інфраструктури та її роль у забезпеченні національної безпеки.

Дослідження показало, що критична інфраструктура є основою функціонування сучасного суспільства та держави, охоплюючи енергетичні системи, транспортні вузли, системи водопостачання, комунікаційні мережі та інші життєво важливі об'єкти. Проаналізовано міжнародний досвід визначення критичної інфраструктури (США, Німеччина, Великобританія, Нідерланди) та запропоновано визначення для України, яке враховує як фізичні об'єкти, так і об'єкти в кіберпросторі.

Встановлено, що захист критичної інфраструктури стикається з численними проблемами, включаючи фізичні та кіберзагрози, терористичні атаки, саботаж і природні катастрофи. Аналіз подій 2022-2025 років підтвердив критичну важливість надійного захисту об'єктів для забезпечення життєдіяльності держави в умовах збройної агресії.

2. Досліджено типологію об'єктів критичної інфраструктури та визначено їх значення для стабільного функціонування суспільства.

Систематизовано основні види критичної інфраструктури: енергетична (електростанції, електромережі, газопроводи, нафтопроводи), транспортна (автомагістралі, залізниці, аеропорти, порти), інформаційна (Інтернет-провайдери, дата-центри, критичні інформаційні системи), системи водопостачання та водовідведення, медична та фінансова інфраструктура.

Обґрунтовано секторальний підхід до організації захисту критичної інфраструктури, який передбачає визначення 14 життєво важливих функцій і

послуг (від надання адміністративних послуг до наукових досліджень). Виявлено, що до 20% залізничних колій перебувають під впливом підтоплення, 40% – у зонах карстових загроз, 59% магістральних газопроводів – в умовах можливого прояву карсту, що підтверджує необхідність постійного моніторингу та технічного обслуговування.

3. Здійснено оцінку потенційних загроз для об'єктів критичної інфраструктури.

Комплексний аналіз виявив багаторівневу систему загроз:

Кібернетичні виклики: У 2022 році зафіксовано 2194 кіберінциденти (1048 високого рівня), у 2023 році – 2554 інциденти (367 серйозних). Основні методи атак включають фішинг (зростання шкідливих URL на 61%, 255 млн атак у 2023 році), SQL-ін'єкції, XSS-атаки, MITM-атаки, DDoS-атаки. Виявлено, що близько третини глобального потоку шкідливих розсилок надходить з Росії.

Природні катастрофи: Обледеніння 2000 року пошкодило понад 20 тисяч ліній електропередач; снігопад 2014 року знеструмив 1605 населених пунктів; паводок 2008 року пошкодив понад 500 мостів.

Терористичні загрози: Включають мінування об'єктів, застосування вибухових пристроїв, хімічної зброї, збройне захоплення заручників.

Воєнно-стратегічні виклики: З 2022 року зафіксовані масовані атаки на енергетичну інфраструктуру, що призвели до економічних втрат понад 10 млрд доларів у 2023 році.

4. Вивчено існуючі стратегії та методи захисту критичної інфраструктури.

Досліджено комплекс нормативно-правових, організаційних та технологічних інструментів захисту. Нормативно-правові інструменти визначають правила, стандарти та вимоги, встановлюють відповідальність за порушення. Організаційні заходи включають створення спеціалізованих центрів управління кризовими ситуаціями, розробку планів реагування на загрози.

Аналіз показав ефективність інтеграції фізичних і цифрових систем безпеки. Впровадження багатофакторної аутентифікації (MFA) підвищує рівень безпеки доступу до об'єктів. Використання автоматизованих систем контролю доступу (ACS) дозволяє ефективно управляти доступом до різних зон об'єкта, автоматично реєструвати дії користувачів та виявляти підозрілу активність.

5. Розглянуто технічні засоби захисту критичної інфраструктури.

Систематизовано сучасні технічні засоби захисту:

Системи кібербезпеки: Екранування вхідних даних, валідація і фільтрація, використання Content Security Policy (CSP), регулярне оновлення програмного забезпечення.

Інтелектуальні системи захисту: Відеоспостереження з високою роздільною здатністю, функціями нічного бачення та розпізнавання облич; безпілотні літальні апарати (БПЛА) для патрулювання великих територій; датчики та аналітичні системи для раннього виявлення загроз.

Системи фізичного захисту: Фізичні бар'єри (огорожі, блокпости, контрольно-пропускні пункти), системи контролю доступу з RFID-технологією та біометричними зчитувачами.

Виявлено, що регулярне технічне обслуговування і оновлення охоронних систем є критично важливим для підтримання їхньої надійності. Важливо вчасно проводити заміну застарілого обладнання, оновлювати програмне забезпечення та проводити технічний огляд систем.

6. Проаналізовано організаційні аспекти захисту критичної інфраструктури.

Дослідження показало критичну важливість організаційних заходів:

Розробка політик безпеки: Регулярний перегляд та оновлення політик доступу дозволяє адаптувати їх до змін у організаційній структурі та нових загроз. Виділення "червоної" зони з підвищеним рівнем контролю доступу дозволяє захистити найважливіші ділянки.

Навчання персоналу: Проведення регулярних тренувань та симуляцій для військовослужбовців і служб безпеки є необхідним для підготовки до надзвичайних ситуацій. Тренування включають навчання з евакуації, протидії атакам та реагування на критичні ситуації.

Планування кризових ситуацій: Розробка детальних планів реагування на різні типи загроз, включаючи природні катастрофи, техногенні аварії, терористичні атаки та кібератаки.

7. Досліджено стратегічні аспекти захисту критичної інфраструктури на національному та міжнародному рівнях.

Встановлено, що ефективна система захисту критичної інфраструктури базується на міжнародному співробітництві та обміні найкращими практиками. Національна гвардія України активно співпрацює з міжнародними організаціями (ЄС, НАТО), що включає обмін передовим досвідом, навчання за міжнародними програмами та участь у спільних навчаннях.

Співпраця з правоохоронними органами, місцевими адміністраціями та міжнародними партнерами є важливою складовою ефективного захисту. Обмін інформацією, спільні навчання та міжнародний досвід дозволяють покращити стратегії і тактики захисту, підвищити рівень безпеки та забезпечити комплексний підхід до охорони.

8. Розроблено рекомендації щодо вдосконалення системи захисту критичної інфраструктури.

На основі проведеного дослідження сформульовано наступні рекомендації:

1. Впровадження інтегрованої системи моніторингу, що поєднує фізичні та кіберзахисні компоненти.
2. Створення резервних систем та планів швидкого відновлення після атак або аварій.
3. Забезпечення стабільного фінансування критичної інфраструктури навіть в умовах економічних криз.

4. Посилення міжвідомчої координації між силовими структурами, місцевими органами влади та приватним сектором.

5. Регулярне проведення тренувань та симуляцій для відпрацювання дій в надзвичайних ситуаціях.

6. Розширення міжнародного співробітництва для обміну досвідом та впровадження передових практик.

Наукова новизна та практичне значення.

Наукова новизна дослідження полягає в комплексному обґрунтуванні організаційно-правового механізму захисту стратегічних об'єктів України в умовах воєнного стану, удосконаленні понятійно-категоріального апарату у сфері захисту критичної інфраструктури та визначенні ролі Національної гвардії України у системі захисту за умов особливого правового режиму.

Практичне значення результатів полягає в можливості їх використання органами державної влади при розробці нормативно-правових актів, командуванням Національної гвардії при плануванні заходів щодо забезпечення безпеки стратегічних об'єктів, а також у навчальному процесі вищих військових навчальних закладів.

Захист об'єктів критичної інфраструктури є комплексним і багатогранним процесом, що включає використання сучасних технологій, постійне удосконалення стратегій і тактик, а також інтеграцію зусиль різних структур. Національна безпека України залежить від здатності держави ефективно захищати стратегічно важливі об'єкти від різноманітних загроз.

Досвід України 2022-2025 років демонструє критичну важливість стійкості критичної інфраструктури для забезпечення життєдіяльності держави в умовах збройної агресії. Масовані атаки на енергетичну інфраструктуру, економічні втрати понад 10 мільярдів доларів, соціальні виклики – все це підтверджує необхідність подальшого вдосконалення організаційно-правового механізму захисту стратегічних об'єктів як одного з найважливіших пріоритетів державної політики.

Застосування передових технологій, регулярне навчання персоналу, постійний моніторинг та аналіз інцидентів, співпраця на всіх рівнях – від місцевих правоохоронних органів до міжнародних партнерів – дозволяє створити інтегровану і ефективну систему безпеки, яка відповідає сучасним викликам і загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

2. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15

3. Концепція створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р

4. Directive 2008/114/EC on the identification and designation of European critical infrastructures. Official Journal of the European Union. 2008. L 345/75.

5. Рекомендації парламентських слухань на тему «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» : Постанова Верховної Ради України від 31 березня 2016 року № 1073-VIII.

6. Стратегія національної безпеки України «Україна у світі, що змінюється» : Указ Президента України від 12 лютого 2007 року № 105/2007. URL: https://zakon.rada.gov.ua/laws/show/105/2007

7. Стратегія національної безпеки України : Указ Президента України від 26 травня 2015 року № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015

8. Про рішення Ради національної безпеки і оборони України від 28 лютого 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» : Указ Президента України від 02 березня 2014 року № 189/2014.

9. NATO's approach to protecting critical infrastructure. NATO Review. 2021. URL: https://www.nato.int/cps/en/natohq/topics_49158.htm

10. Critical Infrastructure Protection in the EU. European Commission. 2022. URL: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

11. Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine. 2001. Vol. 21, No. 6. P. 11-25.

12. Critical Infrastructure Security and Resilience. U.S. Department of Homeland Security. 2023. URL: https://www.dhs.gov/topic/critical-infrastructure-security

13. National Strategy for Critical Infrastructure Protection (CIP Strategy). German Federal Ministry of the Interior. 2009.

14. National Security Strategy and Strategic Defence and Security Review 2015. UK Government. London: HM Government, 2015. 96 p.

15. National Security Strategy of the Netherlands. Ministry of the Interior and Kingdom Relations. The Hague, 2019.

16. Lewis T. G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. 2nd ed. Hoboken: John Wiley & Sons, 2014. 528 p.

17. Moteff J., Parfomak P. Critical Infrastructure and Key Assets: Definition and Identification. Congressional Research Service Report for Congress. 2004. RL32631.

18. Білоус Р. А. Критична інфраструктура як об'єкт національної безпеки України. Стратегічні пріоритети. 2018. № 1 (46). С. 71-78.

19. Дубов Д. В., Ожеван М. А., Гнатюк С. Л. Інформаційна безпека в умовах трансформації суспільства: методологія дослідження та забезпечення. Київ: НІСД, 2017. 252 с.

20. Sukhodolia O., Kharazishvili Y., Bobro D. Developing a Corporate Model for Energy Security Management of an Enterprise. Eastern-European Journal of Enterprise Technologies. 2017. Vol. 5, No. 3 (89). P. 4-13.

21. Бєлов О. М. Організаційно-правові засади захисту критичної інфраструктури України : дис. ... канд. юрид. наук : 12.00.07. Київ, 2019. 228 с.

22. Про затвердження Порядку формування переліку об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943.

23. Horton K. S., Koelm D. M., Lewis J. A. Toward a New Framework for Public-Private Partnership in Critical Infrastructure Security. Center for Strategic and International Studies. 2017.

24. Assaf D. Models of Critical Information Infrastructure Protection. International Journal of Critical Infrastructure Protection. 2008. Vol. 1. P. 6-14.

25. Brown G., Carlyle M., Salmerón J., Wood K. Defending Critical Infrastructure. Interfaces. 2006. Vol. 36, No. 6. P. 530-544.

26. Resilience of Critical Infrastructure Systems: Emerging Developments and Future Challenges / ed. by K. Gopalakrishnan, S. Peeta. Boca Raton: CRC Press, 2010. 306 p.

27. Kröger W., Zio E. Vulnerable Systems. London: Springer-Verlag, 2011. 210 p.

28. Ezell B. C. Infrastructure Vulnerability Assessment Model (I-VAM). Risk Analysis. 2007. Vol. 27, No. 3. P. 571-583.

29. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety. 2014. Vol. 121. P. 43-60.

30. Сіцінська М. В., Онищенко В. О. Кібербезпека критичної інфраструктури: міжнародний досвід та виклики для України. Інформація і право. 2019. № 2 (29). С. 82-90.

31. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19 червня 2021 р. № 518.

32. Pederson P., Dudenhoeffer D., Hartley S., Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Idaho National Laboratory. 2006.

33. Gheorghe A. V., Masera M., Weijnen M., De Vries L. Critical Infrastructures at Risk: Securing the European Electric Power System. Topics in Safety, Risk, Reliability and Quality. Vol. 9. Springer, 2006. 258 p.

34. 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 333/164.

35. Білоус Р. А. Модель державного управління системою захисту критичної інфраструктури в Україні. Державне управління: удосконалення та розвиток. 2019. № 5. URL: http://www.dy.nayka.com.ua/?op=1&z=1431

36. Про об'єкти підвищеної небезпеки : Закон України від 18 січня 2001 року № 2245-III. URL: https://zakon.rada.gov.ua/laws/show/2245-14

37. Про Національну гвардію України : Закон України від 13 березня 2014 року № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18

38. Бобро Д. Г., Семенченко А. І., Чубарук Т. В. Ідентифікація критичної інфраструктури держави: сутність, проблеми та перспективи. Стратегічні пріоритети. 2017. № 4 (45). С. 138-149.

39. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144. 2011.

40. Енергетична безпека в контексті національної безпеки України / за ред. О. О. Суходолі. Київ: НІСД, 2014. 52 с.

41. Сухий П. О. Вітроенергетика в енергетичному балансі України. Відновлювана енергетика. 2020. № 2. С. 6-14.

42. Renewable Energy Policy Network for the 21st Century. Renewables 2021 Global Status Report. Paris: REN21 Secretariat, 2021.

43. Про ринок електричної енергії : Закон України від 13 квітня 2017 року № 2019-VIII. URL: https://zakon.rada.gov.ua/laws/show/2019-19

44. Ten C.-W., Manimaran G., Liu C.-C. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man, and Cybernetics. 2010. Vol. 40, No. 4. P. 853-865.

45. Про транспортування природного газу : Закон України від 30 вересня 2019 року № 142-IX. URL: https://zakon.rada.gov.ua/laws/show/142-20

46. Ілляш О. І., Ковальчук С. В., Хобта В. М. Економіка і організація нафтогазової промисловості. Івано-Франківськ: ІФНТУНГ, 2016. 711 с.

47. Про автомобільні дороги : Закон України від 8 вересня 2005 року № 2862-IV. URL: https://zakon.rada.gov.ua/laws/show/2862-15

48. Про залізничний транспорт : Закон України від 4 липня 1996 року № 273/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/273/96-вр

49. Про затвердження Авіаційних правил України «Правила повітряних перевезень та обслуговування пасажирів і багажу» : наказ Міністерства інфраструктури України від 30 листопада 2012 року № 735.

50. Про морські порти України : Закон України від 17 травня 2012 року № 4709-VI. URL: https://zakon.rada.gov.ua/laws/show/4709-17

51. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15

52. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

53. Akhmetov B. B., Lakhno V. A., Malyukov V. P., Zhumadilova Zh. Sh. The Choice of Protection Strategies during the Bimatrix Games Discrete Approximation. Journal of Theoretical and Applied Information Technology. 2017. Vol. 95, No. 2. P. 324-337.

54. Про питну воду, питне водопостачання та водовідведення : Закон України від 18 травня 2017 року № 2047-VIII. URL: https://zakon.rada.gov.ua/laws/show/2047-19

55. Про банки і банківську діяльність : Закон України від 7 грудня 2000 року № 2121-III. URL: https://zakon.rada.gov.ua/laws/show/2121-14

56. Про Державну службу надзвичайних ситуацій : Закон України від 16 грудня 2014 року № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17

57. Основи законодавства України про охорону здоров'я : Закон України від 19 листопада 1992 року № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12

58. Про боротьбу з тероризмом : Закон України від 20 березня 2003 року № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15

59. Кримінальний кодекс України : Закон України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

60. Баранов О. А. Інформаційна безпека: основні категорії. Інформація і право. 2016. № 2 (17). С. 54-62.

61. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

62. Петров В. В., Лахно В. А. Інформаційні технології в системі національної безпеки. Київ: КНТ, 2018. 312 с.

63. Гнатюк С. Л. Кібербезпека держави: аспекти забезпечення. Київ: ІПММС НАН України, 2019. 280 с.

64. Концепція боротьби з тероризмом в Україні : Указ Президента України від 5 березня 2019 року № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019

65. Звіт Державної служби спеціального зв'язку та захисту інформації України за 2023 рік. URL: https://cip.gov.ua/ua/news

66. Звіт CERT-UA за І квартал 2024 року. URL: https://cert.gov.ua/

67. Корченко О. Г., Казмірчук С. В. Основи побудови систем захисту інформації. Київ: НТУУ "КПІ", 2017. 336 с.

68. Міжнародний стандарт ISO/IEC 27001:2013. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

69. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. Indianapolis: John Wiley & Sons, 2015. 784 p.

70. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2002. 368 p.

71. Anti-Phishing Working Group. Phishing Activity Trends Report, 2005. URL: https://www.apwg.org

72. Anti-Phishing Working Group. Phishing Activity Trends Report, 2016. URL: https://www.apwg.org

73. Грайворонський М. В. Смішинг як новий вид кіберзлочинності. Інформаційна безпека. 2020. № 3. С. 45-52.

74. Бутузов В. М. Вішинг: методи протидії телефонному шахрайству. Кібербезпека в Україні. 2019. № 2. С. 78-85.

75. Whitty M. T., Buchanan T. The Online Romance Scam: A Serious Cybercrime. Cyberpsychology, Behavior, and Social Networking. 2012. Vol. 15, No. 3. P. 181-183.

76. Jiang M., Fu K. Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit? Policy & Internet. 2018. Vol. 10, Issue 4. P. 372-392.

77. Cybersecurity Ventures. 2024 Cybercrime Report. URL: https://cybersecurityventures.com

78. Звіт Національного координаційного центру кібербезпеки при РНБО України за 2023 рік.

79. Clarke J. SQL Injection Attacks and Defense. 2nd ed. Syngress, 2012. 752 p.

80. OWASP Foundation. SQL Injection Prevention Cheat Sheet. 2023. URL: https://cheatsheetseries.owasp.org

81. OWASP Foundation. Cross Site Scripting (XSS) Prevention Cheat Sheet. 2023. URL: https://cheatsheetseries.owasp.org

82. Stuttard D., Pinto M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2nd ed. Wiley, 2011. 912 p.

83. Sanders C. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. 3rd ed. No Starch Press, 2017. 368 p.

84. Callegati F., Cerroni W., Ramilli M. Man-in-the-Middle Attack to the HTTPS Protocol. IEEE Security & Privacy. 2009. Vol. 7, No. 1. P. 78-81.

85. Zargar S. T., Joshi J., Tipper D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials. 2013. Vol. 15, No. 4. P. 2046-2069.

86. Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review. 2004. Vol. 34, No. 2. P. 39-53.

87. Douligeris C., Mitrokotsa A. DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. Computer Networks. 2004. Vol. 44, Issue 5. P. 643-666.

88. GitHub Engineering Blog. February 28th DDoS Incident Report. 2018. URL: https://github.blog

89. Звіт Національного банку України про кібератаки на банківську систему. 2016.

90. Spamlaws. The History of Email Spam. URL: https://www.spamlaws.com/spam-stats.html

91. Moteff J. D. Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service. 2012.

92. Willis H. H., Morral A. R., Kelly T. K., Medby J. J. Estimating Terrorism Risk. RAND Corporation, 2005.

93. Jenkins B. M. Protecting Public Surface Transportation Against Terrorism and Serious Crime. Mineta Transportation Institute, 2001.

94. Baruch E., Baruch Y. Hostage Taking: Prevention and Response. Terrorism and Political Violence. 1992. Vol. 4, No. 4. P. 127-146.

95. McMains M. J., Mullins W. C. Crisis Negotiations: Managing Critical Incidents and Hostage Situations in Law Enforcement and Corrections. 5th ed. Routledge, 2014.

96. Alexander D. Natural Disasters. Routledge, 2018. 994 p.

97. Державна служба України з надзвичайних ситуацій. Класифікація надзвичайних ситуацій. URL: https://www.dsns.gov.ua

98. Національна доповідь про стан техногенної та природної безпеки в Україні у 2000 році. Київ: МНС України, 2001.

99. Національна доповідь про стан техногенної та природної безпеки в Україні у 2014 році. Київ: ДСНС України, 2015.

100. Національна доповідь про стан техногенної та природної безпеки в Україні у 2008 році. Київ: МНС України, 2009.

101. Рудько Г. І., Назаренко М. В. Небезпечні геологічні процеси та їх вплив на критичну інфраструктуру України. Мінеральні ресурси України. 2018. № 2. С. 38-44.

102. Perrow C. Normal Accidents: Living with High-Risk Technologies. Princeton University Press, 1999. 464 p.

103. Mannan S. Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control. 4th ed. Butterworth-Heinemann, 2012. 3776 p.

104. IAEA Safety Standards. Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1 (Rev. 1). Vienna: IAEA, 2016.

105. Crowl D. A., Louvar J. F. Chemical Process Safety: Fundamentals with Applications. 3rd ed. Prentice Hall, 2011. 720 p.

106. Aven T. Risk Assessment and Risk Management: Review of Recent Advances on their Foundation. European Journal of Operational Research. 2016. Vol. 253, Issue 1. P. 1-13.

107. Zimmerman R. Social Implications of Infrastructure Network Interactions. Journal of Urban Technology. 2001. Vol. 8, No. 3. P. 97-119.

108. National Infrastructure Advisory Council. Critical Infrastructure Resilience. Final Report and Recommendations. 2009.

109. Little R. G. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. Journal of Urban Technology. 2002. Vol. 9, No. 1. P. 109-123.

110. Про електроенергетику : Закон України від 16 жовтня 1997 року № 575/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/575/97-вр

111. Міністерство енергетики України. Звіт про функціонування ринку електричної енергії за 2023 рік.

112. Національний банк України. Звіт про фінансову стабільність. Грудень 2009 року.

113. Національний банк України. Звіт про фінансову стабільність. Грудень 2015 року.

114. Garcia-Herrero A., Vázquez F. J. International Diversification Gains and Home Bias in Banking. IMF Working Paper WP/08/281. 2008.

115. Arghyrou M. G., Tsoukalas J. D. The Greek Debt Crisis: Likely Causes, Mechanics and Outcomes. The World Economy. 2011. Vol. 34, Issue 2. P. 173-191.

116. Державна служба статистики України. Транспорт і зв'язок України. Статистичний збірник. 2023.

117. Міністерство інфраструктури України. Звіт про стан транспортної інфраструктури за 2023 рік.

118. Про автомобільні дороги : Закон України від 8 вересня 2005 року № 2862-IV. URL: https://zakon.rada.gov.ua/laws/show/2862-15

119. ПАТ «Українська залізниця». Річний звіт за 2023 рік.

120. Державна авіаційна служба України. Звіт про стан авіаційної галузі за 2023 рік.

121. Асоціація міст України. Звіт про стан комунального господарства в умовах війни. 2023.

122. Про питну воду, питне водопостачання та водовідведення : Закон України від 18 травня 2017 року № 2047-VIII. URL: https://zakon.rada.gov.ua/laws/show/2047-19

123. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг. Звіт за 2023 рік.

124. Про теплопостачання : Закон України від 2 червня 2005 року № 2633-IV. URL: https://zakon.rada.gov.ua/laws/show/2633-15

125. Міністерство розвитку громад та територій України. Моніторинг стану комунального господарства. 2024.

126. Міністерство охорони здоров'я України. Аналітично-статистичний довідник за 2023 рік.

127. Основи законодавства України про охорону здоров'я : Закон України від 19 листопада 1992 року № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12

128. Всесвітня організація охорони здоров'я. Україна: огляд системи охорони здоров'я. 2024.

129. Лехан В. М., Слабкий Г. О., Шевченко М. В. Аналіз реформування системи охорони здоров'я в Україні. Україна. Здоров'я нації. 2018. № 4. С. 187-195.

130. Della Porta D., Reiter H. Policing Protest: The Control of Mass Demonstrations in Western Democracies. University of Minnesota Press, 1998.

131. Звіт Міністерства внутрішніх справ України про забезпечення громадського порядку під час масових заходів. 2021.

132. Звіт ОБСЄ щодо ситуації на сході України. 2022.

133. Tarrow S. Power in Movement: Social Movements and Contentious Politics. 3rd ed. Cambridge University Press, 2011.

134. Звіт Одеської обласної державної адміністрації про стан критичної інфраструктури. 2023.

135. Міністерство енергетики України. Оперативна інформація про стан енергосистеми. 2024.

136. Tilly C., Tarrow S. Contentious Politics. 2nd ed. Oxford University Press, 2015.

137. Міністерство розвитку громад та територій України. Вплив соціальних протестів на комунальне господарство. Аналітична записка. 2023.

138. Office of the President of Ukraine. Russia's War Against Ukraine: Timeline and Key Events. 2024.

139. Міністерство енергетики України. Звіт про пошкодження енергетичної інфраструктури внаслідок військової агресії РФ. 2024.

140. Київська міська державна адміністрація. Хроніка подій жовтня 2022 року.

141. Міжнародне агентство з атомної енергії (МАГАТЕ). Звіт щодо безпеки Запорізької АЕС. 2022.

142. Національний банк України. Макроекономічний та монетарний огляд. Лютий 2024 року.

143. Kyiv School of Economics. Оцінка збитків енергетичної інфраструктури України. 2023.

144. UNICEF Ukraine. Humanitarian Situation Report. December 2023.

145. Міністерство енергетики України. Графіки відключень електроенергії. Зима 2022-2023.

146. Міністерство охорони здоров'я України. Забезпечення функціонування медичних закладів в умовах енергодефіциту. 2023.

147. Міністерство освіти і науки України. Організація освітнього процесу в умовах воєнного стану. 2023.

148. Kaldor M. New and Old Wars: Organized Violence in a Global Era. 3rd ed. Stanford University Press, 2012.

149. Byman D., Waxman M. The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might. Cambridge University Press, 2002.

150. Звіт Координаційного центру з надання правової допомоги. Порушення міжнародного гуманітарного права на Донбасі. 2023.

151. Міністерство енергетики України. Забезпечення паливом енергогенеруючих підприємств в умовах війни. 2023.

152. Міністерство інфраструктури України. Відновлення транспортної інфраструктури. Звіт за 2023 рік.

153. Укравтодор. Огляд стану автомобільних доріг у зонах активних бойових дій. 2024.

154. Звіт Державної служби України з надзвичайних ситуацій. Пошкодження об'єктів комунального господарства. 2024.

155. Міністерство розвитку громад та територій України. Відновлення комунальної інфраструктури. 2024.

156. Всесвітня організація охорони здоров'я. Attacks on Health Care in Ukraine. 2024.

157. Міністерство охорони здоров'я України. Логістика медичного постачання в умовах війни. 2023.

158. Про Національну гвардію України : Закон України від 13 березня 2014 року № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18

159. Національна гвардія України. Звіт про виконання завдань у 2023 році.

160. Про правовий режим воєнного стану : Закон України від 12 травня 2015 року № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19

161. Київська міська військова адміністрація. Охорона критичної інфраструктури столиці. 2023.

162. Національна гвардія України. Методичні рекомендації з організації охорони об'єктів критичної інфраструктури. 2022.

163. NATO. Protection of Critical Infrastructure. ACT Policy. 2021.

164. European Commission. Critical Infrastructure Warning Information Network (CIWIN). Guidelines. 2019.

165. Система державного моніторингу надзвичайних ситуацій. Технічний регламент. 2021.

166. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.

167. Про використання безпілотних авіаційних систем в охоронній діяльності : наказ МВС України від 10 липня 2018 року № 594.

168. Національна система раннього попередження про загрозу або виникнення надзвичайних ситуацій. Положення. 2019.

169. Корченко О. Г. Системи раннього попередження кіберзагроз. Київ: ІПММС НАН України, 2021.

170. Національна академія Національної гвардії України. Програма професійної підготовки особового складу. 2023.

171. ДСТУ ISO 23601:2019. Безпека. Евакуація та евакуаційні плани.

172. NATO. Protection of Critical Infrastructure Against Terrorist Attacks. Handbook. 2020.

173. Національна гвардія України. Стандарти реагування на надзвичайні ситуації. 2022.

174. Київводоканал. План дій в надзвичайних ситуаціях. 2023.

175. Укроборонпром. Система безпеки підприємств оборонної промисловості. 2022.

176. Державна інспекція ядерного регулювання України. Вимоги до планів аварійного реагування на АЕС. 2021.

177. Про взаємодію правоохоронних органів у сфері протидії тероризму : постанова Кабінету Міністрів України від 10 квітня 2014 року № 92.

178. МВС України. Координація дій правоохоронних органів під час особливого правового режиму. 2023.

179. ДСНС України. Міжвідомча взаємодія при ліквідації наслідків надзвичайних ситуацій. 2022.

180. NATO-Ukraine Commission. Annual Report 2023.

181. NATO Partnership for Peace Programme. Crisis Management Exercises in Ukraine. 2023.

182. Міністерство оборони України. Участь України у міжнародних операціях з підтримання миру. 2023.