Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Законодавство України : офіц. вебпортал ВРУ*. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.02.2026).
2. Кібершпигунство. *StopFraud* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-work/kibershpygunstvo-i315 (дата звернення: 19.02.2026).
3. Кібершахрайство: фішинг, вішинг, смішинг, бейтінг. *Kopirait* : [сайт]. URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення: 19.02.2026).
4. Кібератака. *StopFraud* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-wartime/kiberataka-i270 (дата звернення: 19.02.2026).

Савчин Євгенія Андріївна
студентка 117_СПД н.гр. ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВИКЛИКИ ІННОВАЦІЙ І ЗАГРОЗ ЦИФРОВИХ ТЕХНОЛОГІЙ

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. Тому кібербезпека відіграє критичну роль у захисті 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 ШІ 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 роботі використовуються методи порівняльного аналізу, систематизації даних та моделювання можливих сценаріїв кібератак.

Основні загрози 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 [1].

Цифрові атаки на енергетичні системи, транспорт, фінанси та комунікації

Одним із найсерйозніших викликів для об'єктів критичної інфраструктури сьогодні залишаються кібератаки на енергетичний сектор. Електричні мережі, газотранспортні системи, нафтопереробні підприємства та інші енергетичні об'єкти часто стають цілями хакерів. Порушення їхньої роботи може спричинити масштабні відключення електроенергії, що, у свою чергу, впливає на функціонування інших важливих сфер – транспорту, зв'язку та фінансів. Яскравим прикладом є кібератака на енергосистему України у 2015 році, яка призвела до знеструмлення сотень тисяч споживачів.

Не менш вразливою є транспортна інфраструктура. Йдеться як про громадський транспорт, так і про міжнародні перевезення. Втручання в системи управління залізничним, авіаційним чи морським транспортом може викликати серйозні логістичні перебої, розриви постачальних ланцюгів і навіть створити небезпеку для людей. Наприклад, кібератака на компанію Maersk у 2017 році спричинила значні порушення у глобальних морських перевезеннях та завдала суттєвих фінансових втрат.

Фінансова сфера, яка є основою світової економіки, також постійно перебуває під загрозою. Хакери можуть атакувати банки, фондові біржі та платіжні системи з метою викрадення коштів, знищення інформації або маніпуляцій на ринку. Одним із найвідоміших інцидентів стала атака на Bangladesh Bank у 2016 році, коли зловмисники намагалися викрасти близько мільярда доларів, з яких їм вдалося отримати 81 мільйон.

Телекомунікаційна інфраструктура, що забезпечує зв'язок між різними галузями, також є вразливою до кіберзагроз. Атаки на ці системи можуть призвести до збоїв у зв'язку, порушення роботи Інтернету або використання мереж для шпигунства. Особливо ризикованими є мобільні та широкосмугові мережі, які мають застарілі протоколи безпеки або недоліки в архітектурі.

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. Міжнародні кіберзлочинці також мають свої інтереси в атаках на критичну інфраструктуру. Це можуть бути атаки з метою вимагання грошей, 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 [2].

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 [3].

Практичні заходи щодо підвищення рівня кібербезпеки

В умовах постійного зростання кіберзагроз організації мають вживати комплексних заходів для захисту критичної інфраструктури. До ключових підходів належать етичний хакінг (тестування на проникнення), який дозволяє своєчасно виявляти та усувати вразливості, а також впровадження систем моніторингу й реагування, що допомагають швидко виявляти атаки та мінімізувати їх наслідки. Не менш важливим є навчання персоналу, адже людський фактор часто стає причиною інцидентів. Регулярні тренінги та формування культури кібербезпеки сприяють підвищенню обізнаності працівників і зменшенню ризику успішних атак [4].

Висновок та перспективи

У сучасному світі кіберзагрози мають глобальний характер, тому ефективна протидія їм потребує міжнародної співпраці. Атаки можуть здійснюватися з будь-якої країни, тому взаємодія між державами, міжнародними організаціями та бізнесом є необхідною для обміну інформацією, проведення спільних навчань і координації дій під час інцидентів. Таке партнерство сприяє зниженню вразливості критичної інфраструктури та підвищенню рівня її захисту.

Майбутнє кіберзахисту пов’язане з розвитком новітніх технологій, таких як штучний інтелект, блокчейн і хмарні сервіси. Вони допомагають посилити безпеку, але водночас створюють нові ризики. Тому організаціям важливо не лише реагувати на загрози, а й діяти на випередження, впроваджуючи інноваційні рішення та постійно вдосконалюючи системи захисту.

Список використаних джерел:

1. Білявська Ю, Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Commodity science. Technologies. Engineering*. 2022. Т. 43. № 3. С. 47–59. URL: https://doi.org/10.31617/2.2022(43)04.
2. Гончар С. Ф. Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури. *Моделювання та інформаційні технології*. 2017. Вип. 80. С. 27–32. URL: http://nbuv.gov.ua/UJRN/Mtit_2017_80_6.
3. Дрейс Ю. О. Аналіз базової термінології та негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави. *Український журнал досліджень інформаційної безпеки*. 2017. Т. 19. № 3. С. 214–222. URL: https://doi.org/10.18372/2410-7840.19.11900.
4. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*. 2018. Т. 1. № 24. С. 127–132. URL: https://doi.org/10.37750/2616-6798.2018.1(24).273217
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Законодавство України : офіц. вебпортал ВРУ*. URL: https://zakon.rada.gov.ua/laws/show/2163-19.