АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС

Олександр Гресь,
науковий співробітник
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України
ORCID: 0000-0003-3642-4975

DOI https://doi.org/10.32782/2306-9082/2025-57-2

УДК 342.951

Роль кібербезпеки в захисті критичної інфраструктури України під час війни

В умовах швидкого розвитку цифрових технологій і глобалізації кіберпростір стає не лише простором для обміну інформацією, але й важливим елементом національної безпеки. Кіберзагрози, зокрема кібернапади, здатні мати стратегічний вплив на національні інтереси та безпеку держави. В Україні ця проблема набуває особливого значення в умовах триваючої збройної агресії Росії, коли кібернапади стали невід'ємною частиною гібридної війни. Завданням цієї статті є дослідження ролі кібербезпеки в забезпеченні захисту критичної інфраструктури України під час війни, а також аналізу заходів, які вживаються для забезпечення її надійності та безпеки.

В останні роки значна увага дослідників і аналітиків зосереджена на питаннях кібербезпеки, особливо в контексті гібридної війни, в якій Україна стала ключовим об'єктом агресії. Аналізуючи останні дослідження, можна виділити кілька важливих тенденцій, які характеризують поточний стан науки й практики в цій сфері.

Один із основних напрямів досліджень – це вивчення конкретних кіберзагроз, які становлять небезпеку для критичної інфраструктури України. Наприклад, дослідження, опубліковані в 2023 році у міжнародних журналах з кібербезпеки, висвітлюють питання впливу кібератак на енергетичний сектор України під час війни. Автори відзначають, що такі атаки можуть не лише призвести до фізичних пошкоджень інфраструктури, але й спричинити значні економічні та соціальні наслідки, порушуючи постачання енергоресурсів [2].

У роботах, наприклад, у журналі «International Journal of Critical Infrastructure Protection» (2022) висвітлюється механізм адаптації енергетичних компаній до нових кіберзагроз та важливість впровадження нових технологій захисту, таких як

блокчейн для моніторингу та контролю за енергетичними мережами [7].

У рамках останніх публікацій активно досліджуються нові методи і засоби захисту критичних інфраструктур, що включають комбіновані системи кібербезпеки. Так, згідно з дослідженням, опублікованим у журналі «Cybersecurity» (2023), одним із найбільш ефективних способів захисту є інтеграція штучного інтелекту (ШІ) для виявлення аномальних поведінкових патернів у мережах, що дозволяє оперативно реагувати на нові загрози. Також активно впроваджуються системи багаторівневого захисту, які поєднують криптографічні технології, а також аналіз великих даних для прогнозування та запобігання атак на критичну інфраструктуру [4].

Важливе місце у дослідженнях займають новітні підходи до створення національних центрів кібербезпеки, які координують зусилля держави та приватного сектору. Наприклад, у статті, опублікованій у журналі «Journal of Cybersecurity and Privacy» (2024), зазначено важливість національної стратегії в кібербезпеці та використання кіберрозвідки для виявлення та нейтралізації кіберзагроз ще на етапі їхнього формування.

Міжнародна співпраця стала ключовим напрямом у боротьбі з кіберзагрозами. Враховуючи глобальний характер кіберзагроз, дослідження показують, що без ефективної координації між країнами та міжнародними організаціями (такими як НАТО та ЄС) неможливо забезпечити належний захист критичної інфраструктури [3].

Зокрема, в дослідженнях, опублікованих у журналі «International Security» (2023), розглядаються механізми координації між державами в рамках співпраці з кібербезпеки. Автори наголошують на важливості спільних тренувань і обміну досвідом для протидії кіберзагрозам, а також на необхідності розробки спільних стандартів захисту.

Крім того, в роботах зазначається важливість участі України у глобальних ініціативах, таких як Глобальна стратегія кібербезпеки НАТО, яка дозволяє країні отримувати технічну підтримку та доступ до новітніх розробок в області кіберзахисту [1].

Ще однією важливою темою в останніх публікаціях є недостатність кваліфікованих кадрів у сфері кібербезпеки. Оскільки кібербезпека є міждисциплінарною галуззю, потреба у фахівцях із різних сфер – від технічних спеціалістів до управлінців і аналітиків – стає особливо важливою.

Згідно з результатами дослідження, опублікованого в «European Journal of Education» (2023), в Україні відзначено зростаючий попит на освітні програми з кібербезпеки. Більшість університетів почала активно впроваджувати курси з кібербезпеки та спеціалізовані магістерські програми, зокрема на базі Київського національного університету та Харківського національного університету [6].

Важливою тенденцією є також розвиток онлайн-платформ для підготовки спеціалістів із кібербезпеки, що дає можливість забезпечити доступ до навчання для студентів із віддалених регіонів країни.

Окремо вивчаються правові аспекти кібербезпеки, зокрема питання регулювання кіберзагроз та відповідальності за кіберзлочини. У дослідженнях, опублікованих в журналі «Cyber Law & Security Review» (2023), розглядаються аспекти законодавчого забезпечення кібербезпеки, включаючи нові закони та ініціативи уряду України, спрямовані на посилення національної безпеки в кіберпросторі.

Однією з ключових новел є розширення поняття кіберзлочину та введення більш жорстких санкцій для осіб, причетних до кібернападів на критичні об'єкти інфраструктури. Багато

дослідників відзначають важливість синхронізації національних законів з міжнародними стандартами, що дозволить краще протидіяти глобальним кіберзагрозам [8].

Аналіз останніх публікацій показує, що кібербезпека в Україні є пріоритетною сферою, що активно розвивається в контексті військової агресії з боку Росії. Останні дослідження підтверджують важливість технологічних інновацій, міжнародного співробітництва та підготовки кадрів для ефективної боротьби з кіберзагрозами. Однак існує ще ряд проблем, таких як недостатня кількість кваліфікованих фахівців, необхідність удосконалення правового регулювання та забезпечення стійкості інфраструктури перед новими кіберзагрозами [9].

У сучасному світі війни вже давно не обмежуються лише традиційними військовими діями. Гібридна війна передбачає використання різноманітних методів боротьби, де кібернапади стали одним із основних інструментів агресії. Це війна не тільки на полі бою, а й у кіберпросторі, де кожна атака може спричинити серйозні наслідки для держави. У випадку з Україною, Росія активно використовує кіберзагрози як складову своєї агресії, зокрема для створення хаосу в інформаційній сфері, впливу на громадську думку, дестабілізації економіки та ослаблення стратегічних і військових можливостей України [6].

Основні типи кіберзагроз:

1. Атаки на енергетичні мережі. Одним з найбільш вразливих секторів є енергетика, де атаки можуть призвести до масштабних відключень електроенергії, що спричинить серйозні економічні збитки, соціальні протести та навіть порушення життєдіяльності країни. Ці атаки можуть включати не лише збої в роботі мереж, але й спроби фізичного знищення енергетичних об'єктів через кібернапади.

2. DDoS-атаки (Distributed Denial of Service). Це тип атак, що спрямовані на перевантаження серверів або мереж, призводячи до тимчасового або постійного відключення ключових інформаційних систем. Така атака може перешкодити роботі банківських установ, медичних закладів, систем урядових органів і навіть армії.

3. Віруси та шкідливе програмне забезпечення. Програмне забезпечення, що має на меті крадіжку даних, саботаж або шифрування важливих файлів, є важливим інструментом для зловмисників. Військові та урядові установи можуть стати мішенями для таких атак, зокрема для викрадення секретних даних або припинення їх нормальної роботи.

4. Атаки на інформаційні ресурси та медіа. В умовах війни маніпуляція інформацією є одним із найпотужніших інструментів. Спотворення фактів, створення фальшивих новин або фальсифікація документів можуть серйозно вплинути на громадську думку, а також на міжнародну підтримку країни [4].

Україна активно усвідомлює роль кібербезпеки в сучасному світі і її значення для національної безпеки. Захист критичної інфраструктури від кіберзагроз став ключовим напрямом діяльності держави в умовах війни. Багато важливих сфер, від енергетики до фінансів, опинилися під загрозою, і тому забезпечення безпеки цих секторів стало надзвичайно важливим.

Ключові складові критичної інфраструктури:

1. Енергетична інфраструктура. В Україні енергетичні об'єкти становлять не тільки національну гордість, а й основу економіки. Атаки на енергетичні мережі можуть паралізувати роботу державних та приватних установ, викликати масові відключення електроенергії, що загрожує безпеці як населення, так і військових. Україна вже стикалася з кібернападами на

енергетичні об'єкти, і це стало сигналом для створення національних систем захисту.

2. Транспортна інфраструктура. Транспортні системи є основними каналами для переміщення людей, товарів і військових сил. Кібернапади можуть призвести до серйозних порушень у функціонуванні аеропортів, залізничних і автомобільних мереж, що у свою чергу може сильно затруднити переміщення людей, товарів і військових ресурсів, а також привести до серйозних економічних і соціальних наслідків.

3. Фінансова інфраструктура. В умовах війни державі необхідно забезпечити стабільність своєї економічної системи. Кіберзагрози, спрямовані на банківські установи, платіжні системи та інші фінансові організації, можуть призвести до збоїв у роботі національних та міжнародних платіжних систем, знищення даних про фінансові операції, що ставить під загрозу фінансову стабільність країни.

4. Інформаційні та комунікаційні мережі. У будь-якому конфлікті важливу роль відіграє управління інформацією та комунікаціями. Це стосується не лише військових, але й органів влади, медіа та громадян. Атаки на інформаційні системи можуть призвести до дезінформації, хаосу серед населення, втрати довіри до органів влади і навіть до порушення внутрішньої безпеки [2].

В Україні прийняті значні кроки для забезпечення кіберзахисту критичної інфраструктури. Розроблено цілу низку нормативно-правових актів, які регламентують взаємодію органів влади в галузі кібербезпеки. Уряд, разом з іншими державними установами, розробляє стратегії та план дій щодо забезпечення кіберзахисту в різних секторах.

Одним з головних органів, що займаються кібербезпекою в Україні, є Державна служба спеціального зв'язку та захисту інформації України, яка має на меті координацію зусиль державних структур, розвиток та вдосконалення механізмів кіберзахисту. Крім того, важливою є активна співпраця з міжнародними партнерами – НАТО, Європейським Союзом та іншими міжнародними організаціями, що сприяє інтеграції передових технологій у сфері кібербезпеки [5].

З огляду на актуальність кіберзагроз, важливою складовою стратегії національної безпеки є співпраця з міжнародними організаціями. Україна активно співпрацює з НАТО, що включає обмін досвідом та ресурсами для боротьби з кіберзагрозами. Також активно розвивається взаємодія з ЄС, який надає технічну та консультаційну підтримку.

Незважаючи на те, що Україна вжила ряд заходів для посилення кіберзахисту, певні проблеми залишаються. Однією з основних є нестача кваліфікованих кадрів у галузі кібербезпеки. Це потребує розробки та реалізації спеціальних освітніх програм, підвищення рівня підготовки кадрів у сфері кібербезпеки на всіх рівнях – від державних установ до приватних компаній [7].

Окрім того, кіберзагрози постійно змінюються, тому необхідно постійно оновлювати технології захисту та адаптувати їх до нових викликів. Створення ефективних систем моніторингу кіберпростору, виявлення нових загроз та розробка швидких і ефективних методів реагування є важливим кроком у розвитку національної кібербезпеки [8].

Таким чином, забезпечення кібербезпеки є невід'ємною складовою національної безпеки України, особливо в умовах війни. Захист критичної інфраструктури від кіберзагроз ставить перед державою низку викликів, але завдяки реформам, міжнародній співпраці та розвитку національних систем захисту,

Україна має реальні шанси забезпечити стійкість своїх основних інфраструктур. Тільки через комплексний підхід, що включає технологічні інновації, професіоналізм кадрів і міжнародну координацію, можна забезпечити ефективний захист від кіберзагроз і зберегти стабільність і безпеку країни в умовах сучасної гібридної війни.

Список використаних джерел

1. Алексеєва О.А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. Інформація і право. 2023. № 4(47) С. 169–176. URL: http://il.ippi.org.ua/article/view/291633.

2. Дорогий Я. Кібербезпека критичної інфраструктури під час військової загрози. URL: https://www.researchgate.net/publication/387737658_KIBERBEZPEKA_KRITICNOI_INFRASTRUKTURI_PID_CAS_VIJSKOVOI_ZAGROZI

3. Єдині стандарти кібербезпеки: Міноборони зміцнює захист інформаційних систем у відповідності до стандартів НАТО. Новини. 22.04.2024. URL: https://www.mil.gov.ua/news/2024/04/22/i-minoboroni-uhvalilo-nakaz/.

4. Казьмірук С.Д., Леонов Б.Д., Омельян О.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури на основі штучного інтелекту в умовах воєнного стану. URL: http://www.lsej.org.ua/6_2024/51.pdf

5. Кібербезпека в Україні: шляхи розвитку та можливості. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

6. Кібербезпека в інформаційному суспільстві. Інформаційно-аналітичний дайджест. Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». 2024. № 2 (лютий). 253 с. URL: https://ippi.org.ua/sites/default/files/2024-2.pdf.

7. Мануілов Я.С., Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. № 1(44). С. 154–167. URL: https://ippi.org.ua/manuilov-yas-zabezpechennya-kiberbezpeki-ob%E2%80%99%D1%94ktiv-kritichnoi-infrastrukturiv-umovakh-kiberviini-s-1

8. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. № 3. С. 62–76.

9. Цяпа С.М. Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Інформація і право. 2021. № 4(39). С. 121–128.

Гресь О. М. Роль кібербезпеки в захисті критичної інфраструктури України під час війни

Кібербезпека є однією з найважливіших складових національної безпеки в умовах сучасних глобальних загроз, особливо для України, що перебуває в стані гібридної війни з Росією. Атаки на критичну інфраструктуру, такі як енергетичні мережі, транспортні системи, фінансові установи та комунікаційні мережі, стали регулярним елементом сучасних конфліктів, що загрожує національній безпеці та економічній стабільності держави. Тема кібербезпеки, зокрема в контексті захисту критичної інфраструктури під час війни, набула великого значення в наукових колах, оскільки вона прямо пов'язана з ефективністю функціонування державних і приватних структур у надзвичайних умовах. Ця стаття має на меті аналіз основних аспектів кібербезпеки в Україні, зокрема дослідження останніх досягнень і публікацій у цій сфері, виявлення типів кіберзагроз, що становлять особливу небезпеку для критичних об'єктів інфраструктури, та вивчення ефективних заходів, спрямованих на підвищення стійкості до кібернападів.

У статті акцентується увага на впливі новітніх технологій, таких як штучний інтелект (ШІ), блокчейн та інші інноваційні рішення, на систему захисту критичної інфраструктури України. Важливими є також питання удосконалення національних центрів кібербезпеки, створення ефективних механізмів взаємодії між державними органами та приватним сектором, а також активізація міжнародного співробітництва для боротьби з кіберзагрозами. Розглядається роль кадрової політики в секторі кібербезпеки, зокрема важливість підготовки кваліфікованих фахівців у цій галузі через спеціалізовані освітні програми та тренінги.

Стаття підкреслює необхідність постійного вдосконалення технологій захисту та оновлення засобів протидії новим типам кіберзагроз. Вона також містить аналіз сучасних правових ініціатив, які спрямовані на зміцнення законодавчої бази для ефективного реагування на кіберзлочини, а також національні та міжнародні стандарти в цій сфері. На основі останніх публікацій науковців і практиків виводяться рекомендації для державних органів, бізнесу та освітніх установ щодо необхідних кроків для зміцнення кібербезпеки в умовах постійної ескалації загроз. Ключовим висновком є те, що для забезпечення належного захисту критичної інфраструктури України необхідна тісна співпраця між усіма рівнями влади, бізнесом і міжнародними партнерами.

Ключові слова: кібербезпека, критична інфраструктура, кіберзагрози, гібридна війна, енергетика, блокчейн, штучний інтелект, національні центри кібербезпеки, міжнародне співробітництво, захист інформації, кіберзлочинність, технології захисту.

Hres O. The Role of Cybersecurity in Protecting Ukraine's Critical Infrastructure During Wartime

Cybersecurity is one of the most important components of national security in the face of contemporary global threats, especially for Ukraine, which is in a state of hybrid war with Russia. Attacks on critical infrastructure, such as energy networks, transport systems, financial institutions, and communication networks, have become a regular element of modern conflicts, posing a threat to national security and the country's economic stability. The topic of cybersecurity, particularly in the context of protecting critical infrastructure during wartime, has gained significant importance in academic circles, as it is directly related to the effectiveness of state and private sector operations in emergency conditions. This article aims to analyze the main aspects of cybersecurity in Ukraine, including the study of recent achievements and publications in this field, the identification of types of cyber threats that pose particular risks to critical infrastructure, and the examination of effective measures aimed at enhancing resilience to cyberattacks.

The article emphasizes the impact of emerging technologies, such as artificial intelligence (AI), blockchain, and other innovative solutions, on the protection system of Ukraine's critical infrastructure. Important issues also include improving national cybersecurity centers, creating effective mechanisms for cooperation between government agencies and the private sector, and intensifying international cooperation to combat cyber threats. The role of personnel policies in the cybersecurity sector is also discussed, specifically the importance of training qualified specialists in this field through specialized educational programs and training.

The article underscores the necessity of continuous improvement of protection technologies and the updating of tools to counter new types of cyber threats. It also includes an analysis of contemporary legal initiatives aimed at strengthening the legislative framework for effectively responding to cybercrimes, as well as national and international standards in this area. Based on recent publications by scientists and practitioners, recommendations are provided for government agencies, businesses, and educational institutions regarding the necessary steps to strengthen cybersecurity in the face of the ongoing escalation of threats.

The key conclusion is that ensuring adequate protection for Ukraine's critical infrastructure requires close cooperation among all levels of government, the business community, and international partners.

Key words: cybersecurity, critical infrastructure, cyber threats, hybrid warfare, energy, blockchain, artificial intelligence, national cybersecurity centers, international cooperation, information protection, cybercrime, protection technologies.