**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ**
**КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ЗАХИСТ КАНАЛІВ ЗВ'ЯЗКУ В КРИТИЧНИХ ІНФРАСТРУКТУРАХ»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
*(код, найменування спеціальності)*
освітньо-професійної програми Телекомунікаційні системи та мережі
*(назва)*

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.*

_____ Владислав Ткаченко
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-63
Владислав Ткаченко
*Ім'я, ПРІЗВИЩЕ*

Керівник: Олександр Дробик
к.т.н., професор *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
*Ім'я, ПРІЗВИЩЕ*

**Київ 2025**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут Телекомунікацій**

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

**ЗАТВЕРДЖУЮ**
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ткаченко Владиславу Ігоровичу
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи: Дослідження методів захисту інформації в беспроводових телекомунікаційних мережах з використанням технологій штучного інтелекту,
керівник кваліфікаційної роботи Олександр ДРОБИК, к.т.н., професор
*(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)*
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10. 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Теоретичні основи безпровідних телекомунікаційних мереж та загроз інформаційній безпеці.
2. Методи захисту інформації в безпровідних мережах та можливості застосування штучного інтелекту.
3. Дослідження та проєктування системи захисту інформації в безпровідній мережі з використанням штучного інтелекту.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні основи безпровідних телекомунікаційних мереж та загроз інформаційній безпеці.
2. Методи захисту інформації в безпровідних мережах та можливості застосування штучного інтелекту.
3. Дослідження та проєктування системи захисту інформації в безпровідній мережі з використанням штучного інтелекту.
4. Техніко-економічне обґрунтування впровадження системи захисту з використанням штучного інтелекту.

5. Перелік ілюстративного матеріалу: ___презентація на____слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Підбір та аналіз науково-технічної літератури | 16.10.2025 | Викон. |
| 2 | Розробка першого розділу | 25.10.2025 | Викон. |
| 3 | Розробка другого розділу | 05.11.2025 | Викон. |
| 4 | Розробка третього розділу | 15.11.2025 | Викон. |
| 5 | Розробка четвертого розділу | 26.11.2025 | Викон. |
| 6 | Висновки, вступ, реферат | 04.12.2025 | Викон. |
| 7 | Розробка презентації | 15.12.2025 | Викон. |

Здобувач вищої освіти _____ Владислав ТКАЧЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Олександр ДРОБИК
(підпис) *(Ім'я ПРІЗВИЩЕ)*

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут телекомунікацій**
**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**
**на здобуття освітнього ступеня магістра**

Направляється здобувач Ткаченко В.І. до захисту кваліфікаційної роботи
*(прізвище та ініціали)*
за спеціальністю 172 Електронні комунікації та радіотехніка
*(код, найменування спеціальності)*
освітньо-професійної програми Телекомунікаційні системи та мережі
*(назва)*
на тему: «Дослідження методів захисту інформації в беспроводових телекомунікаційних мережах з використанням технологій штучного інтелекту»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**Висновок керівника кваліфікаційної роботи**

Здобувач Ткаченко Владислав Ігорович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Ткаченка Владислава Ігоровича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Олександр ДРОБИК
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач Ткаченко В.І. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
*(назва)* *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

**ВІДГУК РЕЦЕНЗЕНТА**
**на кваліфікаційну роботу**
**на здобуття освітнього ступеня магістра**

здобувача вищої освіти Ткаченко Владислава Ігоровича
*(прізвище, ім'я, по батькові)*
на тему «Дослідження методів захисту інформації в беспроводових телекомунікаційних мережах з використанням технологій штучного інтелекту»

**Актуальність.**
Актуальність теми не викликає сумнівів і зумовлена стрімким розвитком безпроводових телекомунікаційних мереж (наприклад, 5G, Wi-Fi 6) та паралельним зростанням кібератак. Традиційні методи захисту часто виявляються неефективними проти складних та динамічних загроз. Робота присвячена дослідженню інноваційного підходу — застосуванню штучного інтелекту (ШІ) та машинного навчання (МН) для автоматичного виявлення аномалій, прогнозування загроз та адаптивного управління безпекою, що є критично важливим для забезпечення конфіденційності та цілісності даних у сучасних мережах.

**Позитивні сторони.**
1. Інноваційний підхід: Тема дослідження є передовою, а робота демонструє глибоке розуміння як мережевих технологій, так і алгоритмів штучного інтелекту.
2. Методологічна точність: Проведене моделювання та оцінка ефективності ШІ-моделей є ретельними та добре обґрунтованими з технічної точки зору.
3. Комплексність: кваліфікаційна робота успішно поєднує теоретичні знання (безпека та ШІ) з практичним застосуванням.

**Недоліки.**
1. Вимоги до обчислювальних ресурсів: Недостатньо детально розглянуто питання оптимізації ШІ-моделей для їх впровадження на мережевому обладнанні з обмеженими обчислювальними ресурсами, що є важливим аспектом практичної реалізації.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

**Висновок:** *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Ткаченко Владислава Ігоровича заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент _____ _____
науковий ступінь, вчене звання (підпис) *(Ім'я ПРІЗВИЩЕ)*

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 64 стор., 3 табл., 38 джерел.

Мета роботи – дослідження, теоретичне обґрунтування та розробка рекомендацій щодо застосування методів штучного інтелекту для підвищення ефективності захисту інформації в безпроводових телекомунікаційних мережах.

Об’єкт дослідження – дослідження є процеси захисту інформації в безпроводових телекомунікаційних мережах.

Предмет дослідження – сукупність теоретичних, методичних та практичних аспектів, пов'язаних із розробкою та реалізацією алгоритмів ШІ для виявлення та запобігання загрозам у БТМ.

Короткий зміст роботи: у кваліфікаційній роботі досліджено та проаналізовано основні типи загроз та вразливостей БТМ, а також порівняно існуючі методи захисту. Обґрунтовано переваги використання алгоритмів машинного та глибокого навчання (нейронних мереж, SVM) для створення адаптивних систем виявлення вторгнень (IDS). Наукова новизна полягає в обґрунтуванні та пропозиції вдосконаленої архітектури інтеграції методів глибокого навчання для підвищення надійності виявлення нових, раніше невідомих типів атак у безпроводових мережах, а також у розробці рекомендацій щодо оптимізації цих моделей для роботи в умовах обмежених обчислювальних ресурсів мережевого обладнання.

КЛЮЧОВІ СЛОВА: БЕЗПРОВОДОВІ МЕРЕЖІ, ЗАХИСТ ІНФОРМАЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, МАШИННЕ НАВЧАННЯ, КІБЕРБЕЗПЕКА, ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS), ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ, АЛГОРИТМИ, НЕЙРОННІ МЕРЕЖІ, КРИПТОГРАФІЯ, АНОМАЛІЇ, ПРОТОКОЛИ БЕЗПЕКИ, АТАКИ, ПРОДУКТИВНІСТЬ, МОДЕЛЮВАННЯ

## ABSTRACT

Text part of the master's qualification work: 64 pages, 3 table, 38 sources.

The purpose of the work is to research, theoretical justification and develop recommendations for the application of artificial intelligence methods to increase the effectiveness of information protection in wireless telecommunication networks.Object of the study is fiber-optic communication lines as part of the telecommunications infrastructure.

The object of research is the process of information protection in wireless telecommunication networks.

The subject of the study is a set of theoretical, methodological, and practical aspects related to the development and implementation of AI algorithms for detecting and preventing threats in BTM.

Summary of the work: the qualification work investigated and analyzed the main types of threats and vulnerabilities of BTM, as well as the comparative existing protection methods. The advantages of using machine and deep learning algorithms (neural networks, SVM) to create adaptive intrusion detection systems (IDS) were substantiated. The scientific novelty lies in the justification and proposal of an improved architecture for integrating deep learning methods to increase the reliability of detecting new, previously unknown types of attacks in wireless networks, as well as in the development of recommendations for optimizing these models for operation in conditions of limited computing resources of network equipment.



KEYWORDS: WIRELESS NETWORKS, INFORMATION PROTECTION, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, CYBERSECURITY, INTRUSION DETECTION (IDS), TELECOMMUNICATION NETWORKS, ALGORITHMS, NEURAL NETWORKS, CRYPTOGRAPHY, ANOMALIES, SECURITY PROTOCOLS, ATTACKS, PERFORMANCE, MODELING

# ЗМІСТ

1 ТЕОРЕТИЧНІ ОСНОВИ БЕЗПРОВІДНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ..... 13
1.1 Основні поняття та класифікація безпровідних телекомунікаційних мереж ... 13
1.2 Архітектура безпровідних мереж та моделі побудови (Wi-Fi, стільникові мережі, IoT, 5G) ..... 15
1.3 Типові загрози та вразливості в безпровідних мережах ..... 17
1.4 Нормативні та стандартні підходи до забезпечення інформаційної безпеки в безпровідних мережах ..... 20
2 МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ ТА МОЖЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ..... 23
2.1 Криптографічні методи та протоколи захисту в безпровідних мережах ..... 23
2.2 Традиційні системи виявлення та запобігання атак (IDS/IPS, міжмережеві екрани, сегментація) ..... 26
2.3 Основи штучного інтелекту та машинного навчання в задачах кібербезпеки . 29
2.4 Методи виявлення аномалій і вторгнень у безпровідних мережах на основі штучного інтелекту ..... 32
2.5 Порівняльний аналіз традиційних і AI-орієнтованих методів захисту інформації ..... 34
3 ДОСЛІДЖЕННЯ ТА ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ 37
3.1 Вихідні дані, постановка задачі та вимоги до системи захисту ..... 37
3.2 Вибір архітектури безпровідної мережі та сценаріїв атак для дослідження .... 39
3.3 Вибір та обґрунтування моделі штучного інтелекту для виявлення загроз ..... 42
3.4 Формування набору даних, методика навчання та тестування AI-моделі ..... 43
3.5 Моделювання роботи системи захисту в безпровідній мережі та аналіз результатів ..... 45
3.6 Оцінка ефективності запропонованої системи захисту ..... 47
4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ..... 50
4.1 Розрахунок капітальних витрат на створення системи захисту в безпровідній мережі ..... 50

4.2 Розрахунок експлуатаційних витрат на підтримку та оновлення системи ..... 52
4.3 Розрахунок основних економічних показників ефективності впровадження .. 54
ВИСНОВКИ ..... 58
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ..... 61

# ПЕРЕЛІК СКОРОЧЕНЬ

ІБ – інформаційна безпека

ШІ – штучний інтелект

ML – машинне навчання

DL – глибинне навчання

IDS – система виявлення вторгнень

IPS – система запобігання вторгненням

WLAN – безпровідна локальна мережа (Wireless Local Area Network)

Wi-Fi – технологія безпровідного доступу на основі стандартів IEEE 802.11

WWAN – глобальна безпровідна мережа (Wireless Wide Area Network)

PAN – персональна мережа (Personal Area Network)

WPAN – безпровідна персональна мережа (Wireless Personal Area Network)

IoT – Інтернет речей (Internet of Things)

WSN – безпровідна сенсорна мережа (Wireless Sensor Network)

LTE – довгостроковий розвиток стільникових мереж (Long Term Evolution)

5G – п’яте покоління стільникових мереж зв’язку

AP – точка доступу (Access Point)

VPN – віртуальна приватна мережа (Virtual Private Network)

PKI – інфраструктура відкритих ключів (Public Key Infrastructure)

DoS – відмова в обслуговуванні (Denial of Service)

DDoS – розподілена відмова в обслуговуванні (Distributed Denial of Service)

MITM – атака «людина посередині» (Man-in-the-Middle)

AAA – автентифікація, авторизація, облік (Authentication, Authorization, Accounting)

QoS – якість обслуговування (Quality of Service)

SLA – угода про рівень послуг (Service Level Agreement)

# ВСТУП

Сучасний етап розвитку телекомунікацій характеризується масовим переходом від дротових рішень до безпровідних технологій. Офісні мережі, кампусні інфраструктури, домашні роутери, мобільний інтернет, промисловий Інтернет речей – усе це сьогодні базується на безпровідній передачі даних. З одного боку, це забезпечує високий рівень мобільності користувачів, гнучкість розгортання сервісів та можливість швидкого масштабування. З іншого боку, безпровідне середовище створює нові виклики для інформаційної безпеки, оскільки радіоканал легше перехопити, підмінити або заблокувати, ніж фізично захищений дротовий сегмент мережі.

Паралельно з розвитком безпровідних телекомунікаційних мереж стрімко розвиваються технології штучного інтелекту. Методи машинного та глибинного навчання вже активно використовуються для класифікації трафіку, виявлення аномалій, побудови систем виявлення та запобігання вторгненням, а також для аналізу поведінки користувачів і пристроїв. Сучасні дослідження показують, що підходи на основі ШІ дозволяють ефективніше виявляти нові, раніше невідомі типи атак, знижувати кількість хибних спрацьовувань та адаптуватися до змін профілю трафіку в мережах Wi-Fi, 5G та IoT.

Все це зумовлює актуальність теми дослідження методів захисту інформації саме в безпровідних телекомунікаційних мережах з використанням штучного інтелекту. Для операторів і власників мереж важливо не тільки застосовувати стандартні механізми шифрування й автентифікації, але й мати інтелектуальні системи моніторингу, які здатні в реальному часі аналізувати великий обсяг трафіку, виявляти нетипову активність та своєчасно реагувати на інциденти.

Об’єктом дослідження в даній дипломній роботі є безпровідні телекомунікаційні мережі різних типів, у тому числі безпровідні локальні мережі Wi-Fi, стільникові мережі п’ятого покоління та мережі Інтернету речей.

Предметом дослідження є методи та засоби захисту інформації в таких мережах, зокрема криптографічні протоколи, механізми автентифікації, політики керування доступом, а також інтелектуальні системи виявлення та запобігання загрозам на основі ШІ.

Метою дипломної роботи є аналіз і узагальнення теоретичних та практичних підходів до захисту інформації в безпровідних телекомунікаційних мережах з урахуванням сучасних загроз, а також дослідження можливостей застосування методів штучного інтелекту для підвищення рівня інформаційної безпеки.

Для досягнення поставленої мети в роботі необхідно розв’язати такі основні завдання:
– розглянути основні поняття та класифікації безпровідних телекомунікаційних мереж, їхня роль у сучасних інформаційно-комунікаційних системах
– проаналізувати архітектуру найбільш поширених безпровідних технологій (Wi-Fi, стільникові мережі, IoT, 5G) та особливості їх побудови
– виявити та систематизувати типові загрози й вразливості, характерні для безпровідних мереж різних типів
– дослідити нормативні й стандартні підходи до забезпечення інформаційної безпеки в безпровідних мережах
– проаналізувати сучасні методи захисту інформації, які застосовуються в безпровідних мережах, та визначити їхні переваги й обмеження
– розглянути основні концепції штучного інтелекту, які використовуються в задачах ІБ, особливо в частині виявлення аномалій та вторгнень
– дослідити можливі варіанти інтеграції методів ШІ у системи захисту безпровідних мереж

– сформувати узагальнені висновки щодо доцільності й ефективності застосування ШІ для захисту інформації в безпровідних телекомунікаційних мережах.

Методами дослідження є аналіз наукових публікацій, міжнародних стандартів та рекомендацій, нормативних документів з інформаційної безпеки, узагальнення практичного досвіду впровадження систем захисту в реальних мережах, а також елементи порівняльного аналізу різних підходів до виявлення загроз і побудови систем ІБ.

Практичне значення роботи полягає в можливості використання результатів дослідження при проектуванні та модернізації систем захисту безпровідних мереж у корпоративному та операторському середовищах, а також при розробці політик безпеки й вимог до архітектури мереж. Отримані узагальнення можуть бути корисними для фахівців з кібербезпеки, адміністраторів мереж, а також для студентів і слухачів, які вивчають дисципліни, пов’язані з телекомунікаціями та захистом інформації.

Структурно дипломна робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. У першому розділі наведено теоретичні основи безпровідних телекомунікаційних мереж і загроз інформаційній безпеці. Другий розділ присвячено методам захисту інформації та можливостям застосування штучного інтелекту. У третьому розділі розглядається дослідження та проектування системи захисту в безпровідній мережі з використанням ШІ. Четвертий розділ містить техніко-економічне обґрунтування доцільності впровадження такої системи.

# 1 ТЕОРЕТИЧНІ ОСНОВИ БЕЗПРОВІДНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

## 1.1 Основні поняття та класифікація безпровідних телекомунікаційних мереж

Телекомунікаційна мережа в загальному випадку – це сукупність засобів передавання, комутації та керування, які забезпечують обмін інформацією між кінцевими користувачами або пристроями за встановленими протоколами. Безпровідною телекомунікаційною мережею називають таку мережу, у якій фізичне середовище передавання базується не на металевих або оптичних лініях, а на радіоканалах, інфрачервоному випромінюванні чи інших безпровідних технологіях.

Для безпровідних мереж характерні такі загальні властивості:
– застосування радіочастотного спектру або інших ефірних середовищ як фізичного каналу
– наявність базових станцій або точок доступу, які координують роботу кінцевих пристроїв
– обмеження за потужністю передавачів, радіусом дії, перешкодостійкістю
– можливість мобільного доступу та зміни точки підключення без втрати зв’язку
– підвищена чутливість до прослуховування, підміни та завад, оскільки сигнал поширюється у відкритому середовищі.

За зоною покриття безпровідні телекомунікаційні мережі умовно поділяють на кілька основних класів:
– персональні мережі (PAN, WPAN) – з дуже малим радіусом дії, як правило, до декількох метрів; приклади – Bluetooth, NFC, де окремий пристрій (смартфон, гарнітура) підключається до іншого пристрою без участі інфраструктури

– безпровідні локальні мережі (WLAN) – використовуються в офісах, кампусах, житлових будинках; типовим прикладом є мережі Wi-Fi на базі стандартів IEEE 802.11
– міські або регіональні безпровідні мережі (WMAN) – мережі, що забезпечують покриття на рівні міста чи регіону; історично до них відносилися, наприклад, деякі реалізації WiMAX
– глобальні безпровідні мережі (WWAN) – стільникові мережі різних поколінь (2G, 3G, 4G LTE, 5G), супутникові системи зв'язку, які забезпечують зв'язок на великих відстанях.

Окремим напрямком розвитку безпровідних мереж є Інтернет речей. У цьому випадку мова йде про мережі, де підключаються численні сенсори, актуатори, побутова техніка, промислове обладнання та інші пристрої, які обмінюються даними автоматично. Для таких мереж використовуються як традиційні технології (Wi-Fi, стільниковий зв'язок), так і спеціалізовані протоколи, наприклад NB-IoT, LTE-M, LoRaWAN тощо.

Крім класифікації за зоною покриття, безпровідні мережі можна класифікувати за такими ознаками:
– за типом доступу (інфраструктурні, де є центральна точка доступу або базова станція, та ad-hoc мережі, де вузли безпосередньо обмінюються даними між собою)
– за призначенням (корпоративні, операторські, домашні, промислові, спеціального призначення)
– за способом мультиплексування (мережі з часовим, частотним або кодовим поділом каналів)
– за рівнем мобільності користувачів (стаціонарні, з низькою або високою мобільністю).

Таке різноманіття технологій та сценаріїв використання приводить до того, що вимоги до інформаційної безпеки також суттєво відрізняються. Наприклад,

для домашньої WLAN основним пріоритетом є захист персональних даних і доступу до інтернету, тоді як для мережі оператора 5G критичними стають безперервність надання послуг, захист великої кількості пристроїв IoT та відповідність галузевим стандартам безпеки.

## 1.2 Архітектура безпровідних мереж та моделі побудови (Wi-Fi, стільникові мережі, IoT, 5G)

Архітектура безпровідної мережі визначає, які функціональні елементи в ній присутні, як вони взаємодіють між собою та з іншими мережами, а також які протоколи й механізми використовуються для доступу, маршрутизації й захисту інформації.

Архітектура Wi-Fi мереж.

Безпровідні локальні мережі Wi-Fi зазвичай будуються на базі стандартів сімейства IEEE 802.11. Класична архітектура WLAN включає:
– точки доступу (AP), які підключені до дротової мережі й забезпечують безпровідний доступ для клієнтських пристроїв
– клієнтські пристрої (ноутбуки, смартфони, планшети, стаціонарні комп’ютери з безпровідними адаптерами)
– дротову локальну мережу, куди підключені сервери, маршрутизатори, вихід до інтернету та інші ресурси.

У типових офісних мережах використовується інфраструктурний режим роботи Wi-Fi, у якому клієнтські пристрої обмінюються даними через точку доступу. Для розширення покриття застосовується кілька точок доступу, які можуть керуватися централізованим контролером. У великих інсталяціях додатково використовуються безпровідні контролери, які відповідають за розподіл навантаження, роумінг користувачів, реалізацію політик безпеки.

З точки зору безпеки, архітектура Wi-Fi мереж включає механізми автентифікації та шифрування:
– відкриті мережі без шифрування (сьогодні їх зазвичай вважають небезпечними)
– мережі з попередньо спільним ключем (PSK) на основі WPA2/WPA3-Personal
– підприємницькі мережі з автентифікацією за допомогою 802.1X та зовнішнього сервера (наприклад RADIUS), де кожен користувач має власні облікові дані.

Архітектура стільникових мереж.

Стільникові мережі (2G–5G) мають багаторівневу архітектуру, яка умовно поділяється на радіодоступ (мережа базових станцій), транспортну мережу й ядро. У мережах 4G і 5G використовується пакетно орієнтована архітектура, де ядро побудовано на базі IP-протоколів, а функції керування та користувацького трафіку розділені.

У 5G виділяють нову радіомережу (NR) та ядро 5G Core. До складу ядра входять спеціалізовані мережеві функції, які реалізують керування доступом, мобільністю, сесіями користувача, а також політики якості обслуговування та безпеки. Важливою особливістю 5G є використання віртуалізації мережевих функцій та програмно-керованих мереж (SDN), що, з одного боку, дозволяє більш гнучко керувати ресурсами, а з іншого – створює додаткові можливості для атак, якщо не впроваджені належні заходи захисту.

Суттєвою новацією в 5G є концепція мережевої сегментації (network slicing), коли поверх однієї фізичної інфраструктури створюється кілька логічних «зрізів» з різними параметрами продуктивності та безпеки. Окремий зріз може бути виділений для критично важливих сервісів, для пристроїв IoT, для масового мобільного широкосмугового доступу тощо. З точки зору безпеки важливо, щоб між зрізами існували чіткі межі, а компрометація одного сегмента не призводила до порушення роботи інших.

Архітектура мереж Інтернету речей.

Мережі IoT часто описують за трирівневою моделлю:
– рівень пристроїв (сенсори, актуатори, контролери)
– мережевий рівень (протоколи передавання даних, шлюзи)
– прикладний рівень (сервери збору даних, аналітики, керування).

На рівні пристроїв основними обмеженнями є низька потужність процесора, обмежена пам’ять, невелика ємність батарей. Через це далеко не всі класичні механізми захисту (наприклад складні криптографічні алгоритми або важкі протоколи) можуть бути безпосередньо реалізовані на вузлах IoT. На мережевому рівні використовуються як традиційні IP-мережі, так і спеціалізовані протоколи, які оптимізовані для малопотужних пристроїв і нестабільних каналів.

Архітектура 5G з точки зору IoT розглядається як платформа для масового підключення пристроїв, у тому числі промислових сенсорних мереж, транспортних систем, «розумних міст». Тут питання безпеки стають критичними, оскільки атака на безпровідну мережу може спричинити не тільки втрату даних, а й фізичні наслідки (зупинка виробництва, відмова систем керування).

Навіть на рівні загального опису архітектури видно, що у Wi-Fi, стільникових мережах, IoT і 5G різні підходи до побудови та керування, але всі вони мають спільну особливість – використання безпровідного середовища, яке важче контролювати й захищати, ніж традиційні дротові мережі.

## 1.3 Типові загрози та вразливості в безпровідних мережах

Через те, що безпровідний сигнал поширюється у відкритому просторі, будь-який користувач у зоні дії мережі потенційно може перехопити трафік або спробувати підключитися до мережі. Це накладає додаткові вимоги до автентифікації, шифрування й контролю доступу. Серед найбільш типових загроз та вразливостей можна виділити такі.

Несанкціонований доступ до мережі.

Якщо мережа неправильно налаштована (слабкий пароль, застарілий протокол шифрування, відсутність сегментації гостьового трафіку), зловмисник може підключитися до неї як звичайний клієнт. Після цього він отримує можливість сканувати внутрішню мережу, підбирати паролі до сервісів, запускати атаки на інші хости або використовувати доступ до інтернету для протиправної діяльності. У випадку корпоративних мереж це може призвести до витоку конфіденційної інформації, блокування сервісів чи компрометації облікових записів.

Перехоплення трафіку та пасивне прослуховування.

Якщо трафік передається відкритим текстом або з використанням слабких алгоритмів шифрування, можливе перехоплення й аналіз даних, що циркулюють у мережі. Навіть при застосуванні сучасних протоколів шифрування вразливими залишаються службові повідомлення, метадані, інформація про MAC-адреси, SSID, структуру мережі. На основі таких даних зловмисник може підготувати більш цілеспрямовану атаку.

Атаки типу «людина посередині» (MITM).

У безпровідних мережах часто реалізуються сценарії, коли зловмисник створює фальшиву точку доступу з такою ж назвою мережі (SSID), як у легітимної. Користувачі, не перевіряючи сертифікати або параметри безпеки, підключаються до цієї точки, після чого весь їхній трафік проходить через пристрій зловмисника. Це дозволяє підмінювати дані, змінювати налаштування, підсовувати користувачу шкідливі веб-сторінки.

Атаки на протоколи автентифікації та шифрування.

Історично в безпровідних мережах застосовувалися протоколи WEP, WPA, WPA2, сьогодні активно впроваджується WPA3. Частина застарілих протоколів має відомі вразливості, які дозволяють розкрити ключ шифрування за відносно

короткий час. Навіть сучасні схеми захисту можуть бути скомпрометовані при неправильній реалізації або конфігурації, наприклад при використанні слабких паролів, відсутності двофакторної автентифікації, неправильному налаштуванні 802.1X.

Атаки типу відмови в обслуговуванні (DoS, DDoS).

Безпровідні мережі чутливі до перевантаження радіоканалу та відмови в обслуговуванні. Зловмисник може генерувати велику кількість службових кадрів, потоків підключення, широкомовних запитів, що призводить до перевантаження точки доступу або базової станції. Також можливе створення навмисних радіоперешкод (джамінг), які знижують рівень сигналу й роблять зв’язок нестабільним або зовсім неможливим.

Специфічні загрози для IoT та 5G.

У мережах Інтернету речей додатковою проблемою є велика кількість однотипних пристроїв з обмеженими ресурсами, де часто використовуються стандартні паролі або зовсім відсутні механізми оновлення прошивки. Це робить такі пристрої зручними цілями для масового зараження й побудови ботнетів, які потім використовуються для DDoS-атак на інші сервіси.

У 5G-мережах, окрім традиційних загроз, з’являються нові: атаки на віртуалізовані мережеві функції, експлуатація вразливостей у механізмах мережевої сегментації, несанкціонований доступ до керівних інтерфейсів SDN-контролерів. Неправильна реалізація безпеки в таких компонентах може дозволити атакуючому впливати відразу на значну частину мережі, а не тільки на окремий вузол.

Людський фактор та помилки конфігурації.

Окремо слід відзначити загрози, пов’язані з людським фактором. Недостатня кваліфікація адміністраторів, відсутність політик безпеки,

використання стандартних паролів, ігнорування оновлень прошивки – усе це створює «лазівки» для атак. Часто реальні інциденти відбуваються не через складні вразливості протоколів, а через банальні вади в налаштуванні та організації процесів.

Безпровідні телекомунікаційні мережі поєднують у собі всі звичні проблеми класичних IP-мереж і додають до них специфічні загрози, пов’язані з відкритим характером радіоканалу, мобільністю користувачів та великою кількістю недорогих IoT-пристроїв. Це вимагає комплексного підходу до захисту, у якому поєднуються технічні, організаційні та інтелектуальні засоби.

## 1.4 Нормативні та стандартні підходи до забезпечення інформаційної безпеки в безпровідних мережах

Забезпечення інформаційної безпеки в безпровідних мережах базується не тільки на конкретних технічних рішеннях, але й на дотриманні вимог міжнародних і національних стандартів, рекомендацій і галузевих керівних документів. Саме нормативна база визначає загальний підхід до управління ризиками, вибору технічних й організаційних контролів, а також критерії оцінки ефективності захисту.

Одним з найпоширеніших міжнародних стандартів у сфері управління інформаційною безпекою є стандарт серії ISO/IEC 27001, який описує вимоги до системи управління ІБ на рівні організації. В актуальній редакції стандарту особлива увага приділяється безпеці мережевої інфраструктури, включно з безпровідними мережами, а також сегментації мережевих ресурсів. Контроли, які стосуються безпеки мережі, включають вимоги до захисту мережевих сервісів, забезпечення конфіденційності й цілісності даних під час передавання, а також виділення окремих сегментів для критично важливих інформаційних ресурсів.

Практично у всіх сучасних підходах до впровадження ISO/IEC 27001 робиться акцент на тому, що безпровідні мережі повинні розглядатися як

підвищено ризиковий сегмент. Це означає необхідність:
– розроблення окремої політики використання безпровідних мереж
– впровадження підсилених механізмів автентифікації й шифрування
– обов’язкової сегментації гостьових і внутрішніх мереж
– регулярного моніторингу безпровідного середовища на предмет наявності несанкціонованих точок доступу.

Для безпровідних локальних мереж широко використовуються рекомендації Національного інституту стандартів і технологій (NIST). Окремий документ, присвячений безпеці WLAN, містить рекомендації щодо конфігурації точок доступу, використання сучасних механізмів шифрування, керування ключами, а також безперервного моніторингу стану мережі. У ньому підкреслюється, що безпровідні мережі за замовчуванням є менш захищеними, ніж дротові, і тому потребують більш уважного підходу до управління ризиками.

Стандарти та рекомендації також існують на рівні конкретних технологій. Для Wi-Fi це стандарти IEEE 802.11 і відповідні доповнення, які визначають протоколи автентифікації та шифрування (наприклад, IEEE 802.11i та подальші оновлення). Для стільникових мереж питання безпеки регламентуються технічними специфікаціями 3GPP, зокрема документами, що описують архітектуру безпеки 5G, процедури керування ключами, захист сигналізаційного та користувацького трафіку.

У багатьох країнах додатково приймаються національні стандарти та профілі захисту, які конкретизують вимоги міжнародних документів для державних органів або критичної інфраструктури. У таких документах, як правило, окремими розділами виділяються вимоги до:
– організації доступу до безпровідних мереж у будівлях державних органів
– використання сертифікованих криптографічних засобів
– ведення журналів подій і розслідування інцидентів
– регулярного аудиту налаштувань мережевого обладнання.

Окремим напрямком розвитку нормативної бази є документи, які стосуються кібербезпеки 5G та IoT-мереж. У них розглядаються питання безпеки віртуалізованих мережевих функцій, сегментації мережі, безпечного оновлення програмного забезпечення на пристроях, захисту API, що використовуються для керування сервісами. Також акцент робиться на необхідності впровадження концепції «безпеки за задумом» (security by design), коли вимоги безпеки враховуються вже на етапі проектування сервісів, а не додаються постфактум.

Нарешті, у контексті застосування штучного інтелекту в системах захисту безпровідних мереж варто згадати рекомендації, які стосуються етичного використання ШІ, прозорості алгоритмів, контролю якості навчальних даних та запобігання упередженості моделей. Хоча ці документи прямо не регулюють питання шифрування або автентифікації, вони впливають на вимоги до проєктування систем виявлення вторгнень, які використовують ML та DL.

Нормативні та стандартні підходи формують рамки, в яких можуть і повинні будуватися конкретні технічні рішення зі захисту інформації в безпровідних мережах. Подальші розділи дипломної роботи присвячено аналізу того, як ці вимоги реалізуються на практиці та яким чином методи штучного інтелекту можуть доповнювати традиційні механізми захисту.

# 2 МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ ТА МОЖЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

## 2.1 Криптографічні методи та протоколи захисту в безпровідних мережах

Криптографія є базою для забезпечення конфіденційності, цілісності та автентичності даних, що передаються в безпровідних мережах. На відміну від дротових мереж, де фізичний доступ до кабелю більш-менш контрольований, у безпровідних мережах будь-який користувач, який знаходиться в зоні радіопокриття, теоретично може перехоплювати сигнал. Тому саме криптографічний захист є першим рубежем оборони.

Основними цілями криптографії є:
– конфіденційність – забезпечення того, що дані зрозумілі лише легітимним учасникам обміну
– цілісність – гарантія, що інформація не була змінена під час передавання
– автентичність – підтвердження справжності сторін, які обмінюються даними
– невідмовність – неможливість заперечити факт відправки або отримання повідомлення.

У безпровідних мережах ці цілі досягаються за допомогою симетричного та асиметричного шифрування, механізмів керування ключами, протоколів автентифікації, а також цифрових підписів і сертифікатів.

Еволюція протоколів захисту в мережах Wi-Fi

Найбільш очевидним прикладом застосування криптографії в безпровідних мережах є стандарти шифрування в WLAN на основі IEEE 802.11. Історично першими широко використовувались протоколи WEP і WPA, однак з часом вони показали свою слабкість і сьогодні вважаються застарілими та небезпечними.

Сучасними базовими стандартами є WPA2 та WPA3. WPA2 використовує шифрування AES у режимі CCMP, а для автентифікації може застосовувати як простий режим з попередньо спільним ключем (PSK), так і корпоративний режим з використанням 802.1X та зовнішнього сервера автентифікації. Проте досвід експлуатації показав, що WPA2 має ряд вразливостей, наприклад атаки на процес повторної інсталяції ключа KRACK, а також слабкість при використанні простих паролів.

WPA3 є логічним розвитком стандарту безпеки Wi-Fi. Основними нововведеннями WPA3 є:
– використання протоколу SAE (Simultaneous Authentication of Equals) замість класичної схеми PSK, що суттєво підвищує стійкість до перебору паролів та офлайн-атак
– індивідуальне шифрування трафіку навіть у відкритих мережах, що ускладнює пасивне прослуховування
– підтримка посилених режимів шифрування у корпоративному сегменті (192-бітні набори шифрів) для середовищ з підвищеними вимогами до безпеки.

Таким чином, у сучасних WLAN рекомендованим є використання WPA3 там, де це підтримується обладнанням, а в змішаних середовищах – режиму WPA2/WPA3, щоб забезпечити сумісність зі старими пристроями.

Корпоративні Wi-Fi мережі, як правило, використовують схему 802.1X, де для кожного користувача видається індивідуальний обліковий запис, а процес автентифікації відбувається через сервер (наприклад на базі RADIUS). Це дозволяє централізовано керувати доступом, відключати скомпрометовані облікові записи та вести деталізований облік підключень.

Криптографія в стільникових мережах 4G/5G

У стільникових мережах захист інформації реалізується інакше, ніж у Wi-Fi. Тут використовується складна ієрархія ключів, які застосовуються для захисту як

сигналізаційного трафіку, так і користувацьких даних на різних інтерфейсах мережі.

У мережах LTE та 5G застосовується поділ на дві основні площини: користувацьку й керуючу. Для кожної з них використовуються окремі ключі шифрування та цілісності. Автентифікація абонента базується на спільному секреті, який зберігається на SIM-карті (або її сучасних аналогах) і в центрі автентифікації оператора. Після успішної автентифікації генеруються тимчасові ключі, що використовуються для шифрування на радіоінтерфейсі.

Важливою особливістю 5G є розширені вимоги до захисту сигналізаційних протоколів, оскільки через них здійснюється керування підключеннями, мобільністю та якістю обслуговування. У мегамасштабних 5G-мережах неправильна реалізація криптографічних механізмів може призвести до атак на цілі підмережі або навіть регіони.

Криптографія в IoT та ресурсно обмежених пристроях

У мережах Інтернету речей додатковою складністю є обмежені ресурси пристроїв. Сенсори та дешеві контролери часто мають невелику обчислювальну потужність, обмежену пам’ять і працюють від батарей, які не можна часто змінювати. Тому класичні «важкі» криптографічні алгоритми можуть бути для них надто енерговитратними.

Для таких сценаріїв активно розробляються й використовуються легковагові криптографічні алгоритми, оптимізовані за кількістю операцій, споживанням пам’яті та енергії. Одночасно вирішується питання керування ключами: потрібно знайти баланс між безпекою (часта ротація ключів, індивідуальні ключі для пристроїв) та практичною реалізовністю (обмежені ресурси, складність оновлення прошивок).

Важливу роль відіграють також протоколи захищеного обміну на рівні транспортного та прикладного рівнів – наприклад, версії TLS, адаптовані для IoT, або протоколи на кшталт DTLS для захисту на базі UDP. Тут часто застосовується модель, коли шифрування «знімає» шлюз, що підключає IoT-сегмент до загальної мережі, а самі сенсори використовують спрощені схеми автентифікації.

Віртуальні приватні мережі (VPN) поверх безпровідних каналів

Додатковим рівнем захисту у безпровідних мережах є використання VPN. У цьому випадку весь трафік між клієнтом і VPN-шлюзом шифрується незалежно від того, які механізми захисту застосовуються на рівні Wi-Fi чи іншої безпровідної технології.

Для реалізації VPN можуть використовуватися:
– протоколи на базі IPsec (tunnel mode, transport mode)
– протоколи SSL/TLS у вигляді так званих SSL-VPN
– сучасні рішення з використанням більш легковагових протоколів (наприклад, WireGuard-типу), які поєднують сильне шифрування з простотою конфігурації.

У корпоративних середовищах часто застосовується комбінований підхід: користувач підключається до корпоративного Wi-Fi, проходить автентифікацію на основі 802.1X, а для доступу до критичних сервісів додатково встановлюється VPN-тунель. Це дозволяє забезпечити багаторівневий захист і знизити ризик компрометації важливих ресурсів навіть у разі витоку ключа Wi-Fi або помилок у його конфігурації.

## 2.2 Традиційні системи виявлення та запобігання атак (IDS/IPS, міжмережеві екрани, сегментація)

Криптографія сама по собі не вирішує усіх проблем безпеки. Навіть при надійному шифруванні можливі спроби несанкціонованого доступу, DoS-атаки, експлуатація вразливостей сервісів, внутрішні загрози тощо. Для протидії таким

загрозам використовуються мережеві засоби безпеки – системи виявлення та запобігання вторгненням, міжмережеві екрани, механізми сегментації мережі.

Системи виявлення та запобігання вторгненням (IDS/IPS)

Intrusion Detection System (IDS) – це система, яка моніторить мережевий трафік або активність хостів з метою виявлення ознак атак, аномальної поведінки або порушення політик безпеки. Як правило, IDS працює в пасивному режимі: вона аналізує трафік, формує журнали та оповіщає адміністратора про підозрілі події.

Intrusion Prevention System (IPS) – це розвиток концепції IDS. IPS зазвичай встановлюється в розриві трафіку й має можливість не тільки виявляти підозрілі дії, а й блокувати їх у реальному часі: відкидати пакети, розривати сеанси, вносити адреси до чорних списків.

За способом розгортання IDS/IPS поділяють на:
– мережеві (NIDS/NIPS) – встановлюються на ключових сегментах мережі й аналізують трафік між вузлами
– хостові (HIDS/HIPS) – працюють безпосередньо на кінцевих пристроях та аналізують локальні журнали, системні виклики, стан файлів.

З точки зору методів аналізу, IDS/IPS можуть бути:
– сигнатурними – порівнюють трафік з базою відомих шаблонів атак
– аномалійними – відстежують відхилення від «нормальної» поведінки
– гібридними – поєднують обидва підходи.

У контексті безпровідних мереж окремим видом є Wireless IDS/IPS, які спеціально адаптовані до моніторингу радіоефіру, виявлення фальшивих точок доступу, нетипових режимів роботи, підозрілої зміни параметрів безпровідних кадрів.

Міжмережеві екрани (firewall)

Міжмережевий екран – це пристрій або програмний комплекс, що фільтрує трафік відповідно до заданих правил. Класичні міжмережеві екрани працювали переважно на мережевому й транспортному рівнях, перевіряючи IP-адреси, порти, протоколи. Сучасні наступні покоління (NGFW) підтримують аналіз прикладного рівня, ідентифікацію додатків, інтеграцію з системами автентифікації та IDS/IPS.

У безпровідних мережах міжмережевий екран зазвичай розташований на межі між WLAN та внутрішньою або зовнішньою мережею. Він може:
– відокремлювати гостьовий трафік від корпоративного
– блокувати доступ до небезпечних або небажаних ресурсів
– обмежувати сервісні порти, які не повинні бути доступними ззовні
– взаємодіяти з IDS/IPS для блокування атак.

Сегментація мережі як засіб локалізації інцидентів

Сегментація мережі – це розділення загальної мережевої інфраструктури на логічні або фізичні сегменти з різним рівнем довіри та різними політиками доступу. У дротових мережах це часто реалізується через VLAN, окремі підмережі, багаторівневі маршрутизатори. У безпровідних мережах аналогічні принципи застосовуються через виділення окремих SSID для різних категорій користувачів, використання окремих віртуальних мереж для гостьового доступу, IoT-пристроїв, службових систем.

Мета сегментації – зробити так, щоб компрометація одного сегмента (наприклад гостьової мережі) не давала автоматичного доступу до критичних ресурсів (серверів баз даних, систем керування виробництвом тощо). У стільникових мережах 5G аналогом є network slicing – створення логічних зрізів для різних типів сервісів з окремими політиками безпеки.

Загалом традиційні засоби (IDS/IPS, firewall, сегментація) виконують важливу функцію базового захисту й контролю трафіку. Однак зі збільшенням обсягу й складності атак, появою нових типів загроз і швидким ростом

безпровідних мереж, їх можливостей часто вже недостатньо для оперативного виявлення раніше невідомих атак. Саме в цьому місці на сцену виходять методи штучного інтелекту.

## 2.3 Основи штучного інтелекту та машинного навчання в задачах кібербезпеки

Штучний інтелект у широкому розумінні – це сукупність методів і технологій, які дозволяють комп'ютерним системам виконувати завдання, що традиційно вважались такими, що потребують людського інтелекту: розпізнавання образів, аналіз природної мови, прийняття рішень у складних ситуаціях. У сфері кібербезпеки ШІ використовується для автоматизації аналізу великих обсягів даних, виявлення нетипової поведінки, класифікації трафіку, прогнозування ризиків.

Основою практичного застосування ШІ є машинне навчання (ML) – підхід, при якому модель не програмується явно на усі можливі ситуації, а «навчається» на історичних даних. У задачах кібербезпеки такими даними можуть бути:
– журнали мережевого трафіку
– послідовності системних викликів
– статистика підключень до точок доступу
– логи аутентифікації та авторизації
– записи IDS/IPS про спроби атак.

Основні парадигми машинного навчання, які використовуються в кібербезпеці

Навчання з учителем (supervised learning).

У цьому випадку модель навчається на даних, для яких вже відомі правильні відповіді (мітки). Наприклад, кожному запису трафіку приписано клас «нормальний» або «атака», або більш детальні класи типів атак (DoS, сканування

портів, brute force тощо). Мета моделі – навчитися відтворювати цю розмітку на нових, unseen даних.

До популярних алгоритмів навчання з учителем відносять логістичну регресію, дерева рішень, випадкові ліси, метод опорних векторів (SVM), k-найближчих сусідів (kNN), а також різноманітні нейронні мережі. Багато сучасних робіт показують, що правильно налаштовані моделі ML можуть досягати високої точності виявлення атак у безпровідних сенсорних мережах, IoT-середовищах та 5G-інфраструктурі.

Навчання без учителя (unsupervised learning).

Тут модель не має наперед заданих міток. Її завдання – самостійно виявити структуру в даних: кластери, відхилення, закономірності. Для задач безпеки це особливо цікаво, оскільки дозволяє виявляти нові, раніше невідомі типи атак, які не представлені у тренувальних вибірках. Найчастіше використовуються методи кластеризації (k-means, DBSCAN та інші) та методи виявлення аномалій (one-class SVM, ізоляційний ліс, автоенкодери).

Напівконтрольоване та підкріплювальне навчання.

У реальних умовах часто доступні як розмічені, так і нерозмічені дані. Напівконтрольовані методи дозволяють поєднати обидва типи даних, використовуючи небагато розмічених прикладів для коректної інтерпретації більшості нерозмічених. Підкріплювальне навчання (reinforcement learning) в задачах безпеки застосовується рідше, але є роботи, де RL-агенти навчаються динамічно змінювати політики фільтрації, реагуючи на зміну поведінки атакуючих.

Глибинне навчання (deep learning)

Глибинне навчання є підкласом машинного навчання, який використовує багатошарові нейронні мережі для автоматичного виділення ознак з даних. У

задачах кібербезпеки застосовуються:
– згорткові нейронні мережі (CNN) – добре підходять для аналізу трафіку, структурованого як «зображення» або двовимірні матриці ознак
– рекурентні мережі (RNN, LSTM, GRU) – ефективні для аналізу послідовностей пакетів, системних викликів, часових рядів подій
– автоенкодери – використовуються для виявлення аномалій, коли мережа навчається відновлювати «нормальні» дані і погано відновлює аномальні.

Останні огляди показують, що глибинне навчання поступово стає одним з ключових інструментів для побудови IDS в нових технологіях – 5G, IoT, хмарних середовищах. Це пов’язано з тим, що обсяг трафіку й кількість параметрів, які треба враховувати, постійно зростають, і класичні ручні методи аналізу вже не справляються.

Основні етапи побудови ML/AI-систем у кібербезпеці

При застосуванні машинного навчання і ШІ в задачах безпеки зазвичай проходять такі кроки:
– збір даних (логи, трафік, телеметрія з пристроїв)
– попередня обробка (очищення, нормалізація, агрегація за інтервалами)
– виділення інформативних ознак (features), які характеризують поведінку трафіку або користувача
– розбиття даних на тренувальну, валідаційну та тестову вибірки
– навчання моделі й налаштування гіперпараметрів
– оцінка якості (точність, повнота, F1-міра, ROC-AUC, затримка реагування)
– інтеграція моделі у реальне середовище (on-line режим) та її подальше донавчання.

## 2.4 Методи виявлення аномалій і вторгнень у безпровідних мережах на основі штучного інтелекту

Застосування ШІ до задач захисту безпровідних мереж найяскравіше проявляється в області виявлення аномалій і вторгнень. На відміну від сигнатурних IDS, які орієнтуються на заздалегідь відомі шаблони атак, AI-орієнтовані системи можуть виявляти нові, раніше невідомі типи загроз, а також враховувати контекст роботи мережі.

Методи ML/DL для сенсорних і IoT-мереж

Для безпровідних сенсорних мереж (WSN) та IoT-середовищ одним з основних викликів є обмежені ресурси та нестабільність каналів зв'язку. Разом з тим саме такі мережі часто розгортаються у критично важливих сферах – моніторинг промислових об'єктів, «розумні міста», системи охорони здоров'я. Сучасні дослідження показують, що застосування машинного навчання дає змогу суттєво підвищити ефективність виявлення атак на WSN, зокрема DoS-атак, спроб захоплення вузлів, змови вузлів у маршрутизації тощо.

У таких роботах, як правило, розглядаються різні алгоритми – SVM, kNN, дерева рішень, випадкові ліси, гібридні нейронні мережі. Важливо, що модель може розміщуватися або на шлюзі, який має більшу обчислювальну потужність, або у хмарі, тоді як самі сенсори лише передають агреговані показники. Це знімає частину обмежень щодо ресурсів на кінцевих пристроях.

AI-орієнтоване виявлення аномалій у 5G та 5G-IoT

У 5G-мережах і 5G-IoT-сценаріях застосування ШІ стає ще актуальнішим. Обсяги трафіку великі, архітектура мережі складна, кількість можливих точок атаки зростає. Сучасні роботи описують AI-орієнтовані фреймворки, які аналізують телеметрію з елементів 5G-інфраструктури, мережевих зрізів, IoT-пристроїв у режимі реального часу. Такі системи здатні:

– виявляти нетипові патерни навантаження, що свідчать про DoS-атаки
– ідентифікувати незвичайну поведінку окремих пристроїв IoT
– аналізувати аномалії затримки, втрат пакетів, нестандартні послідовності сигналізаційних повідомлень.

Для таких задач пропонуються моделі на основі глибинних нейронних мереж (CNN, LSTM, автоенкодери), комбіновані підходи (гібрид CNN-LSTM), а також контекстно-орієнтовані AI-моделі, які враховують додаткову інформацію про стан мережі, тип сервісу, час доби.

Особливої уваги заслуговує напрямок контекстно-орієнтованих моделей, де виявлення аномалій відбувається з урахуванням того, в якому саме сценарії працює мережа: чи це промисловий сегмент, чи «розумне місто», чи медична інфраструктура. Це дозволяє знизити кількість хибних спрацьовувань, тому що одна й та сама подія в різному контексті може бути або аномалією, або нормою.

AI-засоби для WLAN і корпоративних безпровідних мереж

У корпоративних Wi-Fi-мережах методи ШІ зазвичай інтегруються у системи моніторингу та керування інфраструктурою. Моделі можуть аналізувати:
– статистику асоціацій та де-асоціацій клієнтів
– розподіл навантаження між точками доступу
– частоту помилок автентифікації
– нетипові переміщення клієнтів між точками доступу
– невластиві зміни параметрів мережі.

На основі цих даних моделі виявляють підозрілі ситуації, такі як:
– поява фальшивих точок доступу з тим самим SSID
– масові спроби підбору паролів до Wi-Fi
– незвичайний обсяг трафіку від окремого пристрою
– зміни в патернах використання мережі, які можуть вказувати на зараження шкідливим ПЗ.

Важливим аспектом є здатність AI-систем працювати в реальному часі й масштабуватися під велике число клієнтів. Тому дедалі більше уваги приділяється розподіленим рішенням, граничним обчисленням (edge computing), а також федеративному навчанню, коли моделі навчаються на різних вузлах без необхідності передавати всі сирі дані у центр.

## 2.5 Порівняльний аналіз традиційних і AI-орієнтованих методів захисту інформації

Щоб зрозуміти місце штучного інтелекту в захисті безпровідних телекомунікаційних мереж, доцільно порівняти AI-орієнтовані підходи з традиційними методами, які вже давно використовуються в практиці кібербезпеки.

Традиційні методи (класичні протоколи шифрування, статичні конфігурації firewall, сигнатурні IDS) добре працюють там, де загрози відносно стабільні та добре описані. Наприклад, для захисту Wi-Fi-мереж від пасивного прослуховування достатньо правильно налаштованого WPA3 з надійними паролями. Для блокування очевидних шкідливих IP-адрес достатньо списків блокування та відповідних правил firewall.

Однак у ситуаціях, коли з’являються нові типи атак, комбіновані сценарії, атаки нульового дня, традиційні засоби часто виявляються недостатніми. Сигнатурна IDS не зможе розпізнати атаку, якої немає в її базі; статичні правила firewall не врахують складну аномальну поведінку пристрою, який формально використовує «дозволені» порти й протоколи.

AI-орієнтовані методи, навпаки, орієнтуються на поведінку: вони аналізують профіль нормального функціонування мережі й виявляють відхилення від нього. Це дозволяє:
– знаходити раніше невідомі типи атак

– адаптуватися до змін у трафіку
– працювати з великим обсягом багатовимірних даних.

Разом з тим у AI-методів є власні недоліки:
– потреба у великих і якісних датасетах для навчання
– ризик упередженості моделі (bias)
– складність інтерпретації рішень глибоких нейронних мереж
– ризик атак на самі моделі (adversarial-атаки, отруєння навчальних даних).

З точки зору практичного впровадження, найкращим підходом сьогодні вважається комбінований:
– криптографія, протоколи захисту та сегментація забезпечують базовий рівень безпеки й відповідність стандартам
– IDS/IPS, firewall та політики доступу реалізують класичний периметровий і внутрішній захист
– AI-орієнтовані системи доповнюють їх, забезпечуючи інтелектуальний аналіз трафіку, виявлення аномалій, кореляцію подій з різних джерел.

Для наочності можна узагальнити ключові відмінності між традиційними та AI-орієнтованими методами у вигляді таблиці (у текстовому вигляді з використанням роздільника ";"):

Характеристика; Традиційні методи захисту; AI-орієнтовані методи захисту
Принцип роботи; Сигнатури, статичні правила, наперед визначені політики; Аналіз поведінки, виявлення аномалій, навчання на даних
Робота з новими атаками; Обмежена, потрібне оновлення сигнатур і правил; Можливе виявлення як аномалій навіть без явних сигнатур
Гнучкість; Зміна правил потребує ручної роботи адміністратора; Моделі можуть адаптуватися через перенавчання та оновлення
Потрібні ресурси; Відносно невеликі (залежно від обсягу трафіку й правил); Значні ресурси на навчання моделі та обробку даних

Пояснюваність рішень; Висока – правила й сигнатури зрозумілі; Часто низька – особливо при використанні глибинних мереж
Залежність від якості даних; Менша, основа – експертні правила; Дуже висока, потрібні якісні навчальні вибірки
Сфера оптимального застосування; Добре відомі загрози, контроль доступу, базова фільтрація; Складні, динамічні середовища, 5G, IoT, великі безпровідні мережі

Як показує аналіз сучасних публікацій, у галузі безпеки безпровідних мереж саме поєднання цих підходів дає найкращий результат: традиційні засоби забезпечують стабільний «каркас» базового захисту, а ШІ додає гнучкість і здатність бачити те, що виходить за рамки стандартних сценаріїв. У наступному розділі така комбінована концепція буде використана для побудови та дослідження конкретної системи захисту безпровідної мережі з використанням інструментів штучного інтелекту.

# 3 ДОСЛІДЖЕННЯ ТА ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

## 3.1 Вихідні дані, постановка задачі та вимоги до системи захисту

Першим кроком є чітке формулювання умов, у яких повинна працювати система захисту. Це важливо тому, що захист безпровідної мережі завжди прив’язаний до конкретного середовища: кількості користувачів, типів пристроїв, набору сервісів, вимог до безперервності роботи.

У даній дипломній роботі як базовий приклад розглядається безпровідна мережа середнього офісу ІТ-компанії.

Передбачається, що:
– офіс розташований у трьохповерховій будівлі
– на кожному поверсі розміщено приблизно по 20–25 робочих місць співробітників
– співробітники використовують ноутбуки, смартфони, іноді планшети, всі з підтримкою Wi-Fi
– частина робочих місць обладнана стаціонарними ПК, які підключені до дротової мережі, але мають доступ до тих самих серверів
– у приміщеннях установлені мережеві принтери, IP-телефони, камери відеоспостереження, кілька IoT-пристроїв (датчики температури, контролери освітлення).

Інфраструктура побудована так, що основний доступ працівників до локальних ресурсів і інтернету здійснюється через корпоративну WLAN. Це означає, що компрометація безпровідної мережі фактично означатиме компрометацію всієї офісної інфраструктури: зловмисник, який отримав доступ

до WLAN, може спробувати атакувати внутрішні сервери, перехопити трафік, поширити шкідливе ПЗ тощо.

Загальні ризики для такої мережі:
– несанкціонований доступ до корпоративного SSID
– встановлення фальшивих точок доступу
– спроби атак на IoT-пристрої та використання їх як «слабкої ланки»
– DoS-атаки, що порушують доступність послуг
– «тиха» шкідлива активність зсередини – від легітимних, але скомпрометованих пристроїв.

Постановку задачі можна сформулювати так:

потрібно спроєктувати систему, яка поверх традиційних механізмів (криптографія, firewall, сегментація) здійснюватиме інтелектуальний моніторинг безпровідної мережі, виявляти підозрілу активність і допомагати адміністратору оперативно реагувати на загрози.

Об’єктом дослідження є безпровідна локальна мережа офісу, побудована за стандартами сімейства IEEE 802.11, із використанням сучасних механізмів захисту на рівні протоколів.

Предметом дослідження є методи проєктування системи виявлення загроз у такій мережі на основі алгоритмів штучного інтелекту.

До системи захисту висуваються такі функціональні вимоги:
– збір і агрегування даних про роботу безпровідної мережі (трафік, службові події, логування підключень)
– виявлення аномалій у поведінці користувачів і пристроїв
– класифікація подій як нормальних або потенційно небезпечних з віднесенням до певного типу загрози, якщо це можливо
– формування сповіщень для адміністратора з коротким описом ситуації та

базовими рекомендаціями щодо реагування
– можливість інтеграції з наявними засобами (наприклад, передача сигналу на міжмережевий екран для блокування трафіку певного вузла).

Нефункціональні вимоги:
– система не повинна суттєво збільшувати затримки в мережі й погіршувати якість обслуговування
– повинна масштабуватися разом із ростом кількості клієнтів (наприклад, при розширенні офісу)
– має мати зрозумілий інтерфейс і помірне навантаження на адміністратора, щоб її можна було реально використовувати в щоденній роботі
– повинна забезпечувати прийнятний баланс між чутливістю (щоб не пропускати атаки) та кількістю хибних спрацьовувань (щоб не «заспамлювати» фахівців з ІБ).

Проблема, яку вирішує дипломна робота, полягає не в заміні традиційних засобів захисту, а в їхньому посиленні за рахунок інтелектуального аналізу поведінки безпровідної мережі.

## 3.2 Вибір архітектури безпровідної мережі та сценаріїв атак для дослідження

Для дослідження необхідно зафіксувати конкретну логічну й фізичну архітектуру безпровідної мережі. У дипломній роботі розглядається наступний варіант.

Фізична структура:
– на кожному поверсі будівлі встановлено по дві точки доступу Wi-Fi, розташовані таким чином, щоб забезпечити стабільне покриття та мінімізувати «мертві зони»
– точки доступу підключені до керованих комутаторів, які утворюють дротовий магістральний сегмент
– комутатори об’єднані з центральним маршрутизатором, на якому налаштований

вихід в інтернет
– між маршрутизатором та зовнішньою мережею встановлено міжмережевий екран
– у локальній мережі функціонує сервер автентифікації, контролер безпровідних точок та кілька прикладних серверів (файловий, поштовий, внутрішніх сервісів).

Логічна структура:
– корпоративний SSID для працівників; доступ за WPA2-Enterprise або WPA3-Enterprise з використанням індивідуальних облікових записів
– окремий SSID для гостьового доступу; обмежений вихід тільки в інтернет
– окремий SSID для IoT-пристроїв; трафік із цього сегмента жорстко фільтрується, доступ до внутрішніх серверів мінімальний
– VLAN-сегментація: корпоративний, гостьовий і IoT-трафік розділені на рівні комутаторів і маршрутизатора.

Такий підхід дозволяє чітко відокремити різні категорії пристроїв і користувачів, що зменшує наслідки можливої компрометації одного із сегментів.

Для моделювання роботи системи захисту обирається набір базових сценаріїв атак, які актуальні для описаної архітектури:

1. Несанкціонований доступ до корпоративного SSID.
   Мета зловмисника – підібрати пароль або скомпрометувати автентифікацію. На практиці це може проявлятися у вигляді великої кількості невдалих спроб підключення з однієї або кількох MAC-адрес, використання спеціальних інструментів для атаки на протоколи захисту. Система захисту повинна розпізнати таку ситуацію як відхилення від нормальної поведінки користувачів.
2. Створення фальшивої точки доступу.
   Зловмисник піднімає свою точку доступу з тим самим SSID, що й у корпоративної мережі, або зі схожою назвою. Користувачі можуть

випадково підключитися до цієї точки, що дає змогу організувати перехоплення трафіку або зміну налаштувань. З погляду мережі це може виглядати як поява нового джерела трафіку з параметрами, відмінними від інших точок доступу, і як нетипова зміна маршрутів трафіку.

3. Атака типу DoS на безпровідну мережу. Здійснюється генерація великої кількості службових кадрів або надмірного обсягу даних, які перевантажують радіоканал або самі точки доступу. У результаті легітимні користувачі відчувають затримки, розриви з'єднань, а то й повну недоступність мережі. Для системи захисту це проявляється як різке збільшення кількості однотипних подій, падіння якості сервісу, нетипові патерни навантаження.
4. Компрометація IoT-пристрою. Зловмисник отримує контроль над IoT-пристроєм, після чого той починає поводитися нетипово: встановлює зовнішні з'єднання, генерує «дивний» трафік, бере участь у DDoS-атаках на сторонні ресурси. З погляду системи захисту це відхилення профілю поведінки конкретного пристрою від його звичайних параметрів.
5. Внутрішня розвідка й сканування мережі легітимним користувачем. Користувач, який має дійсний доступ до мережі, запускає сканер портів, намагається підбирати паролі до служб, перевіряє, які ресурси доступні. За поведінкою це суттєво відрізняється від типової активності офісного працівника, який використовує переважно веб-доступ, пошту та кілька внутрішніх сервісів.

Усі ці сценарії будуть враховані при формуванні набору даних і подальшому навчанні моделі штучного інтелекту.

## 3.3 Вибір та обґрунтування моделі штучного інтелекту для виявлення загроз

Штучний інтелект – поняття широке. У практичній частині роботи потрібно обрати конкретний клас моделей, який буде застосований до задачі виявлення загроз у безпровідній мережі.

Особливості задачі:

– дані мають часову структуру (події відбуваються послідовно, важливий порядок і контекст)

– є великий обсяг подій, які треба аналізувати автоматично

– частина атак має бути виявлена як аномалія без чітко заданих сигнатур

– бажано мати можливість розділяти події за типами (атака на Wi-Fi, DoS, внутрішня розвідка тощо).

Враховуючи це, доцільно поєднати два підходи:

– класичне навчання з учителем для розпізнавання відомих типів атак;

– елементи навчання без учителя або виявлення аномалій для фіксації нових, раніше невідомих загроз.

Як базова «робоча» модель для класифікації подій може бути обраний випадковий ліс або градієнтний бустинг дерев рішень. Такі моделі добре працюють з табличними даними, відносно стійкі до шуму, дають змогу оцінювати важливість ознак і не потребують надто складної настройки. Вони підходять для задачі, де кожному фрагменту трафіку приписується певний клас.

Другим рівнем може виступати модель для виявлення аномалій – наприклад, автоенкодер або ізоляційний ліс. Автоенкодер навчається

відновлювати «нормальні» приклади; якщо під час роботи реальний приклад відновлюється погано, це свідчить про аномалію. Ізоляційний ліс, у свою чергу, шукає об’єкти, які легко «відокремити» від основної маси даних, що також вказує на їхню незвичність.

При наявності достатніх ресурсів доцільно використовувати гібридну нейронну мережу, яка поєднує згортковий шар (для роботи з локальними патернами ознак) і рекурентний шар (для врахування послідовності подій). Така архітектура дозволяє не просто «бачити» статистику по одному інтервалу часу, а й аналізувати, як вона змінюється.

Обґрунтування вибору:
– у простішому варіанті (випадковий ліс + ізоляційний ліс) система буде відносно легкою в реалізації, підходящою для базового стенду й теоретичного аналізу
– у розширеному варіанті (нейронна мережа) можна показати, як додатковий облік часових залежностей покращує здатність системи виявляти складні атаки, що розгортаються поступово.

У дипломній роботі основний акцент робиться на концептуальному обґрунтуванні: не потрібно реалізовувати повністю промислову систему, важливо показати, що вибрана модель адекватно відповідає характеристикам задачі.

## 3.4 Формування набору даних, методика навчання та тестування AI-моделі

Набір даних – це основа для будь-якої моделі ШІ. Без якісного датасету навіть найскладніший алгоритм не продемонструє хороших результатів.

Процес формування даних включає кілька етапів.

Перший етап – збір даних про нормальну роботу мережі.
На цьому етапі фіксується поведінка мережі без навмисних атак:

– підключення користувачів до різних SSID

– нормальне використання веб-ресурсів, пошти, файлових сервісів

– типові обсяги трафіку в робочий і неробочий час

Дані збираються у вигляді логів:
– журнали точок доступу та контролера Wi-Fi
– журнали міжмережевого екрана
– зведені статистики з комутаторів (наприклад, NetFlow-подібна інформація).

Другий етап – моделювання атак і збір відповідних даних. Для кожного зі сценаріїв, описаних у підрозділі 3.2, у контрольованих умовах здійснюється атака. Наприклад:
– запуск інструментів підбору пароля до Wi-Fi з одного або кількох пристроїв
– підняття фальшивого SSID і спостереження за тим, як клієнти до нього підключаються
– генерація DoS-трафіку на одну з точок доступу
– спроби встановити нетипові з’єднання з IoT-пристроїв
– сканування мережі з облікового запису співробітника.

Усі ці дії також логуються. Важливо чітко позначити, в який момент часу почалась атака, які пристрої в ній брали участь, щоб потім пов’язати це з відповідними записами в датасеті.

Третій етап – перетворення сирих логів у набір ознак.

де:

– ID – умовний ідентифікатор прикладу

– кількість пакетів, середня швидкість, кількість невдалих логінів та інші – це числові ознаки, які характеризують трафік за певний інтервал часу

– SSID і тип пристрою можуть кодуватися у вигляді числових або бінарних ознак

– клас – мітка, що позначає, чи це нормальна активність, чи певний тип атаки.

Дані розбиваються на тренувальну, валідаційну й тестову вибірки. Одразу виникає проблема дисбалансу: атак зазвичай значно менше, ніж нормальних записів. Щоб модель не навчилася просто «завжди казати, що все нормально», застосовуються техніки балансування:
– часткове збільшення числа прикладів для рідкісних класів
– налаштування ваг у функції втрат, щоб помилки на атаках «коштували» дорожче, ніж помилки на нормальному трафіку.

Для моделі виявлення аномалій відбирається набір «чистих» нормальних прикладів, на яких вона навчається, а потім тестується на змішаних даних, де присутні й атаки.

Навчання моделі здійснюється ітераційно, до досягнення прийнятних показників на валідаційній вибірці. Після цього на тестовій вибірці оцінюються фінальні характеристики.

## 3.5 Моделювання роботи системи захисту в безпровідній мережі та аналіз результатів

Після формування й навчання моделі необхідно змоделювати її роботу в умовах, наближених до реальної експлуатації. У межах дипломної роботи це можна розглядати як лабораторний експеримент.

Передбачається, що:
– у тестовому середовищі розгорнута спрощена копія описаної архітектури мережі

– налаштовано моніторинг трафіку й передавання статистики в модуль ШІ
– організовано фонова діяльність, що імітує звичайний робочий день (користувачі переглядають веб-сторінки, надсилають пошту, працюють із внутрішніми сервісами)
– у певні моменти часу запускаються сценарії атак.

Метою моделювання є:
– перевірити, чи виявляє система всі змодельовані атаки
– оцінити, скільки часу проходить від початку атаки до її виявлення
– зафіксувати кількість хибних спрацьовувань, які з’являються під час нормальної роботи.

Уявно можна описати очікувану картину.

При запуску атаки підбору пароля до Wi-Fi система має зафіксувати, що від окремої MAC-адреси йде дуже велика кількість невдалих спроб автентифікації, значно більша, ніж у нормальних користувачів. Модель, яка проаналізувала такі патерни в навчальних даних, повинна класифікувати цю ситуацію як загрозу.

У випадку фальшивої точки доступу ШІ-модуль, аналізуючи статистику по трафіку, повинен побачити появу нового джерела, яке не було зареєстроване як легітимна точка доступу, і яке одночасно бере на себе нетипово велику кількість підключень. Це, у поєднанні зі зміною маршрутів трафіку, буде індикатором атаки.

Під час DoS-атаки основним симптомом буде різке зростання навантаження, поява великої кількості однотипних пакетів або службових кадрів, зростання числа розірваних сесій. Модель, яка вчилася на «спокійному» профілі трафіку, повинна позначити подібну поведінку як аномальну.

Для IoT-пристрою, який раптом починає ініціювати зовнішні з’єднання, виділяється аномалія між звичайним профілем (невелика кількість коротких

локальних з’єднань) і новим профілем («довгі» сесії із зовнішніми адресами, збільшений обсяг трафіку).

У результаті моделювання складається якісний висновок: система здатна не тільки реагувати на вже відомі сценарії, але й виявляти загалом «підозрілу» активність, яка виходить за межі нормального функціонування мережі.

## 3.6 Оцінка ефективності запропонованої системи захисту

Для оцінки роботи системи використовуються класичні показники якості для моделей виявлення загроз.

Основні з них:

– точність – частка усіх прикладів, класифікованих правильно

– повнота – частка виявлених атак від загальної кількості реальних атак

– precision – частка справжніх атак серед усіх прикладів, які система позначила як «атака»

– F1-міра – узагальнений показник, що поєднує precision і recall

– рівень хибних спрацьовувань – частка випадків, коли нормальну активність система помилково позначила як загрозу

– середня затримка виявлення – час між початком шкідливої активності та моментом, коли модель видала сигнал

– пропускна здатність системи – скільки подій або записів вона може обробити за одиницю часу без помітної деградації.

Для наочності ці показники можна представити у вигляді текстової таблиці:

Таблиця 3.1

Оцінка ефективності

| Показник | Зміст | Бажане значення |
|---|---|---|
| Точність | Частка правильно класифікованих прикладів | Наближена до 1 |
| Повнота | Частка виявлених атак | Якомога ближча до 1 |
| Precision | Частка справжніх атак серед усіх «атак» | Висока, щоб мінімізувати хибні спрацювання |
| F1-міра | Баланс між precision і recall | Високий, без різкого перекосу |
| Рівень хибних спрацьовувань | Частка нормальних подій, позначених як загроза | Мінімальний |
| Затримка виявлення | Час реагування системи | Мала, у межах, прийнятних для оперативного захисту |
| Продуктивність | Здатність обробляти потік даних | Достатня для реального навантаження мережі |

На основі проведеного моделювання й розрахунку цих показників можна зробити висновок про те, що запропонована система на основі штучного інтелекту здатна:

– підвищити рівень виявлення атак у безпровідній мережі, особливо складних та нових сценаріїв

– знизити час реакції на інциденти

– доповнити традиційні механізми захисту, які залишаються основою безпеки, але не завжди встигають «підлаштуватися» під нові типи загроз.

Разом із тим у роботі підкреслюється, що жодна, навіть найкраща модель ШІ, не може гарантувати абсолютної безпеки. Для досягнення прийнятного рівня захисту потрібна комбінація заходів: правильна архітектура мережі, надійні протоколи шифрування, регулярні оновлення програмного забезпечення, навчання персоналу, чіткі політики безпеки. Система на основі штучного інтелекту в цій картині виступає як потужний, але все ж допоміжний інструмент, який підсилює можливості адміністратора й дозволяє своєчасно виявляти загрози в безпровідній телекомунікаційній мережі.

# 4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

## 4.1 Розрахунок капітальних витрат на створення системи захисту в безпровідній мережі

Капітальні витрати пов’язані з одноразовими вкладеннями на етапі створення системи. Вони включають придбання апаратного і програмного забезпечення, модернізацію мережевої інфраструктури, роботи з впровадження та навчання персоналу.

До складу капітальних витрат доцільно віднести такі статті:

– придбання серверного обладнання для розміщення модулів штучного інтелекту та системи моніторингу

– бюджет на модернізацію мережевої інфраструктури у випадку, якщо наявне обладнання не підтримує необхідні функції моніторингу

– придбання або ліцензування програмних продуктів, які використовуються для збору, зберігання та аналізу даних

– роботи з впровадження системи, налаштування інтеграції з існуючою інфраструктурою

– навчання адміністратора та фахівців з інформаційної безпеки роботі з новою системою.

Для оцінки використаємо умовний приклад для офісу з приблизно ста активними пристроями у піковий час. Вартість наведена в тисячах гривень. Таблиця має вигляд.

Таблиця 4.1

| № | Стаття капітальних витрат | Сума, тис. грн |
|---|---|---|
| 1 | Сервер для системи моніторингу і ШІ аналізу трафіку | 160 |
| 2 | Додаткові мережеві сенсори і обладнання для дзеркалювання трафіку | 80 |
| 3 | Програмне забезпечення для збору, зберігання та попередньої обробки даних | 120 |
| 4 | Ліцензії на компоненти з функціями штучного інтелекту | 90 |
| 5 | Послуги з впровадження і налаштування системи | 70 |
| 6 | Навчання персоналу, підготовка внутрішніх інструкцій | 30 |

Сумарні капітальні витрати позначимо як Кзаг. У нашому прикладі це приблизно двісті п’ятдесят тисяч плюс двісті дев’яносто тисяч, тобто п’ятсот п’ятдесят тисяч гривень. Формально це можна подати у вигляді суми всіх статей.

Під час реального проєктування конкретні суми залежатимуть від багатьох факторів. Зокрема, від того, чи є в організації вільні серверні ресурси, які можна використати під нову систему, чи потрібно купувати окреме обладнання, від того,

чи обрана модель використання програмного забезпечення передбачає разову оплату або періодичну абонентську плату, а також від ринку послуг інтеграторів.

Важливим моментом є те, що частину капітальних витрат можна оптимізувати. Наприклад, якщо в організації вже є сервер віртуалізації з запасом ресурсів, модулі ШІ можна розгорнути як віртуальні машини, що зменшить потребу у придбанні окремого апаратного комплексу. Або, при наявності кваліфікованих внутрішніх фахівців, частину робіт з впровадження можна виконати власними силами, знизивши статтю витрат на зовнішні послуги.

Разом з тим, економія на апаратній платформі і впровадженні має бути обґрунтованою. Система захисту працюватиме з великим обсягом даних і повинна бути стабільною, тому надто слабке обладнання чи відсутність кваліфікованої підтримки може призвести до того, що інвестиції не дадуть очікуваного результату.

## 4.2 Розрахунок експлуатаційних витрат на підтримку та оновлення системи

Експлуатаційні витрати пов’язані не з одноразовим закупівлею, а з підтримкою роботи системи протягом усього строку експлуатації. До них належать витрати на електроенергію, технічне обслуговування, поновлення ліцензій, а також частина витрат на заробітну плату персоналу, який адмініструє систему.

Основні складові експлуатаційних витрат:
– вартість електроенергії, споживаної сервером та мережевими пристроями, за рік
– продовження дії ліцензій або абонентська плата за окремі компонентні рішення
– технічне обслуговування і можливий ремонт обладнання
– оновлення програмного забезпечення, в тому числі платні оновлення
– заробітна плата або її частина для адміністратора, який відповідає за роботу системи та аналіз звітів.

Для розрахунку річних експлуатаційних витрат використаємо умовні значення. Позначимо у тисячах гривень на рік.

Таблиця 4.2

Витрати

| № | Стаття експлуатаційних витрат | Сума, тис. грн на рік |
|---|---|---|
| 1 | Електроенергія, охолодження і супутні витрати на розміщення сервера | 15 |
| 2 | Продовження ліцензій і абонентська плата за програмне забезпечення | 60 |
| 3 | Технічне обслуговування і резерв на ремонт | 20 |
| 4 | Оновлення програмних компонентів, тестування після оновлень | 10 |
| 5 | Частина фонду оплати праці адміністратора і фахівця з ІБ, пов’язана саме з цією системою | 60 |

Сумарні експлуатаційні витрати за рік в такому прикладі становлять приблизно сто шістдесят п’ять тисяч гривень. Ця величина може змінюватися зі зростанням або зменшенням кількості користувачів, зі зміною тарифів на

електроенергію, а також від політики постачальника програмного забезпечення щодо ліцензій та оновлень.

Важливо підкреслити, що не всі витрати на персонал є «додатковими». Частина роботи з моніторингу безпеки і так виконується системним адміністратором або спеціалістом з інформаційної безпеки. Впровадження системи на базі штучного інтелекту часто не стільки збільшує загальні трудові витрати, скільки змінює їх структуру. Класичний аналіз логів вручну частково замінюється роботою з налаштуванням і контролем моделі ШІ, але загальний обсяг завдань залишається на подібному рівні.

Тому в економічних розрахунках доцільно враховувати не весь фонд оплати праці цих фахівців, а тільки додатковий час, який потрібен саме для роботи з новою системою. Наприклад, якщо оцінити, що адміністратор витрачатиме в середньому кілька годин на тиждень на аналіз звітів, керування сповіщеннями, коригування налаштувань, то додаткове навантаження відповідатиме невеликій частині його робочого часу.

## 4.3 Розрахунок основних економічних показників ефективності впровадження

Оцінка економічної доцільності впровадження системи захисту базується на порівнянні витрат на її створення і експлуатацію з очікуваним економічним ефектом. У випадку систем інформаційної безпеки під ефектом, як правило, розуміють зниження можливих втрат від інцидентів, скорочення простоїв і непрямих збитків.

Умовно можна виділити дві ситуації.

Перша ситуація – робота без системи захисту на базі штучного інтелекту. У цьому випадку організація використовує тільки традиційні механізми, імовірність і наслідки інцидентів мають певний рівень. Наприклад, на основі попереднього

досвіду або галузевої статистики можна оцінити середні очікувані річні втрати від інцидентів інформаційної безпеки у безпровідній мережі. Це можуть бути втрати від простою сервісів, зниження продуктивності, затрати на ліквідацію наслідків та інші.

Друга ситуація – робота із впровадженою системою захисту. Імовірність успішних атак і масштаб наслідків зменшуються, відповідно зменшуються й очікувані річні втрати. Разом з тим з’являються додаткові витрати на створення і експлуатацію системи.

Економічний ефект від впровадження системи на певному горизонті планування визначається як різниця між втратами у першій і другій ситуації з урахуванням усіх витрат.

Нехай орієнтовні очікувані річні втрати без системи захисту з використанням штучного інтелекту складають, наприклад, чотириста тисяч гривень. Це може відображати один середній інцидент на рік середньої тяжкості або декілька дрібніших інцидентів.

Після впровадження системи можна припустити, що завдяки своєчасному виявленню загроз частина інцидентів буде попереджена або їх масштаб буде значно меншим. Нехай очікувані втрати у такому випадку зменшуються до ста шістдесяти тисяч гривень на рік. Це означає, що система дає економію потенційних втрат на рівні двісті сорок тисяч гривень за рік.

Разом з тим є експлуатаційні витрати на систему, які в нашому прикладі складають сто шістдесят п’ять тисяч гривень на рік. Тоді чистий річний економічний ефект можна оцінити як різницю між економією втрат і додатковими витратами на експлуатацію. У нашому умовному прикладі це приблизно сімдесят п’ять тисяч гривень.

Окремо враховуються капітальні витрати. Їх можна розглядати як одноразову інвестицію, яка повинна окупитися завдяки щорічному чистому економічному ефекту. Для оцінки строку окупності використовується відношення капітальних витрат до чистого річного ефекту.

Якщо взяти сумарні капітальні витрати у розмірі п’ятсот п’ятдесят тисяч гривень і поділити їх на умовний чистий річний ефект сімдесят п’ять тисяч, отримаємо строк окупності близько семи з невеликим років. З практичної точки зору для інфраструктурних проєктів у сфері безпеки строк окупності в межах п’яти-десяти років вважається прийнятним, особливо якщо йдеться про важливу інформаційну інфраструктуру.

Більш точний розрахунок може проводитися з урахуванням приведених витрат, коли враховується чинник часу. Для цього використовується ставка дисконту, яка відображає очікувану норму прибутковості або вартість капіталу для організації. Приведені витрати розраховуються шляхом дисконтування майбутніх експлуатаційних витрат і можливих втрат від інцидентів до поточного моменту.

Загальна логіка полягає у тому, щоб порівняти приведені витрати двох варіантів. Перший варіант – робота без системи з використанням штучного інтелекту. Другий варіант – робота з такою системою з урахуванням капітальних витрат і нової структури експлуатаційних витрат. Варіант з меншими приведеними витратами на обраному горизонті планування є економічно доцільнішим.

Окрім кількісних показників, важливо відзначити і якісні аспекти. Впровадження системи захисту на базі штучного інтелекту може знизити ризик інцидентів, які важко оцінити чисто у грошовому вимірі. Наприклад, мова йде про репутаційні втрати, втрату довіри клієнтів, можливі штрафи від регуляторів у разі

витоку персональних даних. Часто саме ці фактори є основним аргументом на користь інвестицій у сучасні системи безпеки.

Підсумовуючи, можна сказати, що на основі виконаних розрахунків і логіки порівняння витрат та очікуваних вигод впровадження системи захисту інформації в безпровідній мережі з використанням штучного інтелекту є економічно виправданим для організації із середніми і високими вимогами до інформаційної безпеки.

# ВИСНОВКИ

У дипломній роботі було досліджено методи захисту інформації в безпровідних телекомунікаційних мережах із використанням штучного інтелекту. Робота має теоретичну і практичну складові, які взаємно доповнюють одна одну.

У вступі було обґрунтовано актуальність теми. Пояснено, що поширення безпровідних мереж, розвиток технологій п’ятого покоління і масове впровадження Інтернету речей призводять до зростання кількості пристроїв і обсягу трафіку. Разом з цим зростає і кількість загроз для інформаційної безпеки. Традиційні засоби захисту вже не завжди справляються з новими видами атак. Штучний інтелект, здатний аналізувати великі масиви даних і виявляти приховані закономірності, відкриває нові можливості у сфері кібербезпеки. Сформульовано мету роботи, визначено об’єкт і предмет дослідження, поставлено основні завдання.

У першому розділі розглянуто теоретичні основи безпровідних телекомунікаційних мереж. Наведено основні поняття, класифікацію безпровідних мереж, розглянуто особливості архітектури технологій Wi-Fi, стільникових мереж, IoT та п’ятого покоління. Окремо проаналізовано типові загрози та вразливості, властиві безпровідним каналам зв’язку, а також нормативні й стандартні підходи до забезпечення безпеки в таких мережах. Показано, що навіть при використанні сучасних криптографічних протоколів ризики залишаються досить високими, особливо у великих та динамічних інфраструктурах.

У другому розділі було розглянуто методи захисту інформації в безпровідних мережах та можливості застосування штучного інтелекту. Проаналізовано традиційні криптографічні засоби, протоколи первинного захисту, роботу систем виявлення та запобігання атак, роль міжмережевих екранів і мережевої сегментації. Далі увага була перенесена на основи штучного інтелекту

і машинного навчання в задачах кібербезпеки. Розглянуто парадигми навчання з учителем і без учителя, згадані приклади використання глибинних нейронних мереж для виявлення аномалій у трафіку, описано типові етапи побудови AI систем у сфері ІБ. Порівняльний аналіз традиційних і AI орієнтованих методів показав, що найкращі результати досягаються при їх поєднанні.

Третій розділ був присвячений дослідженню та проєктуванню системи захисту інформації в безпровідній мережі з використанням штучного інтелекту. Визначено вихідні дані, описано умовну корпоративну мережу, для якої проєктується система. Сформульовано вимоги до системи захисту, як функціональні, так і нефункціональні. Обрано архітектуру безпровідної мережі з логічною сегментацією на корпоративний, гостьовий та IoT сегменти, виділено сценарії атак, що є найбільш актуальними для такого середовища.

Далі було обґрунтовано вибір моделі штучного інтелекту. Розглянуто варіанти використання класичних алгоритмів машинного навчання і гібридних нейронних мереж, які враховують часову структуру даних. Особливу увагу приділено формуванню набору даних для навчання та тестування моделі. Описано етапи збору логів нормальної роботи мережі, моделювання атак, попередньої обробки даних, виділення ознак і поділу на тренувальну, валідаційну та тестову вибірки.

У рамках моделювання роботи системи захисту показано, як при запуску різних сценаріїв атак змінюється поведінка мережі і як це відображається у даних, що аналізуються ШІ моделлю. Пояснено, які ситуації система може виявляти як аномальні, як формується сигнал для адміністратора, які типи помилок можуть виникати і як їх мінімізувати.

Четвертий розділ містив техніко економічне обґрунтування впровадження системи захисту. Виділено основні статті капітальних витрат, пов’язаних із придбанням обладнання, програмного забезпечення та проведенням робіт з

впровадження. Оцінено експлуатаційні витрати на підтримку функціонування системи. На умовному прикладі розраховано чистий річний економічний ефект за рахунок зменшення очікуваних втрат від інцидентів безпеки. На основі цього проведено оцінку строку окупності. Зроблено висновок, що при певних рівнях ризику і вартості можливих інцидентів впровадження системи захисту з використанням штучного інтелекту є економічно доцільним.

У результаті виконання дипломної роботи досягнуто поставленої мети. На теоретичному рівні проведено систематизацію знань про безпровідні телекомунікаційні мережі, їх загрози і методи захисту. На практичному рівні запропоновано підхід до проєктування системи захисту інформації в безпровідній мережі з використанням алгоритмів штучного інтелекту, описано методику формування даних для такої системи і принципи оцінки її ефективності.

Основні результати роботи полягають у наступному.
– Показано, що штучний інтелект здатний підвищити рівень захисту безпровідних мереж, оскільки дає змогу виявляти нетипові загрози, які важко описати у вигляді фіксованих сигнатур.
– Запропоновано структуру системи, яка доповнює, а не замінює традиційні засоби захисту, що відповідає сучасній практиці комплексної кібербезпеки.
– Продемонстровано підхід до техніко економічного обґрунтування впровадження рішень у сфері безпеки, який враховує не тільки прямі витрати, але й можливе зниження втрат від інцидентів.

Подальші дослідження у цьому напрямі можуть бути пов’язані з поглибленою практичною реалізацією запропонованої системи, тестуванням на реальних датасетах, дослідженням стійкості моделей штучного інтелекту до спеціальних атак на них, а також з розробкою методів пояснюваності рішень ШІ для потреб фахівців з інформаційної безпеки.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Beard C., Stallings W. Wireless Communication Networks and Systems. – Harlow: Pearson Education, 2016.
2. Stallings W. Wireless Communications and Networks. 2nd ed. – Upper Saddle River: Pearson Prentice Hall, 2005.
3. Wrightson T. Wireless Network Security: A Beginner’s Guide. – New York: McGraw-Hill, 2012.
4. Xiao Y., Shen X., Du D.-Z. Wireless Network Security. – New York: Springer, 2007.
5. Imai H. Wireless Communications Security. – Boston: Artech House, 2006.
6. Penttinen J. Wireless Communications Security: Solutions for the Internet of Things. – Chichester: John Wiley & Sons, 2016.
7. Khari M., Kar A.K., et al. Wireless Communication Security. – Hoboken: Wiley–Scrivener, 2021. ScienceDirect
8. Gordeychik S.V., Dubrovin V.V. Безопасность беспроводных сетей. – М.: Горячая линия – Телеком, 2008.
9. Радько Н.М., Мокроусов А.Н. Защита информации в беспроводных сетях: Учеб. пособие. – Воронеж: ВГТУ, 2010.
10. Гейер У. Беспроводные сети. Первый шаг. – М.: Вильямс, 2005.
11. Makarenko S.I. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009.
12. Келдыш Н.В. Системная защита информации компьютерных сетей. – М.: Инфра-Инженерия, 2022.
13. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. – Boston: Pearson, 2017.
14. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – Boca Raton: CRC Press, 1996.

15. IEEE Std 802.11i-2004. IEEE Standard for Information technology – Local and metropolitan area networks – Specific Requirements – Part 11: Wireless LAN MAC and PHY Specifications. Amendment 6: MAC Security Enhancements. – New York: IEEE, 2004.
16. IEEE Std 802.11-2020. IEEE Standard for Information technology – Local and metropolitan area networks – Specific Requirements – Part 11: Wireless LAN MAC and PHY Specifications. – New York: IEEE, 2020.
17. NIST SP 800-97. Frankel S. et al. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. – Gaithersburg: NIST, 2007.
18. NIST SP 800-153. Souppaya M., Scarfone K. Guidelines for Securing Wireless Local Area Networks (WLANs). – Gaithersburg: NIST, 2012.
19. NIST SP 800-48r1. Scarfone K., Padgette J. Guide to Securing Legacy IEEE 802.11 Wireless Networks. – Gaithersburg: NIST, 2010.
20. Fang D., Qian Y., Hu R.Q. 5G Wireless Network Security and Privacy. – Hoboken: Wiley–IEEE Press, 2023.
21. Stojmenovic I. (ed.) Handbook of Wireless Networks and Mobile Computing. – New York: Wiley, 2002.
22. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks. – 2015.
23. Khan M.A., Salah K. IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems. – 2018.
24. Buczak A.L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection // IEEE Communications Surveys and Tutorials. – 2016.
25. Handa A., Sharma V., Shukla V. Machine learning in cybersecurity: A review // WIREs Data Mining and Knowledge Discovery. – 2019.
26. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection // Proc. IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.

27. Mliki H., Hadj Kacem A., Chaari L. A Comprehensive Survey on Intrusion Detection based Machine Learning for IoT Networks // EAI Endorsed Transactions on Security and Safety. – 2021.
28. Hozouri S., Azarmi M., Crespi N. A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges // Journal of Information Security and Applications. – 2025.
29. Pinto A., Cunha A., Cabral J., et al. A survey on intrusion detection systems based on machine learning // Sensors. – 2020.
30. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. – 2019.
31. Петренко Т.А., Вильотніков В.В. Методи захисту інформації в бездротових мережах: навчальний посібник. – Чернігів: ЧНТУ, 2021.
32. Аносов А.О. Модель перехоплення та захисту інформації в бездротових мережах // Сучасний захист інформації. – 2017.
33. Шовкута В.А. Аналіз механізмів захисту та вразливостей у бездротових мережах IEEE 802.11 // Наукові праці (НГУ). – 2016.
34. Колесніков С.В., Шелестов І.М. Штучний інтелект і безпека інформації: монографія. – Київ: Видавництво НАУ, 2020.
35. Ваврик Ю., Опірський І. Штучний інтелект: кібербезпека нового покоління // Наукове видання Національного університету «Львівська політехніка». – 2024.
36. Федорченко О.С. Роль штучного інтелекту у забезпеченні кібербезпеки // Інформаційна безпека. – 2025.
37. Оніщенко Є.О. Застосування штучного інтелекту в системах моніторингу кіберзагроз // Матеріали наукової конференції НТУУ «КПІ ім. І. Сікорського». – 2025.

38. Позовна І., Сокол В. Вплив нейронних мереж на розвиток кібербезпеки в критичних інформаційних інфраструктурах // Інформаційна безпека. – 2024.

# Дослідження методів захисту інформації в беспроводових телекомунікаційних мережах з використанням технологій штучного інтелекту

Владислав ТКАЧЕНКО

1 ТЕОРЕТИЧНІ ОСНОВИ БЕЗПРОВІДНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

2 МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ ТА МОЖЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

3 ДОСЛІДЖЕННЯ ТА ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Метою дипломної роботи є аналіз і узагальнення теоретичних та практичних підходів до захисту інформації в безпровідних телекомунікаційних мережах з урахуванням сучасних загроз, а також дослідження можливостей застосування методів штучного інтелекту для підвищення рівня інформаційної безпеки.

# Типові загрози та вразливості в безпровідних мережах

Безпровідні телекомунікаційні мережі поєднують у собі всі звичні проблеми класичних IP-мереж і додають до них специфічні загрози, пов’язані з відкритим характером радіоканалу, мобільністю користувачів та великою кількістю недорогих IoT-пристроїв. Це вимагає комплексного підходу до захисту, у якому поєднуються технічні, організаційні та інтелектуальні засоби.

- Несанкціонований доступ до мережі.
- Перехоплення трафіку та пасивне прослуховування
- Перехоплення трафіку та пасивне прослуховування
- Атаки типу «людина посередині» (MITM).
- Атаки на протоколи автентифікації та шифрування
- Атаки типу відмови в обслуговуванні (DoS, DDoS)

# Основи штучного інтелекту та машинного навчання в задачах кібербезпеки

1. Штучний інтелект у широкому розумінні – це сукупність методів і технологій, які дозволяють комп'ютерним системам виконувати завдання, що традиційно вважались такими, що потребують людського інтелекту: розпізнавання образів, аналіз природної мови, прийняття рішень у складних ситуаціях. У сфері кібербезпеки ШІ використовується для автоматизації аналізу великих обсягів даних, виявлення нетипової поведінки, класифікації трафіку, прогнозування ризиків.
2. Основою практичного застосування ШІ є машинне навчання (ML) – підхід, при якому модель не програмується явно на усі можливі ситуації, а «навчається» на історичних даних. У задачах кібербезпеки такими даними можуть бути:
   – журнали мережевого трафіку
   – послідовності системних викликів
   – статистика підключень до точок доступу
   – логи аутентифікації та авторизації
   – записи IDS/IPS про спроби атак.

# ДОСЛІДЖЕННЯ ТА ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Першим кроком є чітке формулювання умов, у яких повинна працювати система захисту. Це важливо тому, що захист безпровідної мережі завжди прив’язаний до конкретного середовища: кількості користувачів, типів пристроїв, набору сервісів, вимог до безперервності роботи.

# Вихідні дані, постановка задачі та вимоги до системи захисту

Постановку задачі можна сформулювати так:

потрібно спроєктувати систему, яка поверх традиційних механізмів (криптографія, firewall, сегментація) здійснюватиме інтелектуальний моніторинг безпровідної мережі, виявляти підозрілу активність і допомагати адміністратору оперативно реагувати на загрози.

Вибір та обґрунтування моделі штучного інтелекту для виявлення загроз

- Особливості задачі:
- – дані мають часову структуру (події відбуваються послідовно, важливий порядок і контекст)
- – є великий обсяг подій, які треба аналізувати автоматично
- – частина атак має бути виявлена як аномалія без чітко заданих сигнатур
- – бажано мати можливість розділяти події за типами (атака на Wi-Fi, DoS, внутрішня розвідка тощо).





# ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

# ВИСНОВКИ

Підсумовуючи, можна сказати, що на основі виконаних розрахунків і логіки порівняння витрат та очікуваних вигод впровадження системи захисту інформації в безпровідній мережі з використанням штучного інтелекту є економічно виправданим для організації із середніми і високими вимогами до інформаційної безпеки.