УДК: 004.056.5 DOI: **10.33099/2311-7249/2025-54-3-75-83**

МУРАСОВ Рустам Камілович,
доктор технічних наук,
Національний університет оборони України,
https://orcid.org/0000-0003-0800-2062

ФАРАОН Сергій Іванович,
доктор філософії,
Національний університет оборони України,
http://orcid.org/0000-0002-5500-7352

ГУК Олександр Миколайович,
доктор філософії,
Національний університет оборони України,
https://orcid.org/0000-0002-0311-7162

КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ОЦІНЮВАННЯ ТА УПРАВЛІННЯ РИЗИКАМИ КІБЕРАТАК

Стаття зосереджується на важливому аспекті сучасної безпеки – кібербезпеці систем критичної інфраструктури. ***Метою статті*** *є дослідження сучасних викликів і загроз, що виникають у зв'язку з кібербезпекою критичної інфраструктури, а також визначення стратегій та технологій, необхідних для її ефективного захисту.*

Методи дослідження. *Під час написання статті застосовано методи аналізу та синтезу для розгляду сучасних підходів до стратегії та технологій кіберзахисту, включно з використанням штучного інтелекту, машинного навчання та інших інноваційних методів.*

Отримані результати дослідження. *Досліджуються можливі варіанти співпраці між різними секторами та країнами з метою підвищення рівня захисту критичної інфраструктури від кібератак. У статті створено огляд новітніх тенденцій у сфері кібербезпеки, розроблено рекомендації щодо покращення кіберзахисту критичних систем.*

Елементами наукової новизни *є уточнення та конкретизація існуючих даних, розширення їх застосування на нові об'єкти та системи, а також запропоновано нові методи виявлення та запобігання кіберзагрозам.*

Теоретична й практична значущість викладеного у статті *полягає в тому, що отримані результати можуть бути використані для підвищення рівня національної безпеки та вдосконалення стратегій захисту критичної інфраструктури у сфері технічних наук. Вони спрямовані на зниження вразливості інформаційних мереж і систем, впровадження сучасних технологій кіберзахисту та забезпечення ефективного реагування на кіберзагрози. Практичне значення дослідження полягає у можливості застосування його результатів для формування політик безпеки, підготовки персоналу та розроблення програмного й апаратного забезпечення для потреб кібероборони. Представлені положення поглиблюють наукове розуміння проблематики та сприяють розвитку заходів із забезпечення кібербезпеки критичної інфраструктури, що є ключовим чинником зміцнення національної безпеки та стійкості держави в умовах цифрової епохи.*

Ключові слова: *кіберборотьба, національна безпека, захист критичної інфраструктури, кіберзахисні стратегії, кіберзахист, кібероборона.*

Вступ

На сучасному етапі ери цифровізації критична інфраструктура, до якої належать електроенергетика, транспорт, комунікаційні мережі та фінансові системи, стає об’єктом зростаючої уваги як з боку організованих груп кіберзлочинців, так і державних структур, що дедалі активніше діють у кіберпросторі. Масштабність та комплексність цифрових загроз створюють новий вимір небезпеки, адже навіть локальні атаки здатні призвести до значних соціально-економічних наслідків та порушення безперебійного функціонування ключових сфер життєдіяльності суспільства. У цих умовах забезпечення безпеки зазначених об’єктів критичної інфраструктури перетворюється на пріоритетне завдання державної політики та міжнародної співпраці, набуваючи рис прямого цифрового конфлікту. У цій статті ми розглянемо поняття кіберборотьби як другого фронту захисту критичної інфраструктури, що визначає необхідність комплексного поєднання технічних, організаційних та стратегічних заходів у протидії сучасним кіберзагрозам [1; 2].

Критична інфраструктура є невід’ємною частиною

суспільного життя і включає розгалужений комплекс систем, мереж, послуг та об'єктів, які мають визначальне значення для економічного розвитку держави, гарантування її безпеки та підтримання належного рівня добробуту населення. Вона охоплює широкий спектр життєво важливих функцій і процесів, що забезпечують стабільність державного управління, ефективність виробничого і комерційного секторів, а також сталість діяльності соціальної та громадської сфер. Саме критична інфраструктура створює умови для задоволення базових повсякденних потреб суспільства, підтримання його соціальної стабільності та формування передумов сталого розвитку в умовах зростаючих викликів цифрової епохи [9; 10].

До критичної інфраструктури входять різні сектори, зокрема, енергетика (електроенергетика, газопостачання), транспорт (дороги, залізниці, порти, аеропорти), телекомунікації, водопостачання і водовідведення, охорона здоров'я (лікарні, клініки), фінанси (банки, фінансові установи), безпека (поліція, пожежна охорона), інформаційні технології, харчова промисловість, екологічна безпека та інші галузі, які є критичними для функціювання суспільства. Важливо розуміти, що критична інфраструктура не обмежується лише фізичними об'єктами, але також має у своєму складі інформаційні та комунікаційні системи, які забезпечують передачу даних і комунікацію між різними секторами та органами управління

Постановка проблеми. Постановка проблеми. Критична інфраструктура є постійним об'єктом кібервпливу злочинців (рис. 1).

Рисунок 1 – Сектори держави, що постраждали від кібератак

Упродовж 2023 року було зафіксовано 1105 кіберінцидентів. Це на 62,5% більше, ніж у 2022 році. Система моніторингу виявила 133 млн підозрілих подій також було зареєстровано 148 000 критичних інцидентів [8]. Цифрове підключення об'єктів критичної інфраструктури в сучасних умовах розкриває нові можливості щодо їх ефективного використання, управління та моніторингу, але одночасно створює серйозні виклики і ризики. Одними з найважливіших ризиків є:

кібератаки, зокрема, зі збільшенням підключених пристроїв і мереж зростає потенціал для кібератак. Кіберзлочинці можуть намагатися зламати ці системи для отримання конфіденційної інформації, завдання збитків або перешкоджання нормальному функціонуванню;

віруси та шкідливі програми, адже збільшення підключених пристроїв також збільшує ризик поширення вірусів, троянських коней та інших шкідливих програм, які можуть завдати шкоди системам критичної інфраструктури.

вразливості безпеки – більшість підключених пристроїв і систем мають потенційні вразливості, які можуть бути використані для здійснення кібератак. Недоліки в проєктуванні, програмному забезпеченні та конфігурації можуть стати вихідними точками для зловмисників;

недостатність кіберзахисту: багато суб'єктів можуть бути недостатньо підготовленими до відповідного рівня кіберзахисту, що може призвести до вразливостей та недоліків у захисті пристроїв і мереж;

переповнення мережі, що може призвести до перебоїв у забезпеченні послуг або недоступності важливих систем.

Виявлені ризики акцентують необхідність упровадження ефективних заходів кіберзахисту та застосування комплексних стратегій управління ризиками з метою гарантування безпеки й стійкості критичних систем в умовах інтенсивного розширення цифрового підключення

Аналіз останніх досліджень і публікацій щодо захисту критичної інфраструктури свідчать про актуальність цього питання в сучасному науковому дискурсі, особливо, в контексті російської агресії. Такі дослідники, як М. Хомік, С. Чумаченко, О. Авраменко,

Т. Куртсеітов, у своїх працях акцентують увагу на техногенній безпеці та наслідках надзвичайних ситуацій такого характеру [3; 4; 5]. Однак, важливо відзначити, що їхні дослідження фокусуються переважно на техногенній безпеці та реагуванні на наслідки надзвичайних ситуацій, не надаючи достатньої уваги кібербезпеці.

Крім того, окремі дослідження стосовно нормативно-правового забезпечення також важливі, хоча ми їх не розглядаємо у цьому контексті. Важливо враховувати, що кібербезпека дотепер розглядалась як окрема складова інтернет-забезпечення або фінансової безпеки. Однак у сучасному світі, що характеризується глобалізацією, цифровізацією та впровадженням кібернетики у процеси управління складними системами, кібербезпека стає невід'ємною складовою безпеки критичної інфраструктури.

Новітні дослідження також вказують на важливість інтеграції різних технологій для покращення кіберзахисту. Наприклад, використання штучного інтелекту для виявлення аномалій у мережевому трафіку може значно зменшити час реакції на потенційні загрози [11]. Аналіз великих обсягів даних (Big Data) дає змогу виявляти приховані закономірності та потенційні уразливості в системах критичної інфраструктури [12]. Крім цього, впровадження блокчейн-технологій може забезпечити високий рівень захисту даних та аутентифікації транзакцій [13].

Це відкриває широкі можливості для подальших досліджень та розвитку стратегій захисту критичної інфраструктури від кіберзагроз. Спільні зусилля науковців, урядових організацій і приватного сектору у цьому напрямі сприятимуть створенню більш безпечного та стійкого інформаційного середовища.

Метою статті є дослідження сучасних викликів і загроз, що виникають у зв'язку з кібербезпекою критичної інфраструктури, а також визначення стратегій та технологій, необхідних для її ефективного захисту.

Стаття має на меті підкреслити важливість кібербезпеки у контексті захисту критичних об’єктів, зокрема у сферах енергетики, транспорту, медицини та фінансів, а також охарактеризувати сучасні тенденції та інноваційні підходи у цій сфері. Водночас метою є підвищення усвідомленості щодо необхідності координації зусиль національних та міжнародних організацій задля запобігання кібератакам і забезпечення стійкості критичної інфраструктури в умовах цифрової епохи.

Виклад основного матеріалу дослідження

Основні поняття та визначення

На нашу думку, *кіберзагроза* (cyberthreat, T) це будь-яка потенційна небезпека, що може завдати шкоди системам критичної інфраструктури через інформаційні та комунікаційні технології. В свою чергу, *вразливість* (vulnerability, V) являє собою слабке місце в системі, яке може бути використане для здійснення кібератаки. Формально, вразливість можна представити як функцію:

$$V:S\rightarrow[0,1] \quad (1)$$

де S – множина всіх можливих станів системи. V(s) відображає рівень вразливості стану s. Водночас, *ймовірність успішної атаки* (probability of successful attack, Pa) – це показник, що відображає ймовірність того, що кібератака на критичну інфраструктуру буде успішною. Цей показник є головним для оцінювання ризиків та розроблення ефективних стратегій захисту. Ймовірність успішної атаки може залежати від багатьох факторів, які взаємодіють між собою. Серед цих факторів основними є вразливість системи (V), характер та складність загрози (T), а також рівень захисту (R).

Вразливість системи (V) відображає ступінь, до якого система піддається потенційним атакам. Це може включати як технічні вразливості в програмному або апаратному забезпеченні, так і організаційні слабкості, такі як недостатня підготовка персоналу або відсутність ефективних політик безпеки. Характер та складність загрози (T) містить у собі тип атаки, її інтенсивність, використовувані методи та засоби. Це можуть бути прості атаки, такі як фішинг, або складні багатовекторні атаки, що використовують вразливості нульового дня. Рівень захисту (R) системи є показником заходів, вжитих для запобігання атакам та зменшення їхнього впливу. До них належать технічні засоби, такі як антивірусне програмне забезпечення, брандмауери, системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), а також організаційні заходи, включно з навчанням персоналу, політикою безпеки та процедурами реагування на інциденти.

$$P_a=f(T,V,R)] \quad (2)$$

де R – рівень захисту системи.

Моделі ризиків та захисту

Модель ризику. Для оцінювання ризику кібератак на критичну інфраструктуру використовуються різні моделі. Одна з них базується на оцінці ймовірності та впливу. Нехай L – втрати від успішної атаки, тоді ризик R можна визначити як:

$$R=P_a\cdot L \quad (3)$$

Модель захисту. Рівень захисту системи R можна розглядати як функцію від застосованих засобів захисту. У загальному вигляді рівень захисту визначається ефективністю та взаємодією різних компонентів, які забезпечують безпеку системи. Формально, це можна виразити так:

$$R=g(S,D,C) \quad (4)$$

де: S – заходи безпеки (Security measures), які містять всі технічні, організаційні та адміністративні дії, спрямовані на захист системи від потенційних загроз. Це можуть бути антивірусні програми, брандмауери, системи управління доступом, шифрування даних, регулярні оновлення програмного забезпечення, політики безпеки та інші засоби;

D – детекція загроз (Threat detection), що складається з систем і методів, спрямованих на виявлення потенційних загроз у режимі реального часу. Це можуть бути системи виявлення вторгнень (IDS), моніторинг мережевого трафіку, аналіз логів, використання штучного інтелекту та машинного навчання для виявлення аномалій і підозрілої активності;

C – контрзаходи (Countermeasures), що містять дії, спрямовані на реагування на виявлені загрози та їх нейтралізацію. Це можуть бути системи запобігання вторгнень (IPS), заходи з відновлення після інцидентів, планування безперервності бізнесу, навчання персоналу щодо реагування на інциденти та інші активні заходи з протидії загрозам.

Ефективність моделі захисту залежить від того, наскільки добре інтегровані ці компоненти і як вони взаємодіють між собою. Високий рівень захисту досягається, коли заходи безпеки, детекція загроз і контрзаходи працюють у тісній координації, забезпечуючи своєчасне виявлення та нейтралізацію загроз.

Застосування машинного навчання

Для підвищення ефективності виявлення загроз та запобігання атакам, можуть застосовуватися алгоритми машинного навчання. Припустимо X – множина вхідних даних (логів, мережевих пакетів і т.д.), тоді модель машинного навчання M можна навести як:

$$M: X \rightarrow Y \quad (5)$$

де Y – множина вихідних даних (імовірностей загроз).

Навчання моделі відбувається на множині тренувальних даних:

$$D = \{(x_i, y_i)\}_{i+1}^{n} \quad (6)$$

де $x_i \in X$, $y_i \in Y$.

Алгоритми машинного навчання можуть використовуватися для різних завдань у сфері кібербезпеки, зокрема, стосовно:

виявлення аномалій – алгоритми навчання без учителя (unsupervised learning) можуть використовуватися для виявлення аномальної поведінки в мережевому трафіку або системних логах. Наприклад, методи кластеризації, такі як алгоритм k-середніх (k-means) або алгоритм DBSCAN, можуть групувати схожі дані разом, а аномалії виявляти як точки, що не належать жодному кластеру;

класифікація загроз – алгоритми навчання з учителем (supervised learning) можуть бути використані для класифікації вхідних даних як загрози чи ні. Наприклад, методи на основі дерев рішень (decision trees), випадкових лісів (random forests), або глибоких нейронних мереж можуть навчатися на попередньо мічених даних, щоб точно класифікувати нові зразки;

прогнозування загроз – регресійні моделі можуть використовуватися для прогнозування ймовірності виникнення загрози в майбутньому. Це може бути корисним для проактивного управління ризиками та вжиття превентивних заходів;

аналіз поведінки користувачів – поведінкові моделі можуть аналізувати дії користувачів у системі для виявлення аномальних або підозрілих активностей. Методи машинного навчання можуть вивчати звичайні шаблони поведінки і виявляти відхилення від цих шаблонів.

Навчання моделей машинного навчання вимагає ретельного підбору даних та алгоритмів, а також їх регулярного оновлення, щоб адаптуватися до нових загроз. Важливим аспектом є також оцінка якості моделей за допомогою метрик точності, повноти, точності та F1-міри, щоб забезпечити високий рівень надійності виявлення загроз.

Інтеграція різних підходів

З метою покращення захисту критичної інфраструктури, інтеграція різних підходів та методів стає важливою. Комбінування методів виявлення загроз (IDS) та запобігання загрозам (IPS) дає змогу створити більш комплексну і надійну систему захисту. Кожен із цих методів має свої сильні сторони: IDS ефективні для виявлення потенційних загроз шляхом моніторингу мережевого трафіку та аналізу логів, тоді як IPS можуть активно втручатися для блокування або пом'якшення загроз у реальному часі. Формально, інтеграцію можна навести як зважену суму впливів кожного компонента системи захисту:

$$S_{total} = \alpha \cdot S_{IDS} + \beta \cdot S_{IPS} \quad (7)$$

де α та β – вагові коефіцієнти, що відображають важливість кожного компоненту.

Ці вагові коефіцієнти визначають, наскільки важливим є кожен компонент у загальній системі захисту. Наприклад, якщо IDS мають вищу точність виявлення загроз, ваговий коефіцієнт α може бути більшим, щоб відобразити цей факт. З іншого боку, якщо IPS можуть ефективно блокувати загрози в реальному часі, ваговий коефіцієнт β також буде високим. Визначення оптимальних значень α та β є важливим завданням, яке залежить від специфічних вимог та умов експлуатації системи.

Основні компоненти кіберзахисту

Кіберзахист, або захист інформації в кіберпросторі, складається з різних компонентів, включно з програмним захистом, апаратним захистом та іншими. Ось кілька основних компонентів кіберзахисту:

1. *Програмний захист* (Software Security) включає розробку та використання програмного забезпечення, яке захищає комп'ютерні системи від шкідливих програм, вірусів, вразливостей та інших загроз (антивірусні програми, файрволи, програми виявлення та усунення шкідливого програмного забезпечення тощо).

2. *Апаратний захист* (Hardware Security) охоплює фізичні заходи безпеки, такі як захист апаратних пристроїв від несанкціонованого доступу, фізичний контроль доступу до серверних приміщень тощо (технології шифрування даних на рівні апаратури,

апаратний модуль безпеки (TPM), фізичні замки та ключі тощо).

3. *Мережевий захист* (Network Security) спрямований на захист мережевої інфраструктури від несанкціонованого доступу, атак та перехоплення даних (такі заходи, як встановлення брандмауерів, виявлення та запобігання вторгненням, шифрування мережевого трафіку тощо).

4. *Політики безпеки* (Security Policies), що встановлюють правила та процедури, які регулюють доступ до інформації, управління паролями, використання привілеїв тощо (політики доступу, правила роботи з даними та інші процедури безпеки, що визначаються підприємством (установою, організацією).

5. *Підготовка персоналу* (Education and Awareness) передбачає забезпечення навчання персоналу та користувачів щодо загроз кібербезпеці, процедур безпеки та заходів безпеки інформації (тренінги, вправи та інформаційні кампанії щодо кібербезпеки).

Ці компоненти і багато інших спільно створюють ефективну систему кіберзахисту, яка допомагає захищати інформацію та інфраструктуру від кіберзагроз [6].

Нові вимоги та стратегії кібербезпеки

Розвиток і впровадження сучасних технологій кіберзахисту складаються з досліджень та розроблень новітніх методів й інструментів кіберзахисту, таких як штучний інтелект, машинне навчання, блокчейн, впровадження інтелектуальних систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS) для реагування на загрози в реальному часі. Розглянемо деякі з них:

Мережева безпека та моніторинг. Розроблення методів інтеграції технологій мережевої безпеки та аналітики для ефективного виявлення та відстеження аномальної активності в мережах критичної інфраструктури є одним із головних напрямів. Застосування аналізу поведінки користувачів і машинне навчання для виявлення підозрілих дій та атак в мережах дає змогу значно підвищити рівень захисту. Наприклад, використання алгоритмів машинного навчання для аналізу великого обсягу даних може виявити нетипову активність, що може вказувати на потенційні кіберзагрози.

Розробка кіберстратегій національного та міжнародного рівнів включає визначення стратегічних цілей та пріоритетів у сфері кібербезпеки на рівні держави, що є важливим завданням для забезпечення надійного кіберзахисту. Координація між різними галузями та установами для ефективного впровадження заходів із кібербезпеки та обміну інформацією про загрози сприяє створенню цілісної системи захисту. Співпраця на міжнародному рівні для розробки стандартів, договорів та механізмів спільної реакції на кіберзагрози допомагає уніфікувати підходи до кібербезпеки та забезпечити захист на глобальному рівні. Національні кіберстратегії містять розроблення політик, стандартів та протоколів, які визначають підходи до кібербезпеки на рівні держави, включно із законодавчою базою, створенням органів кібербезпеки, фінансуванням та ресурсами, навчання й підвищення кваліфікації. Міжнародна співпраця є головним елементом забезпечення кібербезпеки на глобальному рівні разом із розробкою міжнародних стандартів, підписанням міжнародних договорів та угод про співпрацю у сфері кібербезпеки, участю у роботі міжнародних організацій, таких як ООН, НАТО, ЄС, обміном досвідом та інформацією. Перевагами кіберстратегій є покращення координації, підвищення стійкості, обмін найкращими практиками, зменшення ризиків. Викликами, що виникають під час реалізації кіберстратегій можуть бути складність координації, фінансові ресурси, постійна адаптація, політичні бар'єри. Розроблення та впровадження національних і міжнародних кіберстратегій є основними для забезпечення безпеки критичної інфраструктури. Співпраця між державними органами, приватним сектором та міжнародними організаціями дає змогу створити ефективну систему захисту від кіберзагроз. Незважаючи на виклики, спільні зусилля у сфері кібербезпеки сприяють зниженню ризиків і забезпеченню стабільності та безпеки у сучасному цифровому світі.

Взаємодія між секторами

Взаємодія між різними секторами в сфері кібербезпеки критичної інфраструктури є головним чинником для забезпечення ефективного захисту від кіберзагроз [7]. Нижче наведено деякі аспекти цієї взаємодії:

1. Співпраця між державними установами, приватним сектором та науковими установами передбачає обмін інформацією та кращими практиками щодо виявлення, аналізу та відвернення кіберзагроз; спільну розробку та впровадження технологічних рішень і таких методів кіберзахисту, як алгоритми виявлення загроз, програмне забезпечення безпеки та системи моніторингу; організацію тренінгів, семінарів та конференцій для обміну знаннями та підвищення кваліфікації фахівців у галузі кібербезпеки. Взаємодія між цими секторами сприяє створенню більш надійної системи захисту та покращує готовність до реагування на сучасні загрози. Участь різних галузей дає змогу забезпечити багатосторонній підхід до вирішення проблем кібербезпеки, зокрема, через використання передових технологій та методологій. Державні установи можуть надавати необхідні ресурси та регуляторну підтримку, тоді як приватний сектор забезпечує технологічні інновації та практичне застосування розробок. Наукові установи, зі свого боку, можуть проводити фундаментальні дослідження та аналізувати нові загрози, а також розробляти нові підходи до кіберзахисту. Разом ці зусилля створюють синергетичний ефект, що сприяє підвищенню загального рівня кібербезпеки та стійкості критичної інфраструктури.

2. Роль міжнародних організацій та стандартів є ключовою для забезпечення координації та ефективності заходів захисту на глобальному рівні. Розробка та впровадження міжнародних стандартів та нормативних документів у галузі кібербезпеки

сприяють уніфікації підходів, що дає змогу державам і організаціям використовувати узгоджені методики й процедури для виявлення, реагування та запобігання кіберзагрозам. Такі стандарти, як ISO/IEC 27001, надають загальні межі для управління інформаційною безпекою, що є основою для формування ефективної політики кіберзахисту. Створення платформ й інструментів для співпраці між державами у виявленні та відповіді на міжнародні кіберзагрози допомагає об'єднати зусилля для більш ефективного захисту. Наприклад, платформи типу FIRST (Forum of Incident Response and Security Teams) забезпечують обмін інформацією про інциденти та сприяють координації дій між національними командами реагування на комп'ютерні інциденти (CERTs). Організація міжнародних форумів та ініціатив для обговорення та розв'язання глобальних проблем у сфері кібербезпеки є важливим кроком для розвитку міжнародної співпраці. Такі заходи, як конференції Black Hat, RSA Conference, та інші, дають змогу експертам із різних країн обмінюватися досвідом, аналізувати новітні загрози та розробляти спільні стратегії захисту. Важливою є також роль міжнародних організацій, таких як ООН, НАТО, ЄС, у формуванні глобальної політики кібербезпеки та розробці відповідних нормативних актів. Вони сприяють об'єднанню зусиль країн-членів у боротьбі з кіберзагрозами, забезпечуючи координацію та підтримку на високому рівні. Спільні навчання та тренування, організовані під егідою цих організацій, допомагають підвищити рівень готовності до кіберінцидентів та забезпечують обмін найкращими практиками між країнами. У цілому, міжнародна співпраця та стандартизація у сфері кібербезпеки є невід'ємними елементами для забезпечення стійкості та захисту критичної інфраструктури на глобальному рівні.

3. Інтеграція новітніх технологій. Впровадження таких технологій, як *блокчейн*, дає змогу забезпечити прозорість і безпеку транзакцій, що є важливим для критичних інфраструктур. Блокчейн, завдяки своїй децентралізованій природі та криптографічним методам захисту, мінімізує ризики несанкціонованого доступу та підробки даних, що робить його ідеальним для захисту чутливих даних у фінансових системах, електронному голосуванні та інших критичних сферах. *Штучний інтелект* (далі – ШІ) і машинне навчання допомагають у прогнозуванні та виявленні нових типів загроз, а також у створенні адаптивних систем захисту. Застосування ШІ допомагає аналізувати великі обсяги даних у режимі реального часу, виявляючи аномалії та потенційні атаки, що можуть залишитися непоміченими традиційними методами. Алгоритми машинного навчання, здатні самонавчатись на основі нових даних про загрози, забезпечують постійне оновлення та вдосконалення систем кіберзахисту. Крім того, ШІ можна використовувати для автоматизації реагування на інциденти, що значно зменшує час реакції на кібератаки та мінімізує можливі збитки. Інші інноваційні технології, такі як *Інтернет речей* (далі – IoT) та *квантові обчислення*, також мають потенціал для підвищення рівня безпеки критичних інфраструктур. IoT допомагає створювати розумні системи моніторингу та управління, які можуть виявляти та реагувати на загрози в режимі реального часу. Квантові обчислення, з їхньою надзвичайною обчислювальною потужністю, відкривають нові горизонти для розробки квантовостійких алгоритмів шифрування, що можуть протистояти навіть найпотужнішим кібератакам майбутнього. Усі ці технології, інтегровані у єдину систему кібербезпеки, здатні забезпечити більш ефективний захист критичної інфраструктури від постійно еволюціонуючих загроз.

4. Залучення громадськості та підвищення обізнаності. Одним із важливих аспектів кібербезпеки є навчання та інформування громадськості щодо існуючих загроз та методів захисту. Проведення інформаційних кампаній та освітніх програм сприяє формуванню кіберграмотності серед населення, що є важливим для загального рівня кібербезпеки. Інформаційні кампанії можуть здійснюватися через розповсюдження матеріалів через соціальні медіа, телебачення, радіо та інші канали комунікації для підвищення обізнаності про потенційні кіберзагрози й способи їх уникнення. Освітні програми, спрямовані на різні вікові групи, можуть допомогти сформувати розуміння основних принципів кібергігієни, таких як створення надійних паролів, розпізнавання фішингових атак і захист особистих даних. Крім того, спеціальні курси та тренінги для фахівців різних галузей допоможуть підвищити їхню компетентність у сфері кібербезпеки, що є необхідним для захисту критичної інфраструктури. Важливим елементом є також співпраця з громадськими організаціями та місцевими спільнотами для розробки та впровадження заходів, спрямованих на підвищення рівня кібербезпеки на місцевому рівні. Така взаємодія сприяє створенню стійкого кіберпростору, де кожен член суспільства усвідомлює свою роль у забезпеченні безпеки цифрового середовища. Успішна реалізація цих заходів не лише підвищує рівень кібербезпеки, але й сприяє зміцненню довіри до цифрових технологій, що є ключовим фактором для їх подальшого розвитку та інтеграції в повсякденне життя.

5. Регулярне оновлення та тестування систем захисту. Постійний моніторинг та аналіз стану систем кібербезпеки, а також проведення регулярних тестів на проникнення допомагають виявляти та усувати вразливості до того, як вони будуть використані зловмисниками. Це забезпечує високу готовність систем до реагування на нові загрози та мінімізує ризики. Підтримка актуальності програмного забезпечення, використання передових методів захисту, таких як багатофакторна автентифікація та шифрування даних, є ключовими аспектами цього процесу. Ці механізми співпраці та взаємодії дають змогу посилювати взаємодію між різними секторами та забезпечувати комплексний підхід до захисту критичної інфраструктури від кіберзагроз. Важливо, щоб ця взаємодія була організованою, ефективною та максимально координованою для досягнення найвищого рівня кібербезпеки. Тільки завдяки спільним зусиллям можливо створити стійку та

безпечну інфраструктуру, здатну протистояти сучасним і майбутнім кіберзагрозам. Регулярні навчання та підвищення обізнаності співробітників також є важливою складовою цього процесу, оскільки людський фактор часто є слабкою ланкою в системах безпеки. Отже, постійне вдосконалення технологічних рішень, підтримка актуальності знань та навичок персоналу є необхідними умовами для забезпечення високого рівня захисту критичної інфраструктури.

Перспективи та виклики

Розвиток квантових технологій та зміна кіберзагроз постійно впливають на кібербезпеку критичної інфраструктури.

Розвиток квантових технологій.

Перспективи. Квантові технології можуть забезпечити нові методи шифрування, що стійкі до атак з боку квантових комп'ютерів, забезпечуючи вищий рівень кібербезпеки. Використання квантових ключів для шифрування даних може значно зменшити ризик несанкціонованого доступу до критичних систем. Крім того, квантові комп'ютери можуть підвищити ефективність обробки великих обсягів даних, що є важливим для аналізу загроз та виявлення аномалій у режимі реального часу.

Виклики. З появою квантових комп'ютерів може збільшитися потенціал для розшифрування зашифрованих даних, що вимагає розробки нових квантовостійких алгоритмів шифрування. Потенційні зловмисники можуть використовувати квантові комп'ютери для розшифровки поточних методів шифрування, що підвищує необхідність у розробці нових технологій захисту. Інфраструктурі також потрібно буде адаптуватися до нових вимог безпеки, що пов'язано зі значними фінансовими та технічними витратами.

Зміна кіберзагроз та постійний розвиток технологій.

Перспективи. Завдяки швидкому розвитку технологій, можливо виявлення та відвернення нових кіберзагроз, використовуючи штучний інтелект, машинне навчання та аналіз великих обсягів даних. Інтеграція цих технологій у системи безпеки дає змогу створювати більш адаптивні та проактивні методи захисту, що можуть виявляти загрози на ранніх стадіях і автоматично реагувати на них.

Виклики. Зміна кіберзагроз та поява нових технологій може створювати нові вразливості, на які необхідно реагувати шляхом постійного оновлення та удосконалення захисту. Нові методи атаки, такі як атаки на основі штучного інтелекту, вимагають розробки складніших систем захисту, які здатні ефективно протистояти цим загрозам. Крім того, швидке впровадження нових технологій може призвести до виникнення нових типів вразливостей, які важко передбачити та контролювати.

Загалом, розвиток квантових технологій та постійна зміна кіберзагроз ставлять перед сучасними дослідниками та експертами в області кібербезпеки значні виклики. Проте наявність нових технологій також відкриває нові можливості для покращення захисту критичної інфраструктури. Для ефективного вирішення цих викликів необхідна постійна інноваційна діяльність та співпраця між різними секторами, включно із державними установами, приватним сектором та науковою спільнотою. Спільні зусилля у розробці нових стандартів, технологій та політик сприятимуть створенню більш безпечного й стійкого кіберпростору, що здатен протистояти сучасним і майбутнім загрозам.

Висновки й перспективи подальших досліджень

Висновки та перспективи подальших досліджень вказують на те, що кіберборотьба стає невід'ємною складовою безпеки критичної інфраструктури в умовах цифрової епохи. Для забезпечення стійкості та безпеки цих систем необхідно постійно вдосконалювати стратегії кібербезпеки, активно співпрацювати між різними секторами економіки та постійно удосконалювати технології захисту. Тільки завдяки цим заходам можна гарантувати стабільність критичної інфраструктури в умовах постійно зростаючих кіберзагроз. Розвиток сучасних технологій кібербезпеки та співпраця між різними галузями економіки та державами стануть головними чинниками у запобіганні та протистоянні кіберзагрозам у майбутньому.

Для подальших досліджень важливо зосередитися на аналізі новітніх тенденцій у сфері кібербезпеки, розробці інноваційних методів захисту та поглибленому вивченні впливу кіберзагроз на суспільство та економіку. Окрім цього, необхідно розробляти комплексні підходи до оцінки ризиків та управління ними, що дозволить підвищити ефективність виявлення та нейтралізації кіберзагроз. Використання штучного інтелекту та машинного навчання у сфері кібербезпеки відкриває нові можливості для прогнозування атак та розробки ефективних контрзаходів. Також важливо надавати увагу підготовці кадрів, що спеціалізуються на кібербезпеці, шляхом проведення навчальних програм та тренінгів, що сприятиме підвищенню кваліфікації та обізнаності працівників. Перспективами подальших досліджень також є вивчення впливу міжнародної співпраці на покращення захисту критичної інфраструктури. Створення спільних стандартів та протоколів, а також обмін інформацією між країнами сприятиме підвищенню рівня глобальної кібербезпеки. Важливо також досліджувати питання захисту персональних даних у контексті кібербезпеки, адже зростання кількості даних, що обробляються та зберігаються, вимагає нових підходів до їх захисту.

Загалом, забезпечення кібербезпеки критичної інфраструктури є складним та багатогранним завданням, яке вимагає постійного вдосконалення методів захисту та активної співпраці на всіх рівнях. Лише комплексний підхід та інноваційні технології дадуть змогу ефективно протистояти кіберзагрозам і забезпечити надійний захист критичних систем в умовах цифрового віку.

Список бібліографічних посилань

1. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 29.07.2024). **2. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури**… Постанова КМУ від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (дата звернення: 29.07.2024). **3. Машталір В. В., Гук О. М., Мурасов Р. К., Фараон С. І., Лоза В. В.** Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2024. № 1(49). DOI: https://doi.org/10.33099/2311-7249/2024-49-1-93-104. **4. Гук О. М., Мурасов Р. К., Фараон С. І., Толмачов І. В.** Стратегії кібербезпеки для захисту критичної інфраструктури: виклики та перспективи. *Матеріали міжнар. наук.-практ. інтернет-конф.* «*Інформаційне суспільство…*». Вип. 86. URL: http://www.konferenciaonline.org.ua/ua/article/id-1649/ (дата звернення: 29.07.2024). **5. Поліковська Ю.** Кількість зареєстрованих в Україні кіберінцидентів у 2023 році зросла на 62,5%. 12.01.2024. URL: https://ms.detector.media/internet/post/33956/2024-01-12-kilkist-zareiestrovanykh-v-ukraini-kiberintsydentiv-u-2023-rotsi-zrosla-na-625-derzhspetszvyazku/ (дата звернення: 29.07.2024). **6. Хомік М. М.** Проблемні аспекти управління екологічною безпекою при застосуванні ЗСУ під час НС і в районі ООС. *Зб. наук. праць ЦВСС НУОУ.* 2020. №2-66. С. 47–51. DOI: https://doi.org/10.33099/2304-2745/2019-2-66/47-51. **7. Мурасов Р., Мельник Я.** Результати оцінювання загроз критичній інфраструктурі методом експертного оцінювання. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2024. №3(48). С. 83–88. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-83-88.
8. Мурасов Р., Машталір В. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2024. № 1(49). С. 93–104. DOI: https://doi.org/10.33099/2311-7249/2024-49-1-93-104. **9. Ільєнко А., Ільєнко С., Яковенко О., Галич Є., Павленко В.** Перспективи інтеграції штучного інтелекту в системи виявлення загроз. *Кібербезпека: освіта, наука, техніка.* 2024. № 1(25). С. 318–329. DOI: https://doi.org/10.28925/2663-4023.2024.25.318329. **10. Котенко Д., Хапонін Ю.** Штучний інтелект у системах виявлення і запобігання кібератакам. *Сучасні технології в машинобудуванні та транспорті*. 2024. № 1(14). С. 48–55. DOI: https://doi.org/10.32347/uwt.2024.14.1203. **11. Данчук В., Данчук М.** Інтеграція блокчейн-технологій у системи забезпечення кібербезпеки для об'єктів критичної інфраструктури: перспективи та виклики. *Вісник ЧДТУ.* 2024. № 4(29). С. 43–52. DOI: https://doi.org/10.62660/bcstu/4.2024.43 (дата звернення: 24.09.2025).

CRITICAL INFRASTRUCTURE CYBERSECURITY: ASSESSMENT AND MANAGEMENT OF CYBERATTACK RISKS

MURASOV Rustam, Doctor of Technical Sciences, National Defence University of Ukraine, Kyiv, Ukraine

PHARAON Serhiy, Doctor of Philosophy, National Defence University of Ukraine, Kyiv, Ukraine

HUK Oleksandr, Doctor of Philosophy, National Defence University of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *In the modern digital age, critical infrastructure, including electric power, transportation, communications, and financial systems, is becoming a growing target for cybercriminals and state actors. Ensuring the security of these systems is becoming a critical task in the ongoing digital conflict. This article examines the concept of cyber combat as a second front in the protection of critical infrastructure.* ***The purpose of this article*** *is to examine the contemporary challenges and threats associated with the cybersecurity of critical infrastructure, as well as to identify the strategies and technologies necessary for its effective protection.*

Research methods. *The methods of analysis and synthesis were applied in writing the article to consider contemporary approaches to cybersecurity strategy and technologies, including the use of artificial intelligence, machine learning, and other innovative methods. This methodological approach enables a comprehensive examination of the strategies and technologies required for the effective protection of critical infrastructures.*

Literature review. *Recent publications on the protection of critical infrastructure highlight the relevance of this issue in contemporary scientific discourse, particularly in the context of Russian aggression. Key researchers, such as M. M. Khomik, S. M. Chumachenko, O. V. Avramenko, and T. L. Kurtseitov, focus on technogenic safety and the consequences of such emergencies. However, it is important to note that their research primarily focuses on technogenic safety and response to emergency situations, without giving sufficient attention to cybersecurity. Additionally, separate studies on regulatory and legal support are also important, although they are not considered in this context. It is crucial to recognise that until now, cybersecurity has been viewed as a separate component of internet provision or financial security. However, in the modern world, characterised by globalisation, digitalisation, and the implementation of cybernetics in the management of complex systems, cybersecurity becomes an integral component of critical infrastructure security. This opens up broad opportunities for further research and the development of strategies to protect critical infrastructure from cyber threats.*

Research results. *The main concepts and definitions of cyber threats (cyber threat, T), vulnerabilities (vulnerability, V), and the probability of a successful attack (probability of successful attack, Pa) are discussed. Risk and protection models are developed, including a risk model that assesses the risk of cyberattacks on critical infrastructure based on the probability and impact of the attacks. The use of machine learning to improve the efficiency of threat detection and prevention is also explored. Integration of different approaches and methods, such as combining intrusion*

detection systems (IDS) and intrusion prevention systems (IPS), is formalised to enhance the protection of critical infrastructure.

Research novelty. *The scientific novelty of the article includes the refinement and specification of existing data, extending their application to new objects and systems, and proposing new methods for detecting and preventing cyber threats. This involves the development and implementation of innovative methods and tools for cybersecurity, such as artificial intelligence, machine learning, and blockchain, as well as the introduction of intelligent intrusion detection (IDS) and intrusion prevention (IPS) systems for real-time threat response.*

Theoretical and practical significance*. The theoretical and practical significance of the article lies in the fact that the obtained results can be used to improve national security and develop strategies for protecting critical infrastructure in the field of technical sciences. The research results can be applied to enhance the protection of critical infrastructure objects from cyber threats by implementing modern cybersecurity technologies and approaches. This will reduce the vulnerability of information networks and systems, ensuring a more effective response to cyber threats. The practical significance of the obtained results lies in their potential application for developing security policies, training personnel, and creating software and hardware for cybersecurity.*

Conclusions and future work. *The conclusions and prospects for further research indicate that cyber combat is becoming an integral component of critical infrastructure security in the digital age. To ensure the resilience and security of these systems, it is necessary to continuously improve cybersecurity strategies, actively collaborate between different economic sectors, and constantly enhance protection technologies. Only through these measures can the stability of critical infrastructure be guaranteed in the face of growing cyber threats. The development of modern cybersecurity technologies and collaboration between various sectors of the economy and states will be key factors in preventing and countering cyber threats in the future. Future research should focus on analysing the latest trends in cybersecurity, developing innovative protection methods, and deepening the study of the impact of cyber threats on society and the economy.*

Keywords*: cyber combat, national security, critical infrastructure protection, cybersecurity strategies, cyber security, cyber defence.*

References

1. ***On Critical Infrastructure*** *[online],* (2021). *Law of Ukraine No. 1882-IX, 16 November.* Available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text [Accessed: 29 July 2024]. **2.** ***On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Objects*** *[online],* (2023). *Resolution No. 415 of 28 April 2023.* Available at: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text [Accessed: 29 July 2024]. **3. Mashtalir, V. V., Huk, O. M., Murasov, R. K., Faraon, S. I. and Loza, V. V.,** (2024). *Cyber warfare under armed confrontation: analysis, strategies, and challenges. Modern Information Technologies in the Sphere of Security and Defence*, 1(49). DOI: https://doi.org/10.33099/2311-7249/2024-49-1-93-104.

4. Huk, O. M., Murasov, R. K., Faraon, S. I. and Tolmachov, I. V. (2024) *Cybersecurity strategies for critical infrastructure protection: challenges and prospects. Proceedings of the International Scientific and Practical Online Conference «Information Society…»*, Is. 86. Available at: http://www.konferenciaonline.org.ua/ua/article/id-1649/ [Accessed: 29 July 2024]. **5. Polikovska, Yu.,** (2024). *The number of registered cyber incidents in Ukraine increased by 62.5% in 2023.* 12 January. Available at: https://ms.detector.media/internet/post/33956/2024-01-12-kilkist-zareiestrovanykh-v-ukraini-kiberintsydentiv-u-2023-rotsi-zrosla-na-625-derzhspetszvyazku/ [Accessed: 29 July 2024]. **6. Khomik, M. M.,** (2020). *Problematic aspects of environmental safety management during the use of the Armed Forces of Ukraine in emergencies and in the JFO area. Collection of Scientific Works of the Center for Military-Strategic Studies of NDU of Ukraine*, 2(66), 47-51. DOI: https://doi.org/10.33099/2304-2745/2019-2-66/47-51.

7. Murasov, R. and Melnyk, Ya., (2024). *Results of assessing threats to critical infrastructure using the expert evaluation method. Modern Information Technologies in the Sphere of Security and Defence*, 3(48), 83-88. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-83-88.

8. Murasov, R. and Mashtalir, V., (2024) *Cyber warfare under armed confrontation: analysis, strategies, and challenges. Modern Information Technologies in the Sphere of Security and Defence*, 1(49), 93-104. DOI: https://doi.org/10.33099/2311-7249/2024-49-1-93-104. **9. Ilienko, A., Ilienko, S., Yakovenko, O., Halych, Ye. and Pavlenko, V.,** (2024). *Prospects for integrating artificial intelligence into threat detection systems. Cybersecurity: Education, Science, Technique*, 1(25), 318-329. DOI: https://doi.org/10.28925/2663-4023.2024.25.318329. **10. Kotenko, D. and Khaponin, Yu.,** (2024). *Artificial intelligence in intrusion detection and prevention systems. Modern Technologies in Mechanical Engineering and Transport*, 1(14), 48-55. DOI: https://doi.org/10.32347/uwt.2024.14.1203.

11. Danchuk, V. and Danchuk, M., (2024). *Integration of blockchain technologies into cybersecurity systems for critical infrastructure: prospects and challenges. Bulletin of Cherkasy State Technological University*, 4(29), 43–52. DOI: https://doi.org/10.62660/bcstu/4.2024.43 [Accessed: 24 September 2025].

Рукопис надійшов до редакції 10.09.2025
Рукопис прийнято до друку після рецензування 19.11.2025
Дата публікації 30.12.2025