Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ**:**
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«_» _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*

на тему: «Методи протидії вторгненням на об’єкти критичної інфраструктури»

Виконавець: студент ІІ курсу, групи КБм-22

_____ **Нікіта МІЩЕНКО**
(підпис) (ім’я, прізвище)

	Ім’я, прізвище	**Підпис**
Керівник	Сергій ТОЛЮПА	
Нормоконтроль	Юрій БАБЕНКО	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«25» жовтня 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека і захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача **КБм-22** (група) **Міщенка Нікіти Андрійовича** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Методи протидії вторгненням на об'єкти критичної інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес забезпечення захисту об'єктів критичної інфраструктури від вразливостей.
Предмет досліджень	методи та технології виявлення, запобігання та нейтралізації вразливостей на об'єкти критичної інфраструктури.
Мета	Обґрунтування ефективних методів протидії вразливостям на об'єкти критичної інфраструктури з метою зменшення ризиків виникнення загроз.
Вихідні дані для проведення роботи	Нормативно-правова база, існуючі методи та системи протидії атакам, аналіз загроз та вразливостей

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна концепція створення кіберсистем, що використовують біоміметичні алгоритми, для динамічного аналізу інформаційних потоків і виявлення невідомих загроз.

Практична цінність можливість використання розробленої експертної системи для оптимізації процесу вибору найефективнішого методу, що дозволить знизити витрати на забезпечення кібербезпеки при одночасному підвищенні рівня захисту об’єкту.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Уточнення постановки задачі	25.10.2024 – 20.01.2025
Аналіз літературних джерел	21.01.2025 – 02.02.2025
Аналіз та класифікація вразливостей	03.02.2025 – 10.02.2025
Огляд існуючих методів та засобів захисту	11.02.2025 – 15.02.2025
Визначення мети та ідеї методу на основі біоміметичних алгоритмів	16.02.2025 – 26.02.2025
Проведення дослідження біоміметичних підходів	27.02.2025 – 20.03.2025
Порівняння представлених методів протидії вторгенням	21.03.2025 – 10.04.2025
Проведення експертного оцінювання ефективності біоміметичних підходів	11.04.2025 – 01.05.2025
Вибір оптимального методу захисту	02.05.2025 – 10.05.2025
Оформлення пояснювальної записки	11.05.2025 – 15.05.2025
Подача пакетів документів на розгляд ЕК	15.05.2025 – 19.05.2025

Завдання видав _____ Сергій ТОЛЮПА
(підпис) (ім’я, прізвище)

Завдання прийняв до виконання _____ Нікіта МІЩЕНКО
(підпис) (ім’я, прізвище)

Дата видачі завдання: 25.10.2024 р.

Термін подання кваліфікаційної роботи до ЕК 19.05.2025 р.

УДК 004.027 : 004.056.5

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної магістерської роботи «Методи протидії вразливостям на об’єкти критичної інфраструктури»: 71 сторінка, 8 рисунків та 10 таблиць. 32 літературних джерела.

Об’єкт дослідження – процес забезпечення захисту об’єктів критичної інфраструктури від вразливостей.

Мета роботи – обґрунтування ефективних методів протидії вразливостям на об’єктах критичної інфраструктури з метою зменшення ризиків виникнення загроз та забезпечення стійкості до різних видів атак.

Методи дослідження базуються на комплексному підході, що враховує специфіку об’єктів критичної інфраструктури та види загроз.

У роботі досліджено сучасні методіи протидії вразливостям на об’єкти критичної інфраструктури та за допомогою експертного оцінювання і багатокритеріального аналізу визначено найефективніший метод захисту об’єктів критичної інфраструктури.

Наукова новизна роботи полягає у концепції створення кіберсистем, що використовують біоміметичні алгоритми, для динамічного аналізу інформаційних потоків і виявлення невідомих загроз.

Актуальність теми: наукові розробки у цій галузі можуть значно підвищити здатність країни протистояти зовнішнім і внутрішнім викликам, а головне підвищить стійкість до сучасних вразливостей, мінімізувавши можливі втрати і значно допоможе швидко відновити об’єкти після атак.

Ключові слова: програмне забезпечення, об’єкт критичної інфраструктуру, кібербезпека, інформаційна безпека, оцінка ефективності, вразливості, вторгнення, захист об’єктів, методи протидії.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ПЗ – Програмне забезпечення;
КСЗІ – Комплексна система захисту інформації;
ОКІ – Об’єкт критичної інфраструктури;
ІБ – Інформаційна безпека;
БД – Бази даних;
АС – Автоматизована система;
ISO – International Organization for Standardization;
ЗЗ – Засоби захисту;
DDoS – Distributed Denial-of-Service;
БТ – Біометричні технології;
СВВ – Система виявлення вторгнень;
SCADA – Supervisory Control And Data Acquisition;
DQL – Deep Q-Learning;
NIDS – Network Intrusion Detection System;
SIEM – Security Information and Event Management;
IoT – Internet of Things;
PSO – Particle Swarm Optimization;
SOC – Security Operations Centers;
GA – Genetic Algorithms;
GWO – Gray Wolf Optimizer;
BA – Bat Algorithm;
OPA – Orca Predator Algorithm;
WSM – Weighted Sum Method;
CR – Consistency Ratio.

ЗМІСТ

ВСТУП

У сучасному світі критична інфраструктура є основою функціонування будь-якої держави, забезпечуючи стабільну роботу енергетичних, водопостачальних, транспортних, інформаційних та інших важливих систем. Однак, зростання глобальних загроз, таких як кібернапади, терористичні акти та військові агресії, ставить під загрозу безпеку цих об’єктів.

Атаки на критичну інфраструктуру можуть призвести до серйозних економічних та соціальних наслідків, а також до порушення нормального функціонування суспільства.

Зважаючи на це, розробка ефективних методів протидії атакам на об’єкти критичної інфраструктури є надзвичайно важливою для забезпечення національної безпеки, стабільності економіки та захисту життєво важливих послуг. Вивчення та вдосконалення технологій і стратегій, що дозволяють знижувати ризики і підвищувати стійкість до атак, є пріоритетними завданнями в умовах сучасних глобальних викликів.

Актуальність теми: Наявність вразливих місць у системах управління та захисту критичної інфраструктури робить країну уразливою до таких загроз, тому важливість дослідження ефективних методів протидії цим вразливостям стає ще більш очевидною.

Наукові розробки у цій галузі можуть значно підвищити здатність країни протистояти зовнішнім і внутрішнім викликам, мінімізувати можливі втрати і допомогти швидко відновлювати об’єкти критичної інфраструктури після атак.

Мета магістерської роботи: Розробка та обґрунтування ефективних методів протидії вразливостям на об’єкти критичної інфраструктури з метою підвищення рівня їх безпеки, зменшення ризиків виникнення загроз та забезпечення стійкості до різних видів атак, таких як кібернетичні, фізичні та комбіновані.

Завдання магістерської роботи:

– Аналіз сучасного стану захисту об’єктів критичної інфраструктури;

– Провести класифікацію загроз та вразливостей, оцінити ризики;

– Проаналізувати методи протидії вразливостям на ОКІ;

– Оцінити ефективність запропонованих методів;

– Дослідити, провести експертне оцінювання і визначити найефективніший метод для захисту ОКІ.

Об’єкт дослідження: процес забезпечення захисту об’єктів критичної інфраструктури від вразливостей.

Предмет дослідження: методи та технології виявлення, запобігання та нейтралізації вразливостей на об’єкти критичної інфраструктури.

У роботі використані методи системного аналізу, експертного оцінювання, багатокритеріального аналізу.

Наукова новизна роботи полягає у концепції створення кіберсистем, що використовують біоміметичні алгоритми, подібні до еволюційних механізмів, для динамічного аналізу інформаційних потоків і виявлення невідомих загроз.

Практичне значення одержаних результатів полягає в можливості використання розробленої експертної системи для оптимізації процесу вибору найефективнішого методу, що дозволить знизити витрати на забезпечення кібербезпеки при одночасному підвищенні рівня захисту об’єктів критичної інфраструктури.

Апробація результатів роботи:

Толюпа С.В., Міщенко Н.А. Методи протидії вразливостям на об’єкти критичної інфраструктури. VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSICS)».

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Поняття та класифікація об'єктів критичної інфраструктури

Об'єкт критичної інфраструктури – це об'єкт, система, її частини або сукупність, що мають значення для економіки, національної безпеки та оборони, а їхнє порушення може завдати шкоди ключовим національним інтересам.

Критична інфраструктура охоплює підприємства та установи різних галузей, зокрема енергетику, хімічну промисловість, транспорт, фінансовий сектор, інформаційні технології, телекомунікації, продовольство, охорону здоров'я та комунальне господарство. Ці об'єкти мають стратегічне значення для забезпечення функціонування економіки, безпеки держави, суспільства і населення. Їх пошкодження або знищення може суттєво вплинути на національну безпеку, оборону, довкілля, а також спричинити значні матеріальні та фінансові втрати та людські жертви [1].

Класифікація об'єктів як критичної інфраструктури здійснюється відповідно до процедури, визначеної Кабінетом Міністрів України. До основних функцій та/або послуг, порушення яких тягне за собою негативні наслідки для національної безпеки України, належать, зокрема: управління та надання критично важливих державних (адміністративних) послуг; енергопостачання (включаючи теплопостачання); водопостачання та санітарія; постачання продуктів харчування; охорона здоров'я; фармацевтична промисловість; виробництво вакцин; стале функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, утримання під вартою; цивільний захист населення та територій, рятувальні служби;

космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність.

Для визначення рівня вимог до захисту об’єктів критичної інфраструктури залежно від їхньої важливості для виконання ключових функцій у межах секторів критичної інфраструктури проводиться їх категоризація за рівнями критичності, встановленими цим Законом. Цю категоризацію виконують секторальні органи у сфері захисту критичної інфраструктури з урахуванням специфіки та норм відповідного секторального законодавства.

Секторальні органи разом із операторами критичної інфраструктури визначають категорії критичності об’єктів у своїх секторах або підсекторах відповідно до Методики категоризації, затвердженої Кабінетом Міністрів України. У банківському та фінансовому секторах цю функцію здійснює Національний банк України, а в інших сферах, що регулюються та контролюються державними органами, категоризацію виконують відповідні державні органи [2].

Встановлюються наступні категорії критичності ОКІ (рис.1.1):

1. Критичність І категорії – особливо важливі об’єкти загальнодержавного значення, що мають сильний вплив на інші об’єкти критичної інфраструктури, порушення роботи яких спричинить кризову ситуацію загальнодержавного значення;

2. Критичність ІІ категорії – цінні об’єкти, порушення роботи яких спричинить кризову ситуацію регіонального значення;

3. Критичність ІІІ категорії – значущі об’єкти, вихід з ладу яких призведе до кризової ситуації місцевого значення.

4. Критичність IV категорії – необхідні об’єкти, переривання роботи яких призведе до виникнення кризової ситуації місцевого значення.

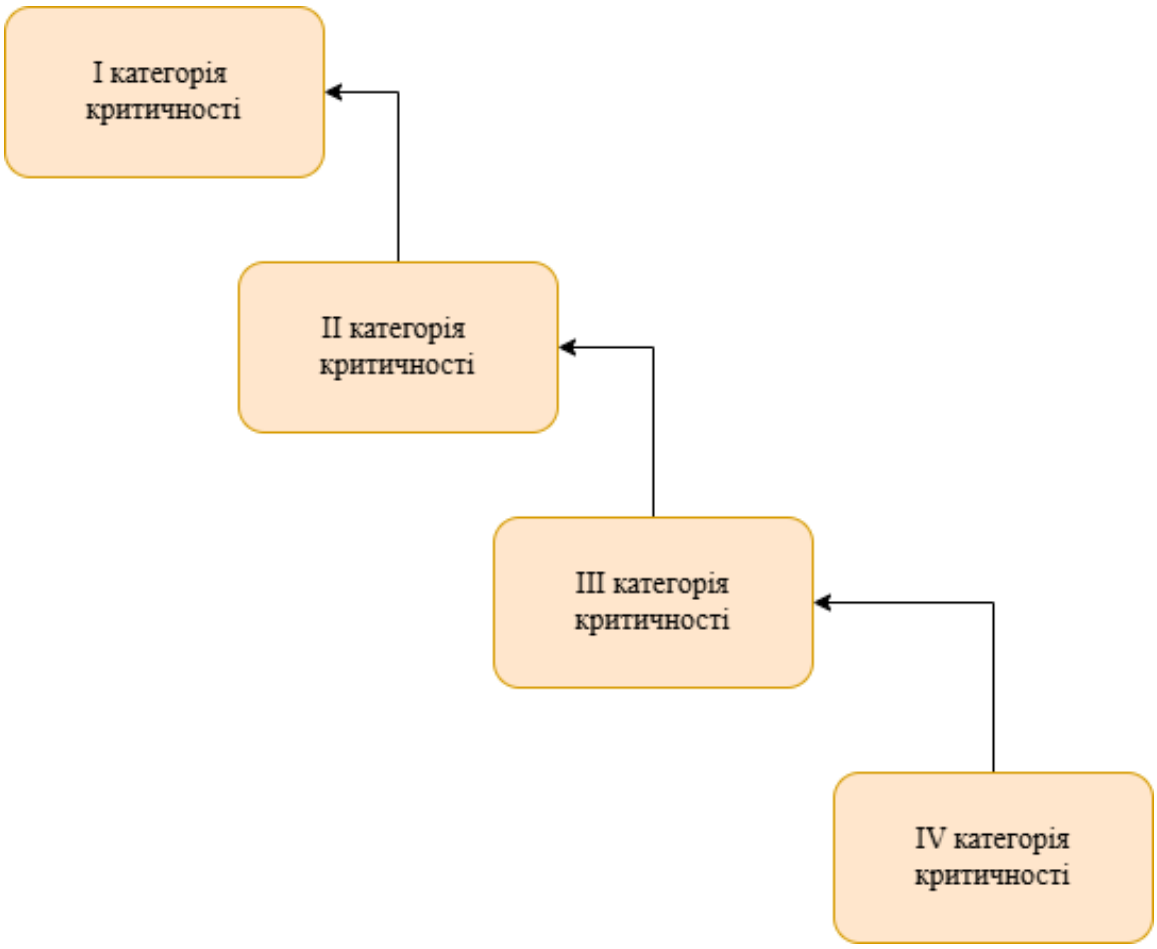

Рисунок 1.1 – Порядок пріорітету категорій критичності

Категорії критичності об’єктів критичної інфраструктури визначають рівень їхнього впливу на національну безпеку, економіку, суспільство та життєдіяльність населення у разі виникнення надзвичайних ситуацій.

Прикладами I категорії критичності, що є найважливішою, можуть виступати об’єкти енергетики, тобто електростанції, стратегічні підстанції тощо, центральні банки, платіжні системи, великі вузли транспортної інфраструктури, національні оператори зв’язку. Втрата працездатності навіть одного об’єкта цієї категорії може впливати на роботу всієї критичної галузі. Вихід з ладу таких об’єктів може призвести до масштабних негативних наслідків для національної безпеки, економіки, функціонування держави, соціальної стабільності та здоров’я/життя значної частини населення. Для II категорії критичності порушення функціонування об’єктів спричиняє суттєві наслідки для регіональної економіки, безпеки, громадського порядку, функціонування

окремих сфер суспільства. Також впливає на забезпечення базових послуг на регіональному рівні. Об’єктами можуть виступати обласні диспетчерські центри електромереж, локальні комунікаційні вузли, водопостачальні підприємства великих міст і регіональні логістичні хаби. ІІІ категорія є категорією помірної критичності об’єктів. Порушення роботи цих об’єктів має локальний вплив, не призводить до критичних наслідків національного чи регіонального рівня, але впливає на життєдіяльність окремих громад, підприємств чи об’єктів соціальної інфраструктури. Це можуть бути міські котельні, локальні системи водопостачання, серверні кімнати муніципальних служб, приватні медичні установи тощо. Для останньої IV категорії критичності, вихід з ладу таких об’єктів не призводить до значних негативних наслідків, можуть вплинути лише на допоміжні чи другорядні процеси певного підприємства чи установи. Об’єктами даної категорії можуть виступати внутрішні корпоративні портали для службового користування, електрощити адміністративних будівель, резервні навчальні платформи, які дублюють основні ресурси, внутрішні системи документообігу підприємств. В Україні офіційно IV категорія може не фігурувати в нормативних документах, однак її часто застосовують у внутрішній класифікації компаній.

1.2. Аналіз основних загроз та вразливостей ОКІ

Для аналізу ключових загроз та потенційних негативних наслідків для об’єктів критичної інфраструктури, а також їх запобігання та прогнозування, оператори таких об’єктів зобов’язані підготувати та подати на затвердження відповідним галузевим органам та функціональному органу у сфері захисту критичної інфраструктури паспорт безпеки для кожного об’єкта.

Паспорт безпеки містить інформацію про ідентифікацію об’єкта, заходи щодо його захисту та безпеки, а також визначає посадових осіб, відповідальних за зв’язок і обмін інформацією із суб’єктами національної системи захисту критичної інфраструктури. Основне призначення паспорта безпеки об’єкта

критичної інфраструктури полягає в систематизації інформації про об’єкт, оцінці рівня його захищеності, фіксації потенційних загроз і вразливостей, а також документуванні заходів щодо забезпечення безпеки. Він слугує офіційним підтвердженням виконання вимог законодавства у сфері кібербезпеки, є основою для планування заходів реагування на інциденти та використовується під час перевірок контролюючих органів, таких як Держспецзв’язок і СБУ. Основні загрози для об’єктів критичної інфраструктури можна поділити на: кіберзагрози, фізичні, внутрішні, економічні й політичні [3].

Кіберзагрози представляють собою віруси та шкідливе програмне забезпечення можуть порушити роботу систем та призвести до втрати даних. Окрім шкідливого ПЗ, до кіберзагроз також можна віднести фішингові атаки, що використовують соціальну інженерію для викрадення конфіденційної інформації, а також DDoS-атаки, які перевантажують ресурси систем, що може спричинити їхню недоступність. Зломи баз даних призводять до витоку критично важливих даних.

Фізичні загрози являють собою терористичні атаки, які можуть бути спрямовані на об’єкти інфраструктури з метою дестабілізації, диверсії, зокрема навмисне пошкодження устаткування або саботаж. Також присутні техногенні аварії через несправність обладнання та його неправильну експлуатацію. Навіть стихійні лиха, такі як землетруси, повені та урагани, можуть неочікованно нагрянути та пошкодити інфраструктуру [4].

Як внутрішні загрози можна виділити некваліфікованих співробітників, які можуть зробити критичні помилки. Окрім некваліфікованих працівників є також працівники, які мають доступ до чутливих даних, вони можуть здійснювати так звані «інсайдерські атаки». Незадоволені або корумповані співробітники можуть навмисно пошкодити систему.

Економічні загрози містять фінансові кризи, наприклад обмеження фінансування на оновлення та підтримку систем. Якщо у внутрішніх загрозах деякі співробітники є корумпованими, то безпосередньо корупція призводить до неефективного управління ресурсами ті їх, можливого зникнення.

В свою чергу політичні загрози представляють собою гібридні війни включаючи кібернетичні атаки та інформаційні кампанії, санкції можуть обмежувати доступ до технологій та ресурсів, а політична нестабільність призводить до непередбачуваних наслідків у сфері безпеки.

Загрози та вразливості об’єктів критичної інфраструктури – це два різні, але взаємопов’язані поняття в контексті безпеки (табл. 1.1) [2].

Таблиця 1.1

Відмінності між загрозами та вразливостями для ОКІ

Критерій	**Загрози ОКІ**	**Вразливості ОКІ**
Визначення	Фактори або події, які можуть спричинити шкоду ОКІ.	Недоліки або слабкі місця системи, що можуть бути використані загрозами.
Джерело	Може бути внутрішнім (людський фактор, технічні несправності) або зовнішнім (хакерські атаки, природні катастрофи).	Виникає через недосконалості в системах захисту, застарілі технології, помилки персоналу.
Вплив	Може реалізуватися у вигляді атаки або інциденту.	Робить систему вразливою до загроз і збільшує ймовірність інциденту.
Залежність	Загрози використовують вразливості для нанесення шкоди.	Вразливості можуть залишатися безпечними, якщо немає відповідних загроз.

Основні вразливості ОКІ можуть включати в себе застарілу інфраструктуру, що являє собою використання обладнання, яке вже не підтримується виробником, а також відсутність модернізації через обмежене фінансування; недостатній рівень кібербезпеки, тобто відсутність сучасних засобів захисту та шифрування даних й використання слабких паролів та недостатній контроль доступу; людський фактор, що демонструє недостатню підготовку персоналу щодо кібербезпеки і використання методів соціальної інженерії для маніпулювання співробітниками; відсутність резервних систем –

недостатня кількість резервних серверів та джерел живлення й відсутність планів аварійного відновлення; низька поінформованість та підготовка персоналу, тобто відсутність регулярних тренінгів з безпеки, окрім цього недостатня кількість навчальних сценаріїв для реагування на кризи.

Атаки на об’єкти критичної інфраструктури можна класифікувати зокрема за методами реалізації, цілями, джерелами та рівнем впливу. Класифікація атак за характером впливу визначає кібератаки та фізичні атаки. Кібератаки представляють собою спробу реалізації інформаційної загрози [9].

Яскравий приклад цьому є DDoS-атаки, що мають на меті виведення з ладу IT-інфраструктури за рахунок перевантаження серверів фіктивними запитами. Для прикладу можна взяти атаки ботнетів на державні портали або фінансові сервіси. Окрім наведених атак існують також фішингові атаки, які шляхом обману користувачів, намагаються отримати доступ до конфіденційної інформації, шкідливі електронні листи дуже часто можна зустріти на власних e-mail адресах. Атаки шкідливого програмного забезпечення (Malware) – це віруси, трояни, шпигунське або інше шкідливе програмне забезпечення, а також до кібератак відноситься і атаки на вразливості програмного забезпечення. Їх мета проявляється у використанні помилок у коді для отримання несанкціонованого доступу або порушення роботи системи.

В свою чергу фізичні атаки можуть бути з різних складових, таких як диверсії та саботаж які безпосередньо представляють собою руйнування або пошкодження критичних об’єктів фізичними засобами, для прикладу можна спостерігати атаки на енергетичну інфраструктуру України після початку повномасштабного вторгнення. Крім цього до фізичних атак також належить несанкціонований доступ до об’єктів критичної інфраструктури, що являє собою проникнення на об’єкти з метою шпигунства або підготовки атак. Можна навести наступний приклад: використання підроблених ідентифікаційних карток для отримання доступу до центрів обробки даних.

Атаки за методами реалізації можуть містити в собі атаки на мережевий рівень, на рівень операційних систем та програмного забезпечення, а також на

атаки на рівень користувачів. Розглянемо їх по порядку: атаки на мережевий рівень представляють перехоплення трафіку, що має на меті тримання конфіденційної інформації через перехоплення даних між двома сторонами і спуфінг IP/MAC адрес, тобто пряма підміна адрес для отримання доступу до системи, наприклад обхід системи контролю доступу через підміну легітимного пристрою. Атаки на рівні операційної системи та програмного забезпечення. експлойт нульового дня стосується слабкості програмного забезпечення, яка ще невідома користувачам та розробникам програмного забезпечення, а механізми захисту від якої ще не розроблені, тобто слабкість потенційно може бути використана проти робочих копій програми без можливості захисту від неї [10]. Використання бекдорів ставить перед собою мету отримання прихованого доступу до системи без автентифікації, наприклад у вигляді зараження ПЗ на етапі розробки чи постачання. Атаки на рівень користувачів містять в собі інсайдерські закони та соціальну інженерію. Інсайдерські закони заключаються в атаках, що були здійснені співробітниками або підрядниками, які мають легальний доступ до об’єктів критичної інфраструктури. Соц. інженерія ж, представляє маніпулювання людьми для отримання конфіденційної інформації або доступу, зловмисники дуже часто можуть видавати себе за адміністратора системи для отримання паролів.

Класифікація атак за мотивами та джерелами. Змістовно можна виділити наступні три атаки: державні атаки, кримінальні атаки та хактивізм. Довготривалі, складні атаки, що здійснюються державними структурами або спонсорованими групами представлять собою державні атаки. В свою чергу, кримінальні атаки проводяться за допомогою програм-вимагачів, що шифрують дані та вимагають викуп. Їх використовують кіберзлочинці. Хактивізм – це атаки, мотивовані політичними чи ідеологічними причинами, вони також часто відбуваються під час політичних криз у різних країнах.

1.3. Огляд існуючих методів та засобів захисту ОКІ

Методи та засоби забезпечення кібербезпеки об’єктів критичної інфраструктури розроблені на основі міжнародних стандартів та передового досвіду. Вони є досить ефективними в мирний час. Однак ці методики не враховують гібридний характер війни, де виникають нові загрози. Серед них є фізичне знищення, захоплення противником, неможливість постійного моніторингу та контролю. У зв’язку з цим існує нагальна потреба у створенні нових та вдосконаленні існуючих методів і засобів кіберзахисту для підвищення рівня кібербезпеки критично важливих об’єктів [5].

Якщо на об’єкті критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога захисту до яких встановлена законодавством, то під час створення (модернізації) комплексної системи захисту інформації на ОКІ слід опиратися на положення цих загальних вимог і перевірятися під час його державної експертизи у сфері технічного захисту інформації.

Розробка інтегрованої системи захисту інформації об’єкта критичної інфраструктури та її державна експертиза проводяться відповідно до вимог законодавства у сфері захисту інформації та захисту державної таємниці [6].

На сьогоднішній день в Україні для захисту ОКІ застосовуються різноманітні методи та засоби, спрямовані на забезпечення їхньої стійкості та безперервного функціонування, а саме використовують організаційні та технічні заходи, такі як: секторальні органи у сфері захисту критичної інфраструктури, які відповідають за різні сектори та підсектори, а також типи основних послуг, що надаються об’єкту критичної інфраструктури, впровадження методичних рекомендацій щодо розробки проектних загроз, які можуть використовуватися операторами критичної інфраструктури.

В свою чергу технічні заходи включать в себе фізичний захист та кіберзахист. Для фізичний захисту ОКІ встановлюються систем відеоспостереження, контролю доступу, охоронних бар’єрів та інших

інженерно-технічних засобів. Кіберзахист передбачає створення комплексних систем захисту інформації, моніторинг та реагування на кіберінциденти [7].

Окрім організаційних і технічних засобів захисту проводяться регулярні тренінги та навчання для персоналу об’єкту критичної інфраструктури з метою підвищення уваги щодо потенційних загроз, відпрацювання дій у надзвичайних ситуаціях та забезпечення належного рівня кібергігієни.

Україна активно співпрацює з міжнародними партнерами для обміну досвідом та використання передового досвіду у сфері захисту критичної інфраструктури. Завдяки цим заходам Україна прагне забезпечити надійний захист своїх об’єктів критичної інфраструктури від різноманітних загроз та забезпечити їх безперебійне функціонування.

Кібератаки на ОКІ здійснюються різними методами, які можуть бути направлені як на технічні засоби, такі як мережеве обладнання, сервери, робочі станції, так й на людський фактор. Вивчення цих методів є ключовим для розробки ефективних стратегій кіберзахисту та підвищення рівня інформаційної безпеки.

Атака на ланцюжок поставок – це метод компрометації програмного чи апаратного забезпечення під час його розробки чи доставки. Кіберзлочинці можуть вбудовувати бекдори або шкідливий код у законні програми, які потім використовуються в критичній інфраструктурі. Наприклад, атака на SolarWinds у 2020 році дозволила хакерам отримати доступ до численних державних і приватних організацій по всьому світу, оскільки шкідливий код був вбудований в оновлення програмного забезпечення Orion.

Не менш небезпечними є атаки на комунікаційні протоколи та промислові системи. Багато систем керування критичною інфраструктурою використовують стандартизовані, але незахищені протоколи зв’язку, що дозволяє зловмисникам маніпулювати фізичними процесами. Наприклад, атака на українську електроенергетичну систему у 2015 році, відома як BlackEnergy, дозволила зловмисникам взяти під контроль системи SCADA, які контролювали підстанції та відключили електроенергію сотням тисяч споживачів.

Атаки через пристрої IoT також є серйозною загрозою для ОКІ, оскільки багато елементів критичної інфраструктури використовують Інтернет речей для моніторингу та контролю процесів. Слабко захищені або неправильно налаштовані пристрої IoT можна використовувати для проникнення в мережу або як частину ботнету для здійснення DDoS-атак. Зокрема, ботнет Mirai у 2016 році використовував десятки тисяч заражених пристроїв IoT для проведення широкомасштабних атак на інтернет-сервіси та телекомунікаційну інфраструктуру.

Успішні кібератаки на об’єкти критичної інфраструктури (ОКІ) можуть мати руйнівні наслідки для економіки, безпеки держави, функціонування суспільства та навіть життя людей. Наслідки таких атак варіюються залежно від типу ОКІ, рівня підготовленості до інцидентів та масштабів компрометації систем. Оцінка цих наслідків є критично важливою для розробки ефективних заходів кіберзахисту та мінімізації ризиків [2].

Одним із найбільш очевидних наслідків є зупинка функціонування важливих державних та приватних структур. Наприклад, атака на енергетичний сектор може спричинити масові відключення електроенергії, що вплине на роботу транспорту, систем водопостачання, лікарень, банків та інших критично важливих сервісів. Відключення електромережі в Україні у 2015 році, викликане атакою BlackEnergy, стало одним із перших відомих випадків використання кібератак для виведення з ладу енергетичної інфраструктури. Перша кібератака найбільше вплинула на споживачів «Прикарпаттяобленерго». Було вимкнено близько 30 підстанцій, а приблизно 230 тисяч людей залишилися без електроенергії на 6 годин.

Фінансові втрати, пов’язані з кібератаками на ОКІ, можуть сягати мільярдів доларів. Компанії та державні установи змушені витрачати значні кошти на відновлення роботи систем, виплату викупу у разі атак програм-вимагачів, юридичні розгляди та штрафи за витік конфіденційних даних. Наприклад, атака NotPetya у 2017 році, що почалася в Україні, спричинила економічні збитки на понад 10 мільярдів доларів у різних країнах світу.

Шкідливе програмне забезпечення містить багато коду зі старого домену, призначеного для вимагання. Однак, через кілька годин після спалаху деякі дослідники безпеки зрозуміли, що ця схожість була більш-менш поверхневою [11].

Одним із найсерйозніших наслідків є порушення національної безпеки та загроза суверенітету країни. Кібератаки, що здійснюються державами або спонсорованими хакерськими угрупованнями, можуть бути частиною гібридної війни, спрямованої на дестабілізацію країни. Виведення з ладу військових, урядових або правоохоронних систем може послабити здатність держави до реагування на кризові ситуації та загрожувати її обороноздатності.

Окрім економічних та політичних наслідків, успішні атаки можуть спричинити фізичні руйнування та загибель людей. Якщо зловмисники отримують контроль над системами управління промисловими об’єктами, такими як гідроелектростанції, газопроводи або транспортні мережі, вони можуть спровокувати катастрофічні аварії. Наприклад, моделювання атак на промислові системи показує, що маніпуляція SCADA-системами може призвести до вибухів, витоків токсичних речовин або виходу з ладу об’єктів критичної інфраструктури, що загрожують життю сотень тисяч людей.

Витік конфіденційної інформації та компрометація даних також є серйозним наслідком атак на ОКІ. Якщо зловмисники отримують доступ до державних реєстрів, медичних записів, банківських баз даних або персональних даних громадян, це може призвести до масштабного шахрайства, шантажу, соціальних потрясінь та довготривалих репутаційних втрат для держави чи компаній [12].

Порушення довіри суспільства до цифрових сервісів є ще одним довготривалим наслідком кібератак. Якщо громадяни регулярно стикаються з витоками даних, неможливістю доступу до державних онлайн-послуг або фінансовими втратами через атаки на банки, вони можуть втратити довіру до цифрових технологій загалом. Це, у свою чергу, гальмує розвиток електронного урядування, цифрової економіки та технологічного прогресу країни.

1.4. Нормативно-правове регулювання захисту ОКІ і приклад категоризації ОКІ

В Україні нормативно-правове регулювання захисту ОКІ базується на низці законодавчих та підзаконних актів, які встановлюють принципи, завдання та механізми забезпечення їхньої безпеки. Ключовими законодавчими актами є Закон України «Про критичну інфраструктуру» (№1882-IX від 16 листопада 2021 року). Цей закон визначає правові та організаційні засади створення та функціонування системи захисту національної критичної інфраструктури, визначає критерії віднесення об’єктів до критичної інфраструктури та визначає повноваження державних органів у цій сфері. Крім того, законом регулюються права та обов’язки операторів критичної інфраструктури щодо забезпечення безпеки їхніх об’єктів.

Наступний є Закон України «Про основні засади забезпечення кібербезпеки України» (№2163-VIII від 5 жовтня 2017 року), що визначає правові та організаційні основи забезпечення кібербезпеки держави, а також встановлює обов’язки суб’єктів забезпечення кібербезпеки, включаючи захист критичної інформаційної інфраструктури.

Окрім Законів України не виключенням є Постанова КМУ від 9 жовтня 2020 року №1109 «Деякі питання об’єктів критичної інфраструктури», що зазначає порядок віднесення об’єктів до критичної інфраструктури, визначає перелік секторів та підсекторів критичної інфраструктури, встановлює методику категоризації об’єктів критичної інфраструктури.

Не менш важливою є Постанова КМУ від 19 червня 2019 року №518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». Дана Постанова визначає загальні вимоги до забезпечення кіберзахисту ОКІ, а також встановлює обов’язки операторів щодо створення систем кіберзахисту та проведення аудиту безпеки.

В свою чергу Постанова КМУ від 22 липня 2022 року №821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів

критичної інфраструктури» визначає механізм проведення моніторингу безпеки ОКІ і встановлює процедури оцінки стану захищеності об’єктів та заходи реагування на виявлені загрози.

Постанова КМУ від 4 серпня 2023 року №818 «Деякі питання паспортизації об’єктів критичної інфраструктури» запроваджує порядок паспортизації ОКІ та визначає вимоги до змісту та форми паспортів безпеки об’єктів.

Відомчі нормативні акти теж мають місце безпосередньо у нормативно-правовому регулюванні захисту об’єктів критичної інфраструктури, а саме:

Наказ Адміністрації Держспецзв’язку від 15 січня 2021 року №23 «Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури», що надає методичні рекомендації для визначення категорій критичності об’єктів і встановлює критерії та показники для оцінки значущості ОКІ; Наказ СБУ та Держспецзв’язку від 19 грудня 2024 року №627/772 «Про затвердження форм планів захисту об’єктів критичної інфраструктури та рекомендацій до їх розроблення» визначає форми планів захисту ОКІ і надає рекомендації щодо розроблення та впровадження заходів безпеки на об’єктах. Впровадження цих наказів посприяло підвищенню ефективності захисту критично важливих об’єктів, забезпечуючи безперервність надання життєво важливих послуг та підвищення рівня безпеки громадян [8].

Розглянемо порядок категоризації об’єкта критичної інфраструктури на прикладі інтернет-провайдеру. Оператор послуг – компанія «Best».

Інтернет провайдери належать до сектору електронних комунікацій та телекомунікацій, які входять до переліку критичних секторів, визначених державою. Вони забезпечують стабільність та безперервність зв’язку, передачу даних, функціонування державних і комерційних систем.

Для того щоб визначити категорію критичності, застосовується методика віднесення об’єкта критичної інфраструктури до однієї з категорій критичності. Ця методика містить у собі два окремі додатки, за допомогою яких визначається

категорія критичності ОКІ. Міра негативного впливу об’єкта критичної інфраструктури визначається галузевими критеріями. (табл 1.2) [13].

Таблиця 1.2

Методики віднесення об’єкта критичної інфраструктури до однієї з категорій критичності (додаток 1)

№	**Сектор/підсектор**	**Рівень негативного впливу: катастрофічні наслідки (4 бали)**	**Рівень негативного впливу: критичні наслідки (3 бали)**	**Рівень негативного впливу: значні наслідки (2 бали)**	**Рівень негативного впливу: незначні наслідки (1 бал)**	**Оцінка PK_i**
7.	Послуги, що надаються підсектором електронних комунікацій	втрата можливості функціонування елементів електронної комунікаційної мережі або мережевої інфраструктури або інфраструктури центру обробки даних чи обміну трафіком для України або значної її частини	збій, переривання у наданні основних послуг або обмеження доступу користувачам послуг чи сервісів для великих міст чи цілих регіонів	відсутність стабільного з’єднання, переривання сесій, зниження пропускної здатності електронних комунікаційних мереж для операторів або частини користувачів	не застосовується	2
				Сумарна оцінка PK_i		**2**

Наступним кроком проводиться оцінка за міжсекторальними критеріями. Проводиться оцінка шляхом вибору варіанта негативного впливу за кожним критерієм та обґрунтування вибору. Всього визначають 5 рівнів впливу, кожен з яких має свою оцінку:

– Катастрофічні наслідки: 4 бали.

– Критичні наслідки: 3 бали.

– Значні наслідки: 2 бали.

– Незначні наслідки: 1 бал.

– Вплив надто малий: 0 балів.

Окрім цього, існує важливість об’єкта критичної інфраструктури, а саме: соціальна важливість об’єкта критичної інфраструктури, державна важливість об’єкта критичної інфраструктури, економічна важливість об’єкта критичної інфраструктури, важливість об’єкта критичної інфраструктури для забезпечення оборони країни та державної безпеки, а також взаємозв’язок між об’єктами критичної інфраструктури.

В кожній з наведених значимостей об’єкта критичної інфраструктури є свої критерії негативного впливу. Наприклад, в соціальній значущісті – це заподіяння шкоди життю та здоров’ю людей, а в економічній значущісті – заподіяння збитків державному або місцевому бюджету тощо.

Визначивши сумарну оцінку PK_i для інтернет провайдеру згідно додатка 2 – отримаємо результат 13. Далі за допомогою формули визначаємо критичність об’єкта:

$$PK_{\text{ОКІ}} = \frac{PK_i}{PK_{max}} = \frac{2+13}{18*4} = \frac{15}{72} = 0{,}208 \qquad (1.1)$$

Відповідно до правила:

Критичність І категорії, якщо $0{,}8 < PK_{OKI} \leq 1$;

Критичність ІІ категорії, якщо $0{,}63 < PK_{OKI} \leq 0{,}8$;

Критичність ІІІ категорії, якщо $0{,}37 < PK_{OKI} \leq 0{,}63$;

Критичність ІV категорії, якщо $0{,}2 < PK_{OKI} \leq 0{,}37$;

об’єкт не є критичним, якщо $PK_{OKI} \leq 0{,}2$.

Інтернет-провайдер Best може бути віднесено до ІV категорії критичності.

Висновок до перешого розділу

У першому розділі отримані результати, що дозволили ідентифікувати зовнішні загрози, тобто кібератаки, терористичні акти та стихійні лиха, а також внутрішні загрози, у тому числі організаційні збої, людський фактор та техногенні аварії, які загрожують продовженню функціонування об’єктів критичної інфраструктури, проведено оцінку наслідків атак на об’єкти критичної інфраструктури, а також розглянуто приклад того, як визначити категорію критичності типового об’єкта критичної інфраструктури та провести його ідентифікацію. Зібрані дані підтверджують необхідність аналітичної стратегії, яка розпізнає унікальні атрибути кожного об’єкта, таким чином захищаючи їх від багатьох загроз.

Наявні методи захисту, а також поточні організаційно-технічні процедури, які використовуються в мирний час, вимагають сучасних коригувань для протидії гібридним загрозам, що виникають. Інституційна підтримка нормативно-правового регулювання залишається сильною, хоча поточні обставини вимагають негайної модернізації законодавства, а також кращого нагляду за системами впровадження.

Загальний синтез даного дослідження дозволяє сформувати наукове завдання побудови інтегрованої системи захисту, яка поєднує кількісні та якісні показники ефективності заходів безпеки, водночас надаючи практичні рекомендації щодо надійної роботи критично важливих об’єктів у сучасних умовах. Притримуючись правил, що регулює методика віднесення об’єкта критичної інфраструктури до однієї з категорій критичності, можна визначити рівень негативного впливу об’єкта критичної інфраструктури у різних секторах.

РОЗДІЛ 2
РОЗРОБКА МЕТОДІВ ПРОТИДІЇ ВТОРГЕННЯМ НА ОКІ

2.1. Аналіз джерел загроз та векторів вторгнення

Вторгнення на об’єкти критичної інфраструктури – це будь-яка несанкціонована дія або серія дій, спрямованих на отримання доступу, вплив чи порушення нормального функціонування інформаційних, технологічних, фізичних або адміністративних систем, що забезпечують життєво важливі послуги держави, суспільства чи економіки.

Аналіз загроз є однією з найважливіших частин аналітичної роботи та відповіддю на питання про те, від чого або від кого необхідно захищати об’єкти захисту. Джерела загроз конфіденційній інформації включають об’єктивні та суб’єктивні події. Загрози можуть виходити ззовні та зсередини.

Аналітична робота з джерелом загрози конфіденційній інформації включає ідентифікацію та класифікацію максимального складу джерел загрози конфіденційній інформації, облік та вивчення кожного окремого суб’єктивного внутрішнього та зовнішнього джерела, ступеня небезпеки його реалізації, розробку заходів щодо локалізації та усунення об’єктивних загроз.

У сфері зовнішніх джерел загроз аналітична робота пов’язана з маркетинговими дослідженнями, що є звичайною справою будь-якої компанії. Вивчення внутрішніх джерел загроз спрямоване на виявлення та аналіз нечесних інтересів та злочинних дій окремих співробітників та партнерів компанії. Аналітична робота проводиться щодо потенційних та пасивних загроз джерелам і каналам поширення інформації. У разі активної загрози також відбувається заздалегідь спланована, продумана та рішуча протидія зловмиснику.

В сучасних реаліях, коли ворог вторгся на територію України, об’єкти критичної інфраструктури активно потребують більшого захисту. Атаки на критичну інфраструктуру України в ході російсько-української війни є воєнним

злочином, скоєним російськими військовими в контексті повномасштабної військової агресії Росії проти України з метою змусити вище українське політичне керівництво вести переговори з кремлівським режимом на вигідних для нього умовах [16].

Так, у період з 28 вересня 2022 року до 1 вересня 2024 року зафіксовано майже 11,5 тис. пусків крилатих ракет, зенітних ракет комплексу С-300, балістичних ракет для ураження наземних цілей, БПЛА-камікадзе типу Shahed-131/136. При цьому лише за вересень 2024 року зафіксовано 1110 пусків. За цей період часу спостерігалося 17 днів інтенсивних обстрілів, протягом яких протягом доби сталося понад 82 пуски ракет (порівняно із середнім показником 23,2 пуски на добу) [17].

Вектори вторгнення на ОКІ поділяються на кібернетичні, фізичні і гібридні.

Кібернетичні вектори представляють атаки через публічні сервіси (ел. пошта, VPN, веб-сервери), експлуатацію різноманітних вразливостей у ПЗ, наприклад вразливість нульового дня [10]. Сюди також входить як впровадження шкідливого ПЗ через флешки й інфіковані сайти, так і соціальна інженерія, фішинг тощо.

Фізичні вектори в свою чергу являють собою несанкціонований доступ до серверних, пунктів управління або каналів зв’язку, використання дронів, лазерних пристроїв або датчиків для шпигунства, підрив або виведення з ладу електроживлення, охолодження, вентиляції. Дані атаки можуть спричинити тривалі збої у роботі ОКІ або стати прелюдією до масштабного цифрового вторгнення. У деяких випадках фізичні вектори комбінуються з кібератаками, утворюючи багаторівневу гібридну загрозу.

Гібридні вектори також називають інтегрованими, вони демонструють сценарії, у яких кіберзагроза підсилюється фізичною дією наприклад, через кібератаку блокується відеоспостереження, після чого виконується фізичне проникнення.

2.2. Метод оцінювання загроз та протидії вторгненням за сценаріями

Метод протидії вторгненням на основі сценаріїв являє собою проактивний підхід до захисту ОКІ, заснований на моделюванні потенційних атак та розробці індивідуальних відповідей на кожну з них. Його головна мета – випередити дії зловмисника, заздалегідь підготувавши персонал, інструменти та алгоритми реагування на конкретні сценарії вторгнення.

Суть методу запобігання вторгненням на основі сценаріїв полягає у прогнозуванні та моделюванні потенційних атак на об’єкти критичної інфраструктури з подальшою розробкою чітких, заздалегідь підготовлених алгоритмів реагування для кожного можливого сценарію. Метод передбачає створення типових ситуацій, які можуть виникнути в результаті кібератак, фізичних вторгнень або дій інсайдерів, та визначення індикаторів цих атак, логіки виявлення, плану дій фахівців та можливих способів мінімізації збитків.

Кожен сценарій будується на основі реальних чи потенційних загроз для конкретного ОКІ з урахуванням його архітектури, рівня критичності, внутрішніх безпекових політик та типових вразливостей. Таким чином, замість загального підходу використовується персоналізована модель, що дозволяє підготуватися до конкретних інцидентів.

Важливою частиною методу є попереднє тестування та періодичне оновлення цих сценаріїв відповідно до змін технологій, законодавства та загроз.

Структурна схема (алгоритм) методики оцінювання загроз і ризиків для об’єктів критичної інфраструктури, що була створена шляхом декомпозиції та синтезу методології оцінки загроз ОКІ, за сценаріями розвитку надзвичайних ситуацій наведена на рисунку 2.1. Можливе створення програмного комплексу для підтримки прогнозування надзвичайних ситуацій та їх оцінки [14].

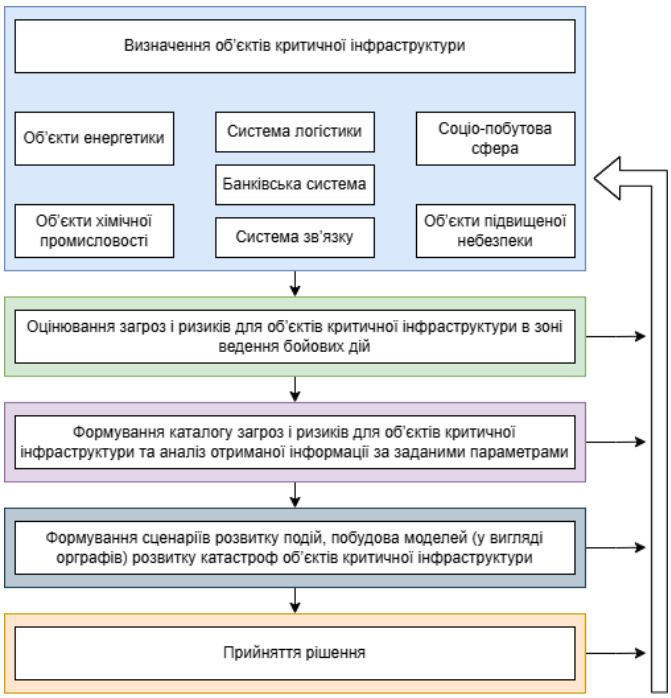

Рисунок 2.1 – Структурна схема методики оцінювання загроз і ризиків для об’єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій

Суть методу. Складається база даних переліку потенційних об’єктів, які можуть стати об’єктами в умовах бойових дій. Оскільки перелік таких об’єктів залежить від конкретної ситуації, він складається на основі інформації щодо зон бойових дій, вогневого впливу противника тощо. Серед ключових об’єктів критичної інфраструктури традиційно виділяють об’єкти енергетичної, нафтопереробної та хімічної промисловості, логістичні системи, мости, дамби, системи та об’єкти зв’язку, об’єкти соціально-побутової сфери. Також необхідно враховувати можливі комплексні дії, які взаємопов’язані між собою, можуть мати високий потенціал загроз та катастрофічні наслідки. Необхідно враховувати взаємодію з іншими ОКІ та специфіку певного об’єкта з метою забезпечення належного рівня безпеки та захисту в умовах конфлікту.

Проводиться оцінка загроз та ризиків для ОКІ в зоні бойових дій. За даними, отриманими на першому етапі, будується план розвитку катастроф, спричинених руйнуванням/знищенням ОКІ; проводяться розрахунки для оцінки

числового значення ймовірності пошкодження ОКІ ракетними та артилерійськими ударами. Визначається ступінь їх пошкодження.

Виконується аналіз інформації, отриманої від заданих параметрів озброєння противника, щодо знищення окремих ОКІ на певних ділянках. Загалом, на цьому етапі буде створено ключове інформаційне ядро щодо типу загроз та ризиків знищення ОКІ, їх способів ураження. Це дозволить визначити сили та засоби протидії ворожим атакам. Що стосується змісту, то він буде відправною точкою для розробки стратегії захисту критичної інфраструктури та протидії ворожій зброї, характеру, фізичної та хімічної природи факторів ураження, що спричинені руйнуванням об’єктів критичної інфраструктури.

Після побудови загальної схеми визначаються деструктивні потенціали та найважливіші сценарії й вузлові події. Схема відображає траєкторії розвитку деструктивних подій у різних сферах внаслідок надзвичайних ситуацій, зокрема, у сфері енергетики, екології та логістики, що спричиняють соціально-економічну кризу. На основі значень руйнівних потенціалів *D* можна визначити основні ОКІ, провести нормування та створити відповідний каталог. Внаслідок руйнування ОКІ визначаються найважливіші сценарії надзвичайних ситуацій з точки зору рівня загрози. Залежно від характеру бойових дій та ракетних і авіаційних ударів обговорюється обґрунтоване перегрупування військ та засобів протиповітряної оборони, а також визначення районів надзвичайних ситуацій для своєчасної евакуації військ та цивільного населення. Це дозволяє зосередити основні зусилля на покращенні захисту та живучості визначених об'єктів оборони.

Отже, відбувається процес прийняття рішень щодо питання розподілу сил та для захисту та оборони об'єктів, їхньої пріоритетності, а також розташування (переміщення) військ і населення в зоні впливу ОКІ. Виявлення зон майбутніх надзвичайних ситуацій та вжиття превентивних заходів безпеки. Всі вищезазначені блоки мають зворотний зв'язок і, за умови отримання оновлених даних або виникнення непередбачених подій, розрахунки можуть бути виконані на відповідних рівнях. Після завершення всіх п'яти блоків методології буде зібрано достатньо інформації для прийняття управлінських рішень, вжиття

відповідних заходів безпеки та оборони, а також для застосування найкращого розподілу сил і засобів безпеки та оборони [17].

Такий підхід забезпечує не лише технічну, а й організаційну готовність до інцидентів, мінімізує час прийняття рішень у кризовій ситуації та знижує ймовірність людського чинника. Метод активно застосовується у критично важливих сферах – енергетиці, транспорті, фінансах, телекомунікаціях – і є частиною національних стратегій кіберстійкості.

2.3. Метод інтелектуального аналізу даних для виявлення мережевих атак

Система виявлення вторгнень (СВВ) – це програма або апаратно-програмний інструмент, який використовується для виявлення несанкціонованого доступу до комп'ютерної системи чи мережі [18].

Залежно від апаратних та програмних компонентів окремих вузлів системи та мережевого обладнання, можна розміщувати різні набори датчиків, модулів детектування та компонентів бази даних. Для ефективної роботи СВВ на вузлах необхідно дотримуватися таких умов:

– склад модулів виявлення повинен відповідати набору потенційних типів атак, які можна визначити на основі інформації, обробленої на хості, та встановленого програмного забезпечення;

– внутрішня структура бази даних повинна відповідати задіяним сенсорам та модулям виявлення;

– склад сенсорів повинен відповідати аналізованим інформаційним потокам, оброблятися повинні лише ті мережеві протоколи, які можна використовувати для здійснення атаки [19]. Більшість сучасних систем виявлення вторгнень мають монолітну архітектуру, яка ускладнює ефективний розподіл обчислювального навантаження (рис. 2.2).

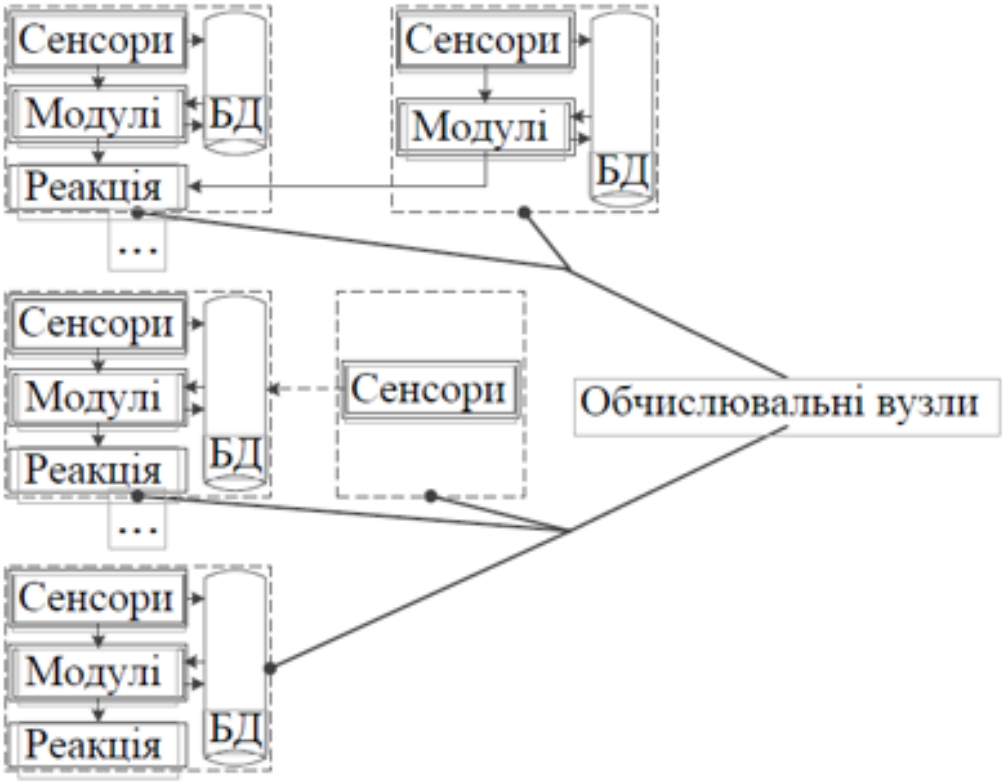

Рисунок 2.2 – Варіанти розміщення компонентів СВВ в розподіленої обчислювальної мережі

Монолітна структура більшості існуючих систем виявлення вторгнень не дає можливості ефективно розподіляти обчислювальні ресурси і саме через монолітну архітектуру більшість наявних систем виявлення вторгнень не здатні ефективно розподіляти обчислювальне навантаження. Також вона обмежує їхню здатність до ефективного розподілу обчислювального навантаження.

Обчислювальне навантаження СВВ на кожен вузол також може змінюватися шляхом створення єдиної бази даних для кількох вузлів та розміщення лише блоку датчиків на окремих вузлах. За такого підходу обсяг мережевого трафіку до вузла, що містить спільну базу даних, може значно зрости, а ризики атаки типу «відмова в обслуговуванні» зростають для вузлів, які не мають власного блоку аналізатора.

Кластери методів інтелектуального аналізу даних для проектування системи виявлення мережевих атак. Як було представлено вище, можна виділити

наступні групи методів інтелектуального аналізу даних відповідно до раніше представлених підзадач, пов'язаних з виявленням мережевих атак.

Більшість СВВ мережевих атак базуються на процесі класифікації, який робить висновок про те, чи було виявлено атаку або аномальну поведінку. Сьогодні проводиться багато досліджень з питань виявлення мережевих атак і саме ці дослідження базуються на таких методах, як генетичні алгоритми, нейронні мережі, дерева рішень, правила асоціації тощо (табл. 2.1).

Таблиця 2.1

Методи і засоби інтелектуального аналізу для виялвення

Метод	**Функції, що обули впроваджені в задачі для виявлення мережевих атак**
Класифікація	Віднесення аналізованих векторів до нормальних та аномальних множин
Метод скорочення розмірностей	Збільшення швидкодії за допомогою формування оптимізованого простору ознак
Кластеризації	Побудова оптимізованих модулів виявлення
Нечітка логіка	Організація взаємодії модулів виявлення, а також створення надлишкової модульної архітектури

На основі результатів аналізу багатьох досліджень як класифікатор було обрано метод опорних векторів. Цей метод демонструє одні з найкращих показників виявлення атак та має широкі можливості внутрішнього налаштування.

Метод опорних векторів знаходить вибірки, що належать до меж між двома класами, і вони називаються опорними векторами. Інші функціональні завдання, які вирішують системи виявлення мережевих атак, в першу чергу зосереджені на підвищенні якості виявлення, продуктивності системи, уніфікації та виконанні інших допоміжних завдань.

Навчання методу головних компонентів є обчислювально складним завданням. Крім того, якість класифікації сильно залежить від внутрішніх налаштувань цього методу, специфічних для різних типів атак та навчальних наборів. У зв'язку з цим необхідно спростити процедуру навчання моделі класифікації. Для вирішення даної проблеми є зменшення розмірності, включаючи відкидання шуму та викидів, та поділ навчального набору на частини – виконання процедури кластеризації [20].

Метою кластерного аналізу є поділ набору даних на групи таким чином, щоб різниця між будь-якими двома елементами, що належать до однієї групи, була мінімальною, і водночас різниця між будь-якими двома іншими елементами, була максимальною. Методи поділяються на ієрархічні та неієрархічні.

Ієрархічні методи дозволяють побудувати оптимальну структуру кластерів, але характеризуються експоненціальною залежністю від кількості записів.

Серед неієрархічних методів кластерного аналізу найбільш поширеними є ітераційні методи. Ці методи є більш універсальними, ніж ієрархічні, проте мають один серйозний недолік, що являє собою необхідність апріорного знання кількості кластерів, що суттєво ускладнює їхню автоматизацію.

2.4. Концепція створення кіберсистем на основі біоміметичних алгоритмів для захисту об’єктів критичної інфраструктури

Концепція базується на використанні природних механізмів адаптації, еволюції та самоорганізації, що спостерігаються у біологічних системах, для динамічного виявлення і нейтралізації нових, раніше невідомих загроз. Основна ідея методу передбачає моделювання кіберзахисної системи, яка працює не за жорстко заданими правилами, а за принципами еволюційного навчання, постійної адаптації та самооновлення в умовах змінного середовища загроз. Такі системи можуть аналізувати інформаційні потоки в режимі реального часу,

виявляти аномалії та потенційні вторгнення, не обмежуючись відомими шаблонами атак, а також самостійно модифікувати захисну логіку, відкидаючи неефективні стратегії.

Для ефективної роботи методу мають використовуватися генетичні алгоритми для оптимізації параметрів аналізу та ухвалення рішень. Наприклад, система автоматично покращує стратегії розпізнавання атак, комбінуючи найуспішніші підходи з попередніх ітерацій. Із переваг можна виділити високу здатність до пошуку в складних, багатовимірних просторах. Також повинні бути імунологічні алгоритми (Artificial Immune Systems). За принципом роботи вони мають моделювати систему, яка виявляє та нейтралізує чужорідні елементи. Виявлення аномального трафіку, що не відповідає нормі також входить в обов'язки імунологічного алгоритму, що також сприятиме виявленню атак нульового дня. Окрім цих двух алгоритмів можна також додати й використання нейромереж, а точніше еволюційні механізми, які будуть використоватися безпосередньо для автоматичного створення та навчання нейронних мереж. Застосування наступне: побудова адаптивних систем виявлення вторгнень, після чого створення гібридних інтелектуальних агентів у Security Operations Centers. Операційний центр безпеки (SOC) – це централізований підрозділ установи, який займається питаннями інформаційної та кібербезпеки на організаційному та технічному рівні. Тобто це об'єкт, де корпоративні інформаційні системи (вебсайти, програми, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюються, оцінюються та захищаються [21]. Перевагою використання еволюційних механізмів є здатність самостійно розробляти архітектуру нейромереж під конкретне середовище загроз.

На ОКІ подібні системи можуть бути впроваджені як для контролю трафіку SCADA-систем і для захисту від нульових днів (zero-day exploits) так і для реального виявлення складних багаторівневих атак, які змінюють поведінку в часі. Також не виключенням є частина адаптивного операційного центру безпеки з функціями прогнозування інцидентів, що декілька схожа з методом

оцінюванням загроз й протидії вторгненням за сценаріями. Дані системи можуть знайти своє застосування у енергетичному секторі об’єкта критичної інфраструктури, а саме система може «вивчити» типову поведінку сенсорів на підстанції, і при виявленні нетипової комбінації сигналів відразу сигналізувати про потенційну атаку, навіть якщо конкретний тип експлойту невідомий. За рахунок високої адаптивності системи, вона реагує на зміну поведінки загроз в реальному часі, а при належному використанні цього методу знижуються потенційні хибні спрацювання за рахунок самонавчання системи.

Атестація та введення в експлуатацію даного методу буде здійснюватися органами, акредитованими Держспецзв’язку. За наявності позитивного експертного висновку система визнається такою, що відповідає вимогам щодо захисту об’єкта критичної інфраструктури.

Висновок до другого розділу

У другому розділі було проведено аналіз сучасних методів атак на об’єкти критичної інфраструктури та оцінено їх вплив на безпеку таких систем. Здійснено класифікацію основних видів атак на ОКІ, серед яких виділено мережеві атаки такі як DoS/DDoS і ARP-спуфінг, атакуюче програмне забезпечення, тобто віруси, трояни, рансомвар тощо, також виділені атаки соціальної інженерії, що представляють собою фішинг і подібні BEC-атаки, а також фізичні вторгнення. Особливу увагу було приділено складним багатовекторним атакам, які комбінують декілька методів для підвищення ефективності. Окрім цього було розглянуто сучасні методи реалізації кібератак на ОКІ, серед яких – використання автоматизованих ботнет-мереж, цільові APT-атаки, експлуатація вразливостей SCADA/ICS-систем, а також застосування шкідливих компонентів у ланцюгах постачання.

Проаналізовано приклади реальних атак на ОКІ на прикладі BlackEnergy, що демонструють високу загрозу для безпеки ОКІ. Проведено оцінку потенційних наслідків успішних атак на ОКІ. Виявлено, що такі інциденти

можуть призводити до масштабних перебоїв у роботі інфраструктури, фінансових втрат, порушення безпеки громадян, а також мати політичні та економічні наслідки на національному рівні. Особливо критичними є сценарії, які впливають на енергетичний сектор, транспортні системи та зв’язок. Визначено основні методи протидії атакам на ОКІ. Проаналізовано як класичні підходи як мережеві екрани, системи виявлення вторгнень, так і сучасні рішення – це використання засобів штучного інтелекту для аналізу аномалій, адаптивних систем захисту. Визначено актуальність інтеграції біоміметичних алгоритмів як перспективного напряму.

Аналіз сучасних загроз та методів атак на ОКІ підтверджує необхідність застосування комплексного підходу до кіберзахисту, що включає поєднання традиційних технологій з інноваційними методами, що здатні адаптуватися до змін середовища й невідомих типів атак.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ І ВИЯВЛЕННЯ КРАЩОГО МЕТОДУ ДЛЯ ЗАХИСТУ ОКІ ВІД ВТОРГНЕНЬ

3.1. Порівняння методів протидії вторгненням на ОКІ

Метод оцінки загроз та протидії вторгненням на основі сценаріїв є одним із ключових інструментів стратегічного захисту об’єктів критичної інфраструктури. Він базується на створенні типових або ймовірних сценаріїв атак, які можуть бути реалізовані в інформаційній або фізичній інфраструктурі, та розробці відповідних алгоритмів реагування. Переваги методу протидії вторгненням за сценаріями за сценарієм можуть бути наступними:

– Проактивність і передбачуваність

Метод дозволяє не лише реагувати на інциденти, а й готуватися до них заздалегідь, спираючись на прогнозування реальних загроз. Він дозволяє уникнути імпровізації під час кризових ситуацій.

– Орієнтація на практику

Розробка сценаріїв зазвичай базується на реальних кейсах, попередніх атаках або міжнародних моделях, наприклад NIST, що забезпечує високу практичну цінність методу.

– Формування алгоритмів реагування

Метод дозволяє створювати чіткі інструкції та протоколи для персоналу у разі інциденту, включаючи зв’язок, перемикання на резервні системи та інформування відповідних органів.

– Можливість інтеграції в автоматизовані системи

Сценарії можуть бути реалізовані як плейбуки в системах SIEM, SOAR чи SOC тобто автоматизовані модулі реагування на певні тригери.

– Покращення рівня підготовки персоналу

Проведення тренувань за сценаріями сприяє підвищенню обізнаності та готовності фахівців, знижуючи людський фактор під час реальних атак.

– Гнучкість адаптації

Сценарії легко оновлюються у разі зміни архітектури об’єкта, появи нових типів загроз або зміни нормативної бази.

– Підвищує готовність персоналу до реальних інцидентів.

Метод сценаріїв дозволяє створювати реалістичні моделі атак, які регулярно використовуються під час навчань та симуляцій. Участь у таких тренуваннях допомагає розвивати навички негайного розпізнавання загроз, правильного прийняття рішень та роботи в умовах інформаційного навантаження. Завдяки цьому співробітники не лише краще розуміють структуру та слабкі сторони систем захисту, але й впевнено діють у кризовій ситуації, що значно зменшує наслідки інциденту.

– Дає змогу скоротити час реакції на вторгнення.

Попередньо розроблені сценарії містять чітко структуровані плани дій: що робити, коли, кого інформувати, які системи активувати або деактивувати. Такий підхід значно скорочує час на аналіз ситуації, оскільки персонал не витрачає час на пошук рішень чи координацію дій у момент інциденту – усі процеси вже визначені та розроблені. У критичних системах це може бути вирішальним фактором для уникнення або обмеження відключення життєво важливих функцій (електропостачання, зв’язок, транспорт тощо).

– Знижує ризик помилок у стресовій ситуації.

У надзвичайних ситуаціях люди схильні до емоційних чи імпульсивних рішень, особливо якщо вони не мають досвіду реагування на кібератаки. Метод сценаріїв мінімізує цей ризик, оскільки дає чіткі алгоритми дій, що багаторазово перевірені на навчаннях. Це дозволяє персоналу діяти системно, послідовно та впевнено, не піддаючись паніці [22].

Недоліками даного методу в свою чергу може виступати висока ресурсозатратність на початковому етапі, а саме створення якісних сценаріїв вимагає глибокого аналізу інфраструктури, оцінки ризиків та консультацій зі

спеціалістами з кібербезпеки – все це вимагає часу, грошей та професійної експертизи. Також до недоліків входить імовірність надмірної стандартизації реакцій, тобто у реальному житті сліпе слідування сценарію може бути неефективним, якщо ситуація виходить за межі запланованого шаблону. Сценарії, засновані на історичних даних, можуть зосереджуватися на відомих загрозах, тоді як нові можуть бути пропущені. Навіть найкращі сценарії можуть не спрацювати, якщо виконуючий персонал недостатньо підготовлений або не виконує інструкції належним чином. І на кінець, метод втрачає свою актуальність без регулярної адаптації до нових загроз. Мається на увазі, що застарілі сценарії можуть включати застарілі компоненти або системи [23].

Таким чином, включення методу сценарного реагування у систему захисту ОКІ дозволяє не лише технічно посилити безпеку, а й формує оперативну та психологічну готовність персоналу, що відіграє значну роль у сфері національної кіберстійкості [24].

Можна узагальнити, що це достатньо ефективний метод швидкого реагування, навчання та планування, який, однак, вимагає комплексного підходу, регулярного оновлення та поєднання з іншими адаптивними інструментами кіберзахисту. Його доцільно використовувати у зв’язці з системами моніторингу в реальному часі та аналітикою інцидентів, особливо в середовищах критичних ІТ-систем.

Наступним в порівнянні є метод інтелектуального аналізу даних, який є одним із найперспективніших підходів до виявлення мережевих вторгнень, особливо у сфері захисту ОКІ. Цей метод базується на використанні алгоритмів машинного навчання, штучного інтелекту та математичної статистики для виявлення прихованих закономірностей, аномалій та невідомих типів атак у великих обсягах мережевого трафіку або журналів [25].

Із переваг даного методу можна виділити його здатність виявляти невідомі атаки (атаки нульового дня). Метод інтелектуального аналізу даних базується безпосередньо на поведінковому аналізі або класифікації здатні виявляти аномалії, що не відповідають відомим сигнатурам атак. Така деталь є важливою

для виявлення нових або модифікованих типів вторгнень, які ще не були описані в базах даних раніше. Також до переваг цього методу входить автоматичне навчання і адаптація за рахунок машинного навчання, що дозволяє їм покращувати точність виявлення атак з часом без постійного втручання фахівців. З цього слідує ще один плюс – метод дозволяє зменшити залежність від операторів системи кіберзахисту, що в свою чергу зменшує ймовірність пропуску або неправильного тлумачення подій. Окрім цього, метод проводить комплексність аналізу, це дозволяє точніше ідентифікувати активність вразливостей. Наприклад, можна одночасно враховувати багато параметрів, таких як частоту запитів, IP-адресу, тип трафіку тощо [26].

До недоліків методу інтелектуального аналізу даних відноситься висока обчислювальна складність, більшість інтелектуальних алгоритмів є ресурсоємними і для цього потребується потужна IT-інфраструктура. В свою чергу для цього так само потрібні кваліфіковані спеціалісти. Окрім цього є ризик високого рівня хибних спрацьовувань, тобто ймовірні помилкові спрацювання, що можуть перевантажити операторів безпеки, особливо це помітно на початковому етапі або при використанні моделей без нагляду [27]. Для досягнення високої точності системного аналізу необхідно великі та збалансовані набори даних, які повинні бути актуальними та мати добре марковані приклади атак і нормальної активності, тобто метод потребує великий обсяг якісних навчальних даних.

Метод інтелектуального аналізу даних є чудовим методом для виявлення складних мережевих вторгнень, цілеспрямованих і нових загроз, характерних для атак на ОКІ. Однак його ефективність безпосередньо залежить від якості даних, ресурсів та професійної підтримки. Для досягнення максимального ефекту, даний метод слід поєднувати з іншими механізмами захисту, такими як сигнатурні IDS та засобами сегментації мереж.

Останнім методом для порівняння являється лише концепція створення кіберсистем на основі біоміметичних алгоритмів для захисту ОКІ. Це інноваційний підхід, який використовує механізми з біології й екології для

розробки адаптивних, самонавчальних та стійких до загроз систем захисту. На відміну від класичних (статичних) інструментів безпеки, біомеметичні системи працюють динамічно – вони аналізують поведінку середовища, навчаються на прикладах та автоматично змінюють свої стратегії реагування на нові, навіть невідомі, атаки. Суть даної концепції полягає в тому, що біоміметичні кіберсистеми імітують властивості природних систем і як виявляється, ці властивості ідеально підходять для динамічного середовища ОКІ, де загрози змінюються швидко, а час реагування має вирішальне значення. Приклад таких властивостей: еволюція поведінки, адаптація до змін, розпізнавання «свій-чужий» тощо. Це дозволяє заздалегідь протестувати ефективність захисту.

Перевагами даної концепції для ОКІ стає адаптивність всієї системи. З цього слідує реакція на зміну поведінки загроз в реальному часі. Як і попередній метод, здатен виявляти навіть невідомі раніше загрози (атаки нульового дня), аналізуючи аномальну поведінку, висока ефективність у динамічному середовищі, а також мінімальна залежність від баз знань/сигнатур. Окрім цього визначається висока ефективність в умовах невизначеності: система не потребує знання конкретного типу атаки. Можливість самонавчання без ручного налаштування кожного компонента і потенційне зниження хибних спрацювань через вдосконалення системи, завдяки самонавчанню та багатоалгоритмічному підходу, система не залежить від одного вектора виявлення. Також система може ефективно працювати в розподіленому середовищі IoT, SCADA та мереж промислового зв’язку.

З недоліків можна виділити висока обчислювальна складність та ресурсоємність, потребу у великих масивах навчальних даних. У деяких моделях – складність верифікації рішень «чорний ящик» [28].

Щодо практичного застосування концепції методу створення кіберсистем на основі біоміметичних алгоритмів для захисту ОКІ, можна навести приклад в енергетичній сфері, а саме найкориснішим застосуванням буде захист систем підстанцій та SCADA-центрів від атак типу BlackEnergy. Це тип шкідливого програмного забезпечення, яке використовується для кібератак, зокрема,

націлених на критично важливу інфраструктуру, таку як електромережі та промислові системи. Потрапивши в систему, він може виконувати різноманітні зловмисні дії, включаючи крадіжку даних, моніторинг активності та навіть порушення роботи або пошкодження критичної інфраструктури, використовуючи слабкі місця в цільових системах. Зловмисники можуть дистанційно керувати системами, зараженими BlackEnergy, що дає їм можливість спричиняти широкомасштабні збої та пошкодження критично важливих служб [29]. Крім енергетичної сфери, цілком логічним буде використання даного методу в урядовій інфраструктурі. Це знизить масовані DDoS-атаки, фішингу, а також буде відбуватися динамічний захист систем документообігу.

Шляхом порівняння трьох методів між собою у кожному з них є свої переваги та недоліки.

3.2. Дослідження біоміметичних підходів, що базуються на глибокому Q-навчанні

Дослідження вдосконалює стратегії для управління центрами операцій з кібербезпеки та розгортання систем управління інформацією про безпеку, інтегруючи точність відомих біоміметичних алгоритмів оптимізації, а саме: оптимізації рою частинок, алгоритму кажана, оптимізатора сірого вовка та алгоритму хижака косаток, з адаптивністю Deep Q-Learning, методу навчання з підкріпленням, який використовує глибокі нейронні мережі для навчання алгоритмів оптимальним діям методом спроб і помилок у складних середовищах. Ця гібридна методологія спрямована на ефективне розподілення та розгортання датчиків виявлення вторгнень у мережу, одночасно балансуючи економічну ефективність з важливими імперативами безпеки мережі. Комплексні обчислювальні тести показують, що версії, вдосконалені за допомогою Deep Q-Learning, значно перевершують свої рідні аналоги, особливо в складних інфраструктурах [30].

У цьому дослідженні пропонується передовий гібридний алгоритм, який поєднує метаевристичні алгоритми з навчанням з підкріпленням для ефективного пошуку та визначення оптимальних рішень у задачах глобальної оптимізації. Даний підхід спрямований на досягнення делікатного балансу між дослідженням та експлуатацією, поступово пропонуючи більш вигідні рішення з часом, уникаючи при цьому пасток передчасної конвергенції. Алгоритм Q-Learning Vegetation Evolution, є прикладом інтеграції Q-Learning для оптимізації покриття в числових та бездротових сенсорних мережах.

На рисунку 3.1 показано спільний робочий процес між біо-натхненними алгоритмами та DQL, демонструючи ефективну та результативну методологію оптимізації, яка поєднує дослідження, натхненне природою, з адаптивним навчанням DQL.

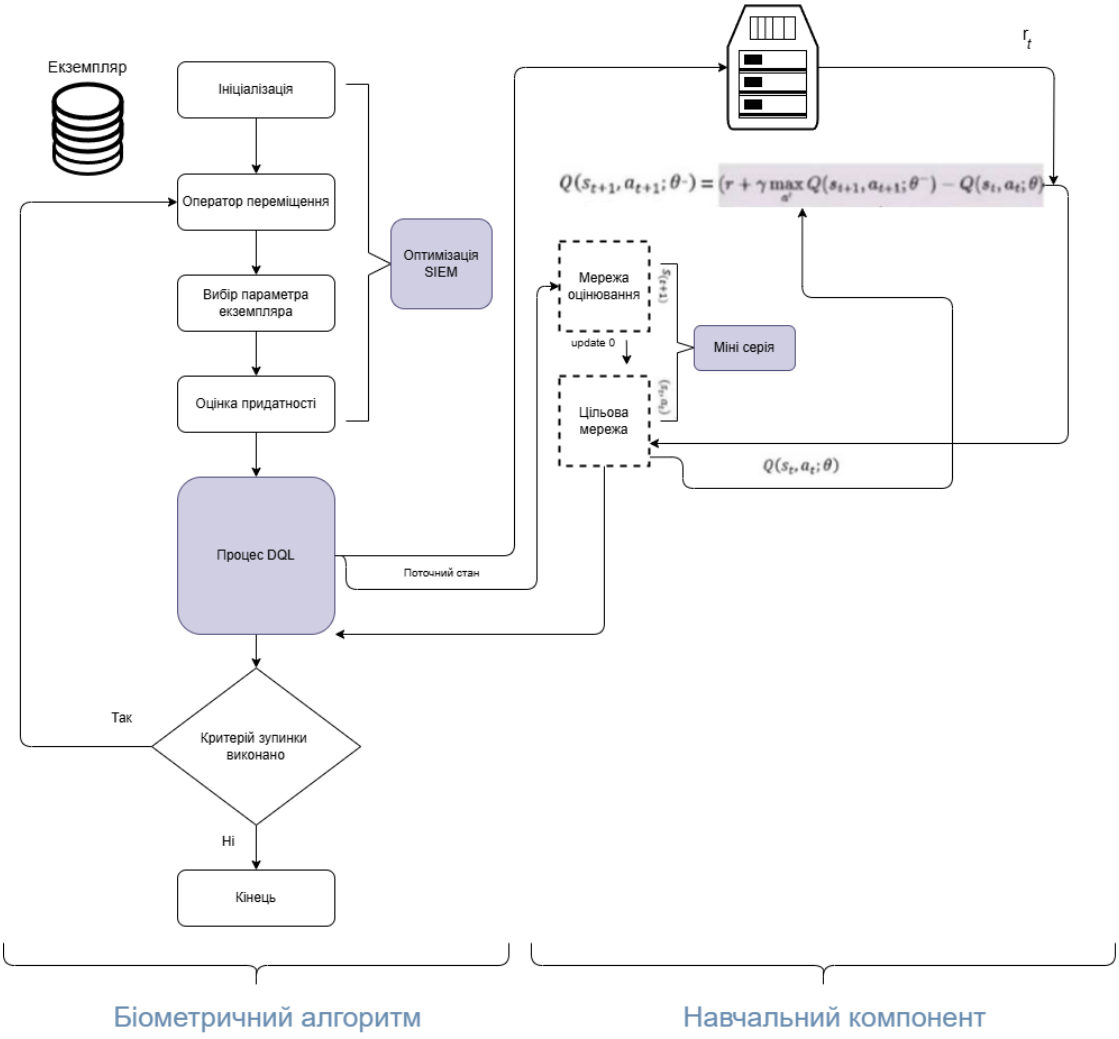

Рисунок 3.1 – Рішення розроблено з використанням чотирьох метаевристик з глибоким Q-навчанням.

Стратегія навчання з підкріпленням DQL точно налаштовує робочі параметри цих алгоритмів, навчаючись на їхніх результатах продуктивності для покращення балансу між дослідженням та використанням. Завдяки пам’яті відтворення DQL отримує користь від історичних даних, поступово покращуючи картографування датчиків NIDS для системи SIEM.

Цей підхід, що включає поєднання стратегій експлуатації та дослідження, а також використання онлайн-Q-Learning для динамічної адаптації, демонструє значні покращення порівняно з традиційними методами завдяки ретельному тестуванню на еталонних функціях CEC2020 та реальних інженерних проблемах.

Обчислювальна складність метаевристики становить $O\,(kn)$, де n – розмірність проблеми, а k – кількість ітерацій або розмір популяції, що відображає загальну кількість обчислень функцій під час виконання алгоритму. Постійний розвиток обчислювальних технологій допомагає компенсувати вплив цієї підвищеної складності.

Для експериментального етапу було запропоновано сорок екземплярів. Ці екземпляри включали випадкові робочі параметри, які детально описані нижче для кожного екземпляра: кількість робочих VLAN, типи використовуваних датчиків, наприклад, IDS, моніторингові або поведінкові сенсори), що відрізняються вартістю, точністю та сферою застосування, діапазон вартості датчиків що враховує фінансові обмеження під час проєктування системи, діапазон переваг, пов’язаних з встановленням датчика в певній VLAN, діапазон непрямих витрат, які можуть виникнути у разі відсутності моніторингу в певному сегменті (наприклад, втрати через затримку виявлення), понесених, коли датчик не встановлено в даній VLAN, та ймовірність непрацездатності даної VLAN,що моделює ризики технічного збою або успішного вторгнення в конкретний сегмент.

Кількість у 40 екземплярів була обрана як компроміс між статистичною репрезентативністю та обчислювальними витратами, що дозволяє охопити широку множину умов без втрати керованості над результатами. В кожному екземплярі враховувались обмеження на кількість доступних сенсорів, що імітує

реальні обмеження в ресурсах. Це дозволило моделювати задачу як задачу оптимального розміщення з обмеженими ресурсами, що наближено до практичних умов захисту об'єктів критичної інфраструктури.

Підхід до формування експериментального середовища забезпечив можливість ретельного тестування біоміметичних алгоритмів та їх покращених версій з інтеграцією Deep Q-Learning, дозволяючи провести достовірне порівняння ефективності різних підходів в умовах складної та динамічної топології мережі.

Конкретні значення для кожного екземпляра детально наведено в Таблиці 3.1.

Таблиця 3.1

Специфікація робочих параметрів для сорока екземплярів.

Екземпляр	**Кількість VLAN**	**Тип датчиків**	**Час безперебійної роботи**	**Діапазон прямих витрат**	**Діапазон якісного прибутку**	**Діапазон непрямих витрат**	**Продуктивність підмереж**
1	10	2	90%	[100–150]	[1–20]	[1–7]	[0.39–0.80]
2	10	2	90%	[100–150]	[5–20]	[1–7]	[0.10–0.80]
3	10	2	90%	[100–150]	[1–20]	[1–7]	[0.02–0.80]
4	10	2	90%	[100–150]	[1–20]	[1–5]	[0.11–0.80]
5	15	2	90%	[100–150]	[1–20]	[1–7]	[0.14–0.85]
6	15	2	90%	[100–150]	[1–20]	[1–7]	[0.01–0.94]
7	15	2	90%	[100–150]	[1–20]	[1–7]	[0.01–0.94]
8	15	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.96]
9	15	2	90%	[100–150]	[1–20]	[3–7]	[0.07–0.96]
10	20	2	90%	[100–150]	[1–20]	[1–7]	[0.04–0.61]
11	20	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.56]

продовження таблиці 3.1

12	20	2	90%	[100–150]	[1–20]	[1–7]	[0.10–0.91]
13	20	2	90%	[100–150]	[1–20]	[1–7]	[0.01–0.99]
14	20	2	90%	[100–150]	[1–20]	[1–7]	[0.05–0.88]
15	25	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.96]
16	25	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.96]
17	25	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.89]
18	25	2	90%	[100–150]	[1–20]	[1–5]	[0.08–0.97]
19	25	2	90%	[100–150]	[1–20]	[1–7]	[0.06–0.99]
20	30	2	90%	[100–150]	[10–20]	[1–7]	[0.50–0.89]
21	30	2	90%	[100–150]	[1–20]	[1–7]	[0.22–0.89]
22	30	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.96]
23	30	2	90%	[100–150]	[1–20]	[1–7]	[0.08–0.97]
24	30	2	90%	[100–150]	[1–20]	[1–7]	[0.05–0.98]
25	35	2	90%	[100–150]	[1–20]	[1–7]	[0.10–0.96]
26	35	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.94]
27	35	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.94]
28	35	2	90%	[100–150]	[1–20]	[1–7]	[0.03–0.98]
29	35	2	90%	[100–150]	[1–20]	[1–7]	[0.08–0.98]
30	40	2	90%	[100–150]	[1–20]	[1–7]	[0.06–0.98]
31	40	2	90%	[100–150]	[1–20]	[1–7]	[0.05–0.98]
32	40	2	90%	[100–150]	[1–20]	[1–7]	[0.04–0.97]
33	40	2	90%	[100–150]	[1–20]	[1–7]	[0.16–0.93]
34	40	2	90%	[100–150]	[1–20]	[1–7]	[0.09–0.95]
35	45	2	90%	[100–150]	[1–20]	[1–7]	[0.01–0.95]
36	45	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.97]
37	45	2	90%	[100–150]	[1–20]	[1–7]	[0.01–0.95]
38	45	2	90%	[100–150]	[1–20]	[1–7]	[0.03–0.97]
39	45	2	90%	[100–150]	[1–20]	[1–7]	[0.07–0.96]
40	50	2	90%	[100–150]	[1–20]	[1–7]	[0.02–0.84]

Після зміни вектора розв'язку стає необхідним реалізувати крок бінаризації для використання неперервних метаевристик у бінарній області [31]. Метою було розробити плани та запропонувати рекомендації для випробувальної фази, тим самим продемонструвавши, що рекомендована стратегія є можливим рішенням для визначення місця розташування датчика NIDS. Час, необхідний для розв'язання задачі, було розраховано для оцінки тривалості метаевристик, необхідних для досягнення ефективних рішень. Було використано найвище значення як критичний показник для оцінки подальших результатів.

$$\sum_{(p,q)_{p\neq q}\in K} \frac{f_p(\overrightarrow{x})}{\underbrace{e_p(\overrightarrow{x}^{best})}_{max}}\omega_p + \frac{\hat{c}-f_q(\overrightarrow{x})}{\underbrace{\hat{c}-e_q(\overrightarrow{x}^{best})}_{min}}\omega_q,\ \omega_{(p,q)} \geq 0 \qquad (3.1)$$

де $\omega_{(p,q)}$ представляє вагу цільових функцій та $\sum \omega_{(p,q)} = 1$ повинні бути задоволені. Значення $\omega_{(p,q)}$ визначаються аналогічним оцінюванням. $f_{(p,q)}(\overrightarrow{x})$ є одноцільовою функцією та $e_{(p,q)}(\overrightarrow{x}^{best})$ зберігає найкраще значення, знайдене незалежно. Зрештою, $\hat{c}$ є верхньою межею мінімізації одноцільових функцій. Після цього було застосовано порядковий аналіз для оцінки адекватності стратегії. Згодом було детально розглянуто апаратне та програмне забезпечення, що використовувалися для дублювання обчислювальних експериментів. Результати зображено у вигляді таблиць та графіків.

Тестові сценарії були розроблені з використанням стандартних змодельованих мереж, призначених для імітації поведінки та характеристик реальних мереж. Ці симуляції представляють експлуатаційні характеристики мереж в організаціях різного розміру, від малих до середніх та великих. Залежно від масштабу та обсягу, що визначається кількістю VLAN, кожна VLAN складається з кількох пристроїв, таких як комп'ютери, комутатори та серверні ферми, а також пов'язаних з ними з'єднань. У дослідженні оцінювалися тестові мережі різного розміру, починаючи від мереж з десятьма VLAN, переходячи до мереж з двадцятьма п'ятьма VLAN та поширюючись на більш розгалужені мережі з кількістю до п'ятдесяти VLAN. У симуляції враховувалися такі

обмеження, як пропускна здатність, затримка, втрата пакетів та перевантаження мережі, шляхом реплікації тестових мереж та врахування їхніх функціональних та робочих властивостей. Також для цього дослідження було вкрай важливо, щоб мережі підтримували мінімальну доступність 90%, оскільки перебої та періоди простою можуть виникати через відмову обладнання, перевантаження мережі або проблеми з підключенням. Впровадження проактивного моніторингу через SIEM забезпечить високу доступність мережі.

Щоб представити результати графічно, виконано завдання аналізу та порівняння вибірок, отриманих з непараметричних базових процесів, тобто процесів, дані яких не мають нормального розподілу (рис. 3.2 – 3.5). З огляду на це, стало необхідним використовувати інструмент візуалізації, такий як violin diagram, яка адекватно враховує непараметричну природу даних і забезпечує чітке та детальне уявлення про їхні відповідні розподіли. Візуалізація цих графіків дозволяє консолідувати раніше проаналізовані результати, що відповідають метриці оцінки. Найскладніші випадки виявились від 15 до 22 включно.

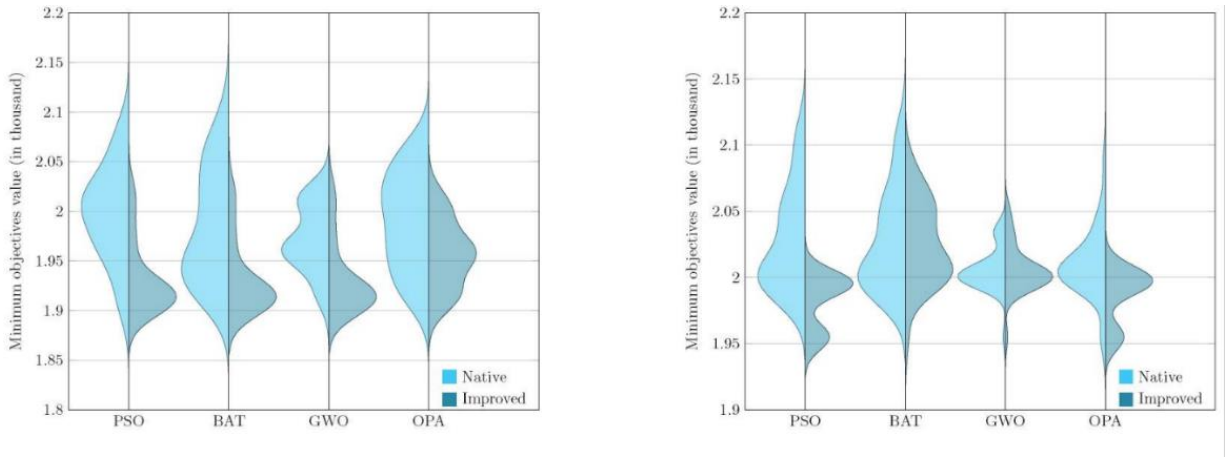

Рисунок 3.2 – Розподіл обчислювальних результатів між покращеними біоміметичними алгоритмами та їх рідними версіями. Найскладніші випадки 15,16.

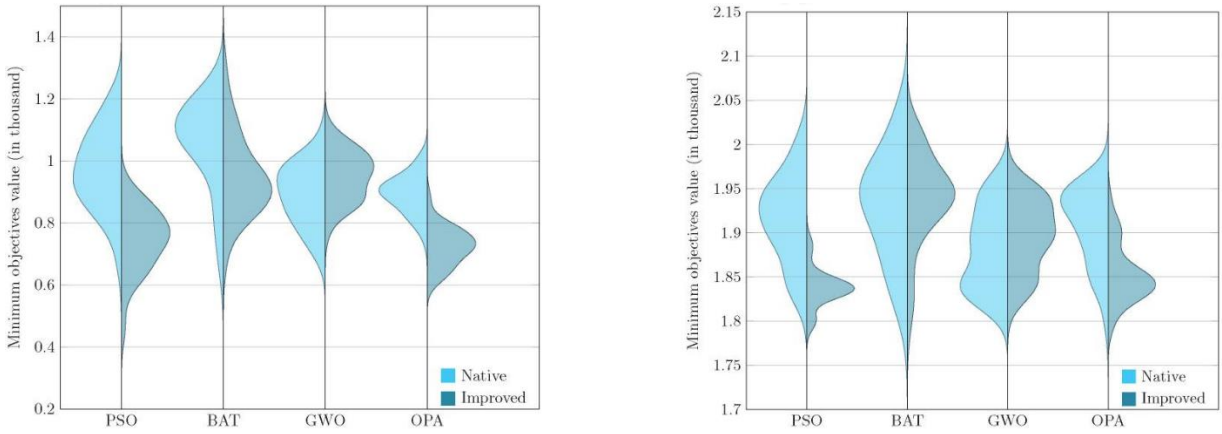

Рисунок 3.3 – Розподіл обчислювальних результатів між покращеними біоміметичними алгоритмами та їх рідними версіями. Найскладніші випадки 17,18.

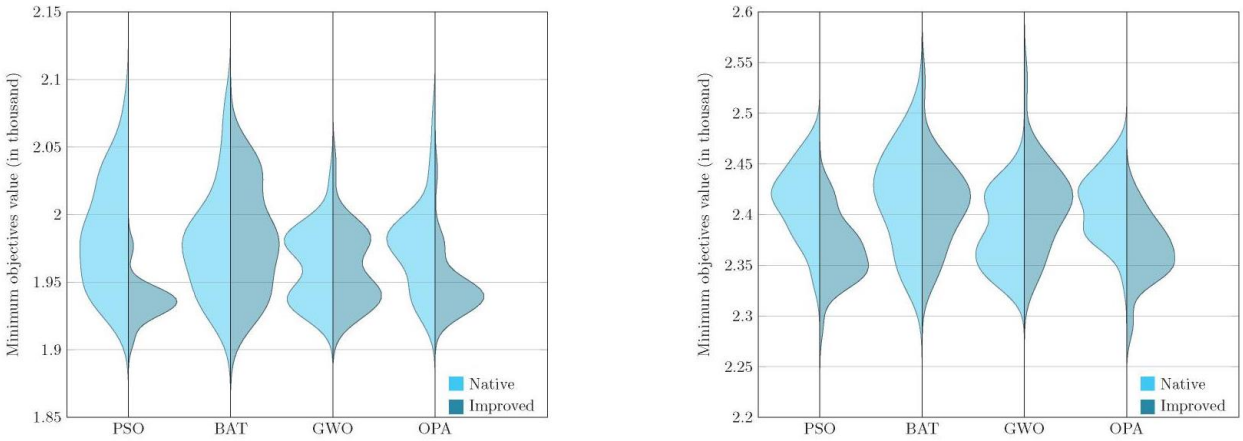

Рисунок 3.4 – Розподіл обчислювальних результатів між покращеними біоміметичними алгоритмами та їх рідними версіями. Найскладніші випадки 19,20.

Для випадків з сімнадцяти по двадцять, окрім незначного стандартного відхилення в метаевристиках з Q-Learning, медіани для PSODQL та OPADQL значно нижчі, ніж для їхніх нативних аналогів. Сценарії з 17-го по 20-й випадки, імовірно, характеризуються більш складною топологією мережі або збільшеним числом конфліктуючих параметрів, через що стандартні алгоритми без компонентів навчання демонструють менш ефективну оптимізацію.

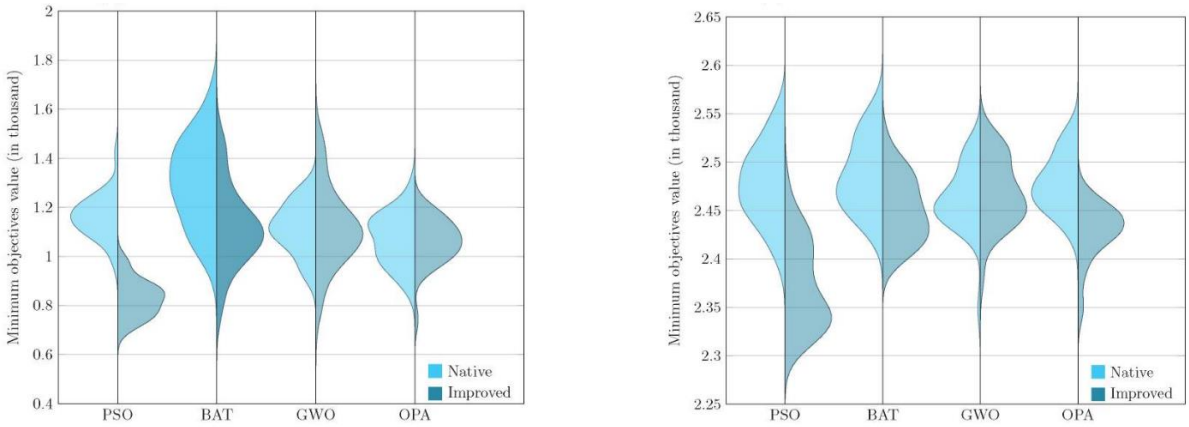

Рисунок 3.5 – Розподіл обчислювальних результатів між покращеними біоміметичними алгоритмами та їх рідними версіями. Найскладніші випадки 21,22.

Діаграма демонструє узагальнену статистику, таку як медіани та квартилі, а також щільність даних вздовж її діапазону. Вона допомагає виявляти та аналізувати суттєві відмінності між двома вибірками, пропонуючи розуміння закономірностей та структури даних. Діаграма виконує порівняльну функцію між різними вибірками, сприяючи виявленню суттєвих відмінностей між ними. Це, в свою чергу, дозволяє робити обґрунтовані висновки про переваги одного підходу чи методу, залежно від контексту дослідження. Завдяки такому представленню користувач отримує цілісне уявлення про закономірності в даних, їхню неоднорідність та потенційні фактори, що впливають на результати.

Таким чином, ми можемо зрозуміти, що у випадках п’ятнадцять та шістнадцять стандартне відхилення в метаевристиках з DQL є невеликим порівняно з нативними метаевристиками, особливо PSODQL, BATDQL та OPADQL. Крім того, медіана в PSODQL у випадку п’ятнадцять набагато нижча, ніж у нативному PSO (табл. 3.2).

Варто зазначити, що візуалізацію рішень з першого по чотирнадцятий екземпляр неможливо зобразити у вигляді графіка, оскільки вони здебільшого генерують однакові статистичні значення.

Таблиця 3.2

Результати дослідження

Екземпляри	**PSO проти PSO DQL**	**PSODQL проти PSO**	**BAT проти BAT DQL**	**BATDQL проти BAT**	**GWO проти GWODQL**	**GWO DQL проти GWO**	**OPA проти OPA DQL**	**OPADQL проти OPA**
15	–	1.4×10^{-12}	–	–	–	–	–	1.5×10^{-3}
16	–	6.5×10^{-15}	–	–	–	–	–	1.5×10^{-12}
17	–	4.2×10^{-16}	–	7.1×10^{-4}	1.1×10^{-2}	–	–	2.4×10^{-15}
18	–	4.8×10^{-16}	–	–	–	–	–	1.1×10^{-13}
19	–	3.7×10^{-15}	–	–	–	–	–	4.6×10^{-12}
20	–	1.8×10^{-13}	–	–	–	–	–	2.6×10^{-13}
21	–	4.2×10^{-15}	–	4.5×10^{-3}	7.1×10^{-4}	–	–	–
22	–	4.1×10^{-17}	–	3.5×10^{-4}	–	–	–	1.8×10^{-15}

Підтверджено, що з п’ятнадцятого та шістнадцятого випадків існують значні відмінності між зразками, згенерованими за допомогою PSODQL та нативного PSO, що робить висновок про покращення результатів, отриманих за допомогою PSODQL. Для BAT та BATDQL немає суттєвих відмінностей між зразками; те саме стосується GWO та GWODQL. Однак для OPA та OPADQL існує суттєва різниця між зразками. PSODQL демонструє більш помітне покращення, оскільки має більш значну різницю, ніж OPADQL, оскільки отримане p -значення нижче, як підтверджено в таблиці. У сімнадцятому випадку для зразків, згенерованих за допомогою PSO, існує значна різниця між зразками, що призводить до кращої продуктивності PSODQL; те саме відбувається з BAT, що призводить до кращого BATDQL; для нативного GWO він кращий, ніж GWODQL, а для зразків, згенерованих за допомогою OPA, існує значна різниця, що призводить до кращого OPADQL. У вісімнадцятому та дев’ятнадцятому випадках підтверджено, що PSODQL кращий за PSO. Для BAT та BATDQL між

зразками немає суттєвих відмінностей, як і для GWO та GWODQL. Більше того, OPADQL кращий для OPA, оскільки між зразками є суттєві відмінності. В обох випадках PSODQL кращий, оскільки має найнижче значення *p*. У двадцятому випадку PSODQL та OPADQL показують значні відмінності між своїми зразками; однак OPADQL кращий, оскільки має найнижче значення *p*. У двадцять першому випадку, враховуючи отримані результати, PSODQL кращий за нативний PSO, і те саме стосується BAT; для GWO нативний GWO кращий, а для OPADQL між зразками немає суттєвих відмінностей. У цьому випадку PSODQL кращий, оскільки має найнижче значення *p*.

p – значення, отримані за допомогою тесту Вілкоксона-Манна-Вітні.

Центральною метою цього дослідження було оцінити вплив інтеграції методу глибокого Q-навчання (Deep Q-Learning) у традиційні метаевристики для підвищення їхньої ефективності в задачах оптимізації. Результати показують, що версії, вдосконалені Deep Q-Learning, зокрема PSODQL, BATDQL та OPADQL, продемонстрували кращу продуктивність порівняно з їхніми рідними аналогами.

Представлене дослідження вирішує проблему підвищення ефективності центрів кібербезпеки шляхом інтеграції біоміметичних алгоритмів та глибокого Q-навчання, методу навчання з підкріпленням. Цей підхід пропонується для покращення розгортання датчиків у мережевих інфраструктурах, балансуючи імперативи безпеки з витратами на розгортання. Дослідження ґрунтується на передумові, що динамічний характер кіберзагроз вимагає адаптивних та ефективних рішень для управління кібербезпекою. Порівняльний аналіз між власними біоміметичними алгоритмами та тими, що були вдосконалені за допомогою DQL, виявив помітне покращення точності та узгодженості отриманих рішень. Це покращення пояснюється здатністю DQL динамічно адаптувати та точно налаштовувати параметри алгоритмів, зосереджуючи пошук на найперспективніших областях простору рішень. Крім того, реалізація пам’яті повторення та стратегії міні-пакетів у DQL сприяла ефективності навчання та стабільності навчання.

Дослідження підкреслює важливість інтеграції методів машинного навчання з алгоритмами оптимізації для вирішення складних проблем кібербезпеки. Майбутні роботи можуть бути спрямовані на створення адаптивних механізмів захисту шляхом інтеграції біоміметичних алгоритмів з глибоким Q-навчанням, зосереджуючись на реагуванні на загрози в режимі реального часу та еволюційних рамках безпеки. Це передбачатиме впровадження етичних принципів штучного інтелекту, щоб гарантувати, що ці передові системи функціонуватимуть без упереджень та з повагою до конфіденційності.

3.3. Проведення експертного оцінювання біоміметичних підходів до виявлення вторгнень

Оцінка ефективності біоміметичних підходів до виявлення вторгнень, зокрема моделей, які базуються на поєднанні біоінспірованих алгоритмів та методів глибокого Q-навчання проводиться на основі результатів попереднього дослідження. Оцінка проводиться з використанням методу експертного аналізу, що дозволяє узагальнити думки кваліфікованих фахівців у галузі кібербезпеки.

Метою експертного оцінювання є визначення переваг та недоліків подібних моделей у контексті захисту об’єктів критичної інфраструктури, а також оцінка доцільності використання Deep Q-Learning у поєднанні з біоміметичними алгоритмами. Для оцінювання потрібно залучити 5 фахівців із досвідом роботи у сферах:

- проектування КСЗІ на ОКІ;
- машинного навчання в мережевій безпеці;
- промислових систем управління (ICS/SCADA);
- кіберрозвідки та аналізу загроз;
- моделювання адаптивних систем.

Чому обрані саме ці категорії експертів: фахівці з проектування КСЗІ на ОКІ мають глибоке розуміння реальної структури систем захисту та вимог до сертифікації, що особливо важливо при оцінці масштабованості рішень.

Спеціалісти з машинного навчання та кібербезпеки розуміють як працюють біоміметичні моделі Deep Q-Learning, та можуть об’єктивно оцінити їхню ефективність, ресурсоємність та адаптивність. Інженери SCADA/ICS-систем на практиці експлуатують критичну інфраструктуру, тож здатні оцінити, чи реально впровадити такі алгоритми у виробничих умовах. Аналітики кіберзагроз володіють знанням актуальних векторів атак і можуть передбачити, наскільки стійка система до сучасних загроз. Фахівці з моделювання адаптивних систем в свою чергу об’єктивно оцінюють методології побудови моделей і рівень навчання.

У експертному оцінюванні середній бал обчислюється математично за формулою: Середній бал $= \frac{\sum_{i=1}^{N} x_i}{N}$, де x_i – оцінка i-го експерта за певним критерієм, а N – кількість експертів.

Виходячи з дослідження, доцільно оцінити наступні критерії досліджувальної моделі:

– Оптимальність розміщення сенсорів. Цей критерій відображає головну мету дослідження – це ефективне стратегічне розташування засобів виявлення загроз у мережі. Вибір обґрунтовано прямою залежністю між алгоритмічною ефективністю і здатністю накривати всі потенційні вектори вторгнення.

– Гнучкість і адаптація до змін у середовищі. Deep Q-Learning використовується у дослідженні саме як механізм підвищення динамічності реагування системи, тобто вона змінює свою поведінку залежно від поточних загроз. Критерій дозволяє оцінити здатність системи навчатися та переорієнтовуватись без людського втручання.

– Стійкість до багатовекторних атак

Враховуючи, що об’єкт критичної інфраструктури зазнає не лише однотипних атак, а складних комбінованих загроз, важливо оцінити здатність системи виявляти і правильно класифікувати нестандартні й комбіновані атаки.

– Практичність для впровадження в інфраструктурі. На жаль не всі моделі, які ефективні в симуляціях, можна адаптувати до SCADA, IoT чи енергетичних

мереж. Даний критерій відображає придатність моделі до розгортання з урахуванням технічних і нормативних обмежень.

– Час навчання та обчислювальна складність. Цей критерій оцінює баланс між продуктивністю та вартістю/складністю її досягнення, біоміметичні алгоритми що ґрунтуються на глибокому навчанні, можуть бути надзвичайно ресурсоємними як фінансово так і технічно, особливо на етапі навчання моделі.

– Інтерпретованість результатів для користувача. Для систем захисту ОКІ важливо не лише діяти, а й обґрунтовувати свої дії. Такі алгоритми, як Deep Q-Learning, часто сприймаються як «чорна скринька», тому ця характеристика є критично важливою.

Використовуючи середовище Visual Studio Code і мову програмування Python було зроблено програму – матрицю експертного оцінювання (обрахунку) для аналізу біоміметичної моделі з Deep Q-Learning.

```
import pandas as pd
from openpyxl import load_workbook
from openpyxl.styles import Font, Alignment
from openpyxl.utils import get_column_letter
```

Дана частина коду відповідає за підключення всіх необхідних бібліотек для проведення розрахунку середнього балу на основі оцінки експертів, а також для комфортного перегляду вихідних даних в Excel.

```
criteria = [
    "Оптимальність розміщення сенсорів",
    "Адаптивність до змін у середовищі",
    "Стійкість до багатовекторних атак",
    "Практичність для впровадження",
    "Час навчання та обчислювальна складність",
    "Інтерпретованість результатів"
]
```

Вищеописана частина коду створює 6 критеріїв попередньо визначених для проведення експертного оцінювання.

Умовні експертні оцінки (на основі висновків авторів):

```
data = [ # None або конкретні значення
   ["Експерт 1", 5, 5, 4, 3, 3, 2],
   ["Експерт 2", 5, 5, 5, 4, 3, 3],
   ["Експерт 3", 4, 4, 5, 4, 2, 2],
   ["Експерт 4", 5, 5, 4, 3, 3, 2],
   ["Експерт 5", 5, 5, 5, 3, 3, 3],
]
```

Ліворуч вказані номера експертів, всього їх 5. Важливо зазначити, що оцінки, продемонстровані праворуч, є лише умовними і зроблені на основі висновків авторів дослідження. При виконанні іншого дослідження дані параметри можна спокійно змінювати як самі оцінки так і кількість експертів.

```
df = pd.DataFrame(data, columns=["Експерт"] + criteria)
df["Середній бал"] = df[criteria].mean(axis=1).round(2)
average_row = ["Середнє значення"] + df[criteria].mean().round(2).tolist() + [df["Середній бал"].mean().round(2)]
df.loc[len(df)] = average_row
print(df)
df.to_excel("Оцінювання_DeepQL.xlsx", index=False)
from openpyxl import load_workbook
from openpyxl.styles import Font, Alignment
from openpyxl.utils import get_column_letter
filename = "оцінювання_DeepQL.xlsx"
wb = load_workbook(filename)
ws = wb.active
```

Дана частина коду створює датафрейм, проводить розрахунок середнього балу по кожному експерту використовуючи *df[criteria].mean(axis=1).round(2)*, а також по кожному критерію за допомогою *average_row* і в кінці проводить виведення й збереження файлу в Excel.

Результат дослідження маємо наступний (табл. 3.3):

Таблиця 3.3

Результати експертного оцінювання

Експерт	**Оптимальність розміщення сенсорів**	**Адаптивність до змін у середовищі**	**Стійкість до багатовекторних атак**	**Практичність для впровадження**	**Час навчання та обчислювальна складність**	**Інтерпретованість результатів**	**Середній бал**
Експерт 1	5	5	4	3	3	2	3,67
Експерт 2	5	5	5	4	3	3	4,17
Експерт 3	4	4	5	4	2	2	3,5
Експерт 4	5	5	4	3	3	2	3,67
Експерт 5	5	5	5	3	3	3	4
Середнє значення	4,8	4,8	4,6	3,4	2,8	2,4	3,8

Виходячи з результатів оцінки можна зробити висновок: модель безумовно має як сильні так і слабші сторони. Сильними сторонами моделі є висока здатність адаптуватися до нових або змінних загроз. Завдяки Q-learning модель швидко оновлює політики реагування, виявляючи навіть складні, раніше невідомі типи атак. При використанні алгоритму біоміметичної оптимізації, модель повинна забезпечувати покриття ключових точок мережі з мінімальною кількістю сенсорів. Також комбіновані атаки й багатоетапні сценарії вторгнення не знижують ефективність виявлення, що підтверджується стабільно високими оцінками. Говорячи про слабкі сторони можна визначити низька інтерпретованість результатів, що значно ускладнює аудит та сертифікацію в реальному житті. Незважаючи на ефективність, впровадження в реальні SCADA або ICS-середовища потребує адаптації та технічного доопрацювання.

Модель, що базується на Deep Q-Learning у поєднанні з біометричними алгоритмами, має високий потенціал для захисту об’єктів критичної

інфраструктури, її варто впроваджувати як частину багаторівневої системи захисту в середовищах з достатнім обчислювальним ресурсом.

3.4. Вибір оптимального методу захисту на основі багатокритеріального аналізу

Розглянуто основні підходи до захисту об’єктів критичної інфраструктури від загроз і вторгнень, зокрема методи виявлення атак на основі класичних систем запобігання IDS/IPS та сучасних біоміметичних алгоритмів з використанням Deep Q-Learning. Результати проведеного експертного оцінювання та дослідження дозволили виявити сильні та слабкі сторони кожного з підходів.

Для вибору оптимального методу захисту на основі багатокритеріального аналізу використано метод зваженої суми (WSM – Weighted Sum Method) – це метод простих адитивних мас, який дозволяє особам, які ухвалюють рішення, призначати ваги критеріям як функції важливості. Загальна оцінка кожної альтернативи дорівнює сумі добутків коефіцієнтів та відповідних значень критеріїв альтернатив [32].

На основі логіки обираються декілька критеріїв, а саме:

- точність виявлення вразливостей;
- адаптивність до нових загроз;
- швидкодія;
- вартість впровадження;
- простота інтеграції.

Кожен з обраних критеріїв є важливим для подальшого розрахунку. Найважливішим критерієм є саме точність, бо помилки виявлення можуть привести до зупинки об’єкта критичної інфраструктури. Адаптивність до нових загроз треба для навчання методу протистояти новим загрозам, так як кібератакам властиво динамічно змінюватись. Вартість визначається задля подальшої економії фінансових ресурсів, в свою чергу швидкодія методу

впливає на ефективність використання. Останнім критерієм є простота інтеграції, вона є менш важливою в порівнянні з іншими наведеними критеріями.

Для початку необхідно визначити вагові коефіцієнти всіх критеріїв. Для цього використано шкалу Сааті. Під час побудови єдиної шкали різних компонентів проблеми метод ієрархічного аналізу застосовує міру ступеня впливу кожного фактора одного рівня на фактори вищого рівня або на кінцеву мету (табл. 3.4). Міра розробляється завдяки винесенню суджень про рівень важливості цих факторів.

Таблиця 3.4

Шкала відносної важливості

Показник порівняльної переваги одного об'єкта щодо іншого	**Міра важливості переваги**
Рівна важливість. Немає переваги	1
Слабка перевага за важливістю. Слабка перевага.	3
Сильна перевага за важливістю. Сильна перевага.	5
Значна перевага за важливістю. Дуже сильна перевага.	7
Абсолютна перевага. Абсолютна перевага.	9
Проміжна оцінка міри переваги між сусідніми значеннями	2, 4, 6, 8

Відповідно до представленої шкали Сааті кожен критерій порівнюється один з одним по важливості. У межах цього дослідження враховано специфіку задачі вибору оптимального методу захисту ОКІ, де ключовими пріоритетами є ефективність виявлення загроз та здатність адаптації до нових умов. Виходячи з цього, точність визначена як найважливіший критерій, адже саме вона безпосередньо впливає на здатність системи своєчасно реагувати на потенційні

атаки, а простота інтеграції є найменш важливим, можна отримати наступну матрицю (табл. 3.5):

Таблиця 3.5

Заповнення матриці

	Точність	**Адаптивність**	**Швидкодія**	**Вартість**	**Інтеграція**
Точність	1	2	5	5	7
Адаптивність	0.5	1	3	3	5
Швидкодія	0.2	0.333	1	2	3
Вартість	0.2	0.333	0.5	1	3
Інтеграція	0.143	0.2	0.333	0.333	1

Після цього сумуємо значення в кожному стовпці і ділимо кожен елемент на суму свого стовпця.

Далі для кожного рядка нормалізованої матриці обчислюється середнє значення. Ці середні значення є основою для визначення ваги кожного критерію в загальній системі оцінювання. Таким чином, для кожного критерію отримуємо числову оцінку його відносної важливості, виражену у вигляді ваги.

Далі визначаємо показник узгодженості (CR), щоб перевірити чи узгоджені оцінки, CR < 0.1 означає прийнятну узгодженість (табл. 3.6).

Таблиця 3.6

Результат знаходження вагового коефіцієнту

Критерій	**Вага**
Точність	0.32
Адаптивність	0.26
Вартість	0.18
Швидкодія	0.14
Інтеграція	0.10

Після того, як було знайдено ваговий коефіцієнт для кожного критерію, необхідно порівняти методи, а саме Класичні IDS/IPS-системи, системи з використанням машинного навчання і біоміметичні методи з використанням Deep Q-Learning та визначити найефективніший з них.

Таблиця результатів допомагає порівняти кожен із методів та чітко оцінити їхні сильні та слабкі сторони. Роблячи це, визначається найбільш підходящий способіб захисту об'єктів критичної інфраструктури з урахуванням сучасних викликів та загроз.

Для цього у кожного методу визначається підсумковий бал за допомогою таблиці (табл. 3.7), яка відображає не тільки числові показники, а й забезпечує аналітичну основу для подальшого обґрунтування вибору найбільш доцільного підходу.

Таблиця 3.7

Розрахунок підсумкових балів

Критерій	**Вага**	**IDS/IPS**	**Машинне навчання**	**Біоміметичні методи**
Точність виявлення атак	0.30	3	4	5
Адаптивність до нових загроз	0.25	2	4	5
Швидкодія	0.15	5	3	4
Вартість впровадження	0.20	5	3	3
Простота інтеграції	0.10	5	4	3

Маємо наступний результат:

– IDS/IPS – підсумковий бал: ~3.95.

– Машинне навчання – підсумковий бал: ~3.70.

– Біоміметичні методи (Deep Q-learning) – підсумковий бал: ~4.30.

За результатами багатокритеріального аналізу можна зробити висновок, що біоміметичні методи на основі Deep Q-learning показали найвищу сумарну оцінку (~4.30), завдяки своїй високій точності виявлення атак та адаптивності до нових загроз.

IDS/IPS-системи показали високу швидкодію та низьку вартість впровадження, проте поступаються в ефективності та адаптивності, що недостатньо для протидії сучасним атакам на ОКІ.

Методи машинного навчання показують середній результат, поступаючись біоміметичним підходам через меншу адаптивність і високу ресурсомісткість.

Висновок до третього розділу

У третьому розділі було здійснено комплексний аналіз методів протидії вторгненням на ОКІ, проведено дослідження використання біоміметичних підходів, зокрема тих, що є на основі Deep Q-Learning. Було проведено метод експертного оцінювання для порівняння ефективності представлених підходів відносно класичних методів виявлення та реагування на загрози.

Результати багатокритеріального аналізу показали, що біоміметичні алгоритми, завдяки своїм адаптивним властивостям та здатності до самонавчання, демонструють високі показники точності та адаптивності. Також спостерігається перевага в показниках швидкодії порівняно з традиційними підходами. Разом з тим, такі системи мають відносно вищу вартість реалізації та, в свою чергу, складність інтеграції. На основі експертного оцінювання визначено, що метод з використанням Deep Q-Learning у поєднанні з біометричними алгоритмами, має високий потенціал для захисту об’єктів критичної інфраструктури, але має високу вартість впровадження.

Багатокритеріальний аналіз з урахуванням вагових коефіцієнтів підтвердив доцільність застосування біоміметичних підходів на об’єктах критичної інфраструктури, особливо в умовах динамічного середовища та еволюції сучасних кіберзагроз. Підсумковий показник ефективності для біоміметичних методів склав приблизно 4.30 бала, що перевищує показники традиційних методів.

Незважаючи на високу складність інтеграції та вартість біоміметичних систем, отримані результати обґрунтовують їх вибір для ОКІ, де вартість компрометації суттєво перевищує витрати на захист. Біоміметичні системи захисту, зокрема на основі DQL, є перспективними у розвитку кіберзахисту ОКІ, особливо у випадках, де існує здатність системи до самостійної адаптації до нових типів атак.

ВИСНОВКИ

Існуючі методи захисту та чинні організаційно-технічні процедури, які застосовуються у мирний час, потребують актуалізації та вдосконалення з урахуванням нових викликів, пов’язаних із гібридними загрозами.

У процесі дослідження було здійснено аналіз основних термінів, пов’язаних з об’єктами критичної інфраструктури, процес категоризації та паспортизації об’єктів, а також проведено оцінку загроз інформаційній безпеці, які мають вирішальне значення для національної безпеки й економічної стабільності. Отримані дані засвідчують актуальність впровадження аналітичного підходу, здатного враховувати специфічні особливості кожного об’єкта, що дозволяє ефективно забезпечувати їхній захист від різноманітних загроз.

Проведено аналіз сучасних методів атак на об’єкти критичної інфраструктури та їх впливу на безпеку таких систем. Здійснено класифікацію основних типів вразливостей на ОКІ, серед яких виділено мережеві, шкідливе ПЗ і атаки соціальної інженерії, а також фізичні втручання. Окрім цього виділено увагу багатовекторним атакам та методам боротьби з ними. Окремо розглянуто сучасні техніки здійснення кібератак на ОКІ та атаки через ланцюги постачання. На реальних прикладах проаналізовано загрози для ОКІ, які підтверджують високий рівень ризиків для таких об’єктів. Найбільш критичними визнано атаки на енергетику, транспорт і засоби зв’язку. Також проаналізовано основні способи протидії атакам на ОКІ. Розглянуто як традиційні методи і сучасні підходи. Відзначено перспективність інтеграції біоміметичних алгоритмів для підвищення ефективності захисту.

Проведений аналіз підтвердив необхідність використання комплексної стратегії кіберзахисту ОКІ, що передбачає поєднання класичних засобів безпеки з інноваційними рішеннями, здатними адаптуватися до динамічних загроз. Досліджено методу захисту об’єктів критичної інфраструктури від вторгнень,

зосереджене на аналізі біоміметичних підходів, зокрема тих, що базуються на алгоритмах Deep Q-Learning. З метою об’єктивного порівняння ефективності різних методів було застосовано експертне оцінювання, яке дозволило зіставити інноваційні рішення з традиційними засобами виявлення. Результати багатокритеріального аналізу продемонстрували, що біоміметичні алгоритми вирізняються високою точністю та здатністю до адаптації завдяки механізмам самонавчання.

Багатокритеріальний аналіз із урахуванням пріоритетності критеріїв підтвердив доцільність впровадження таких підходів у середовищі з високою динамікою загроз. За результатами експертного аналізу встановлено, що поєднання Deep Q-Learning з біоміметичними методами має значний потенціал для підвищення рівня захисту ОКІ, хоча потребує більших ресурсів для реалізації.

Подальші дослідження можуть бути спрямовані на розробку нових методів захисту, зокрема використання штучного інтелекту, машинного навчання та інноваційних криптографічних технологій для забезпечення безпеки даних, дослідження комбінованих загроз, які поєднують фізичні, кібернетичні та соціоінженерні атаки, а також аналіз впливу таких загроз на взаємопов’язані об’єкти інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Об’єкти критичної інфраструктури України [Електронний ресурс]. – Режим доступу до ресурсу: https://www.kyivpost.com/uk/post/28283

2. Про критичну інфраструктуру [Електронний ресурс]: Закон України від 16.11.2021 № 1882-IX – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: Закон України від 05.07.1994 № 80/94-ВР – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

4. Загрози комп’ютерній безпеці: фізичні та нефізичні загрози [Електронний ресурс]. – Режим доступу до ресурсу: https://www.guru99.com/uk/potential-security-threats-to-your-computer-systems.html

5. ВПРОВАДЖЕННЯ НОВИХ ЗАСОБІВ І МЕТОДІВ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ [Електронний ресурс]. – Режим доступу до ресурсу: https://www.researchgate.net/publication/375048106_VPROVADZENNA_NOVIH_ZASOBIV_I_METODIV_PIDVISENNA_RIVNA_KIBERBEZPEKI_OB’EKTIV_KRITICNOI_INFRASTRUKTURI

6. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс]: Постанова Каб. Міністрів України від 19.06.2019 № 518 – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

7. Перелік засобів криптографічного захисту інформації, які мають експертний висновок за результатами державної експертизи у галузі КЗІ [Електронний ресурс]. – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/perelik-zasobiv-kriptografichnogo-zakhistu-informaciyi-yaki-mayut-ekspertnii-visnovok-za-rezultatami-derzhavnoyi-ekspertizi-u-galuzi-kzi

8. Нормативно-правова база у сфері захисту об’єктів критичної інфраструктури України [Електронний ресурс]. – Режим доступу: https://csirt.csi.cip.gov.ua/uk/pages/cio

9. Кібератака [Електронний ресурс]. – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack

10. Вразливість нульового дня [Електронний ресурс]. – Режим доступу до ресурсу: https://cybercalm.org/novyny/shho-take-vrazlyvist-nulovogo-dnya/

11. Pnyetya: Yet Another Ransomware Outbreak [Електронний ресурс]. – Режим доступу до ресурсу: https://web.archive.org/web/20170628131239/https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4

12. Канали витоку інформації [Електронний ресурс]. – Режим доступу до ресурсу: https://www.scribd.com/document/724694959/%D0%9B-5-%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8-%D0%B2%D0%B8%D1%82%D0%BE%D0%BA%D1%83-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97

13. Деякі питання об’єктів критичної інфраструктури [Електронний ресурс] Постанова Каб. Міністрів України від 9 жовтня 2020 р. № 1109 – Режим доступу: https://ips.ligazakon.net/document/KP201109?an=4

14. Мурасов, Р., Нікітін, А., Мещеряков, І., Підгородецький, М., & Поплавець, С. (2023). Методика оцінювання загроз і ризиків для об’єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій – С. 36-38.

15. У МЗС порівняли росію з ІДІЛ після заяви пєскова про обстріли заради переговорів [Електронний ресурс]. – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-ato/3616805-u-mzs-porivnali-rosiu-z-idil-pisla-zaavi-peskova-pro-obstrili-zaradi-peregovoriv.html

16. Assessing Russian Firepower Strikes in Ukraine [Електронний ресурс]. – Режим доступу до ресурсу: https://www.csis.org/analysis/assessing-russian-firepower-strikes-ukraine

17. Метод оцінювання загроз і ризиків для об’єктів критичної інфраструктури за сценаріями [Електронний ресурс]. – Режим доступу до ресурсу: https://www.google.com/url?sa=i&url=https%3A%2F%2Fsit.nuou.org.ua%2Farticle%2Fdownload%2F288288%2F287702%2F680660&psig=AOvVaw2viU8R5hAfWsj_LN94XtxM&ust=1745437733236000&source=images&cd=vfe&opi=89978449&ved=0CAYQrpoMahcKEwigmLuytOyMAxUAAAAAHQAAAAAQBA

18. What is an intrusion detection system (IDS)? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.ibm.com/think/topics/intrusion-detection-system

19. Dovbesko, S.V., Tolyapa, S.V. and Shestak, Y.V. (2019). Application of methods of data mining for the construction of attack detection systems. Modern information security, (1). doi:https://doi.org/10.31673/2409-7292.2019.010615.

20. МЕТОДИ ІНТЕЛЕКТУАЛЬНОГО РОЗПОДІЛУ ДАНИХ В СИСТЕМАХ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ ТА ФУНКЦІОНАЛЬНА СТІЙКІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ДО КІБЕРАТАК [Електронний ресурс]. – Режим доступу до ресурсу: https://www.researchgate.net/publication/371681647_METODI_INTELEKTUALNOGO_ROZPODILU_DANIH_V_SISTEMAH_VIAVLENNA_MEREZEVIH_VTORGNEN_TA_FUNKCIONALNA_STIJKIST_INFORMACIJNIH_SISTEM_DO_KIBERATAK

21. Операційний центр безпеки [Електронний ресурс]. – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-security-operations-center-soc

22. Withdrawn NIST Technical Series Publication [Електронний ресурс]. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

23. ENISA – Threat Landscape Reports [Електронний ресурс]. – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications

24. MITRE ATT&CK Framework [Електронний ресурс]. – Режим доступу до ресурсу: https://attack.mitre.org/

25. 1999 DARPA Intrusion Detection Evaluation Dataset [Електронний ресурс]. – Режим доступу до ресурсу: https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset

26. Anomaly Detection in Network Traffic Based on Machine Learning Algorithms [Електронний ресурс]. – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-030-61629-8_14

27. Unsupervised learning [Електронний ресурс]. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/unsupervised-learning/

28. Яка різниця між Black Box & White Box Testing? [Електронний ресурс]. – Режим доступу до ресурсу: https://training.qatestlab.com/blog/technical-articles/whats-the-difference-between-black-box-white-box-testing/

29. BlackEnergy [Електронний ресурс]. – Режим доступу до ресурсу: https://www.vpnunlimited.com/ua/help/cybersecurity/blackenergy

30. Olivares, R., Salinas, O., Ravelo, C., Soto, R., & Crawford, B. (2024). Enhancing the Efficiency of a Cybersecurity Operations Center Using Biomimetic Algorithms Empowered by Deep Q-Learning. Biomimetics, 9(6), 307 – pp. 12-28.

31. Crawford, B., Soto, R., Astorga, G., García, J., Castro, C., & Paredes, F. (2017). Putting continuous metaheuristics to work in binary search spaces. Complexity, 2017(1), 8404231 – pp. 3-6.

32. D, D. and O, K. (2022). URBAN DISTRIBUTION CENTER LOCATION. *The National Transport University Bulletin*, 1(51), pp.172–180. doi:https://doi.org/10.33744/2308-6645-2022-1-51-172-180.

ДОДАТОК А

```
import pandas as pd
from openpyxl import load_workbook
from openpyxl.styles import Font, Alignment
from openpyxl.utils import get_column_letter


criteria = [
    "Оптимальність розміщення сенсорів",
    "Адаптивність до змін у середовищі",
    "Стійкість до багатовекторних атак",
    "Практичність для впровадження",
    "Час навчання та обчислювальна складність",
    "Інтерпретованість результатів"
]
data = [ # None або конкретні значення
    ["Експерт 1", 5, 5, 4, 3, 3, 2],
    ["Експерт 2", 5, 5, 5, 4, 3, 3],
    ["Експерт 3", 4, 4, 5, 4, 2, 2],
    ["Експерт 4", 5, 5, 4, 3, 3, 2],
    ["Експерт 5", 5, 5, 5, 3, 3, 3],
]
df = pd.DataFrame(data, columns=["Експерт"] + criteria)
df["Середній бал"] = df[criteria].mean(axis=1).round(2)
average_row = ["Середнє значення"] + df[criteria].mean().round(2).tolist() +
[df["Середній бал"].mean().round(2)]
df.loc[len(df)] = average_row
print(df)
df.to_excel("Оцінювання_DeepQL.xlsx", index=False)
from openpyxl import load_workbook
from openpyxl.styles import Font, Alignment
```

```
from openpyxl.utils import get_column_letter
filename = "оцінювання_DeepQL.xlsx"
wb = load_workbook(filename)
ws = wb.active
font = Font(name='Arial', size=12)
bold_font = Font(name='Arial', size=12, bold=True)
alignment = Alignment(horizontal='center', vertical='center', wrap_text=True)
for row in ws.iter_rows():
    for cell in row:
        cell.font = font
        cell.alignment = alignment
for cell in ws[1]:  # Перший рядок
    cell.font = bold_font
for row in ws.iter_rows(min_row=2, max_row=ws.max_row):
    row[0].font = bold_font
# ширина
for i, column_cells in enumerate(ws.columns, 1):
    max_length = max(len(str(cell.value)) if cell.value else 0 for cell in column_cells)
    ws.column_dimensions[get_column_letter(i)].width = max_length + 5
# висота
for row in ws.iter_rows(min_row=1, max_row=ws.max_row):
    ws.row_dimensions[row[0].row].height = 35
wb.save(filename)
```

ДОДАТОК Б

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Копія наукової публікації

Толюпа С.В., Міщенко Н.А. Методи протидії вразливостям на об’єкти критичної інфраструктури. VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSICS)». – Київ 2025. – С. 144-145.

Методи протидії вразливостям на об’єкти критичної інфраструктури

Нікіта Міщенко[1], Сергій Толюпа[2]

[1] Кафедра кібербезпеки, Київський Національний університет імені Тараса Шевченка, Україна,
м.Київ, вул.Б.Гаврилишина, 24,
E-mail: bigporlono@gmail.com

[2] Кафедра кібербезпеки, Київський Національний університет імені Тараса Шевченка, Україна,
м.Київ, вул.Б.Гаврилишина, 24,
E-mail: serhii.toliupa@knu.ua

By reviewing established legal frameworks, documented case studies, and current best practices, the research aims to identify the strengths and weaknesses of conventional organizational and technical defenses versus modern solutions that

incorporate advanced information technologies. The expected outcome is to develop recommendations for integrating and enhancing security strategies, ultimately increasing the resilience of critical infrastructure against diverse cyber threats. The ultimate goal is to facilitate better decision-making and enhance the overall security posture of critical infrastructure.

Ключові слова – програмне забезпечення, критична інфраструктура, кібербезпека, прийняття рішень, інформаційна безпека, оцінка ефективності, загрози, кібератаки, захист об’єктів, методи протидії.

Вступ

В умовах триваючої збройної агресії росії проти України, забезпечення безпеки людини, суспільства та держави значною мірою залежить від стабільної роботи об’єктів критичної інфраструктури. Окрім використання летальної зброї для фізичного впливу, росія разом із союзниками активно застосовує кіберзброю для атак на системи управління таких об’єктів через кіберпростір. Особливе занепокоєння викликає той факт, що об’єкти критичної інфраструктури, які діють у єдиному інформаційному просторі та використовують сучасні інформаційні технології, попри значні зусилля для протидії втручанню через кіберпростір, залишаються вразливими до нових типів загроз. У сучасному світі критична інфраструктура є основою функціонування будь-якої держави, забезпечуючи стабільну роботу енергетичних, водопостачальних, транспортних, інформаційних та інших важливих систем. Однак, зростання глобальних загроз, таких як кібернапади, терористичні акти та військові агресії, ставить під загрозу безпеку цих об'єктів. Атаки на критичну інфраструктуру можуть призвести до серйозних економічних та соціальних наслідків, а також до порушення нормального функціонування суспільства.

Зважаючи на це, розробка ефективних методів протидії атакам на об’єкти критичної інфраструктури (ОКІ) є надзвичайно важливою для забезпечення національної безпеки, стабільності економіки та захисту життєво важливих

послуг. Вивчення та вдосконалення технологій і стратегій, що дозволяють знижувати ризики і підвищувати стійкість до атак, є пріоритетними завданнями в умовах сучасних глобальних викликів.

Аналіз ефективності традиційних та інноваційних методів протидії кібератакам на об’єкти критичної інфраструктури

Дослідження має на меті провести порівняльний аналіз існуючих методів захисту (організаційних, технічних, нормативних) із сучасними технологічними підходами, що застосовуються для протидії як кібернетичним, так і фізичним атакам.

Документ свідчить про недостатню адаптивність традиційних методів захисту в умовах гібридних загроз. Аналіз їх ефективності дозволить виявити слабкі місця та сформувати комплексну стратегію модернізації систем захисту критичної інфраструктури.

Можна виділити декілька основних методів дослідження, а саме аналіз нормативно-правової бази та стандартів захисту ОКІ; вивчення кейсів успішних та невдалих атак з практики (наприклад, приклади кібератак на енергетичну систему або транспортну інфраструктуру); моделювання сценаріїв атак з використанням методів багатокритеріального аналізу та експертного оцінювання [1].

Результати дослідження сприятимуть розробці рекомендацій для державних органів та операторів критичних об’єктів щодо модернізації систем захисту, що дозволить мінімізувати економічні та соціальні наслідки атак [2].

Розробка методології оцінки ризиків та вразливостей об’єктів критичної інфраструктури з використанням сучасних інформаційних технологій

Ця тема орієнтована на створення методології, яка дозволить комплексно оцінити рівень ризиків та вразливостей об’єктів критичної інфраструктури з

урахуванням як кібернетичних, так і фізичних загроз. Дослідження включає розробку моделей для ідентифікації слабких місць та побудови систем раннього попередження.

Сучасні загрози вимагають точного і оперативного аналізу ризиків. Документ акцентує увагу на комплексному підході до оцінки як технічних, так і організаційних аспектів безпеки. Це дослідження сприятиме підвищенню готовності систем до можливих атак [3].

Отримана методологія дозволить здійснювати комплексний моніторинг стану безпеки об’єктів критичної інфраструктури, сприятиме розробці ефективних заходів протидії та зниженню економічних втрат у разі виникнення інцидентів.

Аналіз впливу людського фактору на безпеку об’єктів критичної інфраструктури та розробка системи управління внутрішніми загрозами

Цей напрямок дослідження орієнтований на виявлення та аналіз основних вразливостей, пов’язаних з людським фактором, таких як інсайдерські атаки та недостатня підготовка персоналу. Метою є розробка системи управління внутрішніми загрозами та рекомендацій щодо підвищення кваліфікації співробітників.

Документ підкреслює важливість людського фактору як одного з ключових чинників безпеки об’єктів критичної інфраструктури. Розуміння внутрішніх загроз дозволяє не лише запобігати інцидентам, але й розробляти ефективні програми навчання та підвищення обізнаності співробітників [4].

Оцінка наслідків атак на ОКІ

Одним із найбільш очевидних наслідків є зупинка функціонування важливих державних та приватних структур. Наприклад, атака на енергетичний сектор може спричинити масові відключення електроенергії, що вплине на

роботу транспорту, систем водопостачання, лікарень, банків та інших критично важливих сервісів.

Наслідки таких атак варіюються залежно від типу ОКІ, рівня підготовленості до інцидентів та масштабів компрометації систем. Оцінка цих наслідків є критично важливою для розробки ефективних заходів кіберзахисту та мінімізації ризиків [5].

Фінансові втрати, пов’язані з кібератаками на ОКІ, можуть сягати мільярдів доларів. Компанії та державні установи змушені витрачати значні кошти на відновлення роботи систем, виплату викупу у разі атак програм-вимагачів, юридичні розгляди та штрафи за витік конфіденційних даних.

Одним із найсерйозніших наслідків є порушення національної безпеки та загроза суверенітету країни. Кібератаки, що здійснюються державами або спонсорованими хакерськими угрупованнями, можуть бути частиною гібридної війни, спрямованої на дестабілізацію країни. Виведення з ладу військових, урядових або правоохоронних систем може послабити здатність держави до реагування на кризові ситуації та загрожувати її обороноздатності. Окрім економічних та політичних наслідків, успішні атаки можуть спричинити фізичні руйнування та загибель людей. Якщо зловмисники отримують контроль над системами управління промисловими об'єктами, такими як гідроелектростанції, газопроводи або транспортні мережі, вони можуть спровокувати катастрофічні аварії. Витік конфіденційної інформації та компрометація даних також є серйозним наслідком атак на ОКІ. Якщо зловмисники отримують доступ до державних реєстрів, медичних записів, банківських баз даних або персональних даних громадян, це може призвести до масштабного шахрайства, шантажу, соціальних потрясінь та довготривалих репутаційних втрат для держави чи компаній.

Порушення довіри суспільства до цифрових сервісів є ще одним довготривалим наслідком кібератак. Якщо громадяни регулярно стикаються з витоками даних, неможливістю доступу до державних онлайн-послуг або

фінансовими втратами через атаки на банки, вони можуть втратити довіру до цифрових технологій загалом.

Висновок

У рамках статті проаналізовано ефективність різних методів протидії кібератакам на об’єкти критичної інфраструктури, наведено приклад методології, що дозволяє здійснювати комплексний моніторинг стану безпеки об’єктів. Окірм цього проведено аналіз нефізичних загроз, а саме вплив людського фактору на безпеку, а також проведено оцінку наслідків різних типів атак на ОКІ.

Література

[1] Деякі питання об'єктів критичної інфраструктури [Електронний ресурс] Постанова Каб. Міністрів України від 9 жовтня 2020 р. № 1109 – Режим доступу до ресурсу: https://ips.ligazakon.net/document/KP201109?an=4

[2] Нормативно-правова база у сфері захисту об'єктів критичної інфраструктури України [Електронний ресурс]. – Режим доступу до ресурсу: https://csirt.csi.cip.gov.ua/uk/pages/cio

[3] Впровадження нових засобів і методів підвищення рівня кібербезпеки об’єктів критичної інфраструктури [Електронний ресурс]. – Режим доступу до ресурсу: https://www.researchgate.net/publication/375048106_

[4] Загрози комп’ютерній безпеці: фізичні та нефізичні загрози [Електронний ресурс]. – Режим доступу до ресурсу: https://www.guru99.com/uk/potential-security-threats-to-your-computer-systems.html

[5] Про критичну інфраструктуру [Електронний ресурс]: Закон України від 16.11.2021 № 1882-IX – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-20#Text