УДК 004.056.5

АКТУАЛЬНІ НАПРЯМКИ І ВИКЛИКИ. ОЦІНКА РИЗИКІВ КІБЕРІНЦИДЕНТІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Тетяна Саламанова

CURRENT TRENDS AND CHALLENGES. RISK ASSESSMENT OF CYBER INCIDENTS FOR CRITICAL INFRASTRUCTURE

Tetiana Salamanova

Волинський національний університет імені Лесі Українки, просп.. Волі, 13, Луцьк 43025, Україна

Abstract. *This article explores the current trends and challenges in assessing cyber incident risks to critical infrastructure. With the growing digitalization of key sectors, such as energy, healthcare, and transportation, the vulnerability to cyber threats has significantly increased. The paper emphasizes the importance of dynamic risk assessment models, national strategies, and international cooperation. It also highlights the role of legal regulations, technological solutions, and human factors in building cyber resilience.*

У XXI столітті цифрові технології стали невід'ємною частиною повсякденного життя людини, а також функціонування ключових секторів економіки, державного управління та національної безпеки. Стрімкий розвиток інформаційно-комунікаційних систем спричинив трансформацію інфраструктури більшості країн світу, зробивши її водночас ефективнішою, але й вразливішою до нових типів загроз. Критична інфраструктура це сукупність об'єктів, систем та мереж, порушення функціонування яких може спричинити серйозні наслідки для здоров'я, безпеки, економіки чи навіть життя громадян. Серед основних секторів критичної інфраструктури – енергетика, транспорт, зв'язок, фінансові установи, охорона здоров'я, водопостачання, державні інститути та сфера оборони.

У сучасному світі питання кібербезпеки критичної інфраструктури вийшло далеко за межі національних інтересів і стало глобальним викликом. Зростаюча взаємозалежність країн, цифровізація всіх сфер життя та перехід ключових функцій держави у віртуальний простір створюють умови, у яких кібератаки можуть мати транснаціональні наслідки. Збої в роботі енергосистеми, банківських структур або медичних сервісів в одній країні можуть призвести до ланцюгових реакцій в інших регіонах. Саме тому боротьба з кіберінцидентами на міжнародному рівні стає пріоритетом для міждержавних об'єднань, союзів, а також спеціалізованих міжнародних організацій.

Зростання рівня цифровізації критичної інфраструктури, включно з активним використанням інтернету речей (IoT), штучного інтелекту (AI), хмарних технологій, SCADA-систем та інших цифрових інструментів, значно підвищує ефективність управління, проте водночас створює нові «точки входу» для кібератак. Відповідно, кібератаки на критичну інфраструктуру вже не є лише технічними інцидентами, вони перетворюються на інструмент впливу, шантажу, економічного та політичного тиску, гібридної війни. Наприклад, атаки на енергетичні системи можуть призвести до знеструмлення цілих регіонів, зриву логістичних ланцюгів, паралічу медичних закладів чи банківської системи, що, у свою чергу, призводить до колапсу соціально-економічної стабільності [3, с. 54-57].

Актуальність питання оцінки ризиків кіберінцидентів для критичної інфраструктури зумовлена не лише частотою атак, але й їх складністю, анонімністю джерел та потенційною катастрофічністю наслідків. Ризик у сфері кібербезпеки це ймовірність того, що конкретна загроза використає певну вразливість системи та призведе до небажаних наслідків. Оцінка ризиків дозволяє виявити слабкі місця, спрогнозувати сценарії потенційних атак, визначити критичні активи та побудувати ефективну систему захисту. Цей процес охоплює як технічні аспекти – аналіз систем, мереж, протоколів, так і організаційні – рівень підготовки персоналу, наявність політик безпеки, плани реагування на інциденти.

На сучасному етапі в розвинених країнах створюються національні стратегії кібербезпеки, які визначають підходи до захисту критичної інфраструктури. Ці стратегії, як правило, базуються на міжнародних стандартах, таких як ISO/IEC 27001, NIST Cybersecurity Framework, а також на галузевих рекомендаціях. Оцінка ризиків здійснюється за допомогою кількісних та якісних методів, серед яких побудова матриць ризиків, сценарне моделювання, SWOT-аналіз, методи FMEA (аналіз видів і наслідків відмов) тощо. Результати оцінки використовуються для визначення пріоритетів у розподілі ресурсів, підготовці кризових планів та реалізації заходів кіберзахисту [5, с. 1-5].

Одним із пріоритетних напрямків розвитку є створення центрів кіберстійкості, спеціалізованих структур, що здійснюють безперервний моніторинг, аналіз та реагування на кіберінциденти в режимі 24/7 [4]. Такі центри активно використовують системи SIEM (Security Information and Event Management), технології штучного інтелекту для виявлення аномалій, а також інструменти автоматизованого реагування. Вони співпрацюють із національними структурами, такими як Computer Emergency Response Team (CERT), а також з приватними компаніями, що володіють значними обсягами технічної інформації.

Крім технічних засобів захисту, вагоме значення має правове регулювання. Багато держав приймають спеціальні закони про кібербезпеку критичної інфраструктури, які встановлюють вимоги до операторів, визначають правила обміну інформацією про інциденти, передбачають відповідальність за порушення вимог безпеки. У Європейському Союзі діє Директива NIS2, яка встановлює єдиний підхід до кібербезпеки в державах-членах. У США реалізується ініціатива CISA (Cybersecurity and Infrastructure Security Agency), яка координує дії з кіберзахисту на федеральному рівні.

Ключові міжнародні структури в сфері кібербезпеки

Організація / Альянс	Роль / Функції
ITU (ООН)	- Рекомендації для країн- Сприяння створенню CERT- Підтримка нац. стратегій кіберзахисту
ENISA (ЄС)	- Гармонізація законодавства- Кібернавчання (Cyber Europe)- Підтримка захисту інфраструктури
NATO CCDCOE	- Аналітика та стратегії- Навчання (Locked Shields)- Кібератаки = колективна оборона
Інтерпол (Cybercrime Directorate)	- Операції проти кіберзлочинців- Захист транспорту й медицини- Співпраця з тех. експертами
WEF – Centre for Cybersecurity	- Партнерство «держава-бізнес»- Захист цифрових ланцюгів- Глобальна координація зусиль
Five Eyes (США, Британія, Канада тощо)	- Обмін кіберрозвідкою- Швидке виявлення атак- Спільне реагування

Однією з провідних міжнародних структур у сфері кібербезпеки є Міжнародний союз електрозв'язку (ITU), що функціонує під егідою ООН. Він розробляє рекомендації для держав

щодо підвищення кіберстійкості, сприяє обміну досвідом і підтримує розробку національних стратегій кіберзахисту. Особливу увагу ITU приділяє створенню національних центрів реагування на комп'ютерні інциденти (CERT), які координують зусилля уряду, бізнесу та громадськості у випадку кібератак [2].

Велике значення має діяльність Європейського агентства з кібербезпеки (ENISA). Його місія це зміцнення кібербезпеки в межах ЄС через гармонізацію законодавства, підтримку держав-членів у розвитку національних систем захисту критичної інфраструктури та проведення міждержавних навчань. В 2023 році ENISA організувала міжнародні кібернавчання «Cyber Europe», в яких взяли участь десятки країн, відпрацьовуючи реагування на умовні кібератаки на енергетичні та фінансові системи [8].

У межах НАТО діє спеціальний підрозділ, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), розташований в Естонії. Цей центр займається аналітикою, розробкою стратегій, а також організацією навчань, зокрема, найвідомішого у світі кіберзмагання Locked Shields. У рамках цієї ініціативи учасники мають змогу в режимі реального часу протидіяти складним симульованим кібератакам на критичну інфраструктуру [9]. НАТО визнає кібератаки як потенційну підставу для активації Статті 5, тобто колективної оборони Альянсу.

Важливою є також роль Інтерполу, який у межах підрозділу Cybercrime Directorate координує міжнародні операції проти кіберзлочинних угруповань. За останні роки Інтерпол провів низку успішних операцій з виявлення та знешкодження хакерських мереж, що атакували медичні системи та транспортну інфраструктуру в різних регіонах. Співпраця правоохоронних органів з технічними експертами та приватним сектором дозволяє виявляти сліди злочинів навіть у зашифрованих цифрових середовищах [6].

На рівні глобальної економіки Світовий економічний форум (WEF) ініціював створення платформи для публічно-приватного партнерства у сфері кібербезпеки – Centre for Cybersecurity [7]. Цей центр об'єднує представників урядів, бізнесу, технологічних компаній і наукової спільноти для спільної протидії кібератакам, що загрожують стабільності глобальної економіки. Він також координує зусилля щодо захисту логістичних ланцюгів і цифрових інфраструктур, зокрема в енергетичній та фінансовій галузях.

У відповідь на зростання кількості атак державного походження з'явилася тенденція до створення міжнародних альянсів з обміну інформацією. Наприклад, об'єднання Five Eyes (США, Велика Британія, Канада, Австралія, Нова Зеландія) має постійну взаємодію у сфері кіберрозвідки та швидкого обміну технічними індикаторами атак. Подібні мережі дозволяють оперативно реагувати на нові типи шкідливого ПЗ, фішингові кампанії або спроби саботажу інфраструктури.

Окрему увагу слід приділити нормативно-правовому регулюванню. У 2023 році в ЄС набрала чинності Директива NIS2, яка зобов'язує операторів критичної інфраструктури впроваджувати стандарти кіберзахисту, повідомляти про інциденти та проходити регулярні аудити. Вона поширюється на ширший перелік секторів, від енергетики до цифрових послуг, і встановлює санкції за порушення вимог безпеки. Аналогічні ініціативи реалізуються у США в межах Cybersecurity and Infrastructure Security Agency (CISA), яка координує політику кіберзахисту на національному рівні та здійснює партнерство з приватними компаніями [1].

Ще одним суттєвим викликом є людський фактор. Незважаючи на всі технічні засоби захисту, велика кількість атак починається з помилок користувачів, таких як відкриття підозрілих листів, використання слабких паролів, нехтування оновленнями. Тому важливим елементом системи захисту є підготовка персоналу: проведення навчань, симуляцій атак, роз'яснювальна робота з кібергігієни. Без усвідомлення працівниками своєї ролі у забезпеченні кібербезпеки не можна гарантувати стабільність функціонування систем.

Кібербезпека критичної інфраструктури не є лише внутрішньою справою держави. В епоху глобалізації важливо розвивати міжнародне співробітництво, обмін інформацією та кращими

практиками. У цьому контексті велику роль відіграють міжнародні організації: ООН, НАТО, Європейське агентство з кібербезпеки (ENISA), Міжнародний союз електрозв'язку (ITU). Завдяки спільним навчанням, міждержавним угодам і мережам реагування можна значно посилити загальну кіберстійкість регіону.

У підсумку, міжнародна боротьба з кіберінцидентами в критичній інфраструктурі є багатовимірною, вона охоплює технічні, правові, стратегічні та освітні аспекти. В епоху цифрової трансформації жодна країна не здатна самостійно протистояти масштабним кіберзагрозам. Тільки через тісну взаємодію, обмін інформацією, стандартизацію підходів та колективну відповідальність можна побудувати ефективну систему кіберзахисту критичної інфраструктури на глобальному рівні.

Узагальнюючи вищенаведене, можна стверджувати, що оцінка ризиків кіберінцидентів для критичної інфраструктури є не просто актуальною, а життєво необхідною для безпеки кожної країни. Успішна реалізація заходів у цій сфері вимагає цілісного підходу, що включає технологічні інновації, правове забезпечення, підвищення кваліфікації персоналу, розвиток партнерства між державою та бізнесом, а також активне міжнародне співробітництво. Лише в умовах такої комплексної взаємодії можливо створити надійний щит для захисту ключових функцій суспільства та забезпечити стабільний розвиток у цифрову епоху.

Бібілографія

1. Директива ЄС NIS2: що це таке, для яких потреб розроблена та для чого Україна її імплементує. Державна служба спеціального зв'язку та захисту інформації України. 2025. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye (дата звернення 12.05.2025)
2. Міжнародний союз електрозв'язку (МСЕ). Співробітництво з міжнародними організаціями в Женеві. URL: https://geneva.mfa.gov.ua/posolstvo/2616-itu#:~:text=Міжнародний%20союз%20електрозв'язку%20(МСЕ)%20–%20спеціалізована%20установа%20ООН,та%20формулювати%20рекомендації%2C%20спрямовані%20на (дата звернення 12.05.2025)
3. Ткаченко І.В., Козачок В.А., Гахов С.О., Дмітрієв В.Є. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів. *Сучасний захист інформації №1 (41).* 2020. С. 54-57. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2408/2309 (дата звернення 12.05.2025)
4. Чуб Д. Важливість аудитів кібербезпеки для об'єктів критичної інфраструктури. *IT specialist.* 2025. URL: https://my-itspecialist.com/importance-of-cybersecurity-audits-for-critical-infrastructure (дата звернення 12.05.2025)
5. Шульга В.П., Іванченко Є.В., Вишневська Н.С. Бербер А.С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. *Сучасний захист інформації. №3(59).* 2024. С. 1-14. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/3002/2902 (дата звернення 12.05.2025)
6. Cybercrime. When cybercriminals go global, our response must be international. URL: https://www.interpol.int/Crimes/Cybercrime (date of application 12.05.2025)
7. Centre for Cybersecurity. URL: https://www.centreforcybersecurity.com/en-sg (date of application 12.05.2025)
8. ENISA European Union Agency Cybersecurity. URL: https://www.enisa.europa.eu (date of application 12.05.2025)