Challenges and Issues of Modern Science, 3 (2024). ISSN: 3083-5704
URL: https://cims.fti.dp.ua/j/article/view/210
PURL: https://purl.org/cims/2403.019

Кібербезпека критичної інфраструктури: виклики інновацій і загрози цифрових технологій

Анна Андрух, Юрій Юрченко

Purpose. The article aims to explore the characteristics, development prospects, and potential threats associated with the cybersecurity of critical infrastructure. As critical systems become increasingly dependent on digital technologies and interconnected networks, safeguarding these infrastructures from cyberattacks is paramount. **Design / Method / Approach**. This research adopts a conceptual approach, drawing from case studies, technical reports, and regulatory frameworks to synthesize the current state of cybersecurity in sectors like energy, telecommunications, and transportation. The study evaluates the integration of emerging technologies such as Artificial Intelligence (AI) and Internet of Things (IoT) in enhancing the resilience of critical systems, while highlighting their vulnerabilities. **Findings**. The research demonstrates that although AI and IoT technologies are enhancing efficiency and control, they also introduce significant risks, including new cybersecurity challenges, regulatory gaps, and vulnerabilities in supervisory control systems like SCADA. **Theoretical Implications**. This study contributes to a deeper theoretical understanding of critical infrastructure cybersecurity by addressing both the opportunities and risks associated with technological advancements. It offers a conceptual model for balancing innovation with security measures. **Practical Implications**. For policymakers and practitioners, the paper provides actionable recommendations on strengthening regulatory frameworks, improving resilience to cyberattacks, and implementing more secure IoT and AI deployments in critical systems. **Originality / Value**. The research offers a comprehensive overview of the dual nature of technological advancements in critical infrastructure, combining analysis of cybersecurity innovations with an exploration of the challenges and gaps that need to be addressed. **Research Limitations / Future Research**. The study relies on available literature and reports; future research should involve empirical investigations on the long-term impact of cybersecurity measures in critical infrastructure. **Paper Type**. Conceptual.

Keywords:

cybersecurity, critical infrastructure, SCADA systems, artificial intelligence (AI), Internet of Things (IoT), cyber threats

Contributor Details:

Anna Andrukh, Undergraduate Student, State University of Trade and Economics: Kyiv, UA, A.Andrukh_FIT_6_21_B_d@knute.edu.ua

Yurii Yurchenko, Senior Instructor, State University of Trade and Economics: Kyiv, UA, y.yurchenko@knute.edu.ua

Захист критичної інфраструктури від кіберзагроз є однією з ключових умов забезпечення стабільності та безпеки сучасних держав. Критична інфраструктура включає такі сектори, як енергетика, водопостачання, транспорт, телекомунікації, охорона здоров'я, фінансові послуги та державне управління. Ці системи забезпечують функціонування суспільства, і будь-яке порушення їхньої роботи може призвести до значних соціальних та економічних наслідків, таких як перебої в наданні послуг, загроза для життя людей та економічні втрати. У цьому контексті кібербезпека відіграє критичну роль у захисті цих систем від потенційних кіберзагроз.

Метою даного дослідження є вивчення основних принципів і підходів до захисту критичної інфраструктури в умовах сучасних кіберзагроз. Основні завдання включають аналіз існуючих ризиків, вивчення методів захисту операційних і інформаційних технологій, що використовуються в управлінні критичними об'єктами, та оцінка можливостей застосування новітніх технологій, таких як штучний інтелект і Інтернет речей, для покращення кіберзахисту.

Дослідження базується на аналізі наукових публікацій, державних документів та звітів з кібербезпеки, а також на вивченні практичних випадків кіберінцидентів, що впливали на критичну інфраструктуру. У процесі роботи використовуються методи порівняльного аналізу, систематизації даних та моделювання можливих сценаріїв кібератак. Особлива увага приділяється дослідженню ролі державних акторів, хактивістів та організованих кіберзлочинних угрупувань у створенні нових загроз.

Захист критичної інфраструктури є стратегічним викликом для урядів та міжнародних організацій, тому ефективне управління кіберризиками стає основою стабільності економіки, національної безпеки та благополуччя суспільства (Про основні засади забезпечення кібербезпеки України, 2024).

Основні загрози для критичної інфраструктури

Критична інфраструктура, яка забезпечує ключові функції держави та суспільства, все більше піддається загрозам у цифровому просторі. Це пов'язано із зростаючою залежністю від інформаційних технологій і підключених до Інтернету систем, які керують різними процесами. Кіберзагрози стають серйозним викликом для захисту енергетичних мереж, транспорту, фінансових систем та телекомунікацій. Найпоширенішими загрозами є цифрові атаки, вразливість промислових систем управління (SCADA), а також кібератаки з боку національних та міжнародних злочинних угрупувань. (Рогов et al., 2017)

Цифрові атаки на енергетичні системи, транспорт, фінанси та комунікації

Одним із найсерйозніших викликів для критичної інфраструктури є кібератаки на енергетичні системи. Електромережі, газопроводи,

нафтопереробні заводи та інші енергетичні об'єкти є важливими цілями для хакерів. Збій у роботі таких систем може призвести до відключення електроенергії на великій території, паралізуючи інші сектори інфраструктури, включаючи транспорт, комунікації та фінанси. Прикладом є атака на українську енергомережу у 2015 році, яка стала першим відомим випадком успішної кібератаки на енергосистему і призвела до відключення електроенергії для сотень тисяч людей.

Транспортна інфраструктура також є важливою мішенню. Це стосується як громадського транспорту, так і міжнародних перевезень. Кібератаки на системи керування залізницями, авіацією чи морськими портами можуть спричинити величезні збої в логістиці, переривання транспортних ланцюжків і навіть потенційно створити загрози для життя людей. Наприклад, атака на датську судноплавну компанію Maersk у 2017 році спричинила глобальні збої в морських перевезеннях, завдавши значних економічних збитків.

Фінансові системи, які є хребтом світової економіки, також піддаються постійним кібератакам. Зловмисники можуть атакувати банки, біржі, платіжні системи з метою викрадення грошей, знищення даних або проведення маніпуляцій на фінансових ринках. Однією з найвідоміших атак є випадок з банком Bangladesh Bank у 2016 році, коли хакери намагалися викрасти близько 1 мільярда доларів, з яких їм вдалося отримати 81 мільйон.

Телекомунікаційні системи, що забезпечують зв'язок між різними секторами критичної інфраструктури, також знаходяться під загрозою. Атаки на ці системи можуть призвести до відключення зв'язку, порушення роботи Інтернету або навіть використання мереж для шпигунства і збору інформації. Особливо вразливими є мобільні та широкосмугові мережі, що використовують старі протоколи безпеки або мають вразливості в їх архітектурі.

Вразливість промислових систем управління (SCADA)

Промислові системи управління (SCADA — Supervisory Control and Data Acquisition) відіграють вирішальну роль у керуванні критичною інфраструктурою. Вони забезпечують автоматизацію та моніторинг роботи таких об'єктів, як електростанції, водопостачальні системи, нафтові платформи та інші промислові об'єкти. Однак ці системи мають низку вразливостей, оскільки більшість SCADA-систем були розроблені з мінімальним врахуванням кібербезпеки. Часто вони використовують застарілі протоколи та операційні системи, що робить їх вразливими для атак.

Хакери можуть використовувати вразливості SCADA для того, щоб отримати доступ до систем управління, змінювати параметри роботи обладнання або викликати збої в його функціонуванні. Наприклад, у 2010 році вірус Stuxnet став відомим через те, що був спрямований на іранські центрифуги збагачення урану. Це перший задокументований випадок, коли шкідливе програмне забезпечення фізично знищило частину критичної інфраструктури, вивівши з ладу промислове обладнання.

Ці атаки показують, наскільки вразливими є SCADA-системи, і як їх захист залишається нагальним завданням. Нещодавнє впровадження

технологій Інтернету речей (IoT) та збільшення кількості пристроїв, підключених до мережі, лише підвищує ризики для цих систем. (Дрейс, 2017)

Атаки з боку національних та міжнародних кіберзлочинців

Одним із найбільших джерел загроз для критичної інфраструктури є дії національних та міжнародних кіберзлочинних угруповань. На відміну від одиночних хакерів або хактивістів, організовані угрупування можуть мати значні фінансові та технічні ресурси. Вони часто діють за підтримки держав або як незалежні злочинні організації, що переслідують фінансову, політичну або навіть військову мету.

Державні актори можуть використовувати кібератаки як інструмент геополітичного тиску або шпигунства. Такі атаки можуть бути спрямовані на порушення роботи інфраструктури, знищення інформації або навіть викликати паніку та хаос у суспільстві. Наприклад, атаки російських кіберугрупувань на енергетичні мережі України показали, як державні актори використовують кібератаки в контексті гібридних воєн.

Міжнародні кіберзлочинці також мають свої інтереси в атаках на критичну інфраструктуру. Це можуть бути атаки з метою вимагання грошей (наприклад, через шкідливе програмне забезпечення типу ransomware), саботаж або викрадення важливих даних. Злочинні угруповання часто використовують такі методи, як фішинг, соціальна інженерія та ін'єкції шкідливого ПЗ для проникнення в системи.

Таким чином, основні загрози для критичної інфраструктури включають цифрові атаки на ключові сектори економіки, вразливість SCADA-систем, а також дії організованих кіберзлочинних угрупувань. В умовах зростаючих кіберризиків уряди та організації повинні постійно вдосконалювати свої системи захисту, аби запобігти катастрофічним наслідкам.

Тренди в розвитку кібербезпеки критичної інфраструктури

Зі зростанням складності та масштабів кібератак на критичну інфраструктуру, кібербезпека стає пріоритетним напрямом розвитку для держав та організацій у всьому світі. Нові технології та підходи до кіберзахисту постійно з’являються для забезпечення надійної оборони критично важливих об’єктів, таких як енергетичні системи, транспорт, фінанси та телекомунікації. Серед ключових трендів у розвитку кібербезпеки виділяються використання штучного інтелекту (ШІ) та машинного навчання (ML), нові загрози, пов'язані з розвитком Інтернету речей (IoT), а також розширення міжнародних кіберстратегій. (Білявська & Шестак, 2022)

Використання штучного інтелекту та машинного навчання для захисту

Штучний інтелект і машинне навчання стають невід'ємною частиною сучасних підходів до забезпечення кібербезпеки критичної інфраструктури. Завдяки своїм можливостям обробляти великі обсяги даних, виявляти аномалії та автоматично реагувати на загрози в реальному часі, ШІ та ML пропонують новий рівень захисту від кібератак.

Однією з найважливіших переваг ШІ є здатність досягати високої точності у виявленні потенційних атак на ранніх стадіях. Традиційні методи кіберзахисту, що базуються на фільтрації трафіку або блокуванні відомих шкідливих програм, часто не здатні ефективно виявляти нові або складні атаки. Натомість алгоритми машинного навчання можуть аналізувати аномальну поведінку в мережі, виділяючи потенційні загрози, навіть якщо вони раніше не зустрічалися.

ШІ також може використовуватись для автоматизації реакції на інциденти. Наприклад, системи на базі машинного навчання можуть самостійно відключати доступ до мережі, ізолювати заражені системи або блокувати шкідливий трафік без необхідності втручання людини. Це значно підвищує ефективність захисту критичної інфраструктури, особливо в умовах, коли атаки можуть розгортатися за лічені хвилини або навіть секунди.

Поява нових загроз у зв'язку з розвитком Інтернету речей (IoT)

Розвиток Інтернету речей (IoT) відкриває нові можливості для автоматизації та покращення управління критичною інфраструктурою, але разом з тим створює нові вразливості. Із збільшенням кількості пристроїв, підключених до мережі, зростає і площа для потенційних атак. Багато пристроїв IoT мають слабкі системи безпеки або використовують стандартні налаштування безпеки, що робить їх вразливими для кіберзлочинців.

IoT пристрої, такі як датчики в енергетичних системах, камери відеоспостереження, розумні лічильники та інші, можуть стати мішенню для хакерів. Якщо ці пристрої будуть скомпрометовані, зловмисники можуть отримати доступ до ключових систем управління інфраструктурою або навіть організувати розподілені атаки на відмову в обслуговуванні (DDoS). Наприклад, масивна DDoS-атака у 2016 році, організована через заражені IoT пристрої (зокрема, розумні камери та маршрутизатори), тимчасово паралізувала інтернет у великих регіонах США.

Крім того, багато пристроїв IoT використовуються для збору даних, що також створює загрози витоку інформації. Це особливо критично у випадках, коли мова йде про медичне обладнання, транспортні системи або фінансові служби, де компрометація конфіденційних даних може мати серйозні наслідки.

Щоб мінімізувати ці ризики, сучасні підходи до кібербезпеки включають

розробку стандартів безпеки для IoT, а також впровадження нових технологій захисту, таких як блокчейн для захисту комунікацій між IoT пристроями та шифрування даних на рівні кожного окремого пристрою.

Розширення кіберстратегій на міжнародному ринку

В сучасному глобалізованому світі загроза кібератак на критичну інфраструктуру не обмежується кордонами однієї країни. Кіберзлочинці та державні актори можуть організовувати атаки на інфраструктуру в будь-якій точці світу, тому країни повинні активно співпрацювати для забезпечення кібербезпеки. Одним із ключових трендів останніх років є розширення міжнародної співпраці у сфері кіберзахисту.

Організації, такі як НАТО, Європейський Союз та ООН, активно працюють над створенням спільних стратегій боротьби з кіберзагрозами. Наприклад, НАТО визнала кіберпростір п'ятою сферою військових дій, що означає, що альянс готовий реагувати на кібератаки так само, як і на фізичні загрози. Держави-члени НАТО співпрацюють у сфері кіберзахисту, обмінюються інформацією про загрози та проводять спільні навчання з кібербезпеки.

Крім того, створюються міжнародні альянси для боротьби з кіберзлочинністю. Один із таких прикладів — Європейське агентство з кібербезпеки (ENISA), яке координує зусилля держав-членів ЄС у захисті критичної інфраструктури від кіберзагроз. Також розвиваються стандарти та норми, які регулюють поведінку держав у кіберпросторі, зокрема в рамках Будапештської конвенції з кіберзлочинності.

У зв'язку з поширенням нових видів загроз, таких як кібершпигунство, атаки на ланцюжки постачання та дезінформація, міжнародна співпраця стає критично важливою. Впровадження узгоджених кіберстратегій дозволяє забезпечити краще реагування на загрози, а також покращити обмін технологіями та досвідом між державами.

Інновації в кіберзахисті критичної інфраструктури

Сучасний розвиток технологій привносить нові можливості в сферу кібербезпеки критичної інфраструктури. Інновації в цій галузі, такі як блокчейн, квантові технології та хмарні сервіси, дозволяють підвищити ефективність захисту даних і систем управління, а також забезпечити більшу стійкість до атак (Subach et al., 2019).

Блокчейн та його роль у забезпеченні безпеки даних

Блокчейн, технологія, що лежить в основі криптовалют, демонструє значний потенціал у сфері кібербезпеки, зокрема у забезпеченні безпеки даних критичної інфраструктури. Завдяки своїй дистрибутивній природі, блокчейн забезпечує збереження інформації в незмінному вигляді, що робить її стійкою до підробок і несанкціонованих змін.

Використання блокчейн-технології у системах критичної інфраструктури може допомогти вирішити проблему безпеки даних, забезпечуючи автентифікацію транзакцій та обмежуючи доступ до конфіденційної інформації. Наприклад, в енергетичних системах блокчейн може використовуватися для ведення обліку споживання енергії, а також для управління дистрибуцією електроенергії між різними споживачами, забезпечуючи прозорість і захист від шахрайства.

Крім того, блокчейн може використовуватися для забезпечення безпеки IoT-пристроїв, адже його дистрибутивна структура дозволяє знизити ризик централізованих атак. Завдяки інтеграції технології блокчейн у мережі IoT, дані можуть зберігатися на розподілених вузлах, що ускладнює доступ до них зловмисників і підвищує загальний рівень безпеки.

Квантові технології у сфері шифрування та захисту

Квантові технології, хоча ще перебувають на стадії розвитку, обіцяють революціонізувати сферу кібербезпеки, зокрема у шифруванні даних. Квантове шифрування використовує принципи квантової механіки для забезпечення рівня безпеки, недоступного для традиційних методів. Це можливо завдяки явищу, відомому як квантова заплутаність, що дозволяє створювати ключі для шифрування, які не можуть бути перехоплені або зламані без виявлення.

Квантова криптографія забезпечує захист даних у режимі реального часу, що є критично важливим для систем, що управляють критичною інфраструктурою. Це дозволяє безпечно передавати інформацію між елементами інфраструктури, наприклад, між електростанціями та мережами управління. У разі спроби перехоплення або зміни квантових сигналів, система автоматично виявляє вторгнення, що дозволяє миттєво вжити заходів для захисту даних.

Крім того, квантові комп'ютери, хоч і ще не стали масовими, обіцяють змінити ландшафт шифрування. Вони здатні виконувати обчислення, які є непосильними для класичних комп'ютерів, включаючи злому традиційних методів шифрування. Тому розробка нових квантових алгоритмів для шифрування даних є нагальною потребою для забезпечення довгострокової безпеки критичної інфраструктури.

Використання хмарних сервісів для розподіленої безпеки

Хмарні технології стають все більш популярними у сфері кібербезпеки завдяки своїй здатності забезпечити гнучкість, масштабованість та розподілену безпеку. Хмарні сервіси дозволяють організаціям зберігати та обробляти дані в безпечних середовищах, забезпечуючи одночасно захист від кібератак.

Однією з ключових переваг використання хмарних сервісів є можливість реалізації механізмів резервного копіювання та відновлення даних. У разі кібератаки чи збою системи дані можуть бути швидко

відновлені без значних втрат. Також хмарні провайдери зазвичай пропонують потужні засоби для виявлення загроз і моніторингу безпеки, що дозволяє організаціям зосередитися на основних бізнес-процесах, залишаючи управління безпекою фахівцям.

Крім того, хмарні технології забезпечують можливість централізованого управління безпекою, що дозволяє реалізувати спільні стратегії захисту для всіх підрозділів організації. Це дозволяє вчасно виявляти та реагувати на загрози, підвищуючи загальний рівень захисту критичної інфраструктури.

Практичні заходи щодо підвищення рівня кібербезпеки

В умовах постійно зростаючих кіберзагроз організації повинні вжити практичні заходи для підвищення рівня кібербезпеки своєї критичної інфраструктури. Серед найефективніших стратегій можна виділити етичний хакінг, інтеграцію систем моніторингу та реагування на інциденти, а також навчання персоналу (Марущак, 2018).

Етичний хакінг та тестування на проникнення

Етичний хакінг, або тестування на проникнення, є важливою практикою для виявлення вразливостей в системах і мережах критичної інфраструктури. Цей підхід передбачає залучення спеціалістів, які мають ліцензію на тестування систем безпеки з метою виявлення потенційних загроз і недоліків.

Етичні хакери використовують ті ж методи, що й зловмисники, проте їхні дії мають законний характер і спрямовані на підвищення безпеки. Вони можуть виявити уразливості в системах, які можуть бути використані зловмисниками для атак, і надати рекомендації щодо їх усунення. Регулярне проведення тестувань на проникнення допомагає підтримувати безпеку систем на високому рівні, а також підвищує обізнаність про потенційні загрози.

Цей процес не лише дозволяє виявити вразливості, але й сприяє створенню культури безпеки в організації. Підприємства, що активно впроваджують етичний хакінг, демонструють готовність до проактивного захисту своїх систем і даних.

Інтеграція систем моніторингу та реагування на інциденти

Інтеграція систем моніторингу та реагування на інциденти є ключовим елементом забезпечення кібербезпеки. Це дозволяє організаціям оперативно виявляти та реагувати на загрози, зменшуючи час реагування і запобігаючи потенційним збиткам.

Системи моніторингу зазвичай включають в себе автоматизовані рішення, які відстежують мережевий трафік, системи управління даними та інші критичні елементи інфраструктури.

Однак просто виявлення загроз недостатньо. Важливо також мати чіткі процедури реагування на інциденти, які дозволяють організаціям швидко реагувати на загрози, ізолювати скомпрометовані системи та відновити нормальну роботу. Регулярні тренування для команд реагування на інциденти забезпечують готовність до дій у разі реальної атаки (Гончар, 2017).

Навчання персоналу та підвищення культури безпеки

Один з найбільших ризиків для кібербезпеки критичної інфраструктури — це людський фактор. Недостатня обізнаність про загрози та вразливості може призвести до помилок, які можуть стати причиною успішних атак. Тому навчання персоналу та підвищення культури безпеки є невід'ємною частиною стратегій захисту.

Організації повинні регулярно проводити тренінги для співробітників з метою підвищення обізнаності про кіберзагрози, методи фішингу та безпечне використання технологій. Крім того, необхідно впроваджувати політики безпеки, які регулюють поведінку співробітників у кіберпросторі.

Висновок та перспективи

Необхідність міжнародної співпраці в сфері кібербезпеки

В сучасному глобалізованому світі загрози кібербезпеки не знають кордонів. Атаки на критичну інфраструктуру можуть бути ініційовані з будь-якої точки світу, що підкреслює необхідність міжнародної співпраці для їхнього запобігання та реагування. Спільні зусилля держав, міжнародних організацій і приватного сектору є критично важливими для розвитку ефективних стратегій захисту та зменшення вразливості критично важливої інфраструктури.

Співпраця може включати обмін інформацією про загрози, спільні навчання, розробку міжнародних стандартів безпеки та координацію дій у разі кіберінцидентів. Створення міжнародних альянсів та партнерств, таких як Європейське агентство з кібербезпеки (ENISA) і програми НАТО, свідчить про готовність держав до колективних дій у боротьбі з кібератаками. Лише через спільні зусилля можливо досягти стійкості до кіберзагроз і забезпечити безпеку критично важливих об'єктів інфраструктури на глобальному рівні.

Майбутнє кіберзахисту критичної інфраструктури

Майбутнє кіберзахисту критичної інфраструктури буде визначатися технологічним прогресом, розвитком нових загроз та необхідністю адаптації до швидко змінюваного середовища. Інновації в галузі штучного інтелекту, блокчейну, квантових технологій та хмарних сервісів обіцяють підвищити рівень захисту даних і систем, проте разом з тим відкривають нові

можливості для зловмисників.

Крім того, підвищена увага до питань кібербезпеки в світовій політиці, а також усвідомлення важливості захисту критичної інфраструктури з боку урядів і бізнесу створюють позитивний фон для розвитку ефективних заходів захисту. Важливо, щоб організації не лише реагували на існуючі загрози, але й проактивно шукали нові рішення для забезпечення безпеки.

Посилання

Subach, I., Mykytiuk, A., & Kubrak, V. (2019). Architecture and functional model of a perspective proactive intellectual SIEM for cyber protection of objects of critical infrastructure. *Collection" Information Technology and Security"*, *7*(2), 208-215. https://doi.org/10.20535/2411-1031.2019.7.2.190570

Білявська, Ю., & Шестак, Я. (2022). Кібербезпека та кібергігієна: нова ера цифрових технологій. *The international scientific-practical journal "Commodities and markets," 43*(3), 47–59. https://doi.org/10.31617/2.2022(43)04

Гончар, С. Ф. (2017). Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури. *Моделювання та інформаційні технології*, (80), 27-32. http://nbuv.gov.ua/UJRN/Mtit_2017_80_6

Дрейс, Ю. О. (2017). Analysis of basic terminology and negative consequences from cyber attaks on information-telecommunication systems of objects state's critical infrastructure. *Ukrainian Information Security Research Journal, 19*(3). https://doi.org/10.18372/2410-7840.19.11900

Марущак, А. І. (2018). Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право, 1*(24), 127-132. https://ippi.org.ua/marushchak-ai-informatsiino-pravovi-aspekti-protidii-kiberzlochinnosti-st-127-132

Про основні засади забезпечення кібербезпеки України, Закон України No. 2163-VIII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

Рогов, П. Д., Ворович, Б. О., & Ткаченко, В. А. (2017). Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, 59*(1), 64-72. http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13