Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікаціїі*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

Дослідження засобів безпеки безпроводових мереж

(тема)

Виконав:
студент 2 курсу, групи *ІМІм-22-1*
Єфремов Н.С.

Спеціальності *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц., к.т.н. Чеботарьова Д.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Єфремов Н.С.*
(підпис) (прізвище та ініціали)

Керівник _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри ІМІ_____
(підпис)
“____” _____2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентові *Єфремову Нікіті Сергійовичу*
(прізвище, ім’я, по батькові)

1. Тема роботи *Дослідження засобів безпеки безпроводових мереж*

затверджені наказом університету від *23 жовтня 2023* року № *1233 Ст*

2. Термін подання студентом роботи до екзаменаційної комісії *10 січня 2024 р.*

3. Вихідні дані до роботи

Виконати порівняльний аналіз сучасних безпроводових технологій, проаналізувати тенденції розвитку безпроводового зв'язку. Дослідити загрози та вразливості в безпроводових мережах, зокрема новітні ризики. Дослідити інструменти, методи та засоби безпеки в безпроводових мережах. Запропонувати ефективне рішення для захисту безпроводових мереж та сформулювати рекомендації для організації та підтримки високого рівня безпеки.

4. Перелік питань, що потрібно опрацювати в роботі

Вступ.
1. Аналіз безпроводових мереж.
2. Джерела загроз інформації в безпроводових мережах.
3. Засоби безпеки безпроводових мереж.
4. Ефективні рішення для захисту безпроводових мереж.
Висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *Слайди у форматі Power Point (назва, мета і задачі роботи, аналіз сучасних безпроводових технологій, аналіз тенденцій розвитку безпроводового зв'язку, загрози та вразливості в безпроводових мережах, новітні ризики, інструменти мережної безпеки, методи та засоби безпеки в безпроводових мережах, тестування на проникнення, рекомендації для організації та підтримки високого рівня безпеки, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ*	*22.10.23*	*виконано*
2	*Підбір літератури за темою роботи*	*23.10 - 02.11.23*	*виконано*
3	*Виконання розділу 1*	*03.11 - 19.11.23*	*виконано*
4	*Виконання розділу 2*	*20.12 – 02.12.23*	*виконано*
5	*Виконання розділу 3*	*03.12 – 19.12.23*	*виконано*
6	*Виконання розділу 4*	*20.12 - 02.01.24*	*виконано*
7	*Оформлення пояснювальної записки*	*03.12 - 07.01.24*	*виконано*
8	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК	*08.01 - 10.01.24*	*виконано*

Дата видачі завдання *22.10.2023 р.*

Студент _____ *Єфремов Н.С.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 18 рис., 4 табл., 28 джерел, 2 додатки.

Об'єкт дослідження – безпека безпроводових мереж.

Мета роботи – дослідити засоби безпеки та запропонувати ефективні рішення для безпеки безпроводових мереж.

Результати – в роботі виконано порівняльний аналіз сучасних безпроводових технологій та аналіз основних тенденцій розвитку безпроводового зв'язку. Досліджено загрози та вразливості в безпроводових мережах, в тому числі і найновіші ризики. Детально розглянуто методи та засоби безпеки в безпроводових мережах. В якості ефективного рішення для захисту безпроводових мереж запропоновано використовувати комплексний підхід, що серед інших засобів обов'язково включає такі сучасні засоби як тестування на проникнення, архітектуру нульової довіри, системи запобігання вторгненням та цілий комплекс рекомендацій для організації та підтримки високого рівня безпеки.

БЕЗПЕКА, БЕЗПРОВОДОВА МЕРЕЖА, КОРИСТУВАЧ, ЗАХИСТ, ЗАГРОЗА, ВРАЗЛИВІСТЬ, ВТОРГНЕННЯ, ПРИСТРІЙ, ТЕХНОЛОГІЯ

THE ABSTRACT

Explanatory note: 75 p., 18 fig., 4 tabl., 28 sources, 2 app.

The object of study is security of wireless networks.

The purpose of the work is investigate security measures and propose effective solutions for wireless network security.

Results - the work includes a comparative analysis of modern wireless technologies and an analysis of the main trends in the development of wireless communication. Threats and vulnerabilities in wireless networks are explored, including the latest risks. Methods and means of security in wireless networks are considered in detail. As an effective solution for the protection of wireless networks, it is proposed to use a comprehensive approach, which, among other means, necessarily includes such modern tools as penetration testing, zero trust architecture, intrusion prevention systems and a whole set of recommendations for organizing and maintaining a high level of security.

SECURITY, WIRELESS NETWORK, USER, PROTECTION, THREAT, VULNERABILITY, INTRUSION, DEVICE, TECHNOLOGY

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

2FA (Two-Factor Authentication) – двофакторна автентифікація;

AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування;

AFC (Automatic Frequency Control) - автоматична координація частот

AP (Access Point) - точка доступу;

APT (Advanced Persistent Threats) - розширені постійні загрози;

BLE (Bluetooth Low Energy) - bluetooth із низьким енергоспоживанням;

BR (Broadcast Radio) - трансляція радіо;

CCK (Complementary Code Keying) - модуляція додаткового коду;

DDoS (Distributed Denial-of-Service) – розподілена атака на відмову в обслуговуванні;

DoS (Denial-of-Service) – атака на відмову в обслуговуванні;

EDR (Endpoint Detection and Response) - захист кінцевих точок;

IDPS (Intrusion Detection / Prevention System) – технологія системи виявлення та запобігання вторгненням;

IDS (Intrusion Detection System) – система виявлення вторгнень;

IPS (Intrusion Prevention System) – система запобігання вторгненням;

IoT (Internet of Things) – інтернет речей;

LAN (local area network) - локальна мережа;

LoRaWAN (Long Range Wide Area Network) - протокол глобальної мережі з низьким енергоспоживанням для IoT;

LPWAN (Low Power Wide Area Network) – глобальна мережа малої потужності з низьким енергоспоживанням;

MAN (Metropolitan Area Network) - міська мережа;

MIMO (Multiple In Multiple Out) – теологія рознесення передавальних і приймальних антен;

MITM (Man in the middle) – атака «людина-в-середині»;

MFA (Multi-Factor Authentication) – багатофакторна автентифікація;

OFDM (Orthogonal Frequency-Division Multiplexing) - метод мультиплексування з ортогональним частотним поділом;

PAN (Personal Area Network) - персональна мережа;

RF (Radio Frequency) - радіочастота;

RFID (Radio Frequency Identification) - радіочастотна ідентифікація;

SAE (Simultaneous Authentication of Equals) – технологія обміну автентифікацією рівних;

SIEM (Security Information and Event Management Tools) - інформація про безпеку та інструменти керування подіями;

SSID (Service Set Identifier) – ідентифікатор безпроводової мережі;

SSL (Secure Sockets Layer) - протокол захищених сокетів;

TKIP (Temporary Key Integrity Protocol) – протокол тимчасової цілісності ключів;

TLS (Transport Layer Security) - протокол захисту транспортного рівня;

VPN (Virtual Private Network) – віртуальна приватна мережа;

WAN (Wide Area Network) - глобальна мережа;

WEP (Wired Equivalent Privacy) – стандарт захисту безпроводового трафіку на основі шифрування RC4;

Wi-Fi (Wireless Fidelity) – це стандарт безпроводового підключення на основі IEEE 802.11;

WPA (Wi-Fi Protected Access) – протокол безпеки для захисту безпроводових мереж;

WPA2 (Wi-Fi Protected Access 2) – друга версія WPA;

WPA3 (Wi-Fi Protected Access 3) – третя версія WPA;

МН - машинне навчання;

ШІ - штучний інтелект.

ВСТУП

Безпроводові електронні комунікації – це найшвидше зростаюча та найбільш динамічніша технологічна галузь у сфері електронних комунікацій. Безпроводовий зв’язок – це спосіб передачі інформації з однієї точки в іншу без використання будь-якого з’єднання (зокрема проводів чи кабелів).

Як правило, в електронних комункаціях інформація передається від передавача до приймача, які знаходяться на обмеженій відстані. За допомогою безпроводових електронних комунікацій передавач і приймач можуть бути розташовані один від одного на відстані від кількох метрів (наприклад, пульт дистанційного керування телевізором) до кількох тисяч кілометрів (супутниковий зв’язок).

Сьогодні безпроводові електронні комунікації є ключовою частиною нашого життя. Мережі Wi-Fi, мобільні телефони, GPS-приймачі, пульти дистанційного керування, Bluetooth Audio та інші системи безпроводового зв’язку все частіше використовуються в нашому повсякденному житті. Вони широко використовуються в різних галузях, таких як інфокомунікації, мережі, розваги, охорона здоров’я, безпека, навчання, бізнес тощо.

Основною проблемою безпроводових мереж є безпека даних, що передаються в мережі. Кількість загроз та атак останнім часом значно збільшилася, тому надзвичайно актуальним є питання організації повноцінного захисту інформації в безпроводових мережах. Саме тому, вивчення цього напряму є дуже актуальним. Таким чином, кваліфікаційна робота, що присвячена дослідженню засобів безпеки безпроводових мереж, є актуальною.

1 АНАЛІЗ БЕЗПРОВОДОВИХ МЕРЕЖ

1.1 Принципи функціонування безпроводових мереж

Безпроводова мережа – це комунікаційна мережа, у якій для зв’язку між вузлами мережі використовуються радіохвилі, а не проводи чи кабелі. Термін безпроводовий зв’язок означає той факт, що він не потребує жодного фізичного з’єднання між пристроями в мережі [1]. Натомість кожен пристрій спілкується з іншими пристроями, надсилаючи та приймаючи радіосигнали по повітрю.

Безпроводова мережа дозволяє пристроям залишатися підключеними до мережі, але переміщатися без прив’язки до будь-яких проводів. Точки доступу підсилюють сигнали Wi-Fi, тому пристрій може бути далеко від маршрутизатора, але все одно бути підключеним до мережі. Коли відбувається під’єднання до точки доступу Wi-Fi у кафе, готелі, залі очікування в аеропорту чи іншому громадському місці, то відбувається під’єднання до безпроводової мережі цього підприємства.

Проводова мережа використовує кабелі для підключення пристроїв, наприклад ноутбуків або настільних комп’ютерів, до Інтернету чи іншої мережі. Проводова мережа має деякі недоліки порівняно з безпроводовою мережею. Найбільшим недоліком є те, що пристрій користувача прив’язаний до маршрутизатора. У найпоширеніших проводових мережах використовуються кабелі, під’єднані одним кінцем до порту Ethernet на мережному маршрутизаторі, а іншим – до комп’ютера чи іншого пристрою [2].

Раніше вважалося, що проводові мережі швидші та безпечніші ніж безпроводові. Але постійне вдосконалення безпроводових мережних технологій зменшило відмінності у швидкості та безпеці між проводовими та безпроводовими мережами.

Існують більш тонкі технологічні відмінності між проводовим і безпроводовим зв’язком. Більшість сучасних проводових мереж зараз є

повнодуплексними, тобто вони можуть передавати та отримувати пакети в обох напрямках одночасно. Крім того, більшість проводових мереж мають спеціальний кабель, який проходить до кожного пристрою кінцевого користувача [3].

У безпроводовій мережі Wi-Fi середовище (радіочастота, яка використовується для мережі) є спільним ресурсом не лише для користувачів мережі, але часто й для інших технологій (Wi-Fi працює у спільній смузі, що схвалена для роботи багато різних електронних пристроїв) [3].

На сьогоднішній день існує три типи розгортання безпроводової мережі:

– централізоване розгортання,

– конвергентне розгортання,

– хмарне розгортання.

Найпоширеніший тип системи безпроводової мережі – централізоване розгортання, воно традиційно використовується в містечках, де будівлі та мережі знаходяться в безпосередній близькості. Це розгортання консолідує безпроводову мережу, що спрощує оновлення та забезпечує розширені безпроводові функції. Контролери базуються на місці та встановлюються в централізованому місці.

Конвергентне розгортання використовується для невеликих капідприємств або філій. Конвергентне розгортання забезпечує узгодженість безпроводових і проводових з’єднань. Це розгортання об’єднує проводові та безпроводові мережі на одному мережному пристрої – комутаторі доступу – і виконує подвійну роль як комутатора, так і безпроводового контролера.

Хмарне розгортання – це система, що використовує хмару для керування мережними пристроями, розгорнутими локально в різних місцях. Рішення потребує хмарних пристроїв, які забезпечують повну видимість мережі через свої інформаційні панелі [2].

Сьогодні існує кілька типів поширених безпроводових мереж (рис. 1.1):

– локальна мережа (LAN),

– персональна мережа (PAN),

– міська мережа (MAN),

– глобальна мережа (WAN).

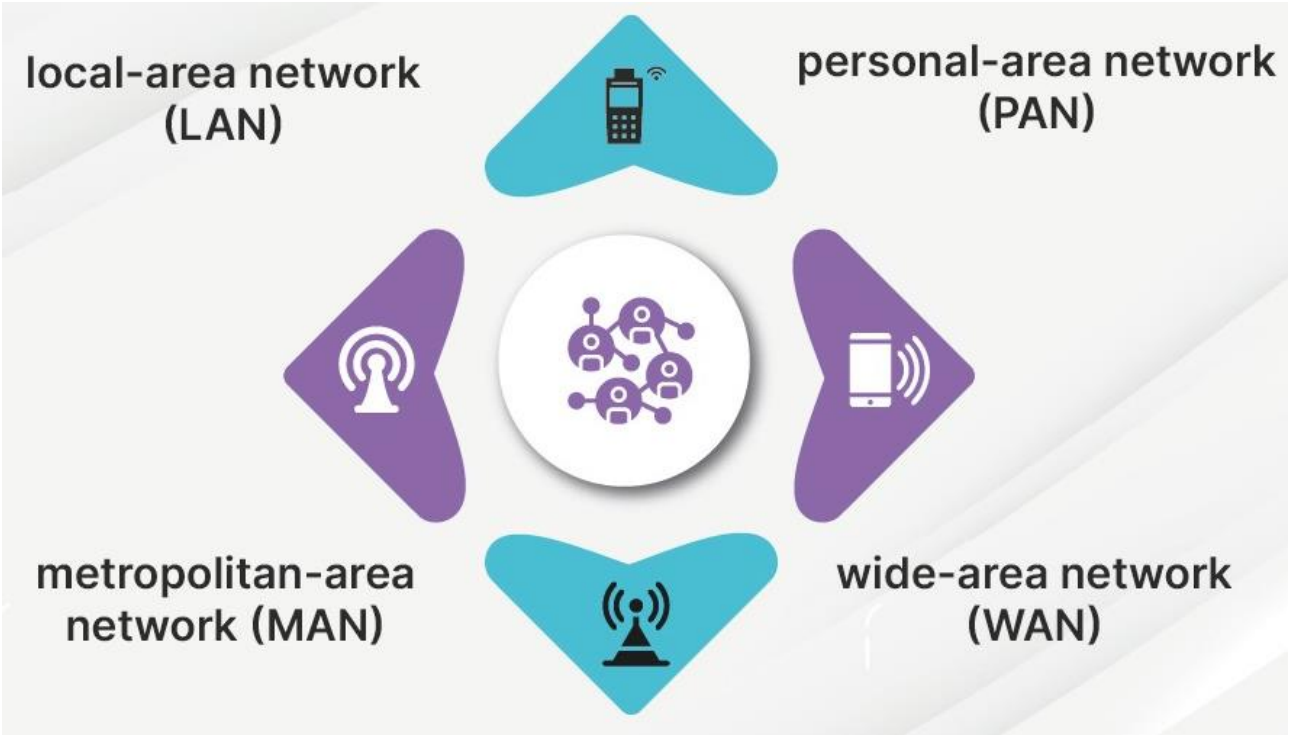

Рисунок 1.1 – Типи безпроводових мереж

Локальна мережа (LAN) – це комп’ютерна мережа, яка існує на одному місці, наприклад в офісній будівлі. LAN можна використовувати для підключення різноманітних компонентів, таких як комп’ютери, принтери та пристрої зберігання даних. Локальні мережі складаються з таких компонентів, як комутатори, точки доступу, маршрутизатори, брандмауери тощо. Wi-Fi є найпоширенішою безпроводовою локальною мережею.

Персональна мережа (PAN) складається з мережі, зосередженої навколо пристроїв однієї особи в одному місці. PAN може мати комп’ютери, телефони, ігрові приставки чи інші периферійні пристрої. Вони часто зустрічаються в будинках і невеликих офісних будівлях. Bluetooth є найпоширенішим безпроводовим PAN [3].

Міська мережа (MAN) – це комп’ютерна мережа, яка охоплює місто або невелику географічну територію. Однією з особливостей, яка відрізняє MAN від LAN, є розмір. Локальна мережа зазвичай складається з окремої будівлі або території. MAN може покривати кілька квадратних кілометрів, залежно від потреб мережі.

Глобальна мережа (WAN) охоплює дуже велику територію, наприклад цілий регіон або країну. Глобальна мережа може містити менші мережі, включаючи LAN або MAN. Послуги стільникового мобільного зв’язку є найпоширенішими безпроводовими глобальними мережами.

Основними компонентами, що складають топологію безпроводової мережі: є клієнти та точки доступа.

Пристрої кінцевого користувача зазвичай називають клієнтами. Оскільки охоплення Wi-Fi розширилося, різноманітні пристрої можуть використовувати Wi-Fi для підключення до мережі, включаючи телефони, планшети, ноутбуки, настільні комп’ютери тощо. Це дає користувачам можливість мобільності у мережі.

Точка доступу (AP) – це центральний пристрій безпроводової мережі, який використовують для з'єднання між безпроводовими клієнтами (пристроями), а також для з'єднання проводової та безпроводової частин мережі.

Схема функціонування безпроводової мережі на прикладі Wi-Fi мережі наведено на рис. 1.2. Принцип роботи безпроводової мережі базується на використанні радіохвиль. Зазвичай схема безпроводової мережі містить щонайменше одну точку доступу і щонайменше одного клієнта. Також можливе підключення двох клієнтів, коли точка доступу не використовується, а клієнти з’єднуються за допомогою мережних адаптерів безпосередньо. Адаптери на кожному комп’ютері перетворюють цифрові дані на радіосигнали, які передаються на інші мережні пристрої, також вони перетворюють вхідні радіосигнали від зовнішніх мережевих пристроїв на цифрові дані.

Радіопередавачі та приймачі однієї Wi-Fi-мережі працюють на тих самих частотах і використовують один і той же вид модуляції даних в радіохвилі [4].

Рисунок 1.2 – Схема функціонування безпроводової мережі Wi-Fi

Клієнтський пристрій отримує маяк, переданий точкою доступу, і перетворює радіочастотний сигнал у цифрові дані, після чого ці дані передаються на пристрій для інтерпретації. Якщо користувач хоче підключитися до мережі, він може надсилати повідомлення до точки доступу, намагаючись приєднатися та надати відповідні облікові дані, щоб підтвердити, що він має право приєднатися. Ці процеси відомі як асоціація та

автентифікація. Якщо будь-яке з них не вдасться, пристрій не приєднається до мережі та не зможе надалі спілкуватися з точкою доступу [3].

Дані від клієнта або від точки доступу до клієнта перетворюються з цифрових даних у радіочастотний модульований сигнал і передаються по повітрю. При отриманні вони демодулюються, перетворюються назад на цифрові дані, а потім пересилаються до місця призначення (часто в інтернет або на ресурс у більшій внутрішній мережі).

Зв’язок Wi-Fi схвалений лише для передачі на певних частотах, у більшості країн світу це частотні діапазони 2,4 ГГц і 5 ГГц, хоча зараз багато країн також додають частоти 6 ГГц [3]. Ці діапазони частот відрізняються від тих, які використовують стільникові мобільні мережі, тому стільникові телефони та Wi-Fi не конкурують за використання однакових частот. Але є без проводові технології, які працюють у діапазоні 2,4 ГГц (наприклад, Bluetooth, ZigBee, безпроводові клавіатури, аудіо/відео обладнання), вони використовують ті самі частоти і це може спричиняти перешкоди.

1.2 Переваги та недоліки безпроводових мереж

Безпроводові мережі можуть виконувати всі ті завдання, що і проводові, але при цьому також забезпечувати мобільність користувачів мережі, що на сьогоднішній момент є найважливішою вимогою сучасних користувачів.

Окрім мобільності, безпроводовий зв’язок також пропонує гнучкість і простоту використання, що робить його з кожним днем все більш популярним. Безпроводовий зв'язок, такий як мобільна телефонія, може здійснюватися будь-де та будь-коли зі значною пропускною здатністю [5].

Важливою перевагою також є інфраструктура. Налагодження та встановлення інфраструктури проводових систем зв’язку – дорога та трудомістка робота. Інфраструктуру для безпроводового зв'язку можна встановити легко та дешево [5]. У надзвичайних ситуаціях і віддалених місцях,

де важко або неможливо налаштувати проводовий зв’язок, без проводові мережі можуть бути єдиним можливим варіантом організації зв’язку.

Основні переваги та недоліки безпроводових мереж наведено на рис. 1.3.

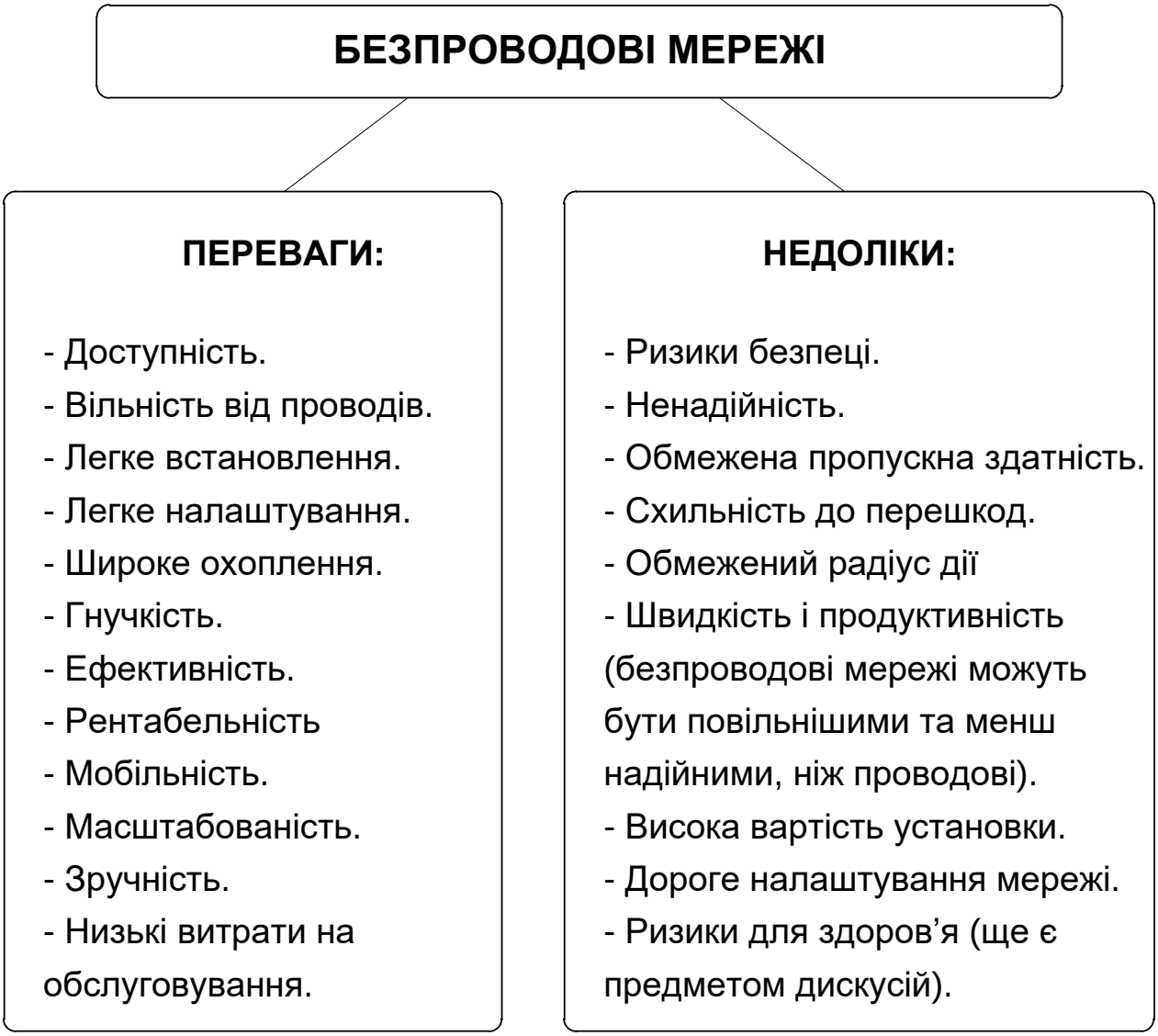

Рисунок 1.3 – Переваги та недоліки безпроводових мереж

Таким чином, технології безпроводового зв’язку, безпроводові мережі та безпроводові системи мають численні переваги перед проводовим зв’язком, такі як вартість, мобільність, простота встановлення та надійність тощо.

Незважаючи на те, що безпроводові мережі мають ряд переваг перед проводовими, вони також мають деякі недоліки. Однією з головних проблем

безпроводових мереж є безпека даних. Оскільки сигнали передаються у відкритому просторі, то є ймовірність перехоплення зловмисниками інформації, що передається, можливі перехоплення сигналів, доступ до конфіденційних даних тощо. Саме тому основна увага в цій роботі приділена питанням безпеки та засобам захисту безпроводових мереж.

1.3 Порівняльний аналіз сучасних безпроводових технологій

Найкращі безпроводові технології, які формують майбутнє зв'язку та передачі даних наведені на рис. 1.4. Вони пропонують зручність, гнучкість, ефективність і безпеку як для користувачів, так і для компаній [6]. В табл. 1.1 представлено порівняльний аналіз найбільш сучасних безпроводових технологій.

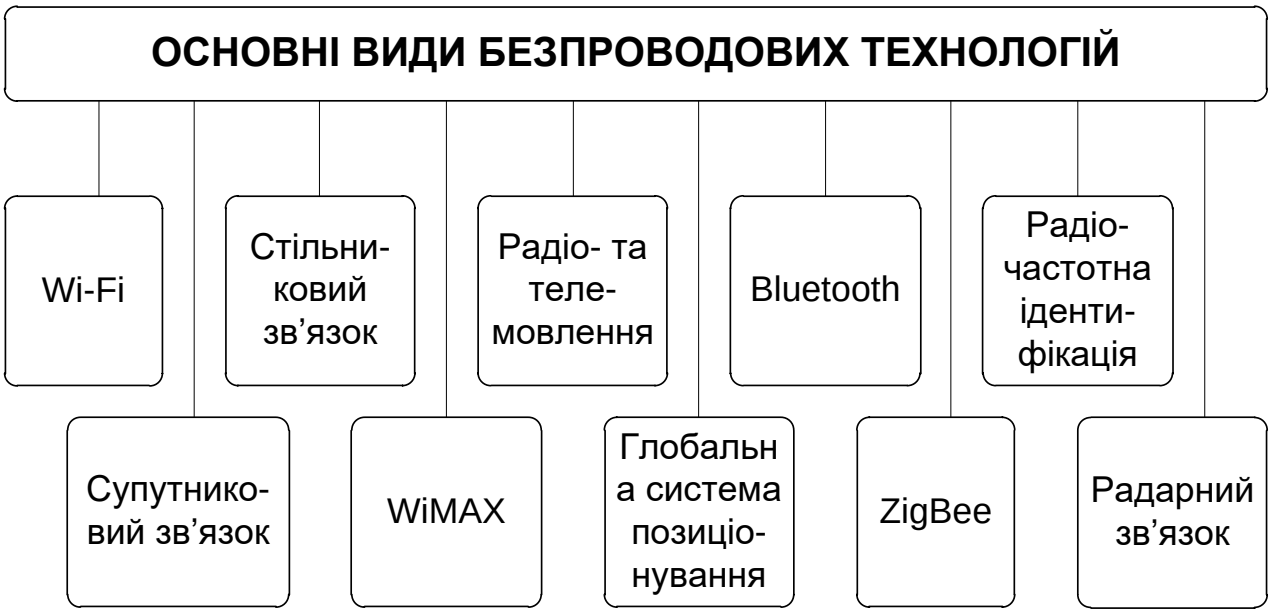

Рисунок 1.4 – Види безпроводових технологій

Таблиця 1.1 – Переваги та недоліки безпроводових технологій

Безпроводова технологія	Переваги	Недоліки
Стільникові мобільні мережі (3G/4G/5G)	– Широка доступність (доступний практично з будь-якої точки світу). – Висока швидкість передачі даних, особливо в 4G і 5G. – Надійніше, ніж мережі Wi-Fi, оскільки на них не впливають перешкоди від інших пристроїв. – Широкий спектр послуг.	– Висока вартість. – Повільність в районах із поганим покриттям. – Вплив погодних умов. – Менш безпечні, ніж проводові мережі, оскільки вони більш вразливі до злому.
Wi-Fi	– Зручність підключення.. – Мобільність (дозволяє користувачам підключатися в безпосередній близькості до роутера). – Високошвидкісний доступ до Інтернету. – Низька вартість розгортання. – Легке налаштування та можливість розширення.	– Питання безпеки. – Висока затримка. – Деякі тарифні плани Wi-Fi можуть мати обмеження щодо передачі даних.
Zigbee	– Радіус дії до 100 метрів і підтримка до 65 000 пристроїв в одній мережі [6]. – Низьке енергоспоживання і може працювати від батарейок роками.	– Сприйнятливість до мережевих перешкод через шум і переповненість каналу.

Продовження таблиці 1.1.

Безпроводова технологія	Переваги	Недоліки
LPWAN	– Зменшення витрат на технічне обслуговування: трансивери LPWAN можуть працювати від маленьких недорогих батарей протягом 10–15 років [6]. – Спрощені, легкі протоколи LPWAN зменшують складність апаратного забезпечення та знижують вартість пристрою. – Використання моделі передплати дозволяє апаратному забезпеченню бути дешевим, тоді як річна передплата стягується за кожен пристрій, підключений до роботи.	– Низькі швидкості передачі даних не можна використовувати для високих швидкостей передачі даних. – Пропонує високу затримку між наскрізними вузлами.
Супутнико-вий зв'язок	– Глобальне покриття та надійність. – Може досягати областей, які традиційна наземна інфраструктура не може. – Основний інструмент для віддалених місць, боротьби зі стихійними лихами та міжнародного зв’язку. - Широкий спектр послуг.	– Високі витрати. – Висока затримка. – Деякі супутникові плани також мають обмеження щодо даних.

Продовження таблиці 1.1

Безпроводова технологія	Переваги	Недоліки
mmWave	– Висока роздільна здатність і точність: радар mmWave може забезпечити високу роздільну здатність і точність виявлення об’єктів і їх характеристик. – Міцність і надійність: радар mmWave міцний і надійний за різних погодних умов і умов освітлення. – Значні покращення продуктивності мережі: mmWave 5G може забезпечити вищу швидкість передачі даних, вищу пропускну здатність і різке скорочення затримки мережі порівняно з мережами на частоті нижче 6 ГГц, а також мережами 4G LTE і LTE Advanced [6].	– Вартість і складність: технологія mmWave може бути дорогою та складною. – Обмеження зони покриття та радіусу дії: електромагнітні хвилі з вищими частотами не можуть поширюватися на великі відстані та є більш чутливими до фізичних перешкод.
Bluetooth	– Забезпечує безперервний зв'язок у двох напрямках. – Може виконувати передачу даних зі швидкістю 1-3 МБ [6]. – Підтримує голос.	– Високе енергоспоживання. – Обмежений діапазон до 10 метрів.

Продовження таблиці 1.1

Безпроводова технологія	Переваги	Недоліки
LoRaWAN	– Доступний у всьому світі. – Широкий діапазон покриття: 5 км в міській місцевості і 15 км в приміській зоні [6]. – Менша потужність і, отже, батареї вистачить на більший термін служби. – Один пристрій LoRa Gateway може обслуговувати тисячі кінцевих пристроїв.	– Швидкість передачі даних нижча, ніж у Wi-Fi або стільникових мережах. – Обмежена кількість каналів, доступних для передачі.
Radio Frequency (RF)	– ПД на великі відстані без використання проводів. – Може пробивати стіни та інші перешкоди. – Можна використовувати в інших засобах безпроводового зв’язку, пультах дистанційного керування та RFID.	– Під впливом перешкод від інших пристроїв. – Впливають такі фактори навколишнього середовища, як погодні умови. – Висока вартість.
Bluetooth Low Energy (BLE)	– Низьке енергоспоживання і, отже, час автономної роботи може бути дуже довгим. – Менша потужність, ніж традиційні пристрої Bluetooth, і мають більший радіус дії. – Можна використовувати для ПД невеликого розміру.	– Спілкується лише короткими пакетами, а деякі з’єднання BLE йдуть лише в одному напрямку. – Швидкість передачі даних обмежена 125-2 МБ [6]. – Не підтримує голос.

Продовження таблиці 1.1

Безпроводова технологія	Переваги	Недоліки
RFID	– Підвищення ефективності і зменшення витрат. – Автоматизація збору і відстеження даних. – Можна читати на відстані без прямої видимості. – Мітки RFID можна використовувати для відстеження предметів.	– Дорожче, ніж зчитувачі штрих-кодів. – Реалізація може бути важкою та довготривалою. – Створюють загрозу безпеці.
Трансляція радіо (Broadcast radio)	– Безкоштовність та вільний доступ. – Можна слухати під час виконання іншої діяльності. – Можна використовувати для швидкого й легкого охоплення великої аудиторії. – Можна використовувати для надання місцевих новин.	– На нього можуть впливати перешкоди від інших електронних пристроїв. – Низька популярність. – Обмежений обсяг інформації, яку можна передати порівняно з іншими формами медіа.
Infrared (інфрачер-воний зв’язок)	– Може використовуватися для виявлення змін температури в об'єктах без контакту з ними. – Може використовуватися для виявлення руху об’єктів. – Може використовуватися для безпроводової передачі даних на короткі відстані.	– Не проходить крізь тверді предмети, що обмежує радіус дії та ефективність. – Вплив перешкод від інших електропристроїв, що призводить до проблем із якістю сигналу.

Порівняння безпроводових технологій за такими критеріями, як діапазон частот, діапазон дії, швидкість ПД, безпека тощо, наведено в табл. 1.2.

Таблиця 1.2 – Порівняння безпроводових технологій

Технологія	Діапазон частот	Діапазон дії	Швидкість ПД	Споживання енергії	Втручання	Безпека	Застосування
3G/4G/5G	Різні бенди	до км	до Гбіт/с	Середнє - високе	Високе	Висока	Мобіл. зв'язок
Wi-Fi	2,4 ГГц, 5 ГГц	до сотень метрів	Мбіт/с – Гбіт/с	Середнє - високе	Середнє	Висока	LAN, інтернет
Zigbee	2,4 ГГц, 915 МГц	до сотень метрів	кбіт/с – Мбіт/с	Низьке	Низьке	Середня	IoT, дом.авт.
LPWAN	Різні бенди	до км	кбіт/с – Мбіт/с	Низьке - середнє	Низьке	Середня	IoT, роз.міста
Супутн. зв.	Залеж. від суп.	Глобал. покриття	кбіт/с – Гбіт/с	Високе	Низьке - середнє	Висока	Суп.тел., GPS
mmWave	30ГГц – 300ГГц	Близької дії	Кілька Гбіт/с	Високе	Високе	Висока	Мережі 5G, VR
Bluetooth	2,4 ГГц	до десят. метрів	Мбіт/с	Низьке	Середнє	Середня	Аудіо, перефер.
BLE	2,4 ГГц	до сотень метрів	кбіт/с – Мбіт/с	Низьке	Середнє	Середня	IoT, нос.прис
LoRaWAN	Суб-ГГц	Кілька км	кбіт/с – Мбіт/с	Низьке	Низьке	Середня	IoT, роз. сіл.госп.
RF	Різні бенди	до км	кбіт/с – Мбіт/с	Низьке - середнє	Середнє	Низька - висока	Пульти, датчики
RFID	НЧ, ВЧ, УВЧ	до кільк. метрів	кбіт/с – Мбіт/с	Низьке	Низьке - середнє	Низька - середня	Контрол. доступу
Радіо (BR)	Різні бенди	Регіон. – глобал.	кбіт/с – Мбіт/с	Низьке - середнє	Високе	Низька - середня	AM/FM радіо
Infrared	ІЧ спектр	Кілька метрів	кбіт/с – Мбіт/с	Низьке	Середнє	Середня	Пульти, ПД

Сучасні стільникові мережі (3G, 4G і 5G) – це найважливіші безпроводові технології, які забезпечують мобільний зв’язок у великих географічних зонах.

Wi-Fi – це технологія безпроводової мережі, яка використовує радіохвилі для забезпечення безпроводового високошвидкісного інтернету та мережних з’єднань.

Zigbee – це безпроводовий протокол, який використовує сітчасту мережу для підключення пристроїв на великих відстанях.

LPWAN – це глобальні мережі з низьким енергоспоживанням, призначені для додатків із невеликими повідомленнями лише кілька разів на годину, а не для додатків із великим об’ємом даних, таких як потокове передавання [6].

Супутниковий зв'язок - це спосіб передачі та отримання даних за допомогою орбітальних супутників.

Міліметрові хвилі (mmWave) – це особливий клас радіолокаційних технологій, які використовують електромагнітні хвилі короткої довжини. Вловлюючи відбитий сигнал, радарна система може визначити дальність, швидкість і кут об’єктів [6].

Bluetooth використовується для зв’язку на короткій відстані між такими пристроями, як смартфони, ноутбуки та навушники.

Bluetooth Low Energy (BLE) призначений для пристроїв із низьким енергоспоживанням і зазвичай використовується в таких додатках, як переносні пристрої, розумні домашні пристрої та промислові датчики [6].

LoRaWAN – це технологія безпроводового зв’язку, розроблена для сценаріїв застосування на великій відстані та з низьким енергоспоживанням.

Радіочастотна технологія (Radio Frequency, RF) дозволяє використовувати набір частот в інших зонах, якщо зони не межують одна з одною. Кілька абонентів в одній зоні можуть використовувати одну частоту, оскільки виклики можна переключити на найближчу базову станцію з цією частотою.

RFID (радіочастотна ідентифікація) – це безпроводова технологія, яка використовує радіохвилі для зчитування та захоплення інформації, що зберігається на тегах, прикріплених до об’єктів.

Трансляція радіо – це технологія безпроводового зв’язку, яка використовує радіохвилі для передачі аудіовмісту великій кількості слухачів.

Infrared (інфрачервоний зв’язок) – це безпроводова технологія, яка використовує інфрачервоне світло для передачі даних між пристроями.

1.4 Стандарти технології Wi-Fi

Одними з найбільш популярних безпроводових мереж є мережі побудовані на основі технології Wi-Fi. Стандарт мережі, який використовується безпроводовою архітектурою Wi-Fi, є IEEE 802.11. Однак цей стандарт постійно вдосконалюється, і регулярно з’являються нові поправки. Поправки до стандарту позначаються літерами, і хоча було опубліковано багато поправок, найвідоміші з них: 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax (Wi-Fi 6 та 6E). Порівняння стандартів за різними характеристиками наведено в табл. 1.3.

802.11a – це оригінальна поправка 802.11, що додала підтримку діапазону 5 ГГц, дозволяючи передавати до 54 мегабіт даних на секунду. Стандарт 802.11a використовує мультиплексування з ортогональним частотним поділом (OFDM). Він розбиває радіосигнал на підсигнали, перш ніж вони потраплять до приймача[3].

802.11b додав вищі швидкості в діапазоні 2,4 ГГц до оригінального стандарту. Він може передавати до 11 мегабіт даних за секунду. Він використовує модуляцію додаткового коду (CCK) для досягнення кращої швидкості.

802.11g стандартизував використання технології OFDM, яка використовується в 802.11a в діапазоні 2,4 ГГц. Він був зворотно сумісний із 802.11 і 802.11b.

802.11n – це колись найпопулярніший стандарт, він був першим, коли єдина специфікація охоплювала діапазони 2,4 ГГц і 5 ГГц. Цей протокол забезпечує кращу швидкість у порівнянні з попередніми протоколами,

використовуючи ідею передачі за допомогою кількох антен одночасно (технологія Multiple In Multiple Out, MIMO).

Таблиця 1.3 – Порівняння стандартів Wi-Fi

Стандарт	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Рік ратиф.	1997	1999	1999	2003	2009	2014	2017-2019
Робоча частота	2,4 ГГц	2,4 ГГц	5 ГГц	2,4 ГГц	2,4/5 ГГц	5 ГГц	2,4/5 ГГц
Частотні канали	20 МГц	20 МГц	20 МГц	20 МГц	20/40 МГц	20/40/80/160 МГц	20/40/80/160 МГц
Пікова фізична швидкість	2 Мбіт/с	11 Мбіт/с	54 Мбіт/с	54 Мбіт/с	600 Мбіт/с	6,8 Гбіт/с	10 Гбіт/с
Макс. кільк. SU портів	1	1	1	1	4	8	8
Макс. кільк. MU портів	NA	NA	NA	NA	NA	4	8
Модуляція	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM/OFDMA
Макс.тип та швидкість кодування	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Макс. кільк. тонів OFDM	NA	NA	64	64	128	512	2048
Рознесення субтонів	NA	NA	312,5 кГц	312,5 кГц	312,5 кГц	312,5 кГц	78,125 кГц

802.11ac був визначений лише для діапазону 5 ГГц. Він побудований на основі механізмів, представлених у 802.11n. Хоча він не був таким революційним, як 802.11n, він все ж розширив швидкість і можливості в діапазоні 5 ГГц. Більшість пристроїв, які зараз доступні, є, швидше за все, 802.11ac. Технологія 802.11ac була представлена у двох основних групах,

основна відмінність полягає в тому, що пристрої Wave 2 мають трохи більше технічних можливостей порівняно з Wave 1, але всі вони сумісні.

802.11ax (подібно до 802.11n) уніфікував специфікацію для всіх застосовних діапазонів частот. Його також називають Wi-Fi 6. Wi-Fi 6 розширив технології, що використовуються для модуляції, включивши OFDMA, що дозволяє певну кількість паралелізму для передачі пакетів у системі, ефективніше використовуючи доступний спектр і покращуючи загальну пропускну здатність мережі. Wi-Fi 6 – це сучасна технологія, з якою постачається більшість нових пристроїв [3].

Протягом багатьох років до стандартів було внесено ще багато поправок. Додаткові стандарти 802.11 зосереджені на таких речах, як краща безпека, підвищена якість обслуговування, а також багато інших покращень.

1.5 Аналіз основних тенденцій розвитку безпроводових технологій

В робот було виконано аналіз джерел інформації [7 – 10] щодо перспектив розвитку безпроводових технологій. В результаті цього аналізу було визначено основні тенденції та перспективи розвитку безпроводових технологій в світі на 2024 рік.

Основні десять тенденцій розвитку безпроводових технологій наведено на рис. 1.5.

Сфера безпроводових технологій значно розвинулася. На початку 2024 року багато нових ідей змінять світ безпроводових технологій [7]. Розширення мереж 5G і 6G для більшого використання Wi-Fi 6 і підключення до пристроїв IoT вже на горизонті. Тенденції розвитку безпроводових технологій революціонізують комунікацію людей та їх взаємодію зі світом. Ці тенденції виникають через потребу в гнучкості у задоволенні вимог ринку, проблеми безпеки даних і зростаючий вплив Інтернету речей (IoT) і штучного інтелекту (ШІ) [7].

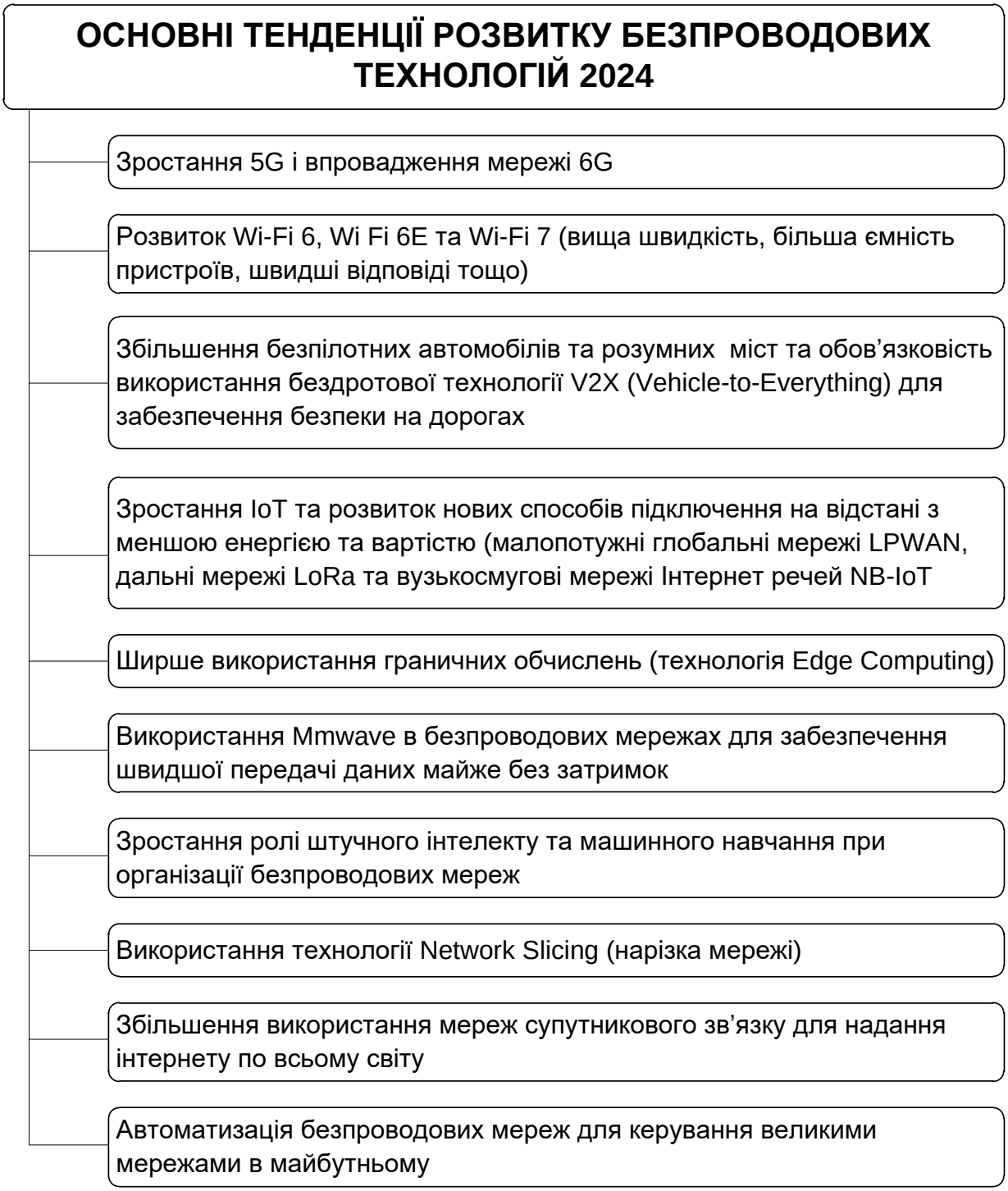

Рисунок 1.5 – Основні тенденції розвитку безпроводових технологій

Зростання 5G і впровадження мережі 6G є основними майбутніми тенденціями в безпроводових технологіях. 5G, надшвидкісний Інтернет із кращим з'єднанням, вже є популярним. Він може доповнити Wi-Fi, особливо у великих місцях, таких як аеропорти та заводи, де потрібні швидкі з'єднання для передачі даних. У 2023 році багато компаній інвестували у нього, що дає йому

поштовх у всьому світі. Для повного розкриття можливостей 5G знадобиться від 5 до 8 років [7].

Розгортання оптоволоконного широкосмугового зв'язку продовжуватиме розширюватися на більшості розвинених ринків і ринків, що розвиваються, створюючи потребу в модернізації домашніх мереж Wi-Fi для передачі збільшеної пропускної здатності на пристрої, що сприятиме швидкому впровадженню Wi-Fi 6E і Wi-Fi 7. Швидке впровадження Wi-Fi 6E/7 також буде зумовлене його можливістю доступу до додаткового спектру в діапазоні 6 ГГц, оскільки все більше країн відкривають цей діапазон [8].

Неможливо переоцінити роль штучного інтелекту та машинного навчання, адже адаптивний штучний інтелект швидко розвивається в мережах, від увімкнення автоматичної координації частот (AFC) до прогнозування потреб у ресурсах мережі. ШІ допоможе підприємствам і провайдерам прискорити пошук несправностей; упорядкувати моніторинг; і завчасно передбачити збої, збої обладнання та зниження продуктивності.

Інтернет речей (IoT) стрімко розвивався протягом багатьох років, і очікується, що ця тенденція збережеться. У результаті з'явилися різноманітні рішення для підключення IoT, такі як глобальні мережі з низьким енергоспоживанням (LPWAN), вузькосмугові IoT (NB-IoT) і мережі великого радіусу дії (LoRa). Ці технології дають змогу створювати економічно ефективні рішення великої радіусу дії, з низьким енергоспоживанням для підключення великої кількості пристроїв IoT [9].

Таким чином, розвиток безпроводових технологій виходить за межі лише технологічного прогресу; сучасні тенденції символізують нову еру комунікацій, відзначену ефективністю, безпекою та неперевершеним досвідом користувачів. Бути в курсі цих тенденцій і сприймати майбутні зміни буде вкрай важливо як для компаній, так і для окремих користувачів. Наступне десятиліття обіцяє більш динамічний, взаємопов'язаний та інноваційний розвиток безпроводових технологій, ніж будь-коли раніше.

2 ДЖЕРЕЛА ЗАГРОЗ ІНФОРМАЦІЇ В БЕЗПРОВОДОВИХ МЕРЕЖАХ

Відповідно до Закону України «Про електронні комунікації» безпека мереж визначається наступним чином: безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги [11].

Для організації безпеки безпроводових мереж спочатку важливо проаналізувати можливі загрози та вразливості безпроводових мереж. Логічний ланцюг взаємодії джерела загроз та вразливості [12] наведено на рис. 2.1.

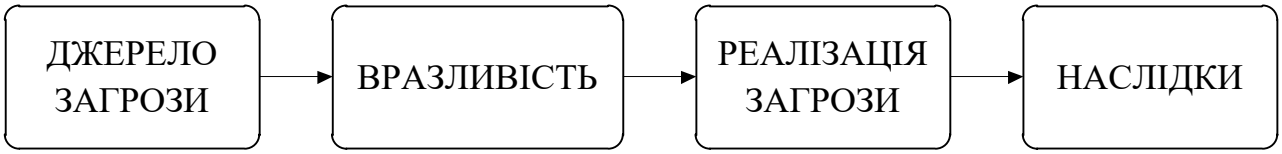

Рисунок 2.1 – Логічний ланцюг взаємодії джерела загроз та вразливості

З рис. 2.1 видно, що для забезпечення захисту та уникнення негативних наслідків необхідно ідентифікувати можливі джерела загроз, виявляти та усувати вразливості мережі, попереджати можливу реалізацію загрози, тобто застосовувати методи захисту на кожному етапі цього ланцюга.

2.1 Загрози в безпроводових мережах

Загроза безпеці це потенційно можлива подія, процес або явище, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформації [12]. Класифікація загроз представлена на рис. 2.2.

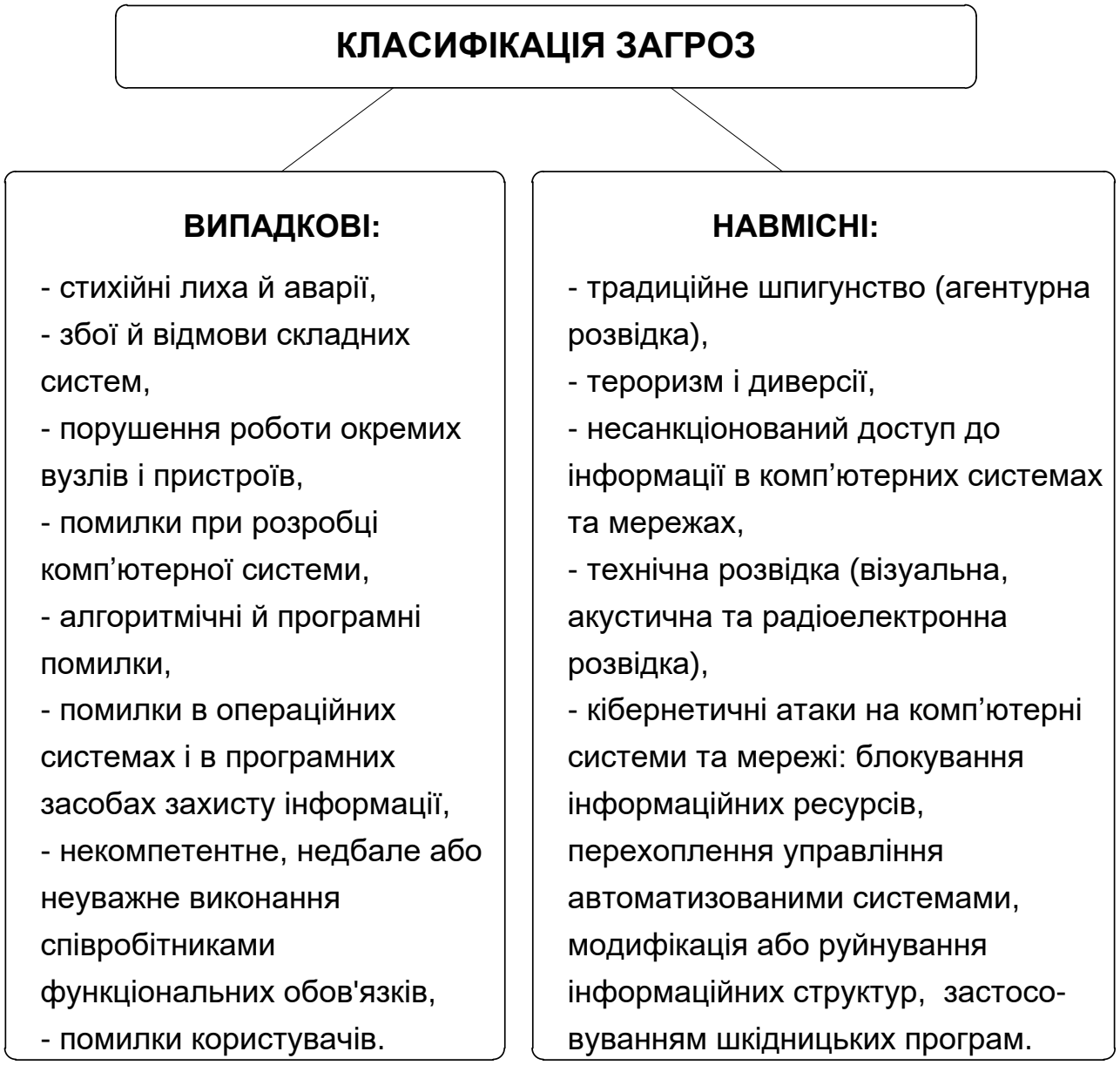

Рисунок 2.2 – Класифікація загроз

Крім класичних загроз, представлених на рис. 2.2, в безпроводових мережах існують специфічні загрози, притаманні безпроводовим мережам у зв'язку з особливостями їхньої організації та функціонування. Безпроводові мережі вразливі до широкого спектру загроз безпеці через свої властиві характеристики, такі як трансляція, відсутність фізичних кордонів і залежність від радіохвиль. Основні ризики безпеки безпроводової мережі наведено на рис. 2.3.

Рисунок 2.3 – Загрози безпроводових мереж

Серед найпоширеніших загроз у світі безпроводових мереж є неавторизований (несанкціонований) доступ, тобто зловмисники можуть скористатися незахищеними безпроводовими мережами або слабкими паролями для підключення без авторизації, що призводить до крадіжки пропускної здатності, перехоплення даних і використання вразливостей у підключених пристроях. Безпроводові мережі вразливі до несанкціонованого доступу з боку хакерів, які можуть отримати доступ до конфіденційних даних.

Для отримання доступу до безпроводових мереж зловмисники можуть встановлювати несанкціоновані точки доступу та використовувати їх для перехоплення даних або здійснення атак на інші пристрої в мережі [13].

Безпроводові сигнали можуть бути перехоплені зловмисниками, які потім можуть підслуховувати конфіденційну інформацію, що передається через мережу.

Безпроводові мережі можуть піддаватися атакам DoS (атаки на відмову в обслуговуванні), які переповнюють мережу трафіком і перешкоджають законним користувачам отримати доступ до мережі.

Зловмисники можуть використовувати шкідливе програмне забезпечення для зараження безпроводових пристроїв. Це може поставити під загрозу безпеку мережі та призвести до крадіжки конфіденційних даних і компрометації мережних ресурсів.

Атаки MITM (атаки «людина-в-середині») передбачають перехоплення зловмисниками спілкування між двома сторонами та потенційну зміну вмісту спілкування. У безпроводових мережах атаки MITM можуть здійснюватися зловмисниками, які перебувають у зоні дії мережі [13].

Безпроводові пристрої можуть бути фізично вкрадені, або зловмисники можуть отримати фізичний доступ до пристроїв і поставити під загрозу їх безпеку.

2.2 Вразливості безпроводових мереж

Вразливості безпроводових мереж – це не тільки недоліки мереж, але і слабкі місця безпроводового з'єднання, які можуть стати причиною втрати безпеки. Вразливості безпроводових мереж можуть бути використані зловмисниками для викрадення інформації та порушення нормальної роботи мережі.

Основні вразливості безпроводових мереж наведено на рис. 2.4.

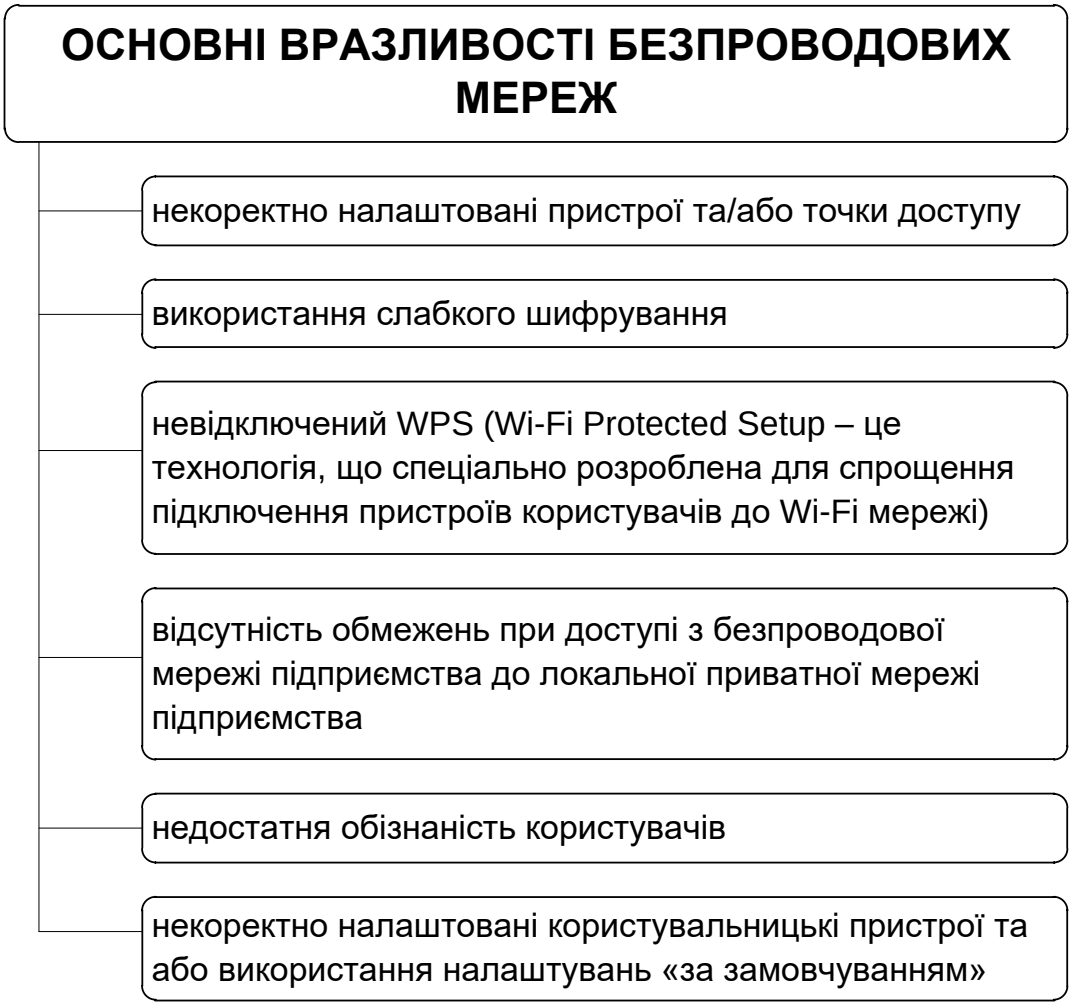

Рисунок 2.4 – Основні вразливості безпроводових мереж

Однією з найбільш відомих і небезпечних вразливостей є використання слабких або передбачуваних паролів. Багато користувачів досі використовують прості паролі [14]. Вразливим місцем також є використання застарілих протоколів безпеки. Наприклад, протокол безпеки Wired Equivalent Privacy (WEP) зараз застарів і піддається відносно простим атакам злому.

Безпроводові мережі також можуть бути вразливими через неправильне налаштування точок доступу. Це включає в себе використання налаштувань за замовчуванням, відомих зловмисникам, таких як імена мереж (SSID) або попередньо встановлені паролі, які не були змінені. Крім того, відсутність оновлення мікропрограми точки доступу може створити відомі вразливості, які виробники усувають за допомогою оновлень [14].

Потрібно розуміти, що зловмисники використовують всі можливі вразливості, які існують на апаратному, програмному та комунікаційному рівнях. Саме тому вразливості необхідно виявляти та усувати, а за неможливості усунення - обов'язково захищати. Незважаючи на всі переваги безпроводових мереж, їхні вразливості є дуже серйозними вадами. Більшість успішних зломів відбувається через використання цілого ряду існуючих вразливостей.

2.3 Новітні ризики в безпроводових мережах

З поширенням пристроїв, підключених до інтернету, перелік загроз для безпроводових мереж значно розширився. Кіберзлочинці постійно знаходять нові способи використання вразливостей і отримання несанкціонованого доступу до мереж. Наслідки можуть варіюватися від витоку даних і фінансових втрат до репутаційної шкоди для компаній і окремих осіб. Мережним адміністраторам і користувачам вкрай важливо знати про ці загрози та вживати відповідних заходів безпеки, щоб пом’якшити їх [15].

З розвитком технологій з’являються нові ризики для безпеки безпроводової мережі. Новітні ризики безпеки безпроводової мережі наведено на рис. 2.5.

Мережі 5G стають дедалі популярнішими та створюють нові ризики безпеці, зокрема підвищену вразливість до атак типу «відмова в обслуговуванні» (DoS), а також можливість для зловмисників перехоплювати та маніпулювати даними, що передаються через мережу.

Поширення пристроїв інтернету речей (IoT), таких як розумні будинки, розумні автомобілі та розумні міста, призвело до збільшення кількості безпроводових пристроїв, якими можуть скористатися зловмисники. Багато з цих пристроїв мають слабкий контроль безпеки та можуть бути легко зламані.

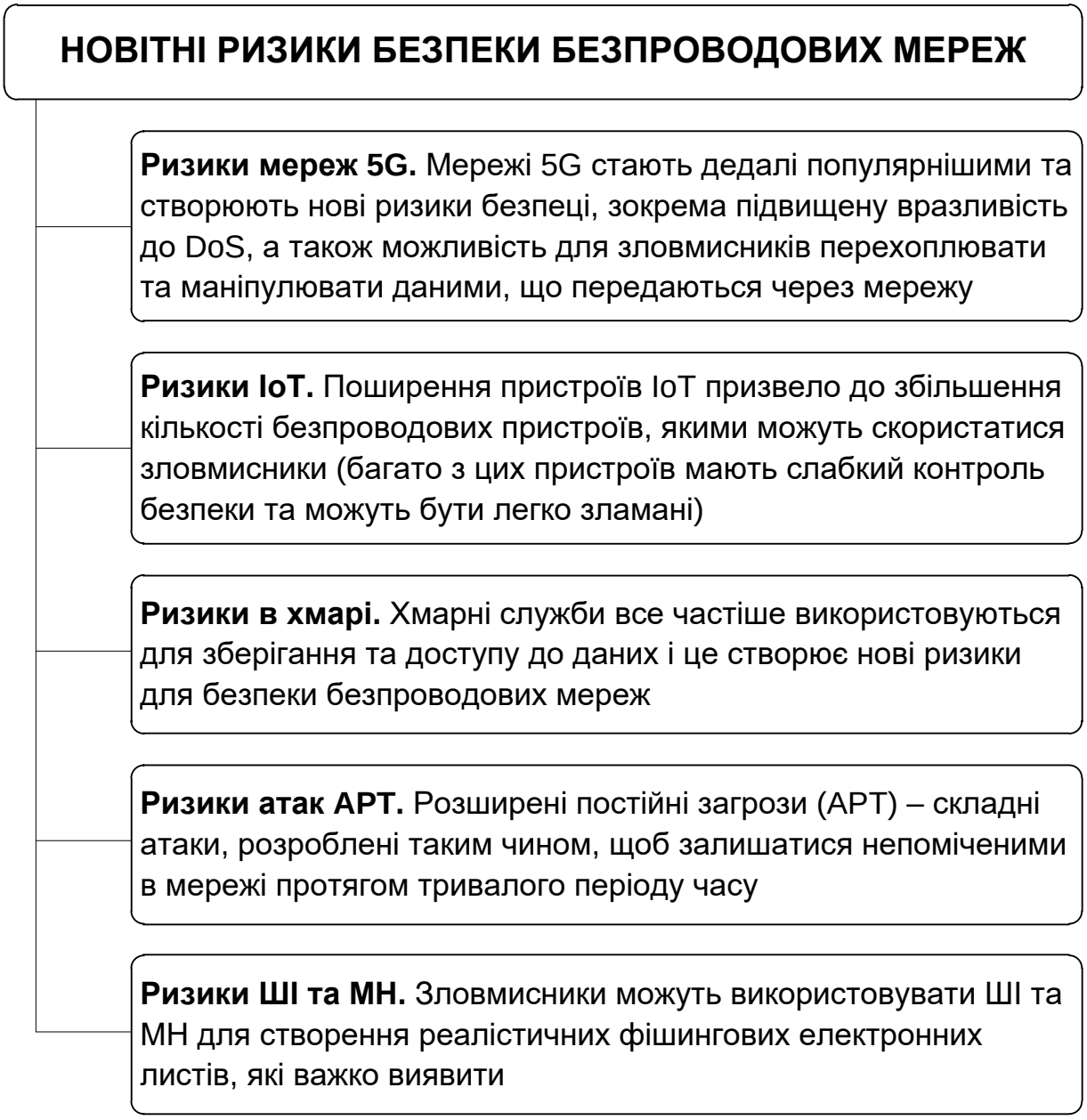

Рисунок 2.5 – Новітні ризики безпеки безпроводової мережі

Хмарні служби все частіше використовуються для зберігання та доступу до даних, і це створює нові ризики для безпеки безпроводових мереж. Зловмисники потенційно можуть отримати доступ до конфіденційних даних, що зберігаються в хмарі, і поставити під загрозу безпеку мережі.

Розширені постійні загрози (Advanced persistent threats, APT) – це складні атаки, розроблені таким чином, щоб залишатися непоміченими в мережі протягом тривалого періоду часу. APT може бути особливо важко виявити в

безпроводових мережах, де зловмисники можуть використовувати складні методи, щоб залишатися прихованими.

Штучний інтелект (ШІ) і машинне навчання (МН): ШІ і МН все частіше використовуються для покращення безпеки безпроводової мережі, але вони також можуть використовуватися зловмисниками для здійснення більш складних атак. Наприклад, зловмисники можуть використовувати ШІ та МН для створення реалістичних фішингових електронних листів, які важко виявити.

Щоб пом’якшити ці нові ризики безпеки безпроводової мережі, організації повинні бути в курсі останніх загроз безпеці та впроваджувати відповідні заходи безпеки. Це може включати використання розширених інструментів безпеки, таких як ШІ та МН, для виявлення потенційних загроз і реагування на них, а також забезпечення регулярного оновлення та виправлення всіх пристроїв і точок доступу в мережі для запобігання вразливостям.

3 ЗАСОБИ БЕЗПЕКИ БЕЗПРОВОДОВИХ МЕРЕЖ

3.1 Типи інструментів мережної безпеки

Оскільки питання безпеки мережі є одним з найважливіших, то організації та уряди повинні використовувати найбільш потужні інструменти безпеки для пом’якшення сучасних загроз та захисту різних мереж, в тому числі і безпроводових.

Інструменти мережної безпеки – це пристрої та програми, розроблені спеціально для забезпечення безпеки мережі, у якій вони знаходяться, використовуючи такі методи, як моніторинг, сповіщення та перевірка мережних з’єднань. Основні типи інструментів мережної безпеки наведено на рис. 3.1.

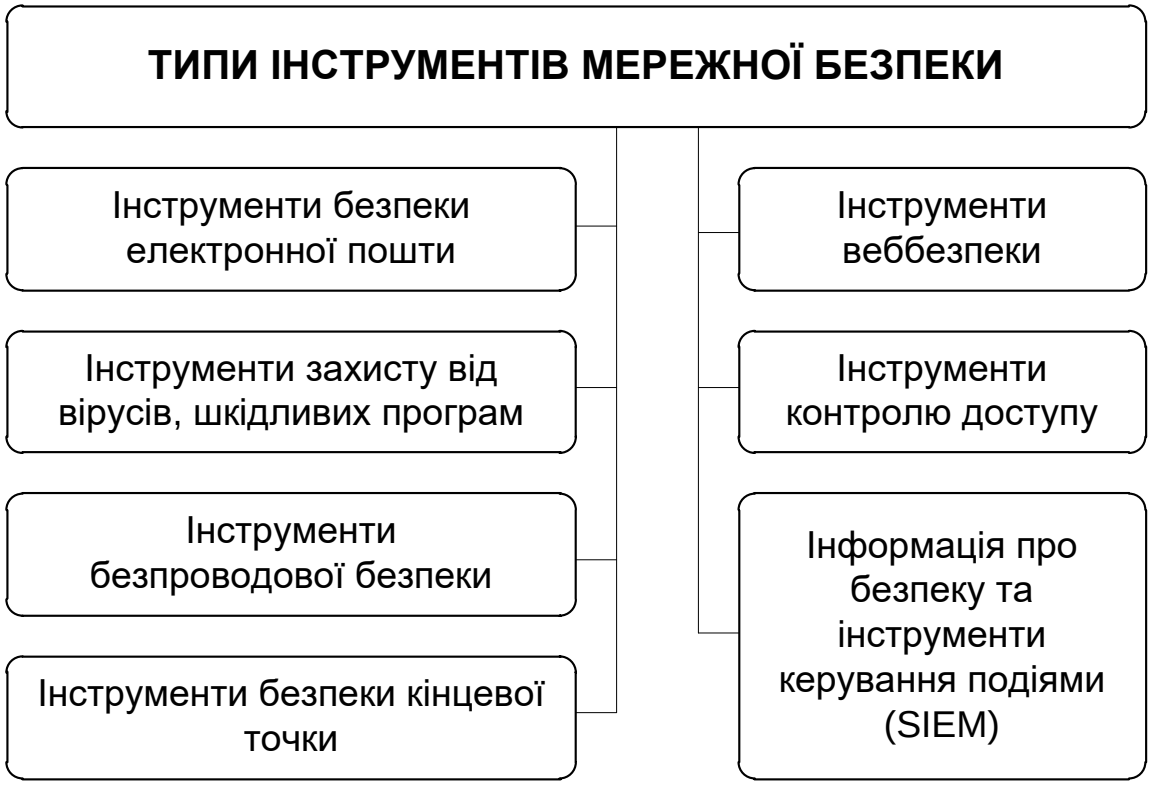

Рисунок 3.1– Типи інструментів мережної безпеки

Інструменти безпеки електронної пошти суттєво залежать від людського фактору, оскільки основні атаки на електронну пошту – це різноманітні види фішингу. Інструменти безпеки електронної пошти допомагають ідентифікувати небезпечні електронні листи, а також можуть використовуватися для блокування атак і запобігання витоку конфіденційних даних.

Інструменти захисту від вірусів, шкідливих програм (від будь-якого зловмисного програмного забезпечення) – це тип програмного забезпечення безпеки мережі, призначений для виявлення та запобігання поширенню небезпечних програм, які використовують переваги слабких систем або програмних помилок для поширення. Вони також можуть допомогти виправити зараження зловмисним програмним забезпеченням і мінімізувати шкоду мережі.

Інформація про безпеку та інструменти керування подіями (Security Information and Event Management Tools, SIEM) – це рішення, яке допомагає організаціям виявляти, аналізувати та реагувати на загрози безпеці до того, як вони вплинуть на бізнес-операції [16].

Інструменти контролю доступу є дуже важливими для будь-яких мереж. Контроль доступу інтегровано в корпоративне IT-середовище. Це може бути система керування ідентифікацією та доступом. Ці інструменти надають системи контролю доступу, бази даних користувачів і адміністративні інструменти для політики контролю доступу, аудиту та примусового виконання.

Інструменти безпеки кінцевої точки – це програмне забезпечення, призначене для відстеження, моніторингу та керування набором кінцевих пристроїв, що використовуються в мережі.

Інструменти безпроводової безпеки будуть детально розглянуті в 3.2. Безпроводові мережі не такі безпечні, як традиційні мережі. Тому необхідні суворі заходи безпеки безпроводового зв’язку, щоб запобігти доступу зловмисників.

Інструменти веббезпеки необхідні для будь-якої організації, яка має вебсервіси, оскільки поверхня атак дуже широка, коли йдеться про вебпрограми. Інструменти веббезпеки періодично сканують вебсайти, щоб з’ясувати, чи є якісь шкідливі дії чи загрози безпеці.

3.2 Методи та засоби безпеки в безпроводових мережах

Для ліквідації або мінімізації ризиків безпеки в безпроводових мережах, важливо впровадити суворі заходи безпеки, такі як використання надійних паролів, шифрування та регулярні оновлення та виправлення мережних пристроїв. Також важливо регулярно відстежувати та перевіряти мережу на наявність підозрілої активності [13].

Сьогодні існує багато засобів, що використовуються для захисту безпроводових мереж. Найбільш діючі засоби безпеки наведено на рис. 3.2.

Застосування надійних паролів для всіх безпроводових пристроїв і точок доступу є важливим засобом безпеки. Паролі мають містити принаймні 12 символів із поєднанням великих і малих літер, цифр і спеціальних символів [13].

Шифрування допомагає захистити дані, що передаються через безпроводові мережі. Це можна зробити, запровадивши спеціальні протоколи, (наприклад WPA2 або WPA3), які використовують надійне шифрування для захисту даних.

Обмеження доступу до безпроводових мереж лише авторизованим користувачам можна зробити шляхом впровадження заходів контролю доступу, наприклад, вимагаючи від користувачів автентифікації перед тим, як отримати доступ до мережі. Найбільш актуальними сьогодні є біометричні методи автентифікацію. Для суттєвого підвищення точності та надійності автентифікації можна використовувати багатофакторну (як мінімум двофакторну) або мультибіометричну автентифікацію.

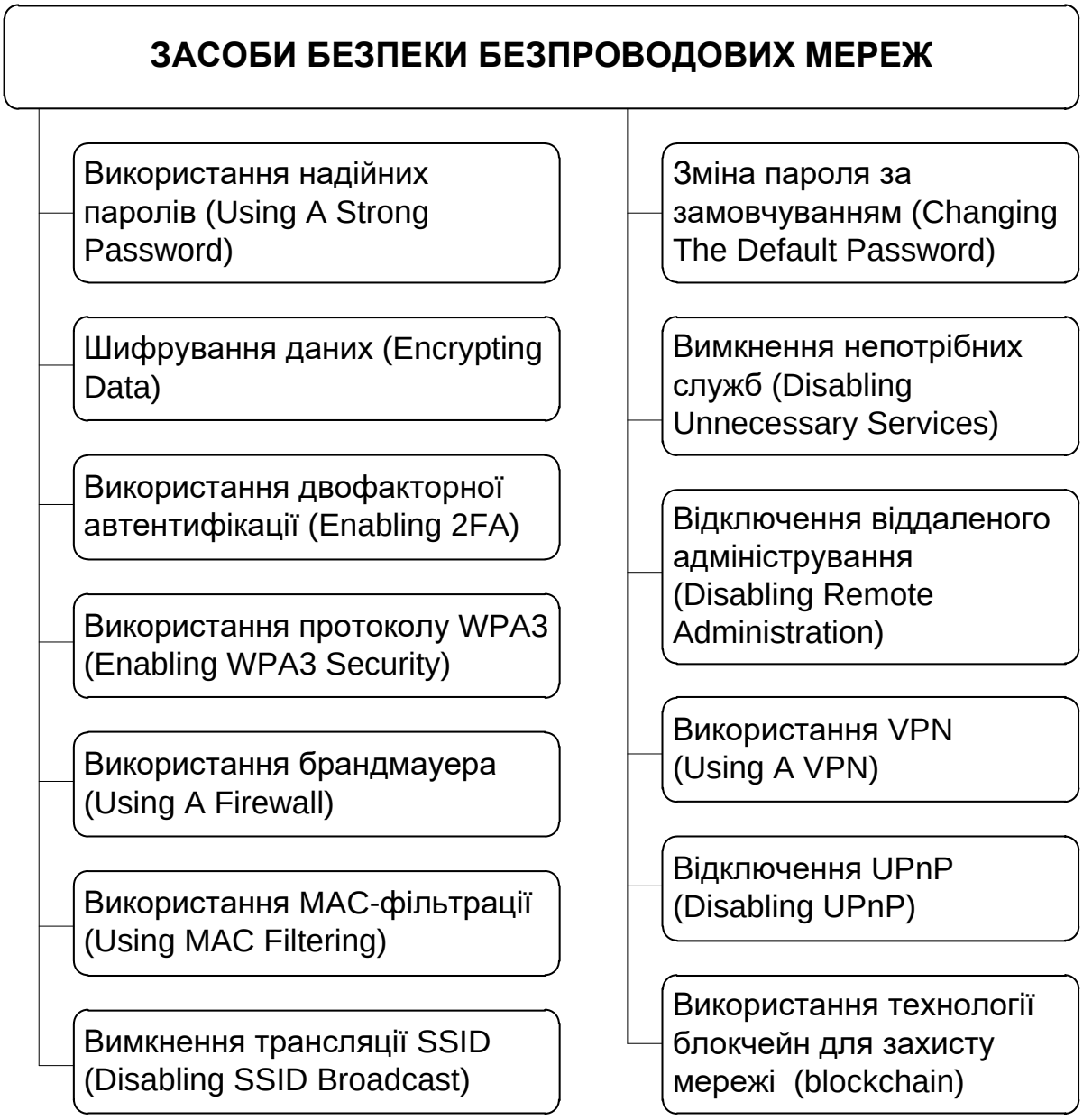

Рисунок 3.2 – Засоби безпеки безпроводової мережі

Регулярне оновлення та виправлення безпроводових пристроїв є необхідним, щоб переконатися, що вони захищені від відомих вразливостей. Це може допомогти запобігти використанню зловмисниками слабких місць у пристроях для отримання несанкціонованого доступу.

Брандмауер – це пристрій безпеки мережі (може бути програмним або апаратним), який діє як кордон між мережею та іншими мережами. Він

відстежує та фільтрує вхідний і вихідний трафік і виявляє різні атаки, наприклад сканування вразливостей [16].

Зворотний брандмауер – це тип брандмауера, який розміщується поза мережею або пристроєм і також діє як кордон між джерелом і одержувачем, його основна мета – відстежувати та очищати вихідний трафік, запобігаючи витоку важливої інформації.

Системи запобігання вторгненням IPS (Intrusion Prevention System) – це тип інструменту безпеки мережі, який постійно відстежує трафік і може вживати заходів у разі виявлення зловмисного трафіку (повідомлення, видалення тощо).

Інформація про безпеку та керування подіями (SIEM) – це рішення безпеки, яке допомагає керувати та виявляти загрози. Інструменти SIEM можуть отримувати та збирати дані журналів із кінцевих точок і різних інструментів безпеки мережі, а також аналізувати їх і створювати звіти на основі попередньо визначених правил [16].

Впровадження віртуальної приватної мережі (VPN) всередині організації – це спосіб встановити безпечне з’єднання між мережними пристроями, оскільки трафік усередині VPN зашифровано та захищено від інтернету.

Виявлення кінцевої точки та відповідь (EDR) – це своєрідне рішення безпеки та одна з найкращих технологій у виявленні загроз і реагуванні на них. EDR відстежують кінцеві точки та можуть виявляти загрози та вразливості, поєднуючи моніторинг у реальному часі та збір даних кінцевих точок із можливостями автоматичного реагування на основі правил [16].

Дієвим засобом безпеки також є моніторинг мережі фізичного розташування.

Зовнішній моніторинг мережі означає розміщення місця за межами мережі та використання його для моніторингу мережної активності. За допомогою пасивного або віддаленого моніторингу мережі зсувний моніторинг мережі можна здійснювати за допомогою простих методів, (таких як ping), щоб

перевірити, чи хости мережі активні та доступні, або за допомогою більш дієвих методів, таких як перехоплення SNMP .

Моніторинг трафіку на межі мережі означає перевірку вихідного та вхідного трафіку до та з мережі. Кінцеві точки – це фізичні пристрої, які є частиною мережі, наприклад сервери, клієнтські пристрої, мобільні телефони тощо. Моніторинг на рівні кінцевої точки означає використання інструментів на тих пристроях, з яких складається мережа.

Моніторинг в мережі звертає увагу на фактичний трафік у межах мережі, що рухається між мережними хостами та мережними пристроями. Важливо перевіряти та контролювати цей трафік.

3.3 Протоколи безпеки

Протоколи безпеки (або протоколи шифрування) відіграють важливу роль у безпеці безпроводової мережі, забезпечуючи конфіденційність і цілісність даних, що передаються через безпроводові мережі. Доступні різні протоколи шифрування: протоколи захищеного доступу (WPA), протокол безпеки транспортного рівня (TLS), протокол захищених сокетів (SSL), протокол віртуального з’єднання (VPN) [17].

Протоколи захищеного доступу до Wi-Fi (різні версії WPA) забезпечують шифрування для мереж Wi-Fi, пропонуючи захист від несанкціонованого доступу та перехоплення даних.

Протоколи TLS (безпека транспортного рівня) і SSL (рівень захищених сокетів) зазвичай використовуються для захисту безпроводового зв'язку через інтернет, наприклад онлайн-транзакцій або електронної пошти.

Протокол віртуального з’єднання VPN (віртуальна приватна мережа) встановлює безпечні з'єднання між віддаленими користувачами та корпоративними мережами, шифруючи передачу даних і забезпечуючи безпечний доступ до ресурсів [17].

Для забезпечення додаткового рівня захисту використовується шифрування будь-якої інформації, яка передається між точками доступу і безпроводовими пристроями. Це запобігає перегляду неавторизованими користувачами, навіть якщо їм вдасться отримати доступ до мережі.

Протоколи шифрування Wi-Fi, які були розроблені для захисту даних, що надсилаються через безпроводові мережі представлені в табл. 3.1.

Таблиця 3.1 – Протоколи шифрування Wi-Fi

Протокол	Повна назва	Поява	Особливості
WEP	Wired Equivalent Privacy	1999	Конфіденційність, еквівалентна проводовій мережі. Легко зламати. Важко налаштувати. Сьогодні вважається не надійним способом гарантування безпеки.
WPA	Wi-Fi Protected Access	2003	Захищений доступ Wi-Fi. Тимчасове розширення для WEP. Використо-вуються ключі для шифрування довжиною до 128 біт (технологія TKIP). Легко зламати. Конфігурація: помірна.
WPA2	Wi-Fi Protected Access Version 2	2004	Допрацьована і більш надійна версія WPA. Використовуються ключі для шифрування довжиною до 256 біт (технологія AES).
WPA3	Wi-Fi Protected Access Version 3	2018	Захист паролем. Безпечний початковий обмін ключами в особистому режимі і секретність пересилання (технологія SAE). Просте підключення Wi-Fi.

Wired Equivalent Privacy (WEP) – цей стандарт використовувався з 1994 по 2004 рік, зараз використовується лише дуже старими маршрутизаторами.

Він має багато відомих проблем безпеки, що робить його дуже вразливим до кібератак. Сьогодні дуже важливо уникати використання WEP через його вразливість до атак.

Протокол WPA – це тимчасове вдосконалення для WEP, поки стандарт безпроводової безпеки 802.11i ще перебував у розробці. Його легше налаштувати, ніж WEP, але все одно легко зламати.

Протокол WPA2 – це протокол на основі стандарту безпроводової безпеки 802.11i. На відміну від WPA, який використовує протокол цілісності тимчасового ключа (TKIP), WPA2 використовує розширений стандарт шифрування (AES), схвалений урядом США для шифрування надсекретної інформації [18].

WPA2 залишається безпечним вибором для багатьох мереж. Він забезпечує баланс між безпекою та сумісністю, що робить його придатним варіантом для середовищ із поєднанням старих і новіших пристроїв.

Протокол WPA3 було представлено в 2018 році, щоб усунути недоліки WPA2 і спростити підключення. На відміну від WPA2, WPA3 робить обов’язковим використання захищених кадрів керування (PMF). Він також замінює протокол обміну Pre-Shared Key (PSK) WPA2 на більш безпечну одночасну автентифікацію рівних (SAE) [18].

Впровадження шифрування WPA3 встановило новий стандарт безпеки безпроводового зв’язку. Він забезпечує надійний захист від атак грубої сили та пропонує більш безпечні методи автентифікації.

Стандарт WPA3 передбачає два режими роботи: WPA3-Personal і WPA3-Enterprise. WPA3-Personal забезпечує надійний захист, особливо якщо користувач задав стійкий пароль. WPA3-Enterprise забезпечує шифрування на основі 192-розрядних ключів [19].

Якщо безпроводові маршрутизатори та безпроводові точки доступу були випущені до 2019 року, вони, швидше за все, пропонують лише шифрування WEP, WPA та WPA2. У будь-якому випадку пристрої безпроводової мережі мають використовувати найнадійніший доступний протокол шифрування.

3.4 Системи IDS/IPS

Системи виявлення та запобігання вторгненням (IDS/IPS) варто використовувати для моніторингу безпроводових мереж на наявність підозрілої активності. Це може допомогти виявити та запобігти атакам до того, як вони завдадуть значної шкоди. Місце систем IDS/IPS в мережі показано на рис.3.3.

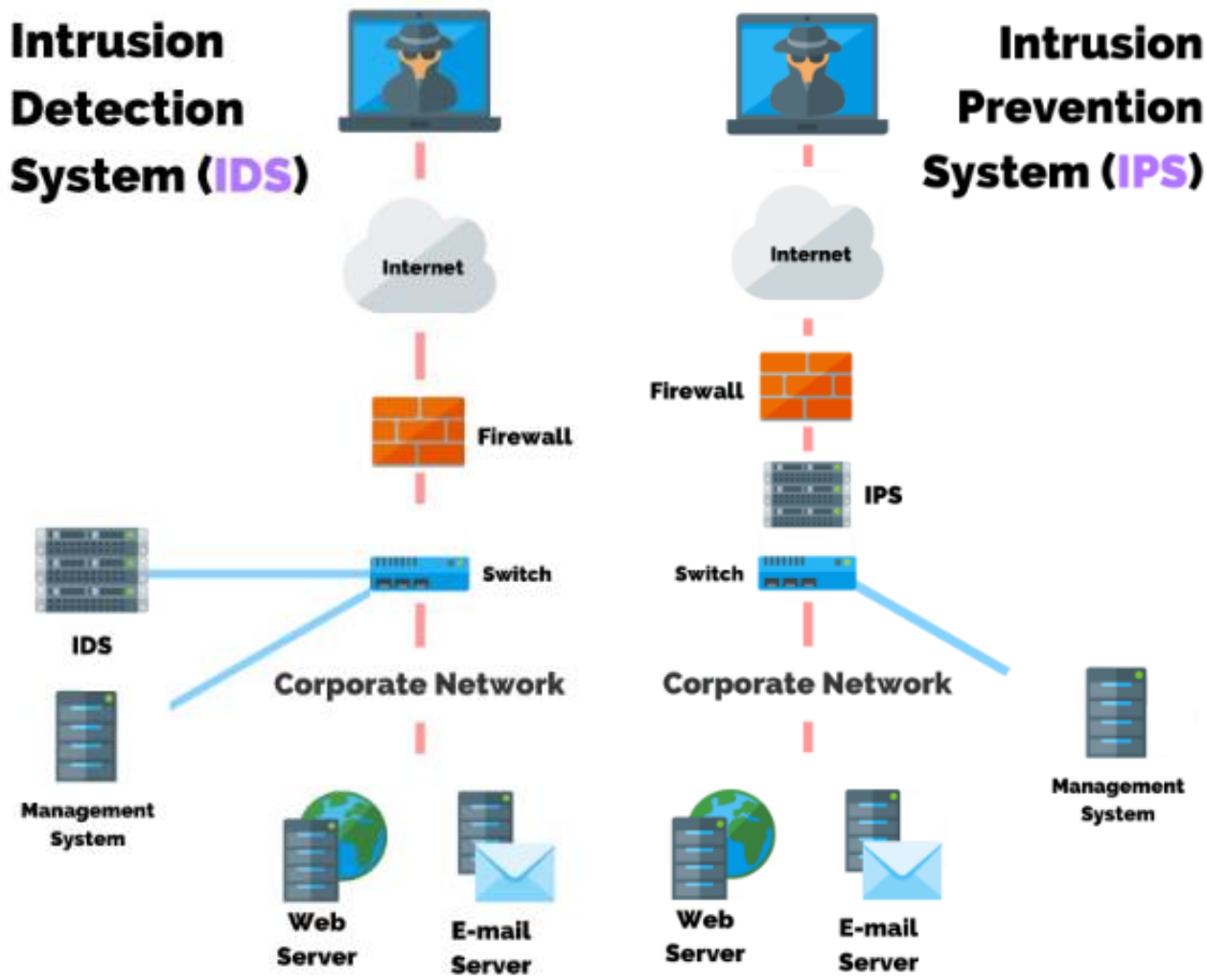

Рисунок 3.3 – Розміщення систем IDS/IPS в мережі

IDS не розміщується безпосередньо на лінії мережного трафіку. На відміну від IDS, IPS розміщується в мережі (на шляху прямого зв'язку між джерелом і одержувачем, безпосередньо за брандмауером), активно аналізуючи

та вживаючи автоматизованих дій щодо всіх потоків трафіку, які надходять у мережу [20].

Для захисту безпроводових мереж від загроз безпеки використовуються системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS). Системи IDS/IPS розроблені для виявлення та запобігання кібератакам шляхом моніторингу мережного трафіку та визначення типових моделей атак [21].

Коли системи IDS виявляють зловмисну поведінку, вони сповіщають адміністраторів мережі про вжиття негайних заходів. Системи IPS, з іншого боку, розроблені для автоматичного вжиття превентивних заходів у разі виявлення зловмисної поведінки.

Системи IDS/IPS здатні виявляти різні типи атак. Наприклад, вони можуть виявити атаку, здійснену зловмисником, який намагається викрасти паролі з будь-якого пристрою в мережі. Крім того, системи IDS/IPS можуть виявляти вірусні атаки, DDoS-атаки та багато інших типів атак.

Роль системи виявлення вторгнень (IDS) полягає у виявленненні загрози та створенні звіту або надісланні попередження адміністратору мережі [22]. Логічна топологія (рис. 3.4) показує, як копія зв'язку надсилається до IDS. Далі копія трафіку перевіряється IDS, що відбувається після того, як вихідний трафік уже знаходиться в локальній мережі.

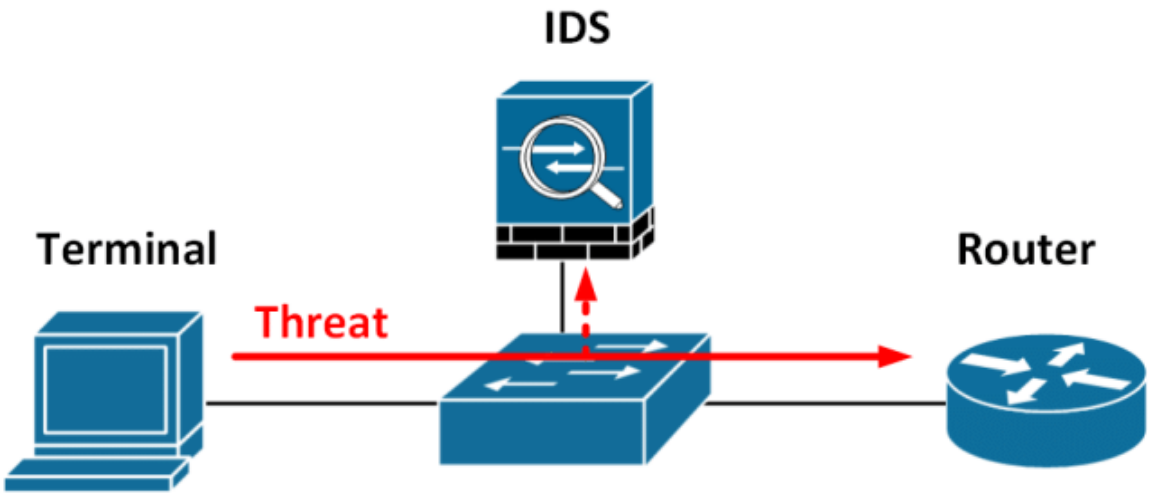

Рисунок 3.4 – Логічна топологія системи виявлення вторгнень

З іншого боку, IPS здатна негайно запобігти виявленій загрозі (рис. 3.5). Інкриміновані пакети відкидаються, однак невеликої затримки уникнути неможливо, оскільки кожен пакет перевіряється за допомогою IPS, яка згодом вирішує, чи буде пакет відкинуто, чи дозволено йому ввійти в цю захищену мережу. Важливо зазначити, що після впровадження помилкових правил IPS також відкидає захищений трафік, тоді як IDS просто створюватиме багато звітів.

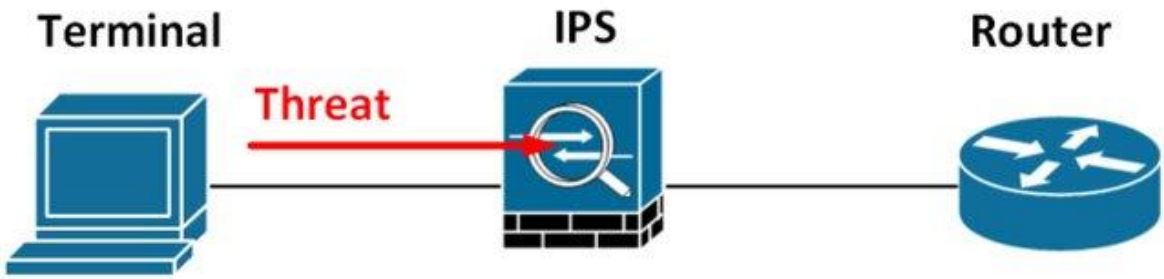

Рисунок 3.5 – Логічна топологія системи запобігання вторгненням

Визначення та режим роботи IPS та IDS відрізняються, але близькі за своєю метою, яка полягає в захисті мережі від зловмисників та їхніх методів атак. В 2005 році виробники об’єднали ці дві технології разом для можливості мати в одному продукті переваги їхньої функціональності [20].

При правильному налаштуванні та оновленні системи IDS/IPS можуть бути ефективним засобом захисту комп’ютерних мереж. Найкращі практики включають підтримку систем IDS/IPS в актуальному стані, належне їх налаштування та постійний моніторинг. Якщо система IDS/IPS встановлена та керована належним чином, вона може допомогти зробити мережу безпечнішою.

4 ЕФЕКТИВНІ РІШЕННЯ ДЛЯ ЗАХИСТУ БЕЗПРОВОДОВИХ МЕРЕЖ

4.1 Тестування на проникнення

Одним із найефективніших способів оцінити та підвищити безпеку безпроводової мережі є тестування на проникнення (penetration testing, pentest). Цей процес передбачає симуляцію атак для виявлення та усунення вразливостей, гарантуючи, що мережа надійна проти потенційних загроз [23].

Вразливості безпроводової мережі можуть варіюватися від проблем у методах шифрування до прогалин у мережних протоколах. Тест на проникнення може активно шукати конкретні слабкі місця, якими потенційно можуть скористатися неавторизовані користувачі. Це допомагає отримати чіткішу картину загального стану безпеки мережі.

Після виявлення вразливостей наступним кроком є оцінка рівня ризику. Це передбачає розуміння серйозності кожної вразливості в контексті потенційних кіберзагроз. Оцінка класифікує ці вразливості на основі простоти використання та впливу, який вони можуть мати на мережу в разі використання.

Після виявлення та оцінки вразливостей фокус зміщується на розробку стратегій для виправлення. Це передбачає створення плану дій для посилення загальної системи безпеки мережі.

Програма пентестування – це серія пентестів, які проводяться протягом визначеного періоду для систематичного пошуку та усунення вразливостей в одному або кількох активах. Програми, як правило, виконуються на щорічній основі, тести виконуються через заздалегідь визначені проміжки часу – наприклад, щомісяця або щокварталу [24].

Такий підхід забезпечує постійне тестування критичних і часто оновлюваних активів, а також високу ймовірність того, що вразливості високого ризику будуть знайдені та швидко виправлені.

Незважаючи на те, що специфіка тестування на проникнення може бути різною, основна структура програми пентесту складається з шести кроків, які наведено на рис. 4.1.

Рисунок 4.1 – Життєвий цикл пентестування

Тестування на проникнення безпроводової мережі виходить за рамки простої відповідності, надаючи відчутні реальні переваги, які наведені на рис. 4.2.

На відміну від стандартних автоматизованих інструментів безпеки, які працюють поверхнево, тести на проникнення глибоко занурюються в архітектуру мережі, що сприяє комплексному розуміння безпеки [23].

Тестування на проникнення допомагає організаціям дотримуватися галузевих правил і стандартів, таких як PCI DSS, ЄС GDPR і ISO 27001 [23]. Регулярне тестування може виявити прогалини в безпеці, які необхідно

усунути, щоб відповідати вимогам відповідності, що є важливим фактором для багатьох компаній.

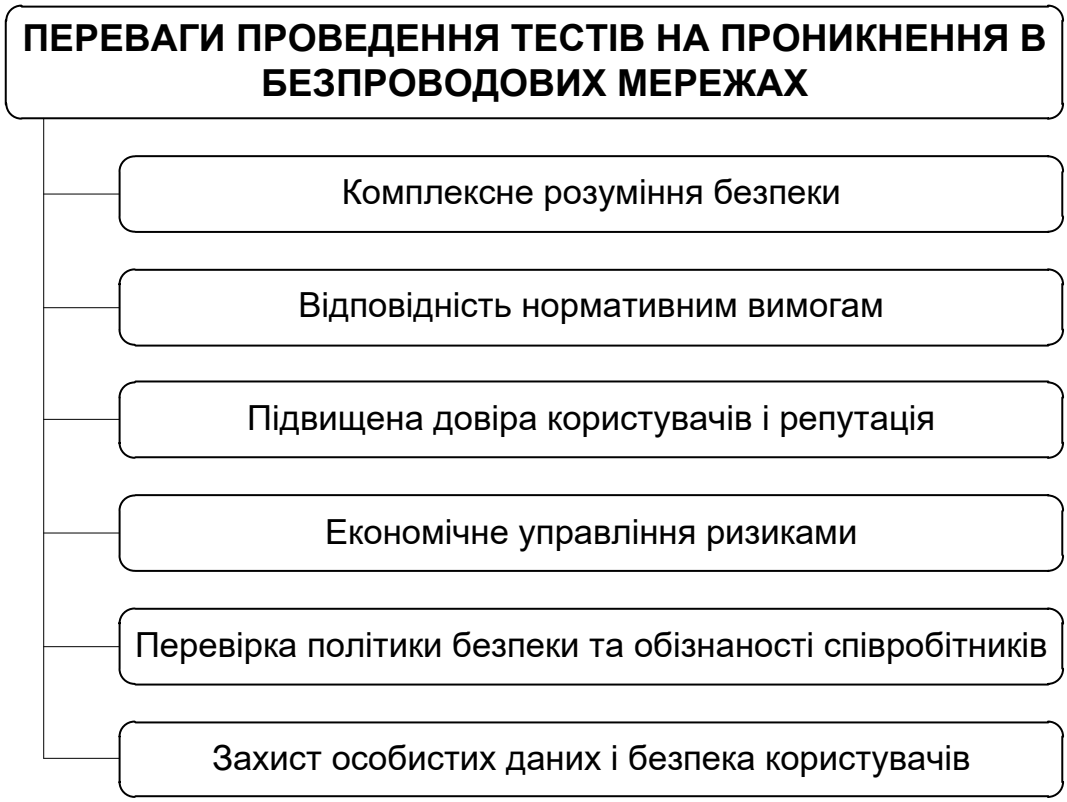

Рисунок 4.2 – Переваги пентестування для безпроводових мереж

Також перевагою є підвищена довіра користувачів і репутація. Демонстрація прихильності надійним методам безпеки є життєво важливою. Успішне проходження суворих тестів на проникнення та усунення виявлених вразливостей може підвищити репутацію організації щодо безпеки даних і підвищити довіру серед клієнтів, партнерів і зацікавлених сторін.

Раннє виявлення та усунення вразливостей за допомогою тестування на проникнення може бути значно рентабельнішим, ніж усунення наслідків порушення безпеки. Витрати, пов’язані з витоком даних, у тому числі регулятивні штрафи, судові збори та втрата бізнесу, можуть бути значними.

Тестування на проникнення безпроводового зв’язку також служить практичним аудитом політики безпеки організації та дотримання працівниками

протоколів безпеки. Це може виявити, чи ефективно впроваджуються політики безпеки та чи знають співробітники передові практики та чи дотримуються їх.

Основою безпеки є захист особистих даних і безпека користувачів. Безпроводові пентести є життєво важливими для запобігання несанкціонованому доступу та крадіжці даних, тим самим захищаючи користувачів від шахрайства. Ці тести забезпечують профілактичний захід для підтримки цифрової безпеки та довіри клієнтів і співробітників.

Кожен тип тесту на проникнення – незалежно від того, націлений він на додатки, API, хмарні інфраструктури, внутрішні чі зовнішні мережі – вирішує конкретні проблеми безпеки та вразливості, унікальні для його домену. Цей розширений погляд на тестування на проникнення підкреслює фундаментальний принцип сучасної безпеки мереж: цілісний підхід має вирішальне значення для комплексного захисту.

Тестування на проникнення в безпроводову мережу є критично важливим, але це лише один із аспектів комплексної стратегії безпеки. Включення різних типів тестів на проникнення відображає еволюцію розуміння складності цифрової безпеки в сучасному взаємопов’язаному світі. Організації, які використовують цей багатогранний підхід до тестування на проникнення, краще оснащені, щоб орієнтуватися в постійно мінливому світі загроз і ефективніше захищати свої цифрові активи.

4.2 Рекомендації для захисту безпроводових мереж

Безпека безпроводових мереж є надзвичайно важливою та потребує ефективних рішень. В даному контексті ефективними можуть вважатися лише такі рішення, які є комплексними, оскільки масштаб вразливостей та ризиків є різноманітним, мінливим та постійно зростаючим. Детальний аналіз найсучасніших джерел в сфері безпеки безпроводових мереж [1 – 27] показав, що на сьогоднійшій момент існує багато різноманітних засобів для захисту безпроводових мереж та підтримки безпеки на різних рівнях. В результаті

проведеного аналізу було сформовано та запропоновано ряд найсучасніших рекомендацій для власників безпроводових мереж, що представлені на рис. 4.3. Комплексне виконання цих рекомендацій дозволить підтримувати належний рівень безпеки безпроводової мережі.

Для максимально ефективного захисту безпроводових мереж вкрай необхідно:

– завжди бути в курсі загроз, що розвиваються, слідкувати за останніми тенденціями та передовими методами кібербезпеки;

– використовувати надійні й унікальні паролі, щоб захистити безпроводову мережу від несанкціонованого доступу;

– шифрувати передачу даних за допомогою найсучасніших протоколів безпеки, щоб запобігти різноманітним атакам;

– регулярно контролювати та перевіряти стан безпеки безпроводової мережі та негайно усувати виявлені вразливості;

– застосовувати надійні механізми автентифікації та сегментацію мережі для підвищення загальної безпеки;

– використовувати інструменти моніторингу мережі для постійного моніторингу та швидкого виявлення будь-якої підозрілої діяльності;

– регулярно оновлювати програми, щоб забезпечити захист пристроїв від відомих вразливостей.

Дотримуючись цих стратегій і залишаючись активними в питаннях безпеки, організації та окремі користувачі можуть створити ефективне безпечне безпроводове мережне середовище.

Дуже важливо пам’ятати, що загрози постійно розвиваються і зловмисники винаходять нові методи, щоб зламати захист. Бути в курсі останніх загроз і тенденцій безпеки є обов’язковим для відповідного адаптування заходів безпеки [25, 26]. Для протистояння новим загрозам, компанії повинні постійно адаптувати свої заходи безпеки. Регулярна переоцінка та оновлення протоколів безпеки має важливе значення для підтримки надійного захисту від нових загроз.

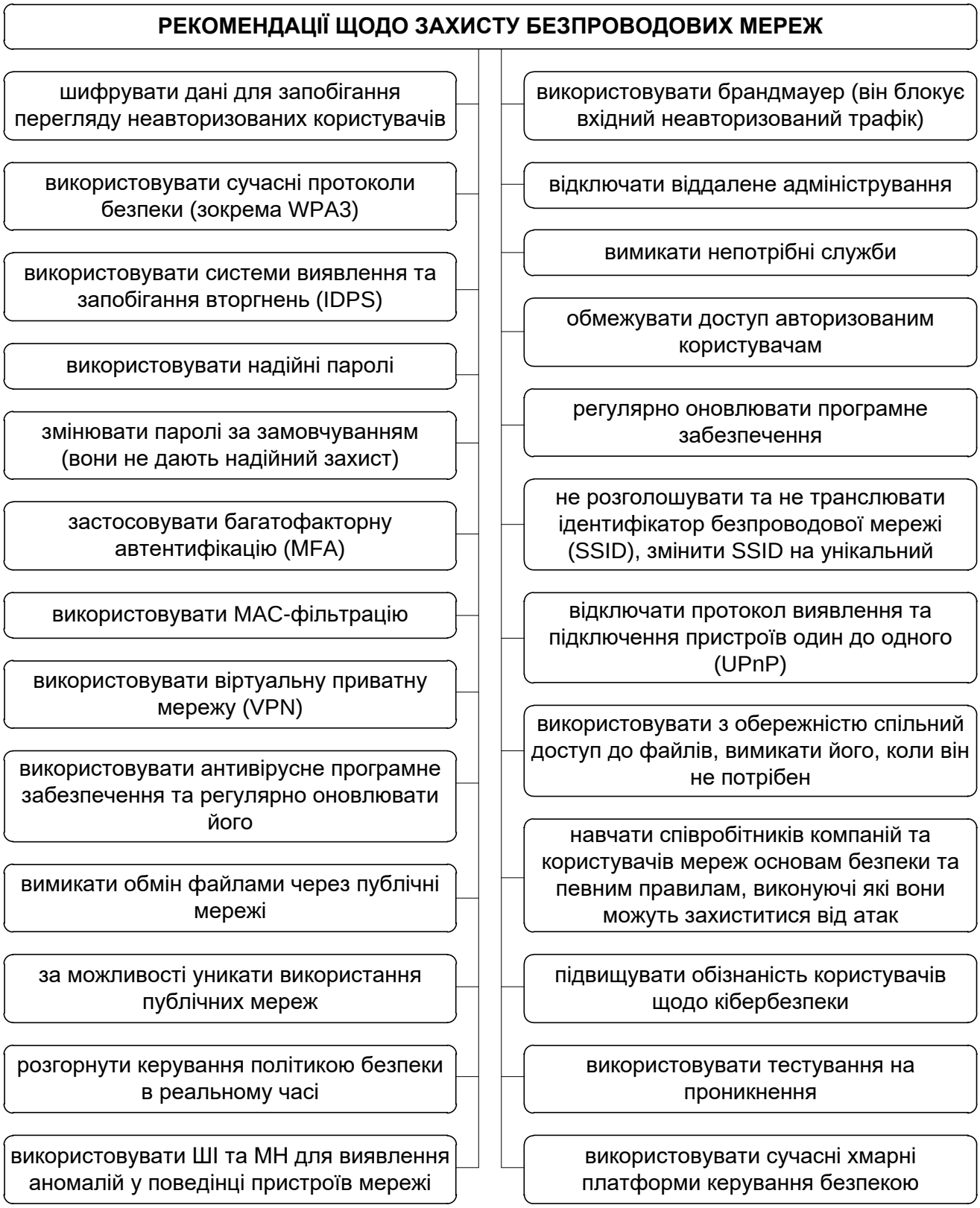

Рисунок 4.3 – Рекомендації для захисту безпроводових мереж

Останнім часом також набирає популярності архітектура нульової довіри (Zero Trust). Модель нульової довіри припускає, що жодному користувачу чи

пристрою не можна легко довіряти. Крім того, вона забезпечує суворий контроль доступу та механізми автентифікації по всій мережі. Кожен користувач і пристрій авторизуються по черзі в середовищі Zero Trust, незалежно від підключення до мережі. Цей підхід гарантує, що навіть якщо зловмисники отримають доступ до однієї частини мережі, вони все одно будуть ізольовані від критичних ресурсів. Архітектура Zero Trust зменшує поверхню атаки та підвищує загальну безпеку мережі. [26, 27].

Широкий спектр рішень мережної безпеки може значно посилити захист безпроводових мереж від сучасних кіберзагроз. Однак дуже важливо адаптувати ці рішення до конкретних потреб та регулярно оновлювати ті тестувати їх для підтвердження їхньої ефективності захисту мережі, даних і конфіденційних активів.

Завдяки проактивному та багаторівневому підходу до безпеки мережі можна зменшити ризики та підтримувати безпечне цифрове середовище. Створення потужної інфраструктури безпеки мережі має вирішальне значення для встановлення комплексних заходів безпеки, спрямованих на усунення потенційної вразливості та захисту від кіберзагроз.

ВИСНОВКИ

Зі збільшенням залежності від безпроводових мереж потреба в надійних засобах безпеки також стає все більш необхідною. Перенесення соціального життя в інтернет-середовище на основі безпроводових мереж посилює кібератаки та їх руйнівний вплив. Помилки та вразливі місця в безпроводових мережах, невідповідність мережних протоколів, збільшення кількості пристроїв, доданих до мережі, і складність критично важливих систем – усе це збільшує ризики безпеки. Крім того, підвищення рівня знань зловмисників і необережне використання мереж користувачами також підвищують ризики безпеки.

В роботі було розглянуто ряд питань, що стосуються організації та підтримки безпеки в безпроводових мережах.

В першому розділі кваліфікаційної роботи було розглянуто принципи функціонування безпроводових мереж, їхні переваги те недоліки, проведено порівняльний аналіз найсучасніших безпроводових мереж та аналіз основних тенденцій розвитку безпроводових технологій.

У другому розділі досліджено джерела загроз інформації в безпроводових мережах, загрози та вразливості в безпроводових мережах. Особливу увагу приділено найновішим ризикам в безпроводових мережах.

Третій розділ присвячено дослідженню засобів безпеки безпроводових мереж. Детально розглянуто типи інструментів мережної безпеки, методи та засоби безпеки в безпроводових мережах, протоколи шифрування та системи IDS/IPS.

В четвертому розділі запропоновано використовувати для організації безпеки пентестування. Тестування на проникнення сприяє загальній стратегії безпеки. Відомості, отримані в результаті цих різноманітних тестів, дозволяють організаціям побудувати багаторівневий захисний механізм, спрямований на усунення потенційних вразливостей на кожному рівні безпроводової мережі.

Цей комплексний підхід не тільки зміцнює окремі компоненти, але й підвищує стійкість усієї мережної архітектури до широкого спектру загроз.

Також в роботі сформульовані та запропоновані найбільш актуальні на сьогоднішній момент рекомендації для захисту безпроводових мереж. Захист безпроводових мереж – це безперервна робота, яка має постійно розвиватися. Розуміння зростаючого середовища загроз, вирішення проблем безпеки, впровадження механізмів шифрування та автентифікації, забезпечення регулярних оновлень і виправлень, а також навчання користувачів є ключовими кроками на шляху до досягнення надійної безпеки мережі.

Деякі результати роботи було апробовано на одинадцятій міжнародній науково-технічній конференції «Проблеми інформатизації» та опубліковано тези доповідей [28] за тематикою кваліфікаційної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. What is a Wireless Network? [Електронний ресурс] // ExterNetworks. – 2024. – Режим доступу до ресурсу: https://www.extnoc.com/learn/general/wireless-network.

2. What Is a Wireless Network? [Електронний ресурс] // Cisco Systems. – 2024. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html#~introduction.

3. What Is A Wireless Network? Types of Wireless Networks [Електронний ресурс] // Fortinet. – 2022. – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/wireless-network.

4. Степаненко О. Мережі Wi-Fi. Робота та стандарти. Застосування та особливості [Електронний ресурс] / Олег Степаненко // APPS4BUISNESS. – 2023. – Режим доступу до ресурсу: https://apps4business.com.ua/merezhi-wi-fi-robota-ta-standarti-zastosuvannya-ta-osoblivosti/.

5. Teja R. Wireless Communication: Introduction, Types and Applications [Електронний ресурс] / Ravi Teja // Electronicshub. – 2021. – Режим доступу до ресурсу: https://www.electronicshub.org/wireless-communication-introduction-types-applications/.

6. A Comprehensive List of Top Wireless Technologies [Електронний ресурс] // DFRobot. – 2023. – Режим доступу до ресурсу: https://www.dfrobot.com/blog-1658.html.

7. Bhatti S. B. Top 10 Wireless Technologies in World in 2024 (Updated List) [Електронний ресурс] / Sukaina Batool Bhatti // Techlatest. – 2023. – Режим доступу до ресурсу: https://techlatest.info/10-top-wireless-technologies/.

8. Future of wireless technology: Key predictions for 2024 [Електронний ресурс] // HelpNetSecurity. – 2023. – Режим доступу до ресурсу: https://www.helpnetsecurity.com/2023/12/22/wireless-technology-2024-predictions/.

9. Hardesty G. Twenty Wireless Technologies Poised for Significant Growth in 2023-24 [Електронний ресурс] / George Hardesty // DataAlliance. – 2023. – Режим доступу до ресурсу: https://www.data-alliance.net/blog/top-20-wireless-technologies-poised-for-significant-growth-in-2023-and-2024/.

10. Top 10 Emerging Wireless Technology Trends in the Telecom Industry [Електронний ресурс] // Blue Signal Search. – 2023. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/top-10-emerging-wireless-technology-trends-telecom-1e.

11. Закон України Про електронні комунікації [Електронний ресурс] // Верховна Рада України. Законодавство України. – 2024. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

12. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: навч. посібник / Г. М. Гулак. – Київ: Видавництво НА СБ України, 2020. – 256 с.

13. Examining to the Top Wireless Network Security Risks [Електронний ресурс] // Portnox. – 2024. – Режим доступу до ресурсу: https://www.portnox.com/cybersecurity-101/wireless-network-security-risks/.

14. Noguera D. Are Wi-Fi networks secure? Learn about the risks and vulnerabilities [Електронний ресурс] / Dario Noguera // flashstart. – 2023. – Режим доступу до ресурсу: https://flashstart.com/are-wi-fi-networks-secure-learn-about-the-risks-and-vulnerabilities/.

15. The Challenges of Wireless Network Security in an Interconnected World [Електронний ресурс] // Utilitiesone. – 2023. – Режим доступу до ресурсу: https://utilitiesone.com/the-challenges-of-wireless-network-security-in-an-interconnected-world.

16. All What you Need to Know about Network Security Tools [Електронний ресурс] // CyberTalents. – 2024. – Режим доступу до ресурсу: https://cybertalents.com/blog/network-security-tools.

17. Wireless Network Security Market Analysis - Industry Size, Share, Research Report, Insights, Covid-19 Impact, Statistics, Trends, Growth and Forecast

2024-2032 [Електронний ресурс] // Mark Wide Research. – 2024. – Режим доступу до ресурсу: https://markwideresearch.com/wireless-network-security-market/.

18. 5 Wireless network security threats you should be aware of [Електронний ресурс] // Integrated Computer Services. – 2024. – Режим доступу до ресурсу: https://www.icssfl.com/blog/wifi-security-threats-you-should-know/.

19. Гарист А. В. Аналіз захищеності Wi-Fi мереж / А. В. Гарист. // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Інформатика, обчислювальна техніка та автоматизація. – 2021. – №2. – С. 97–101.

20. Swanagan M. Intrusion Detection VS Prevention Systems: What's The Difference? [Електронний ресурс] / Michael Swanagan // Purplesec. – 2023. – Режим доступу до ресурсу: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/.

21. Güneşdoğdu E. Intrusion Detection and Prevention Systems (IDS/IPS): Working Principle, Types of Attacks Detected and Best Practices [Електронний ресурс] / Ensar Güneşdoğdu // Medium. – 2023. – Режим доступу до ресурсу: https://medium.com/@ensargnsdogdu/intrusion-detection-and-prevention-systems-ids-ips-working-principle-types-of-attacks-detected-52fdd545113d.

22. Hock F. Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks / F. Hock, P. Kortiš. // 13th International Conference on Emerging eLearning Technologies and Applications (ICETA). – 2015.

23. Hinojosa G. Importance of a Wireless Network Penetration Test [Електронний ресурс] / Gisela Hinojosa // Cobalt. – 2023. – Режим доступу до ресурсу: https://www.cobalt.io/blog/wireless-network-penetration-test-importance.

24. Wong C. The Lifecycle of a Pentest Program [Електронний ресурс] / Caroline Wong // Cobalt. – 2020. – Режим доступу до ресурсу: https://www.cobalt.io/blog/the-lifecycle-of-a-pentest-program.

25. Securing Your Wireless Network: Effective Strategies and Encryption Methods [Електронний ресурс] // LinkedIN. – 2023. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/securing-your-wireless-network-effective-strategies.

26. Desai T. Emerging Trends and Technologies in Wi-Fi Security [Електронний ресурс] / Tejdeep Desai // ItSecurityWire. – 2023. – Режим доступу до ресурсу: https://itsecuritywire.com/featured/emerging-trends-and-technologies-in-wi-fi-security/.

27. How to Build Network Security for Your Business in 2024 [Електронний ресурс] // perimeter 81 A Check Point Company. – 2023. – Режим доступу до ресурсу: https://www.perimeter81.com/blog/network/network-security-for-business.

28. Єфремов Н.С. Дослідження засобів безпеки безпроводових мереж / Н.С. Єфремов, Д. В. Чеботарьова // Тези доповідей одинадцятої міжнародної науково-технічної конференції «Проблеми інформатизації», 16 – 17 листопада 2023 р., Баку – Харків – Бельсько-Бяла. 2023. – Том 2. – С. 39.