КІБЕРЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЕКОЛОГІЧНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ: ІНТЕГРАТИВНИЙ ПІДХІД

Товстенко Б. К., студ. (гр. БС-23, ФБМІ КПІ ім. Ігоря Сікорського);
Мітюк Л. О., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Анотація. Стаття досліджує взаємозв'язок між кіберзахистом критичної інфраструктури (КІ) та екологічною безпекою в умовах воєнного стану в Україні. Обґрунтовано гібридний характер сучасної агресії, де кібератаки поєднуються з фізичним руйнуванням об’єктів КІ (енергетика, водопостачання, хімічна промисловість), спричиняючи каскадні відмови та екологічні катастрофи [3, 4, 6]. Запропоновано концепцію «еко-кібербезпеки» як інтегративний підхід для забезпечення національної стійкості [3, 5, 7]. Розглянуто основні кіберзагрози (Wiper-малварі, атаки на SCADA/ICS) та їхні наслідки для довкілля, включаючи проблему екоциду [4, 6]. Наголошено на необхідності гармонізації законодавства з Директивою ЄС NIS2 [2] та впровадженні архітектури «Нульової довіри» (Zero Trust) [5] для підвищення стійкості систем. Визначено, що лише інтегративний підхід, який включає правове визнання кібер-екологічних інцидентів та посилену міжвідомчу координацію, є критично важливим для екологічно безпечного відновлення та довгострокової безпеки України.

Ключові слова: кібербезпека, критична інфраструктура, воєнний стан, екологічна безпека, еко-кібербезпека, гібридні загрози, NIS2, екоцид.

Abstract. The article explores the relationship between cyber defense of critical infrastructure (CI) and environmental security during martial law in Ukraine. It substantiates the hybrid nature of modern aggression, where cyber attacks combine with the physical destruction of CI facilities (energy, water supply, chemical industry), causing cascading failures and environmental disasters [3, 4, 6]. The concept of “eco-cybersecurity” is proposed as an integrative approach to ensure national resilience [3, 5, 7]. Key cyber threats (Wiper malware, SCADA/ICS attacks) and their environmental consequences, including the issue of ecocide, are reviewed [4, 6]. The necessity of harmonizing legislation with the EU NIS2 Directive [2] and implementing the Zero Trust Architecture (ZTA) [5] to enhance system resilience is emphasized. It is concluded that only an integrative approach, which includes the legal recognition of cyber-environmental incidents and enhanced inter-agency coordination, is critical for Ukraine's environmentally safe recovery and long-term security.

Keywords: cybersecurity, critical infrastructure, martial law, environmental security, eco-cybersecurity, hybrid threats, NIS2, ecocide.

Вступ. Воєнний стан в Україні докорінно змінив ландшафт національної безпеки, вивівши на перший план гібридні виклики, які поєднують кібератаки та фізичне руйнування об’єктів [1, 5]. Критична інфраструктура (КІ) – це хребет держави, що забезпечує життєво важливі функції суспільства: енергетику, водопостачання, транспорт, фінанси та комунікації. У воєнний час ці об'єкти стають пріоритетними цілями агресора, адже їхнє виведення з ладу здатне

спричинити не лише соціально-економічний колапс, але й катастрофічні екологічні наслідки [4]. Руйнування енергоблоків, нафтобаз, чи, як продемонструвало знищення Каховської ГЕС, гідротехнічних споруд, є актами, що поєднують тероризм, фізичну агресію та екоцид [4, 6].

Аналіз стану питання. Кіберпростір став повноцінним театром військових дій. Під час воєнного стану характер кіберзагроз суттєво змінився: вони стали більш інтенсивними, цілеспрямованими та деструктивними. Атаки спрямовані не просто на викрадення даних чи порушення роботи окремих сервісів, а на фізичне руйнування систем управління промисловими процесами (SCADA, ICS), що безпосередньо призводить до реальних, фізичних наслідків [5]. Головною особливістю є синхронізація кібератак із фізичними обстрілами, що ускладнює відновлення та посилює паніку.

Мета роботи. Акцентуалізація негайного впровадження інтегративного підходу, який базується на юридичному визнанні категорії «кібер-екологічного інциденту», посиленні технологічної інтеграції систем моніторингу (включно з використанням AI/ML для прогнозного моделювання) та безшовному міжвідомчому співробітництві.

Методики, матеріали і результати досліджень. Згідно з аналізом Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ), основні кіберзагрози критичній інфраструктурі під час війни включають:

- **Деструктивні атаки (Wiper Malware).** Шкідливе програмне забезпечення, призначене для незворотного знищення даних та виведення з ладу апаратних компонентів. Прикладом залишається вірус «NotPetya», а у воєнний час ці інструменти еволюціонували до більш специфічних, націлених на промислові системи, як, наприклад, вайпери, що маскуються під програми оновлення, компрометуючи ланцюжок поставок (*Supply Chain Attacks*) [5]. Це дозволяє агресору отримати доступ до систем операторів КІ через довірених постачальників програмного забезпечення.

- **Атаки на системи управління технологічними процесами (ICS/SCADA):** Цілями є енергетичні підстанції, системи водоочищення, хімічні заводи. Успішна атака може призвести до вибухів, зупинки виробництва або, що критично для екології, неконтрольованого викиду небезпечних речовин [3, 5]. Особлива небезпека полягає у використанні специфічних TTPs (тактик, технік і процедур), розроблених для маніпуляції фізичними процесами: наприклад, приховане перепрограмування контролерів для створення надлишкового тиску або температури, що призводить до фізичного пошкодження обладнання (як у випадку з атаками на енергетичну систему в 2015-2016 роках) [3, 5].

Обговорення. Необхідне впровадження правового та інституційного підґрунтя захисту. В умовах воєнного стану Україна активізувала гармонізацію свого законодавства з нормами Європейського Союзу, зокрема з Директивою NIS2, що розширює перелік критичних секторів та посилює вимоги до їхнього кіберзахисту [2, 3]. Закон України «Про критичну інфраструктуру» [1] та відповідні підзаконні акти визначили ДССЗЗІ як уповноважений орган у сфері

захисту КІ. Додатково важливу роль відіграє Національний координаційний центр кібербезпеки (НКЦК) при РНБО, який забезпечує міжвідомчу координацію та формує стратегічні пріоритети [5].

Важливим аспектом є екологічна безпека як невід'ємний компонент критичної інфраструктури. Екологічна безпека у воєнний час перетворюється з питання якості життя на питання виживання нації. Військові дії завдають прямої та опосередкованої шкоди довкіллю, створюючи ризики, які за своєю масштабністю можуть перевищувати збитки від військових втрат [4].

Пряма фізична шкода КІ з екологічними наслідками. Руйнування промислових об'єктів (хімічних заводів, нафтопереробних підприємств) призводить до неконтрольованих викидів токсичних речовин, важких металів та продуктів горіння в атмосферу, ґрунти та водні об'єкти. Катастрофа на Каховській ГЕС (2023) є найяскравішим прикладом [4, 6], коли фізичне руйнування об'єкта критичної інфраструктури спричинило екоцид: затоплення величезних територій, знищення біорізноманіття, забруднення питної води та деградацію сільськогосподарських земель.

Забруднення територій та ґрунтів. Широкомасштабне використання важкої техніки, мінування, вибухи та обстріли руйнують ґрунтовий покрив та екосистеми [6]. Залишки палива, мастильних матеріалів та боєприпасів, що містять токсичні сполуки, проникають у ґрунти та підземні води. Проблема нерозірваних боєприпасів (НБП) та мін є окремою екологічною загрозою, яка перешкоджає проведенню відновлювальних робіт.

Ключовим аргументом на користь інтегративного підходу є те, що кібератаки та екологічні катастрофи є елементами єдиного системного ризику, який визначається як еко-кібербезпека. Цей ризик виникає через каскадні відмови (*cascading failures*), де порушення в одному секторі КІ (наприклад, енергетика) через кіберінцидент миттєво викликає ланцюгову реакцію відмов в інших секторах (наприклад, водопостачання та хімічна безпека) [3, 5].

Еко-кібербезпека вивчає, як кібератаки на критичну інфраструктуру, що відповідає за життєзабезпечення, можуть спричинити екологічну катастрофу.

- **Сценарій «Водоканал і Хімічне Забруднення».** Зловмисник отримує контроль над автоматизованою системою управління водоочисними спорудами (АСУ ТП). Замість викрадення даних, він змінює параметри хімічної обробки або відкриває шлюзи для несанкціонованого скиду неочищених стоків чи технологічних рідин у річку. Це миттєво створює екологічну катастрофу та ставить під загрозу здоров'я населення [5].
- **Сценарій «Транспорт і Логістика Небезпечних Вантажів».** Кібератака на системи управління рухом залізничного транспорту може призвести до зіткнення поїздів, що перевозять небезпечні хімічні або паливно-мастильні матеріали. Це спричинить масштабне забруднення ґрунтів і водних ресурсів на місці аварії та вимагатиме негайної екологічної локалізації та очищення [5].

Системна стійкість (Resilience). Інтегративний підхід до еко-кібербезпеки має бути орієнтований на підвищення системної стійкості (*resilience*), що

включає здатність не лише захистити об'єкт від атак, але й швидко відновити його функціонування та мінімізувати супутні наслідки [5].

Наявність автономних систем екологічного контролю та живлення. Системи моніторингу мають працювати незалежно від основної мережі управління КІ, щоб у разі кібератаки екологічні параметри продовжували фіксуватися і передаватися [5].

Інтеграція планів реагування та їхня синхронізація. Плани реагування на кіберінциденти на об'єктах КІ повинні містити чіткий розділ про потенційні екологічні наслідки та інструкції для екологічних служб щодо негайного відбору проб, ізоляції забруднених ділянок та попередження населення.

Висновки. В умовах воєнного стану безпека держави вимірюється її здатністю протистояти гібридним атакам, де кіберпростір, фізичний простір та довкілля стають єдиним полем бою [5]. Кіберзахист критичної інфраструктури та екологічна безпека більше не можуть розглядатися як окремі дисципліни, адже їхні загрози мають синергетичний та каскадний характер [3, 4]. Напади, що мають на меті виведення з ладу систем управління водопостачанням, енергетикою або хімічним виробництвом, за своєю суттю є актами екологічної агресії, ініційованими кіберзасобами.

Успішна протидія цим викликам вимагає негайного впровадження інтегративного підходу. Цей підхід базується на юридичному визнанні категорії «кібер-екологічного інциденту», посиленні технологічної інтеграції систем моніторингу (включно з використанням AI/ML для прогнозного моделювання) та безшовному міжвідомчому співробітництві [7].

Література

1. Закон України «Про критичну інфраструктуру» № 1882-IX від 16 листопада 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20
2. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради щодо заходів із забезпечення високого спільного рівня кібербезпеки в межах Союзу (NIS2).
3. Зубок В.Ю., Давидюк А.В., Клименко Т.М. Кібербезпека критичної інфраструктури в законодавстві України та в директиві (ЄС) 2022/2555. *Електронне моделювання*. 2023. Т. 45. № 5. С. 54–66.
4. Смоляник І.І., Гуменюк М.М. Забезпечення екологічної безпеки в Україні в умовах воєнного стану. *Юридичні науки*. 2025. № 1(2025). С. 104-108.
5. Потій О.В. Національна кібербезпека: управління та стратегічне планування в умовах воєнного стану. Київ: ДССЗЗІ України, 2024.
6. *Environment and Conflict Alert Ukraine*. Risks and impacts from attacks on energy infrastructure in Ukraine. Pax for Peace, December 2022.
7. Венгровська І.В. Правове забезпечення кібербезпеки України в умовах воєнного стану та європейської інтеграції. *Право та інновації*. 22(3), 2024. С. 76-85.