ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби захисту інформації для Інтернету речей»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Скавронський Олександр
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
Скавронський Олександр
(прізвище, ім'я)

Керівник д. т. н., професор Зибін С.В.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Скавронському Олександру Геннадійовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
Засоби захисту інформації для Інтернету речей

керівник кваліфікаційної роботи д. т. н., професор Зибін С.В.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 04.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
Інфраструктура Інтернету речей (IoT) організації
хмарна платформа AWS IoT Security;
наукова та технічна література;
експлуатаційна документація;
нормативні документи та міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз технології інтернету речей та її вразливості.
2. Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.

3. Дослідження методів захисту інформації в інтернеті речей
4. Практична реалізація: Впровадження та налаштування обраних рішень
5. Розроблення рекомендацій на прикладі платформи AWS IoT Security
6. Оформлення результатів дослідження.

7. Дата видачі завдання 02.03.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз технології інтернету речей та її вразливості.	02.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	15.04.2025 р	
3.	Дослідження методів захисту інформації в інтернеті речей	01.05.2025 р	
4.	Практична реалізація: Впровадження та налаштування обраних рішень	11.05.2025 р.	
5.	Розроблення рекомендацій на прикладі платформи AWS IoT Security.	20.05.2025 р.	
6.	Оформлення результатів дослідження.	01.06.2025 р.	
7.	Підготовка доповіді до захисту.	04.06.2025 р.	

Здобувач вищої освіти _____ Скавронський Олександр
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ д. т. н., професор Зибін С.В.
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача СКАВРОНСЬКОГО Олександра
на тему: «Засоби захисту інформації для Інтернету речей»

Актуальність:

Позитивні сторони:

Недоліки:

Висновок:

Рецензент: д. т. н., професор _____ _____ Зибін С.В.

(науковий ступінь, вчене звання) *(підпис)* *(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Скавронський Олександр до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Засоби захисту інформації для Інтернету речей».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Керівник кваліфікаційної роботи _____ Зибін С.В.
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 69 сторінок, 21 рисунків, 6 табличок, 16 джерел.

Об’єкт дослідження — процеси захисту інформації і системі Інтернету речей (IoT).

Предмет дослідження — методи та засоби захисту інформації в IoT-інфраструктурах.

Мета роботи — дослідити загрози безпеці в Інтернеті речей, провести аналіз сучасних методів і засобів захисту, здійснити порівняльну оцінку провідних платформ IoT-безпеки та розробити рекомендації щодо впровадження AWS IoT Security на підприємстві.

Методи дослідження — аналіз літературних та нормативних джерел, порівняльна характеристика технічних рішень, моделювання загроз, практичне впровадження засобів захисту в середовищі AWS.

У роботі висвітлено основи побудови IoT-інфраструктур та принципи їхньої роботи, класифіковано основні кіберзагрози (DDoS-атаки, витоки даних, підміна трафіку, вразливості прошивки), розглянуто приклади інцидентів у 2023–2024 роках. Проведено порівняльний аналіз провідних рішень у сфері захисту IoT: AWS IoT Security, Microsoft Azure Defender, Cisco IoT Threat Defense, IBM Watson IoT Platform. На основі визначених критеріїв (масштабованість, аналітика, підтримка протоколів, інтеграція, вартість володіння) обґрунтовано доцільність вибору саме AWS IoT Security.

Практична частина роботи включає налаштування архітектури IoT-захисту з використанням сервісів AWS IoT Core, AWS Device Defender, CloudWatch, Lambda. Реалізовано приклад для сенсорної мережі з виявленням аномалій і автоматизованим реагуванням.

На основі результатів розроблено рекомендації для підприємств щодо захисту IoT-інфраструктур: від розмежування доступу і використання сертифікатів до централізованого моніторингу і життєвого циклу безпеки пристрою.

Галузь використання - захист IoT-інфраструктур в системах автоматизації, виробництві, логістиці, розумних будівлях та промисловому інтернеті речей.

ІНТЕРНЕТ РЕЧЕЙ, КІБЕРБЕЗПЕКА, IoT-ПРИСТРОЇ, ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, AWS IOT SECURITY, ВРАЗЛИВОСТІ, DDoS, ШИФРУВАННЯ, МОНІТОРИНГ, АНОМАЛІЇ, ПОЛІТИКИ БЕЗПЕКИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT — Internet of Things (Інтернет речей)

RFID — Radio-Frequency Identification (радіочастотна ідентифікація)

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

GPS — Global Positioning System (глобальна система позиціонування)

AI — Artificial Intelligence (штучний інтелект)

API — Application Programming Interface (інтерфейс прикладного програмування)

Edge computing — обчислення на краю мережі

Fog computing — туманні обчислення (проміжний рівень між краєм та хмарою)

SLA — Service Level Agreement (угода про рівень обслуговування)

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

MAC-адреса — Media Access Control address (фізична адреса мережевого інтерфейсу)

SCADA — Supervisory Control and Data Acquisition (система диспетчерського керування та збору даних)

MQTT — Message Queuing Telemetry Transport (легкий протокол обміну повідомленнями)

CoAP — Constrained Application Protocol (протокол для пристроїв з обмеженими ресурсами)

HTTP/HTTPS — Hypertext Transfer Protocol / Secure (протокол передавання гіпертексту)

UART/JTAG — Низькорівневі апаратні інтерфейси доступу до пристроїв

Zigbee / Z-Wave / LoRaWAN — Бездротові протоколи зв’язку для IoT

GDPR — General Data Protection Regulation (Загальний регламент захисту даних ЄС)

Spoofing — Підміна справжнього об’єкта фейковим

TLS (Transport Layer Security) — криптографічний протокол, що забезпечує захищену передачу даних між пристроями через Інтернет.

MQTT (Message Queuing Telemetry Transport) — легкий протокол обміну повідомленнями, який широко використовується в IoT через мале енергоспоживання та швидкість.

OTA (Over-the-Air) — технологія бездротового оновлення прошивки або програмного забезпечення IoT-пристроїв.

X.509 — стандарт сертифікатів цифрового підпису, що використовується для автентифікації пристроїв в IoT.

TCO (Total Cost of Ownership) — загальна вартість володіння рішенням, яка враховує прямі та непрямі витрати.

IDS / IPS (Intrusion Detection System / Intrusion Prevention System) — системи виявлення та запобігання вторгненням до мережі.

SIEM (Security Information and Event Management) — комплексна система управління інформацією про безпеку та подіями кібербезпеки.

SOAR (Security Orchestration, Automation, and Response) — система автоматизованої координації та реагування на інциденти безпеки.

IAM (Identity and Access Management) — система керування ідентичностями користувачів і контролем доступу до ресурсів.

SNS (Simple Notification Service) — хмарний сервіс AWS для надсилання сповіщень за допомогою електронної пошти, SMS або HTTP.

AWS (Amazon Web Services) — провідна хмарна платформа, яка надає масштабовані сервіси для обчислень, зберігання та безпеки.

VPC (Virtual Private Cloud) — віртуальна ізольована мережа в межах хмари AWS, яка дозволяє керувати мережевими конфігураціями.

SDK (Software Development Kit) — набір інструментів для розробки програмного забезпечення під певну платформу

NIS2 (Network and Information Security Directive 2) — оновлена директива ЄС про кібербезпеку, яка посилює вимоги до захисту цифрових систем.

ERP (Enterprise Resource Planning) — система управління бізнес-процесами підприємства.

ВСТУП

Інтернет речей (Internet of Things, IoT) – одна з найдинамічніших і водночас найбільш вразливих сфер сучасних інформаційних технологій. Його стрімкий розвиток відкрив нову еру взаємодії між фізичними об’єктами та цифровими системами. Завдяки вбудованим датчикам, мережевим модулям, контролерам та програмному забезпеченню, пристрої, які раніше були автономними, сьогодні здатні збирати, обробляти та обмінюватися даними з іншими пристроями або серверними хмарними системами. Це породжує новий рівень автоматизації, ефективності та зручності в побуті, промисловості, медицині, логістиці, сільському господарстві та багатьох інших сферах.

Втім, разом з перевагами поширення IoT приносить і серйозні загрози. За прогнозами дослідницької компанії Statista, до 2025 року кількість активних IoT-пристроїв у світі сягне понад 75 мільярдів одиниць. Це не лише відкриває нові економічні перспективи, а й формує безпрецедентну поверхню атаки для кіберзлочинців. Вразливості IoT можуть використовуватись для витоку конфіденційних даних, маніпуляцій у виробничих процесах, саботажу критичної інфраструктури або побудови потужних ботнетів для DDoS-атак.

Відсутність єдиного міжнародного стандарту захисту IoT, застаріле програмне забезпечення, використання стандартних паролів, відсутність оновлень безпеки, погано налаштовані API, відкриті порти — усе це є реаліями сучасної інфраструктури IoT. Кожен з цих факторів несе загрозу не лише окремому пристрою, а й усій мережі, до якої він підключений. У деяких випадках це може загрожувати безпеці даних тисяч людей або безперебійній роботі цілих промислових підприємств.

Особливо актуальною ця проблема стає для підприємств, які все активніше впроваджують елементи Інтернету речей у свою інфраструктуру. Застосування IoT у виробничих ланцюгах, енергетичних системах, транспортних платформах, складах, офісах чи кліматичних установках дозволяє зменшити витрати, оптимізувати процеси, збільшити швидкість і точність виконання завдань. Проте при цьому зростає і відповідальність за безпеку даних, які циркулюють у таких системах. Атака на слабко захищений смарт-пристрій може призвести до витоку комерційної таємниці, блокування роботи або масштабного фінансового збитку.

Досвід останніх років підтверджує серйозність цих загроз. У 2023–2024 роках було зафіксовано десятки резонансних кіберінцидентів у сфері IoT. Зокрема, атаки на медичні заклади у США та Європі через вразливі носимі пристрої, злам «розумного» освітлення в мегаполісах, саботаж у логістичних

компаніях через несанкціонований доступ до IIoT-контролерів. В окремих випадках атаки на IoT-платформи впливали не лише на інфраструктуру, а й безпосередньо загрожували здоров'ю та життю людей.

У цьому контексті особливої ваги набуває питання **розробки, впровадження та підтримки надійних засобів захисту IoT-систем**. Йдеться не лише про захист каналів зв'язку та шифрування даних, але й про наявність політик автентифікації, сегментацію мереж, постійний моніторинг аномалій, резервне копіювання, аудит дій пристроїв, а також своєчасне оновлення та ізоляцію скомпрометованих вузлів.

Мета цієї дипломної роботи полягає в комплексному аналізі сучасного стану безпеки Інтернету речей, вивченні ключових загроз, дослідженні найпоширеніших методів захисту, оцінці існуючих технологічних рішень, а також у розробці практичних рекомендацій для підприємств, що використовують IoT у своїй діяльності.

Для досягнення цієї мети робота структурована таким чином:

- **Перший розділ** присвячено аналізу технології Інтернету речей: розкрито її принципи роботи, архітектуру, а також класифікацію основних кіберзагроз і наслідків, які можуть бути спричинені атаками на IoT-пристрої. Особливу увагу приділено статистиці реальних інцидентів, що відбулися в останні роки.
- **Другий розділ** зосереджений на дослідженні сучасних методів захисту IoT-систем. Розглянуто такі механізми як автентифікація, шифрування, сегментація, IDS/IPS, блокчейн-інтеграція, аналіз аномалій тощо. Оцінено ефективність та обмеження різних рішень. Проведено порівняння найвідоміших платформ кіберзахисту для IoT — AWS IoT Security, Azure IoT Defender, Cisco IoT Threat Defense.
- **У третьому розділі** подано практичні рекомендації щодо впровадження захисних засобів на рівні підприємства. На прикладі платформи AWS IoT Security розглянуто процес підключення пристроїв, налаштування політик безпеки, моніторингу, журналювання та ізоляції підозрілої активності. Сформульовано загальні поради щодо управління ризиками, політик безпеки, навчання персоналу та технічного супроводу.

Таким чином, дипломна робота поєднує теоретичний огляд, практичний аналіз і конкретні приклади для забезпечення інформаційної безпеки у сфері IoT. Отримані результати можуть бути використані не лише науково-дослідними установами, а й приватними компаніями, державними структурами та інженерами, які безпосередньо впроваджують розумні пристрої в інфраструктуру підприємств.

1. АНАЛІЗ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ ТА ЇЇ ВРАЗЛИВОСТІ

1.1. Поняття та принципи роботи технології IoT

У сучасному етапі науково-технічного прогресу розвиток технологій Інтернету речей (англ. Internet of Things, далі — IoT) є одним із ключових факторів трансформації цифрової інфраструктури, що охоплює практично всі сфери людської діяльності. Завдяки IoT відбувається глибока зміна парадигми взаємодії людини з навколишнім середовищем: фізичні об’єкти, які раніше функціонували ізольовано, нині здатні здійснювати обмін даними, приймати рішення та впливати на інші об’єкти без прямої участі людини.

IoT — це не лише технологія, а й нова філософія побудови розумного простору, в якому будь-який предмет — від побутової техніки до промислового верстата — може мати вбудовану здатність до збирання, передавання, зберігання та аналізу інформації. У цьому контексті речі (об'єкти) набувають нової ролі: вони стають активними учасниками інформаційних процесів, а не пасивними носіями чи інструментами.

Уперше поняття Internet of Things було запропоноване у 1999 році Кевіном Ештоном, співробітником Массачусетського технологічного інституту (MIT), який обґрунтував необхідність створення цифрових засобів для автоматичного виявлення об'єктів у ланцюгах постачання, з використанням радіочастотної ідентифікації (RFID). З того часу технологія пройшла етапи від теоретичного концепту до глобально впроваджуваної інфраструктури.

За даними компанії Statista, станом на 2024 рік у світі налічувалося понад 17 мільярдів активних IoT-пристроїв, а до 2030 року прогнозується зростання цього показника до понад 29 мільярдів [1]. Це свідчить про стрімке поширення технології та її критичне значення для економік і суспільств.

Сутність та визначення IoT

Під поняттям Інтернету речей мається на увазі складна система, що включає фізичні пристрої, програмні модулі, мережеву інфраструктуру, протоколи зв'язку та інтелектуальні алгоритми обробки даних. Головною відмінністю IoT від традиційних мереж є те, що тут комунікація ведеться не лише між людьми або між людиною та пристроєм, а переважно — **«річ-річ» (device-to-device, D2D)** або **«річ-система» (device-to-system)**.

Згідно з визначенням Міжнародного союзу електрозв'язку (ITU-T), IoT — це глобальна інфраструктура, що забезпечує розширені сервіси шляхом взаємодії (фізичних та віртуальних) речей на основі інформаційно-комунікаційних технологій [2].

Інакше кажучи, будь-яка система, яка відповідає трьом ключовим критеріям, може вважатися частиною IoT:

1. **Здатність до збирання даних із навколишнього середовища** (фізичні, хімічні, біологічні або інші параметри).
2. **Можливість передавання інформації до інших пристроїв або систем** (з використанням локальних або глобальних мереж).
3. **Присутність механізму прийняття рішень**, який може реалізовуватись як через просту автоматизацію, так і через складні алгоритми з елементами штучного інтелекту.

Основні принципи роботи IoT

Для глибшого розуміння сутності IoT доцільно окреслити його фундаментальні принципи, які визначають функціональність будь-якої IoT-системи.

- *Принцип тотального з'єднання*

Головною особливістю IoT є те, що всі пристрої в екосистемі повинні бути здатними підключатися до інших пристроїв або до центрального вузла. Цей принцип передбачає уніфіковані інтерфейси, протоколи та стандарти, які дають змогу забезпечити масштабованість мережі. Відомими прикладами таких протоколів є MQTT, CoAP, Zigbee, LoRaWAN, Bluetooth LE, Wi-Fi та NB-IoT.

- *Принцип унікальної ідентифікації*

Кожен об'єкт в IoT має бути унікально ідентифікований. Ідентифікація здійснюється на базі унікальних адрес (IP, MAC), серійних номерів, сертифікатів або цифрових токенів. Це дозволяє здійснювати точне відстеження дій конкретного пристрою, налаштовувати політики доступу та протоколи аутентифікації.

- *Принцип взаємодії у реальному часі*

Однією з ключових вимог до IoT-систем є обробка інформації у режимі реального або майже реального часу. Це особливо актуально для критичних застосувань — наприклад, в медицині (моніторинг стану пацієнтів), транспорті (управління рухом) або промисловості (аварійні системи зупинки).

- *Принцип автономного функціонування*

Більшість пристроїв в IoT повинні функціонувати без постійної участі людини. Це означає необхідність наявності вбудованих рішень з локального керування, алгоритмів реакції, програмованих сценаріїв або штучного інтелекту, що дозволяє об’єктам реагувати на зміну умов самостійно.

- *Принцип енергоефективності*

Через масове розгортання IoT у сферах, де недоцільно або неможливо часто обслуговувати пристрої (наприклад, у полі, під землею, в тілі пацієнта), всі компоненти мають бути оптимізовані для надзвичайно низького енергоспоживання. Це досягається за рахунок використання протоколів з коротким циклом передачі, глибокого сну, автономних джерел живлення (сонячні батареї, кінетичні генератори) тощо.

Архітектура Інтернету речей, попри різноманітність реалізацій, базується на універсальних принципах багаторівневої взаємодії компонентів. Така структура дозволяє зручно розділити функціональне навантаження між фізичними пристроями, мережевою інфраструктурою та програмним забезпеченням. У класичному розумінні IoT-система охоплює рівні сприйняття, передачі даних, обробки інформації та взаємодії з користувачем.

Фізичні пристрої, які складають основу будь-якої IoT-екосистеми, включають сенсори, виконавчі механізми, контролери, передавачі та приймачі даних. Сенсори — це технічні компоненти, що забезпечують первинний зв'язок між фізичним світом і цифровим середовищем. Вони здатні вловлювати широкий спектр параметрів — від температури, вологості та рівня освітленості до концентрації газів у повітрі, біометричних характеристик людини чи руху в просторі. Їхнім завданням є збирання інформації про середовище і передача її для подальшого аналізу.

Актуатори, натомість, мають протилежну функцію — вони реагують на оброблені дані, перетворюючи цифрові сигнали на фізичну дію. Це можуть бути мотори, електромагнітні замки, світлові або звукові індикатори, механізми подачі рідини чи перемикачі живлення. У комплексі з сенсорами вони дозволяють створювати замкнуті системи автоматичного регулювання, які не лише вимірюють зміни, а й реагують на них у реальному часі.

Передача даних у таких системах здійснюється через різні типи мереж — дротові та бездротові. Залежно від умов експлуатації, обираються ті чи інші протоколи. Для пристроїв, розташованих у безпосередній близькості, доцільно використовувати енергоефективні стандарти короткого радіуса дії, тоді як для розосереджених систем — застосовуються мережі широкого покриття. Усе це має

забезпечити надійність і стабільність комунікації між пристроями, незалежно від географії чи інтенсивності використання.

Надзвичайно важливим є програмне середовище, що керує взаємодією між пристроями. Це стосується як операційних систем для мікроконтролерів, так і хмарних платформ для централізованого моніторингу. Програмна інфраструктура виконує функції синхронізації, маршрутизації, обробки даних, шифрування та логування. Багато IoT-пристроїв працюють на мінімалістичних версіях відомих ОС або на спеціалізованих прошивках, які підтримують лише критично необхідні функції. Такий підхід зменшує енергоспоживання і підвищує безпеку.

В обробці інформації особливої уваги заслуговує концепція периферійних обчислень, або обробки на краю мережі. Суть цього підходу полягає в тому, що частина обчислювальних завдань виконується не в центрі, тобто не в хмарі, а безпосередньо на пристроях або проміжних вузлах, таких як шлюзи або локальні сервери. Це дозволяє мінімізувати затримки при прийнятті рішень, зменшити навантаження на мережу та забезпечити базову автономність при втраті зв’язку з центральною системою.

Ще одним важливим аспектом є обробка великих обсягів даних, що генеруються мережею IoT-пристроїв. Для цього використовуються системи керування базами даних, інструменти аналітики, алгоритми машинного навчання, які здатні виявляти патерни, передбачати аномалії та автоматизувати управлінські рішення. Аналітична частина може функціонувати у форматі статистичного аналізу, прогнозування на основі історичних даних або у вигляді адаптивних моделей, які навчаються в процесі експлуатації системи.

Важливо також враховувати, що IoT не існує у вакуумі — ця технологія тісно інтегрується з іншими сферами, такими як штучний інтелект, блокчейн, кібербезпека, мобільні додатки та хмарні сервіси. Така інтеграція дозволяє створювати гібридні системи, що об'єднують переваги кожної з технологій. Наприклад, поєднання IoT та блокчейну може забезпечити незмінність та прозорість даних, що особливо цінне в логістиці, фінансовій звітності або медичних системах.

Особливу роль у цьому контексті відіграє взаємодія з користувачем. У більшості сучасних реалізацій IoT передбачається наявність спеціального інтерфейсу — це може бути веб-панель керування, мобільний застосунок або інтеграція в існуючу корпоративну систему. Через ці інтерфейси відбувається не лише перегляд інформації, а й налаштування параметрів, отримання сповіщень, формування звітів, введення команд. Інтерфейс повинен бути інтуїтивно зрозумілим, захищеним, адаптивним до змін і зручним у повсякденному використанні.

Таким чином, принципи роботи IoT базуються на чітко структурованій взаємодії між фізичними компонентами, логікою передачі й обробки даних,

алгоритмами реагування та засобами інтерфейсу. Ці елементи створюють складну, але гнучку екосистему, яка може масштабуватись від кількох сенсорів у смарт-домі до мільйонів пристроїв у розподіленій промисловій інфраструктурі.

Застосування технології Інтернету речей охоплює величезну кількість сфер, трансформуючи їх зсередини. У побутовому середовищі IoT найчастіше асоціюється з концепцією «розумного дому», де світло, клімат-контроль, безпека, побутова техніка й мультимедійні системи можуть взаємодіяти між собою та керуватися через мобільний застосунок або голосового асистента. Такий рівень автоматизації підвищує комфорт, ефективність енергоспоживання, а також безпеку житлового простору.

У транспортній галузі IoT відіграє ключову роль у розвитку інтелектуальних транспортних систем, автономного водіння, управління міським трафіком та моніторингу рухомого складу. Завдяки GPS-датчикам, акселерометрам, камерам і хмарним платформам можлива побудова моделей реального часу для відстеження вантажів, оптимізації маршрутів, попередження про несправності чи перевищення швидкості.

В аграрному секторі — зокрема, в рамках концепції «розумного фермерства» — впровадження IoT дозволяє контролювати мікроклімат теплиць, автоматично вносити добрива, визначати вологість ґрунту, спостерігати за станом поголів’я чи рівнем захворюваності рослин. Ці дані інтегруються у цифрові системи управління господарством, що дозволяє істотно знизити витрати ресурсів і підвищити врожайність.

У промисловості IoT став основою концепції «Індустрія 4.0», яка передбачає створення так званих кіберфізичних систем — об'єднаних у мережу інтелектуальних машин, які самостійно ухвалюють рішення на основі аналізу даних із датчиків. Вони можуть координувати свої дії, регулювати виробничі параметри, проводити технічну діагностику в режимі реального часу. Такий підхід значно скорочує втрати часу та знижує витрати на обслуговування.

У сфері охорони здоров’я IoT відкриває нові горизонти для дистанційної діагностики та лікування. Смарт-браслети, глюкометри, кардіомонітори, імплантовані сенсори передають медичну інформацію до централізованих баз даних, де її можуть проаналізувати лікарі або автоматичні системи на основі штучного інтелекту. Це критично важливо для пацієнтів із хронічними захворюваннями або тих, хто знаходиться у віддалених регіонах, де доступ до медичних установ обмежений.

Попри всі переваги, широке впровадження IoT породжує низку викликів. Один із них — проблема уніфікації стандартів. Через велику кількість виробників, протоколів і закритих платформ часто виникають труднощі із забезпеченням сумісності пристроїв між собою. Це стримує розвиток глобальних екосистем та ускладнює інтеграцію нових рішень.

Ще серйознішим викликом є забезпечення безпеки та конфіденційності. IoT-пристрої, особливо недорогі споживчі моделі, часто мають слабке програмне забезпечення, використовують прості паролі, не шифрують передані дані або не отримують оновлень безпеки. Через це вони стають легкою ціллю для зловмисників, які можуть отримати несанкціонований доступ, перехопити трафік або використати пристрої для організації DDoS-атак.

Окремо варто згадати й про проблему масштабованості: зі зростанням кількості пристроїв, мережеве навантаження збільшується експоненційно, а кількість згенерованих даних потребує нових способів зберігання та обробки. Саме тому великі компанії впроваджують edge computing (обчислення на краю мережі) і fog computing (туманні обчислення), де аналіз даних відбувається ближче до джерела інформації, що зменшує затримки та покращує продуктивність.

Зважаючи на усе вищенаведене, поняття та принципи роботи Інтернету речей охоплюють не лише технічну сторону питання, а й глибоко впливають на соціально-економічні процеси, правове регулювання, кібербезпеку, екологію та навіть етику. Створення по-справжньому ефективного, надійного та етичного IoT-середовища вимагає міждисциплінарного підходу, гармонізації інтересів виробників, розробників, державних органів і кінцевих користувачів.

Таким чином, Інтернет речей — це не просто технологія, це фундаментальна зміна у способі сприйняття навколишнього світу, де кожна річ стає частиною єдиного цифрового простору, здатного бачити, чути, думати та діяти.

1.2 Класифікація загроз та їх наслідки

Таблиця 1.1 Загрози та наслідки

Тип загрози	Можливі наслідки
Несанкціонований доступ	Перехоплення керування пристроєм, крадіжка або підміна даних
DDoS-атаки	Паралізація сервісів, фінансові втрати, відмова в обслуговуванні
Витоки конфіденційної інформації	Порушення приватності, втрати персональних або корпоративних даних
Шкідливе програмне забезпечення	Створення бекдорів, зловмисне керування, витоки інформації

Тип загрози	Можливі наслідки
Вразливості прошивки	Можливість перехоплення контролю через експлойти
Підміна пристроїв (spoofing)	Ін’єкція шкідливих даних, маніпуляції процесами
Фізичний доступ	Саботаж, фізичне втручання, крадіжка або модифікація обладнання
Стандартні паролі	Автоматизований злам, масштабна компрометація пристроїв

Інтернет речей (IoT) стрімко перетворюється на один із головних технологічних рушіїв сучасності. Завдяки підключеним пристроям ми оптимізуємо побут, автоматизуємо промислові процеси, покращуємо медичні послуги, забезпечуємо інтелектуальну інфраструктуру міст. Водночас така повсюдність і швидке розгортання IoT викликають не менше зростання ризиків у сфері інформаційної безпеки. Через відсутність єдиних стандартів, обмежені ресурси пристроїв, слабкі засоби захисту, величезну кількість вузлів і глибоку інтеграцію з реальним світом, IoT-платформи стають привабливою мішенню для кібератак.

Для ефективного забезпечення захисту IoT-систем необхідно здійснювати класифікацію загроз, що дозволяє не лише впорядкувати відомі вектори атак, а й краще передбачати потенційні ризики у різних сценаріях використання. Загрози, притаманні Інтернету речей, можуть мати як суто технічну природу, так і соціальну, фізичну, правову. У цьому підрозділі подається детальна класифікація таких загроз із глибоким аналізом їх наслідків для індивідуальних користувачів, організацій і державних структур.

Несанкціонований доступ до пристроїв

Однією з найтиповіших, але водночас найбільш небезпечних загроз у середовищі IoT є несанкціонований доступ до пристроїв або їхніх компонентів. Більшість IoT-пристроїв мають уразливі інтерфейси — веб-панелі, відкриті порти, API, або працюють із заводськими паролями, які ніколи не змінюються користувачами. Додаткову небезпеку становлять пристрої, які не підтримують оновлення прошивки, що робить неможливим усунення вразливостей після їх виявлення.

Прикладом є численні випадки компрометації камер відеоспостереження, які використовувалися не лише для стеження за користувачами, а й як частина ботнетів. У більшості випадків зловмисники використовували відкриті бази даних для пошуку пристроїв із дефолтними логінами та паролями (наприклад, admin/admin), після чого отримували повний контроль над камерою.

Наслідки несанкціонованого доступу можуть бути масштабними:

- повний контроль над функціоналом пристрою;
- доступ до зібраних даних (аудіо, відео, логів);
- можливість фізичного впливу (вмикання/вимикання пристроїв, відкриття замків);
- використання пристрою як «точки входу» для атак на інші елементи мережі;
- вивід системи з ладу шляхом некоректного конфігурування.

DDoS-атаки із залученням IoT-пристроїв

Ще однією категорією загроз, які стали особливо актуальними після атаки Mirai у 2016 році, є DDoS-атаки (Distributed Denial of Service), де IoT-пристрої використовуються не як об’єкт атаки, а як **засіб її реалізації**. Через слабкий захист, мільйони пристроїв по всьому світу можуть бути заражені шкідливим ПЗ, що об’єднує їх у мережу ботів.

Ці мережі потім використовуються для масованих атак на інтернет-ресурси, що призводить до:

- недоступності онлайн-сервісів;
- фінансових втрат підприємств;
- репутаційних збитків;
- проблем із виконанням договорів SLA (service level agreement);
- блокування критичної інфраструктури (DNS, банкінг, e-commerce).

DDoS-атаки можуть супроводжуватися шантажем (наприклад, вимогою викупу за припинення атаки), або відволікати увагу від основного вектора злому.

Витоки конфіденційної інформації

IoT-пристрої є джерелом величезного обсягу персональних, корпоративних та службових даних. Ці дані можуть включати:

- фізіологічні показники користувача (у випадку медичних пристроїв);
- геолокаційні дані;
- аудіо- і відеопотоки;

- поведінкову аналітику;
- команди керування системами (освітленням, опаленням, замками тощо).

Неналежне зберігання цих даних, передача незашифрованими каналами або відсутність механізмів автентифікації відкривають шлях до масових витоків. Компанії можуть втратити критично важливу інформацію про свої процеси або клієнтів, а приватні особи — конфіденційність власного життя.

У деяких випадках витоки можуть мати **правові наслідки**, пов’язані з порушенням міжнародного законодавства про захист персональних даних (наприклад, GDPR), що тягне за собою багатомільйонні штрафи.

Шкідливе програмне забезпечення та IoT

Окрему категорію загроз становить впровадження шкідливого програмного забезпечення (малваре), яке використовує вразливості в прошивці або відкриті комунікаційні інтерфейси для проникнення у пристрої. Пристрої Інтернету речей через свої технічні обмеження — обмежену обчислювальну потужність, пам’ять, спрощені операційні системи — зазвичай не мають належного захисту від таких загроз. Відсутність вбудованих антивірусних систем, неможливість користувача переглянути чи виявити аномалії, а також повільний або взагалі відсутній процес оновлення призводять до того, що пристрої можуть залишатися скомпрометованими тривалий час без жодного виявлення.

Типовими прикладами шкідливого ПЗ в IoT є:

- **Бекдори (backdoors)** – надають прихований віддалений доступ до пристрою без відома власника;
- **Руткіти (rootkits)** – дозволяють приховати наявність шкідливих програм або змін у системі;
- **Трояни (trojans)** – маскуються під легітимне ПЗ, але виконують шпигунські чи деструктивні функції;
- **Криптомайнери** – використовують ресурси пристрою для нелегального майнінгу криптовалюти;
- **Шпигунське ПЗ (spyware)** – збирає дані, записує аудіо, відео або логіни/паролі користувача.

Ураження одного пристрою може спричинити ланцюгову реакцію в мережі — зараження інших пристроїв, перехоплення даних у реальному часі, або навіть саботаж у промисловому середовищі.

Вразливості у прошивці та протоколах зв'язку

Ще однією критичною проблемою у сфері IoT є велика кількість вразливостей у прошивках пристроїв. Дуже часто виробники пристроїв, намагаючись скоротити витрати, використовують застарілі компоненти або спрощують безпеку в ім’я зручності. В результаті ми отримуємо пристрої, які:

- не підтримують оновлення без участі користувача;
- мають відкриті дебаг-порти;
- використовують нешифровані канали зв’язку (HTTP замість HTTPS);
- застосовують слабкі механізми шифрування або авторизації.

Протоколи зв’язку, як-от MQTT, CoAP, Zigbee, Z-Wave, LoRaWAN, також мають власні недоліки. Наприклад, MQTT передбачає передачу повідомлень через брокера, але без додаткових механізмів шифрування або авторизації, що робить його вразливим до атак типу «людина посередині» (MITM), підміни даних або сесійного викрадення.

Наслідки експлуатації таких вразливостей можуть бути:

- перехоплення трафіку та крадіжка даних;
- підміна команд (наприклад, увімкнення чи вимкнення пристрою);
- «тихе» перенаправлення інформаційних потоків з метою шпигунства або аналітики;
- вивід з ладу шляхом перевантаження системи запитами.

Особливо небезпечні вразливості у прошивках пристроїв, які виконують критичні функції — медичні імплантати, контролери нафтопроводів, електромереж, автоматизовані системи водопостачання тощо. Їх ураження може мати не лише фінансові, а й **людські наслідки**.

Підміна пристроїв і спуфінг

У контексті IoT підміна пристрою (spoofing) означає ситуацію, коли в систему вводиться фальшивий вузол, який маскується під справжній. Це може бути реалізовано як шляхом апаратної інсталяції підробленого пристрою, так і програмним шляхом — підміною ідентифікаторів, MAC-адрес або ключів.

Підміна дозволяє:

- перехоплювати та змінювати потоки даних;
- підсилювати сигнали або вносити хибні вимірювання (наприклад, неправдиву температуру чи рівень забруднення);
- впливати на алгоритми автоматичного керування;

- запускати події або сигнали тривоги за відсутності реальної підстави;
- отримати доступ до внутрішньої мережі через зовнішній фейковий вузол.

У системах «розумного транспорту» або автономного руху така атака може мати катастрофічні наслідки — зіткнення, зупинка машин, неправильна навігація.

Фізичні загрози та маніпуляції

IoT-пристрої зазвичай розміщені у відкритому середовищі або в доступних місцях: на вулицях, у громадських місцях, на транспорті, в офісах. Це створює широкі можливості для **фізичного втручання**:

- злам корпусу й доступ до внутрішніх портів;
- зчитування вмісту пам’яті;
- заміна або викрадення мікросхем;
- підключення до UART/JTAG портів для відлагодження;
- підміна живлення, що викликає помилки або аварії.

Фізичний злам у поєднанні з відсутністю систем виявлення втручань дозволяє отримати критичну інформацію або змінити функціональність пристрою без помітних наслідків у короткотерміновій перспективі.

Системні наслідки реалізації загроз у IoT

Інформаційні атаки в середовищі Інтернету речей, на відміну від класичних кіберзагроз, мають мультиплікаційний ефект. Якщо традиційні атаки можуть бути спрямовані лише на комп’ютери, сервери чи веб-ресурси, то IoT-пристрої діють **у фізичному світі**, впливаючи на реальні процеси: електропостачання, безпеку пересування, медичні процедури, логістику, інженерну інфраструктуру, оборону.

Більшість атак на IoT не зупиняються лише на доступі до пристрою — вони переходять у фазу:

- модифікації систем керування;
- деструкції цільових процесів;
- саботажу промислових установок;
- компрометації конфіденційної інформації;
- або утворення “тіньової” інфраструктури, що діє паралельно з легальною мережею.

Організації, які впроваджують IoT без комплексної політики безпеки, ризикують не лише матеріальними втратами, але й втратами **довіри клієнтів**,

регуляторними штрафами, **позовами від третіх осіб** та навіть **зупинкою бізнесу**.

Галузеві приклади впливу загроз

Енергетика

Інфраструктура Smart Grid базується на розгалуженій IoT-мережі з мільйонами датчиків. Вразливість лише одного компонента, наприклад, інтелектуального лічильника, дозволяє вивести з ладу цілі сегменти мережі, спричиняючи перебої в енергопостачанні, некоректні розрахунки, або підміни даних.

Медицина

IoT-монітори пацієнтів, насоси введення ліків, дефібрилятори — усе це може стати об’єктом маніпуляції. Так, у 2020 році компанія Medtronic була змушена відкликати тисячі інсулінових помп через можливість дистанційного злому з боку зловмисника.

Транспорт

Системи контролю дорожнього руху, автономні авто та інфраструктура «розумних» світлофорів використовують IoT для координації. Атака на ці системи може викликати хаос у русі, зіткнення або навіть керований саботаж.

Промисловість

SCADA-системи, які контролюють заводи, трубопроводи, об'єкти водопостачання, масово інтегрують IoT-модулі. У разі проникнення в систему, зловмисник може змінити температурний режим, тиск, увімкнути/вимкнути двигуни — що веде до дорогих поломок або навіть загроз життю.

Агросектор

Дрони, сенсори вологи, GPS-моніторинг урожайності. У разі втрати контролю — неправильний розподіл добрив, некоректне зрошення або викрадення даних про стан полів.

Розуміння типології загроз в IoT — критично важливий етап для розробки стратегії захисту. На відміну від класичних IT-систем, IoT характеризується високою гетерогенністю, фізичною розосередженістю, обмеженими обчислювальними потужностями та слабкими механізмами оновлення. Через це

традиційні методи кіберзахисту часто виявляються недостатніми або неефективними.

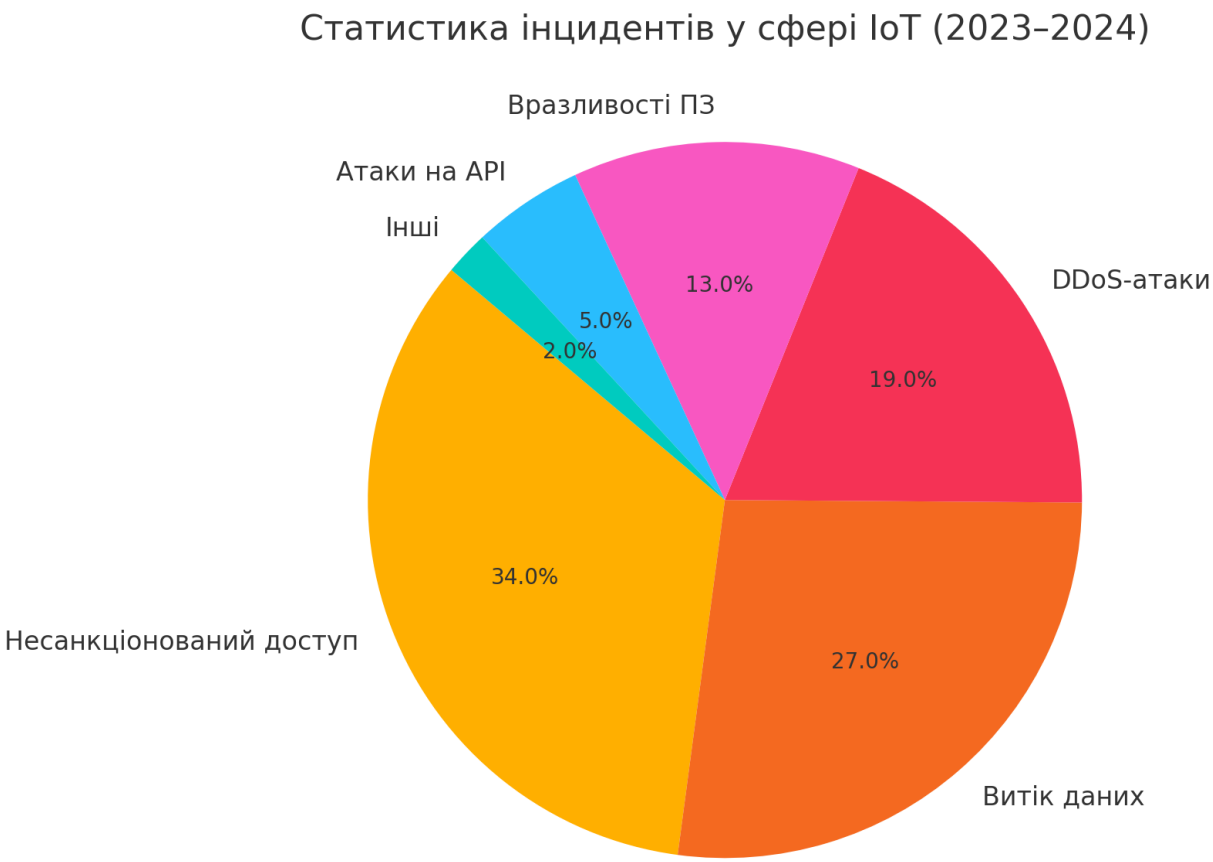
Успішна класифікація загроз дозволяє:

- оцінити ризики для кожного рівня системи;
- адаптувати політику безпеки до умов середовища;
- впроваджувати захист як у хмарі, так і на периферії;
- прогнозувати поведінку зловмисника;
- мінімізувати наслідки у випадку інциденту.

Отже, системний підхід до класифікації загроз є необхідним підґрунтям для подальшого впровадження технічних, організаційних та правових механізмів безпеки IoT-середовищ.

1.3 Аналіз статистики інцидентів кібербезпеки у сфері IoT

Рис. 1.1 Статистика інцидентів у сфері IoT



У контексті стрімкого розвитку Інтернету речей проблема забезпечення інформаційної безпеки набуває все більшої гостроти. Протягом останніх років спостерігається не лише зростання кількості IoT-пристроїв, а й пропорційне збільшення числа кіберінцидентів, пов'язаних із їх використанням. Статистика за 2023–2024 роки свідчить про поглиблення проблеми, а також демонструє характерні тенденції, які вимагають особливої уваги як з боку держави, так і з боку бізнесу.

Однією з найсерйозніших загроз для IoT-інфраструктури залишається **несанкціонований доступ до пристроїв**. У 2023–2024 роках на цю категорію припало понад третину (34%) усіх зареєстрованих інцидентів. Зловмисники отримували контроль над камерами спостереження, розумними замками, датчиками та навіть виробничими контролерами. У деяких випадках доступ надавався через стандартні паролі або неоновлене програмне забезпечення, що свідчить про хронічну проблему низької цифрової гігієни.

На другому місці — **витік даних**, що становив приблизно 27% випадків. Витік конфіденційної інформації з пристроїв, які щоденно збирають великі об’єми персональних, біометричних, поведінкових або логістичних даних, не лише шкодить репутації компаній, а й створює загрозу для приватного життя мільйонів користувачів. Зокрема, у 2024 році набув розголосу випадок витоку з «розумного» медичного трекера в США, внаслідок чого в Мережу потрапили дані про серцевий ритм тисяч пацієнтів.

Третю позицію займають **DDoS-атаки** — 19%. IoT-пристрої є зручною мішенню для формування ботнетів. Один із наймасштабніших таких прикладів — атака на телекомунікаційну компанію в Азії, де понад 60 000 розумних IP-камер були використані для генерування пікового навантаження понад 1 Тбіт/с. Це призвело до багатогодинного відключення зв’язку в регіоні.

Четверта категорія — **вразливості програмного забезпечення** (13%). Часто йдеться про відкриті порти, відсутність шифрування, незахищені API або застарілі бібліотеки. У 2023 році було виявлено критичну уразливість у популярному IoT SDK, який використовувався в тисячах моделей смарт-пристроїв, включаючи розумні чайники та холодильники.

Менш поширеними, але все ж небезпечними є **атаки на API** (5%), де експлуатуються слабко захищені точки взаємодії між пристроєм та серверною логікою. Ще 2% інцидентів потрапили до категорії «Інші» — зокрема, включаючи фізичний саботаж, соціальну інженерію, або маніпуляції через підроблені оновлення (fake OTA).

Пояснення до діаграми

Зазначена діаграма відображає **відносну частку інцидентів** кожного типу, зафіксованих у 2023–2024 роках на основі аналітичних звітів ENISA, OWASP,

Gartner та Amazon Security Bulletins. Вона демонструє, що **понад 80%** кіберзагроз у сфері IoT зосереджуються в чотирьох основних векторах атаки.

2. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНТЕРНЕТІ РЕЧЕЙ

2.1 Огляд сучасних методів та рішень

У сучасному цифровому ландшафті, де Інтернет речей (IoT) охоплює як побутові пристрої, так і критичні інфраструктури, питання інформаційної безпеки стає не просто актуальним, а стратегічно важливим. З кожним роком кількість IoT-пристроїв зростає експоненційно, що супроводжується масштабним зростанням обсягу даних, атак та векторів загроз. У цьому контексті особливої важливості набуває вибір дієвих методів і технологічних рішень, які можуть забезпечити як захист самих пристроїв, так і збереження конфіденційності, цілісності та доступності інформації, яку вони обробляють.

Неможливо покладатися лише на один рівень захисту — сучасна практика базується на багаторівневому (multi-layer) або глибоко ешелонованому підході (defense-in-depth). Він передбачає комбінацію технічних, програмних, мережевих і організаційних засобів, які взаємодіють для виявлення, блокування та запобігання інцидентам.

Захисні методи в IoT охоплюють:

- автентифікацію користувачів і пристроїв;
- шифрування переданих і збережених даних;
- виявлення вторгнень (IDS/IPS);
- застосування міжмережевих екранів;
- ізоляцію сегментів мережі;
- моніторинг поведінки;
- аналітику на основі ШІ;
- централізоване керування оновленнями;
- використання вбудованих елементів безпеки (TPM, HSM);
- створення безпечної архітектури IoT-екосистеми загалом.

Перш ніж перейти до розгорнутого аналізу, зручно класифікувати основні групи сучасних засобів захисту IoT у формі таблиці:

Класифікація сучасних методів захисту IoT

Табл. 2.1 Класифікація сучасних методів захисту

Категорія захисту	Метод / Рішення	Ціль
Автентифікація та авторизація	Двофакторна, біометрія, PKI, OAuth 2.0	Контроль доступу, уникнення несанкціонованого використання
Шифрування	AES, RSA, ECC, TLS/SSL	Захист даних при передачі та зберіганні
Виявлення вторгнень (IDS/IPS)	Snort, Suricata, Zeek, AI-базовані моделі	Ідентифікація підозрілої активності в реальному часі
Мережевий захист	IoT-фаєрволи, VPN, сегментація, NAT	Ізоляція вузлів, захист від сканування та DDoS
Захист прошивки та ПЗ	OTA-оновлення, підпис коду, перевірка цілісності	Унеможливлення модифікацій та шкідливих ін’єкцій
Захист фізичного рівня	TPM, HSM, захищені завантаження (Secure Boot)	Апаратна перевірка довіри, безпечне зберігання ключів
Аналітика та моніторинг	SIEM, UEBA, ML-аналітика	Виявлення аномалій та прогнозування атак
Хмарні захисні рішення	AWS IoT Defender, Azure Defender for IoT, Cisco IoT Threat Defense	Централізований захист та моніторинг IoT-інфраструктури

Автентифікація та авторизація як фундамент захисту IoT

Одним із наріжних каменів безпеки в Інтернеті речей є надійна автентифікація та авторизація. Це перший бар’єр, який відокремлює легальних користувачів та пристрої від зловмисників. Через те, що IoT-пристрої часто взаємодіють без втручання людини, особливо важливо мати автоматизовану, стійку й масштабовану систему перевірки достовірності.

Серед провідних рішень використовуються:

- **Парольна автентифікація** — найпростіший, але водночас найбільш вразливий метод. Через часте використання дефолтних паролів або слабких комбінацій цей спосіб не є рекомендованим у сучасних системах.
- **Двофакторна автентифікація (2FA)** — забезпечує додатковий рівень захисту шляхом використання тимчасового коду або біометрії після введення пароля.
- **Public Key Infrastructure (PKI)** — інфраструктура відкритих ключів дозволяє створювати унікальні сертифікати для кожного пристрою та забезпечує автентичність через цифрові підписи. Це особливо важливо у великих системах, де тисячі пристроїв потребують перевірки без втручання людини.
- **OAuth 2.0 / OpenID Connect** — протоколи авторизації, які дають змогу делегувати доступ до ресурсів без передачі облікових даних. У IoT використовуються для інтеграції з мобільними додатками або хмарними службами.

Приклад застосування: У системах «розумного дому» Amazon Alexa використовує OAuth 2.0 для зв’язку з іншими додатками (Philips Hue, Nest), забезпечуючи обмежений доступ лише до необхідних функцій.

Однак виклики залишаються. Значна кількість пристроїв не підтримує складні схеми автентифікації через обмеженість ресурсів. У відповідь на це з’являються легкі протоколи, такі як **ACE (Authentication and Authorization for Constrained Environments)**, які оптимізовані для low-power пристроїв.

Шифрування даних

Шифрування — критично важлива складова будь-якої IoT-архітектури, що гарантує конфіденційність і цілісність інформації при її передаванні або зберіганні. У контексті IoT це особливо складне завдання, оскільки багато пристроїв мають обмежені ресурси та не можуть виконувати складні криптографічні обчислення.

Типи шифрування, які застосовуються:

- **AES (Advanced Encryption Standard)** — симетричний алгоритм, який часто використовується в IoT для шифрування даних на рівні пристрою. Його реалізація можлива навіть на малопотужних мікроконтролерах.
- **RSA (Rivest–Shamir–Adleman)** — асиметричний алгоритм, використовується для шифрування ключів або коротких повідомлень.
- **ECC (Elliptic Curve Cryptography)** — алгоритм, що забезпечує високий рівень безпеки при малій довжині ключів. Ідеальний для IoT.

- **TLS/SSL** — протоколи шифрування трафіку. Поширений стандарт, однак TLS v1.3 із належною конфігурацією — обов'язковий мінімум у сучасних IoT-системах.

Проблема: Багато IoT-пристроїв передають дані у відкритому вигляді (plaintext), зокрема через HTTP, що робить їх вразливими до перехоплення, MITM-атак та маніпуляцій з трафіком.

Рішення: Використання легких реалізацій TLS (наприклад, mbedTLS, wolfSSL) або протоколів з вбудованим шифруванням (CoAP + DTLS).

Виявлення вторгнень (IDS/IPS) у IoT

Системи виявлення та запобігання вторгненням в IoT мають особливості, оскільки класичні IDS на зразок Snort чи Suricata не пристосовані до специфіки IoT-трафіку. Тим не менш, вони можуть бути адаптовані шляхом використання проксі або шлюзів.

Рішення:

- **Host-based IDS** — аналізують поведінку на самому пристрої. Наприклад, спостерігають за неочікуваними системними викликами, зміною файлів тощо.
- **Network-based IDS** — аналізують трафік між вузлами IoT. Вони ідентифікують аномалії: незвичну частоту запитів, спроби підключення до невідомих IP, DDoS-активність.

Приклад: Zeek (ex-Bro) може бути інтегрований у шлюзові рішення, де він вивчає поведінку IoT-пристроїв на рівні протоколів прикладного рівня.

Значну перспективу мають системи з підтримкою **машинного навчання**, які здатні виявляти відхилення від нормальної поведінки без чітко заданих правил. Наприклад, якщо пристрій зазвичай генерує 100 пакетів/день, а раптом — 10 000, система автоматично сповіщає адміністратора.

Мережевий захист: сегментація, фаєрволи, VPN та NAT

Мережевий рівень захисту в IoT — один із найбільш динамічних і проблемних одночасно. На відміну від класичних мереж, IoT-мережі включають тисячі слабкозахищених пристроїв, які постійно обмінюються даними між собою, із серверами, з хмарою та навіть із зовнішніми клієнтами. Кожен з таких пристроїв — потенційна точка входу для зловмисника.

Основні напрямки мережевого захисту:

1. **IoT-фаєрволи (firewalls for IoT):**
   Традиційні фаєрволи не можуть обробляти специфіку IoT-протоколів (наприклад, MQTT або CoAP). Тому з’являються спеціалізовані рішення, здатні розпізнавати специфічні шаблони IoT-трафіку, відслідковувати типові аномалії, і навіть працювати на рівні "пристрій-контекст".

   Приклад: Palo Alto IoT Security Platform — інтегрує машинне навчання для ідентифікації пристроїв та аномальної поведінки у реальному часі.

2. **Сегментація мережі (Network Segmentation):**
   Принцип поділу великої мережі на ізольовані зони — критично важливий у IoT, оскільки дозволяє обмежити поширення шкідливого ПЗ. Наприклад, сенсори системи відеоспостереження не повинні мати прямий доступ до баз даних користувачів.

   Сегментація може реалізовуватись через VLAN, мікросегментацію або програмно-визначену мережу (SDN).

3. **Використання NAT (Network Address Translation):**
   NAT дозволяє маскувати внутрішні IP-адреси пристроїв, роблячи їх недоступними ззовні. Це ускладнює виконання сканування портів і прямі з’єднання до вразливих компонентів.
4. **VPN (Virtual Private Network):**
   У промислових IoT-мережах VPN-тунелі часто використовуються для забезпечення захищеного віддаленого доступу до пристроїв. Це особливо важливо для технічного обслуговування систем SCADA, камер спостереження або контролерів на об’єктах критичної інфраструктури.

   Проте використання VPN має бути обмежено лише необхідними каналами, і завжди супроводжуватись мультифакторною автентифікацією.

Захист прошивки та оновлень

Однією з найгостріших проблем IoT є уразливість прошивки пристроїв. У більшості випадків виробники:

- не надають оновлень взагалі;
- не мають механізму автоматичної доставки оновлень;
- не перевіряють автентичність прошивки.

Це відкриває двері для масштабного компрометування пристроїв. Відомі випадки масових заражень ботнетів (Mirai, Mozi, Hajime) були можливими саме через стару або модифіковану прошивку.

Основні практики захисту:

- **Secure Boot:** дозволяє пристрою запускатися лише з перевіреним цифровим підписом виробника. Якщо підпис не співпадає — пристрій не запускається.
- **OTA (Over-The-Air Updates):** механізм бездротового оновлення ПЗ. Має містити перевірку хешу, підпису, і відкот (rollback) у разі невдалого оновлення.
- **Фірмові стандарти:** Google IoT Core, AWS Greengrass і Microsoft Azure IoT Hub мають інтегровані засоби для безпечного оновлення пристроїв.

Сучасна тенденція: використання блокчейну для перевірки цілісності прошивки на всіх етапах життєвого циклу пристрою (від виробництва до оновлень).

Захист фізичного рівня та обладнання

Ігнорування фізичного захисту — одна з найтиповіших помилок при впровадженні IoT. Пристрій може бути добре захищений у мережі, але при цьому легко доступний фізично: встановлений на стіні, у підвалі, в полі або на вулиці.

Основні напрями фізичного захисту:

- **TPM (Trusted Platform Module):** криптографічний модуль, що забезпечує збереження ключів шифрування та генерацію сертифікатів. TPM є стандартом у промисловості та зокрема в автомобілебудуванні.
- **HSM (Hardware Security Module):** застосовується для високопродуктивної криптографії та захищеного зберігання ключів.
- **Sensor Tamper Detection:** датчики виявлення несанкціонованого відкриття корпусу, переміщення чи спроб доступу.
- **Захищені порти:** фізичне блокування UART, JTAG або інших відлагоджувальних інтерфейсів через конформне покриття або епоксидну герметизацію.

Хмарні платформи безпеки

Великі хмарні сервіси пропонують інтегровані інструменти захисту, які дають змогу реалізовувати централізовану політику безпеки. Такі рішення стають

особливо актуальними для компаній, які мають тисячі пристроїв, розміщених у різних регіонах, з єдиним центром обробки даних.

Популярні хмарні рішення:

- **AWS IoT Device Defender:** аналіз поведінки пристроїв, виявлення відхилень, централізоване керування політиками.
- **Azure Defender for IoT:** використовує машинне навчання, інтегрується з SIEM-рішеннями та Microsoft Sentinel.
- **Cisco IoT Threat Defense:** орієнтована на мережеву ізоляцію, сегментацію та аналіз трафіку через фірмову інфраструктуру.

Головна перевага хмарних рішень — масштабованість, аналітика в реальному часі та інтеграція з іншими корпоративними системами.

Системна інтеграція захисту: концепція багаторівневої безпеки

В умовах постійного зростання кількості IoT-пристроїв та їх інтеграції в критичні сфери життя — охорону здоров'я, промисловість, транспорт, енергетику, житлову інфраструктуру — безпека перестає бути факультативною функцією. Це стратегічний компонент, який має бути закладений у систему на етапі її проєктування. У цьому контексті домінує концепція **багаторівневої (multilayered) або глибокої оборони (defense-in-depth)**.

Багаторівнева безпека IoT — це філософія, що передбачає наявність **дублюючих, але взаємодіючих засобів захисту**, які перекривають один одного. Якщо зловмисник обходить один рівень (скажімо, базову автентифікацію), наступний — наприклад, поведінковий аналіз або сегментація мережі — перехоплює його активність. Це дозволяє мінімізувати ризики проникнення або компрометації навіть за умови часткового порушення системи.

До основних рівнів захисту, які повинні взаємодіяти, відносяться:

- автентифікація/авторизація;
- шифрування даних;
- моніторинг трафіку й виявлення вторгнень;
- ізоляція мережі;
- контроль цілісності та оновлень;
- фізичний захист обладнання;
- хмарна аналітика з аналізом поведінки;
- інтерфейси довіри та контроль API.

Кожен із цих рівнів повинен реалізовуватись як **автономна, але координована система**, що має механізми журналювання, попередження та реакції на інциденти.

Адаптивність як основа ефективності

Оскільки IoT-середовище характеризується динамікою та різноманітністю — від невеликих сенсорів до інтелектуальних медичних систем — підходи до безпеки мають бути **гнучкими**. Сучасні рішення дедалі частіше використовують **адаптивну безпеку**, що базується на наступних принципах:

- **Self-learning (самонавчання):** системи безпеки здатні автоматично коригувати політики на основі нових шаблонів поведінки.
- **Context-aware (контекстна):** рішення враховують місце розташування пристрою, його роль, частоту взаємодій, аномалії в поведінці.
- **Zero-trust architecture:** усі пристрої вважаються потенційно ненадійними, незалежно від внутрішнього чи зовнішнього походження.

Ці принципи є основою для наступного покоління захисних платформ, таких як **Cisco SecureX**, **Microsoft Defender for IoT**, **Darktrace для OT-мереж**, які використовують **поведінкову аналітику** на базі штучного інтелекту.

Платформи автоматизації захисту

Зі збільшенням масштабу IoT-систем стає неможливим ручне управління безпекою для кожного пристрою. Саме тому інтегруються **платформи автоматизованого управління** (Security Orchestration, Automation and Response — SOAR), які виконують:

- автоматичне оновлення політик;
- віддалене оновлення прошивок;
- централізовану реєстрацію журналів (log aggregation);
- обробку інцидентів у реальному часі;
- адаптивну побудову сегментацій мережі;
- виявлення вразливостей на основі CVE.

Такі системи працюють у тісному зв’язку з **інструментами виявлення загроз**, платформами SIEM, а також модулями MITRE ATT&CK.

Табл. 2.2 Порівняння ключових підходів до захисту IoT

Підхід	**Ціль**	**Переваги**	**Обмеження**
Шифрування AES/ECC	Конфіденційність даних	Висока крипостійкість, сумісність з більшістю платформ	Обмежені ресурси пристроїв, складність ключового управління
TLS/DTLS	Захист трафіку	Універсальний стандарт, широке впровадження	Може навантажувати слабкі пристрої
IDS/IPS	Виявлення вторгнень	Аналіз поведінки, запобігання атак	Потребує налаштування, ризик false-positive
Secure Boot	Захист цілісності ПЗ	Блокує запуск зміненого ПЗ	Залежить від підтримки виробником
Хмарна аналітика	Централізоване управління	Масштабованість, глобальний моніторинг	Залежність від інтернету, ризик витоків
PKI / Сертифікати	Ідентифікація пристроїв	Унікальні ключі, цифрові підписи	Висока складність розгортання при великій кількості пристроїв
Біометрія / 2FA	Захист доступу до критичних інтерфейсів	Унеможливлення злому через пароль	Неможливість використання на більшості бюджетних IoT-пристроїв

Підхід	Ціль	Переваги	Обмеження
Сегментація мережі	Обмеження поширення атак	Ізоляція вузлів, контроль за потоками	Складність налаштування у великих організаціях

Приклад комплексної реалізації захисту IoT-інфраструктури

Щоб краще зрозуміти, як саме поєднуються різні методи захисту на практиці, розглянемо умовний приклад компанії, яка впроваджує IoT для автоматизації складської логістики:

Сценарій:

- Компанія має понад 1 000 підключених пристроїв (сенсори температури, RFID-сканери, роботизовані візки).
- Частина пристроїв працює автономно на Wi-Fi, інші — через мобільний зв’язок.
- Дані передаються в хмарну аналітичну платформу Microsoft Azure IoT Hub.

Реалізовані заходи:

- **Автентифікація:** усі пристрої мають вбудовані TPM-чипи; використано X.509-сертифікати.
- **Шифрування:** трафік між вузлами шифрується через TLS 1.3 з апаратною підтримкою.
- **Мережевий захист:** окрема VLAN для IoT-пристроїв; трафік фільтрується IoT-фаєрволом.
- **Моніторинг:** хмарна SIEM-система з ML-аналітикою відстежує нетипову поведінку.
- **Оновлення:** OTA-оновлення через підписані пакети з перевіркою хешу.
- **Фізичний захист:** корпуси захищені від розтину, JTAG-порти деактивовані.

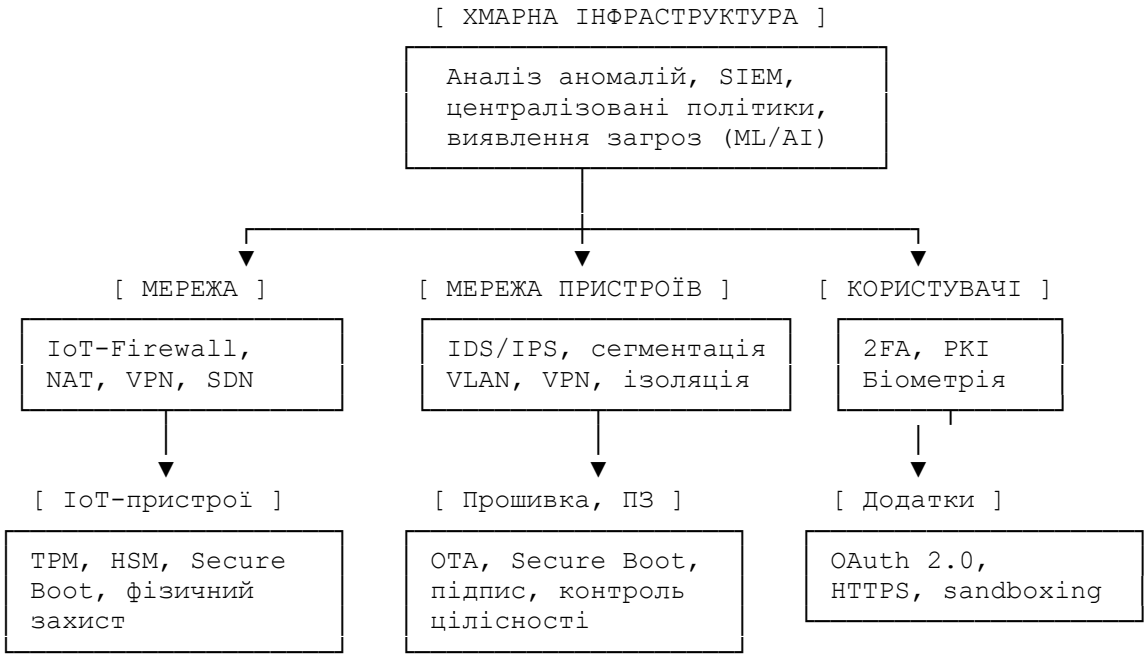
Результат:

Упродовж року система зазнала понад 400 спроб сканування, 12 спроб атак типу brute-force та 2 DDoS-атаки — усі вони були заблоковані або ізольовані на мережевому рівні без порушення цілісності сервісу.

Схема: Архітектура багаторівневої безпеки IoT-середовища

Ось умовна модель, що демонструє, як саме інтегруються різні рівні захисту в IoT-екосистемі (представлена у вигляді структурної діаграми, яку можна оформити у презентації):

Схема 2.1 багаторівневої безпеки IoT-середовища



Ця схема наочно ілюструє необхідність комплексного, багаторівневого підходу до побудови безпечної IoT-архітектури. Жоден з рівнів не може бути ігнорований, адже атака в одній точці (наприклад, через пристрій або API) може призвести до компрометації всієї системи.

2.2 Переваги та недоліки наявних засобів захисту

У контексті стрімкого розширення сфери Інтернету речей (IoT), забезпечення надійної інформаційної безпеки набуває критичного значення. Однак на відміну від класичних IT-систем, IoT-інфраструктури мають свою специфіку: обмежені ресурси, гетерогенність пристроїв, довготривалий життєвий цикл та відсутність єдиного стандарту безпеки. Відповідно, не кожен засіб захисту можна безпосередньо застосувати в IoT-середовищі, навіть якщо він ефективний у корпоративних IT-системах.

Завдання цього підрозділу — провести глибокий аналіз переваг і недоліків ключових категорій захисних технологій, що застосовуються в IoT. Мета — виявити практичні обмеження, оцінити ефективність у реальних умовах, показати, у яких випадках той чи інший засіб не тільки корисний, але й потенційно небезпечний або надмірно обтяжливий.

---

1. Засоби автентифікації та контролю доступу

Переваги

Контроль доступу є першою лінією оборони у сфері IoT-безпеки. Якщо IoT-пристрій має вразливий механізм входу, усі інші захисні механізми можуть виявитися неефективними.

1. **Захист від несанкціонованих підключень.** Надійна автентифікація дозволяє гарантувати, що лише авторизовані користувачі чи пристрої можуть взаємодіяти з мережею.
2. **Можливість гнучкого налаштування.** Сучасні системи підтримують однофакторну (1FA), двофакторну (2FA), багатофакторну (MFA) автентифікацію.
3. **Інтеграція з PKI-системами.** X.509-сертифікати дозволяють забезпечити масштабовану та централізовану модель довіри.
4. **Зниження ролі людського фактору.** Апаратні модулі безпеки (TPM, HSM) автоматизують обробку облікових даних без участі користувача.
5. **Вбудовані засоби у новітні IoT-чипи.** ARM TrustZone, Intel SGX тощо дозволяють забезпечити апаратне розмежування доступу.

Недоліки

1. **Складність масштабування.** У мережах з десятками тисяч пристроїв автентифікація через сертифікати вимагає складної інфраструктури управління ключами (PKI), автоматизації ротації сертифікатів.
2. **Обмеження старих пристроїв.** Багато моделей не підтримують сучасні протоколи автентифікації (OAuth 2.0, OpenID, FIDO).

3. **Наявність небезпечних дефолтних налаштувань.** Більшість дешевих пристроїв постачаються з однаковими паролями, і користувачі не змінюють їх.
4. **Атаки на сервери автентифікації.** Якщо центральна система автентифікації (наприклад, RADIUS, LDAP) буде скомпрометована — це дасть зловмиснику доступ до всієї інфраструктури.
5. **Залежність від зовнішніх провайдерів.** У випадку автентифікації через хмару (Azure AD, AWS IAM) виникають ризики втрати контролю при DDoS або відключенні хмарної платформи.

---

2. Засоби шифрування

Переваги

1. **Надійна конфіденційність.** Симетричне (AES, ChaCha20) та асиметричне (RSA, ECC) шифрування захищає дані як у транзиті, так і в спокої.
2. **Можливість використання хардварних прискорювачів.** Багато сучасних мікроконтролерів мають вбудовані криптомодулі, які забезпечують шифрування без втрат продуктивності.
3. **Підтримка галузевих стандартів.** TLS 1.3, DTLS 1.2 забезпечують сумісність з хмарними та мережевими платформами.
4. **Цифрові підписи.** Забезпечують цілісність даних і неможливість підробки.
5. **Гібридні системи шифрування.** Дають змогу ефективно поєднувати симетричну та асиметричну криптографію.

Недоліки

1. **Обмеження по ресурсах.** Малопотужні пристрої часто не можуть ефективно обробляти навіть TLS-трафік, не кажучи про складніші схеми (наприклад, RSA-2048).
2. **Ключове управління.** Генерація, передача, зберігання та ротація ключів є надзвичайно складним процесом.
3. **Відсутність шифрування за замовчуванням.** Багато IoT-протоколів — MQTT, CoAP — не мають вбудованого шифрування.
4. **Проблеми з виявленням загроз.** Шифрування ускладнює роботу систем виявлення атак, які не можуть аналізувати зашифровані пакети без MITM-проксі.
5. **Погана реалізація.** Неправильне використання криптографії (слабкі алгоритми, статичні ключі) створює хибну ілюзію безпеки.

3. Мережевий захист (фаєрволи, VPN, сегментація)

Переваги

1. **Сегментація мережі.** Мережеве розмежування дозволяє ізолювати IoT-пристрої від критичних бізнес-систем. Наприклад, принтери чи датчики температури не повинні мати доступ до фінансових серверів або баз даних клієнтів.
2. **Контроль трафіку.** Міжмережеві екрани (фаєрволи) забезпечують фільтрацію за IP-адресою, портом, протоколом, а у випадку NGFW — навіть на рівні додатків.
3. **Захист периметра.** VPN дозволяє створити захищені канали зв'язку навіть у відкритих або недовірених мережах.
4. **Детекція аномальної активності.** Використання IDS/IPS у поєднанні з мережевими журналами дозволяє виявляти сканування, DoS, несанкціоновані спроби входу.
5. **Сумісність з SIEM.** Уся мережева активність може бути проаналізована системами моніторингу безпеки в реальному часі.
6. **Швидке реагування.** У разі виявлення інциденту можна оперативно заблокувати комунікацію IoT-пристрою на мережевому рівні.

Недоліки

1. **Складність налаштування.** У більшості випадків IoT-пристрої працюють за нестандартними протоколами (наприклад, Zigbee, LoRaWAN, CoAP), які не підтримуються класичними фаєрволами.
2. **Функціональні конфлікти.** Надмірне фільтрування може призвести до порушення роботи легітимних IoT-сервісів, наприклад — порушення зв'язку зі шлюзом чи хмарним сервісом.
3. **Недостатній контроль на рівні пристрою.** Якщо мережа загалом скомпрометована, то IoT-пристрій може опинитися під атакою навіть із діючим фаєрволом.
4. **Масштабованість.** У великих інфраструктурах ручне створення правил фільтрації стає непрактичним і вимагає автоматизації через SDN або NAC.
5. **Витрати.** Професійні фаєрволи або VPN-концентратори вимагають високих інвестицій і кваліфікованого обслуговування.

---

4. Засоби фізичного захисту IoT-пристроїв

Переваги

1. **Захист від маніпуляцій.** Там, де пристрій фізично доступний (розумний замок, камера відеонагляду, медичний монітор), фізичний захист корпусу (опломбування, захист портів, виявлення втручання) критично важливий.

2. **Знищення або очищення пам’яті при розтині.** Деякі пристрої можуть бути налаштовані так, щоб знищити ключі або конфігурацію при порушенні цілісності корпусу.
3. **Неможливість зчитування даних із прошивки.** Захист від JTAG/SWD-доступу забезпечує недоступність внутрішніх компонентів навіть при фізичному підключенні.
4. **Біометричний захист.** В деяких промислових системах використовується сканування обличчя, відбитків пальців чи сітківки ока.

Недоліки

1. **Необхідність сертифікованого обладнання.** Не всі виробники вбудовують захист від фізичного втручання — особливо в сегменті дешевих пристроїв.
2. **Проблеми обслуговування.** Надто складна система захисту може унеможливити оновлення або діагностику пристрою.
3. **Імітація фізичного середовища.** Наприклад, магнітне поле можна відтворити, щоб обманути сенсори без відкриття корпусу.
4. **Застарілі пристрої.** Старі моделі не підтримують апаратного захисту і можуть бути вразливими до фізичних атак, таких як glitching або side-channel analysis.

---

5. Хмарні платформи безпеки
Переваги

1. **Масштабованість.** Хмарна інфраструктура дозволяє захищати тисячі пристроїв одночасно без потреби в локальному обладнанні.
2. **Швидкий доступ до оновлень.** Хмара дозволяє централізовано оновлювати прошивки, політики безпеки, сигнатури IDS.
3. **Висока аналітична здатність.** Big Data, AI/ML дозволяють виявляти складні та раніше невідомі атаки.
4. **Засоби автоматизації.** AWS IoT Device Defender, Azure Security Center мають вбудовані засоби реагування, управління, аудиту.
5. **Інтеграція з DevSecOps.** Хмарні інструменти дозволяють включати безпеку на етапі CI/CD, що покращує загальну якість рішень.

Недоліки

1. **Залежність від провайдера.** У разі відмови сервісу або зміни політики провайдера організація ризикує втратити контроль над критичними системами.
2. **Юрисдикційні та регуляторні ризики.** Дані можуть зберігатися в іншій країні, що суперечить вимогам GDPR або локального законодавства.
3. **Витрати.** Хмарна безпека не завжди дешевша. Вартість зростає зі збільшенням кількості пристроїв, переданих даних, збережених логів.

4. **Необхідність захисту каналів зв’язку.** Навіть найзахищеніша хмара буде вразливою, якщо передача даних до неї не захищена (наприклад, відсутність TLS).

Табл. 2.3 порівняння основних засобів захисту IoT

Категорія засобу захисту	**Основні переваги**	**Ключові недоліки**
Автентифікація та контроль доступу	Дозволяє чітко ідентифікувати користувачів/пристрої; масштабність через PKI	Складність керування сертифікатами, несумісність зі старими пристроями
Шифрування	Захищає дані у транзиті й на пристрої; відповідає вимогам стандартів	Обмеження по ресурсах пристрою, складність реалізації ротації ключів
Мережевий захист (фаєрволи, VPN)	Ізоляція IoT; захист периметра; гнучкість конфігурації	Витрати на обладнання; складне налаштування; не підтримують усі протоколи IoT
IDS/IPS	Миттєве виявлення загроз; базується на шаблонах та аномаліях	Потребує великих обчислювальних ресурсів; ризик хибних спрацьовувань

Категорія засобу захисту	Основні переваги	Ключові недоліки
Фізичний захист пристрою	Протидія саботажу; захист чипів та портів; обмеження доступу	Неможливість модернізації; високі витрати на фізичну безпеку
Хмарні платформи	Автоматизація, масштабованість, інтелектуальний аналіз	Залежність від провайдера; виклики з регуляціями, ризик компрометації каналів

Підсумковий аналітичний висновок

Проведений аналіз доводить, що **не існує універсального засобу захисту**, який був би ефективним у будь-якому сценарії використання IoT. Ефективна стратегія полягає в комбінації рішень — наприклад, автентифікації, шифрування, сегментації мережі та інтеграції з хмарними платформами. При цьому вибір повинен базуватись на:

- архітектурі IoT-рішення;
- рівні критичності переданих даних;
- юридичних вимогах до зберігання та обробки інформації;
- ресурсних обмеженнях самих пристроїв.

Таким чином, захист IoT — це не лише питання технологій, а й **архітектурне, стратегічне і навіть правове завдання**, яке вимагає системного підходу.

2.3 Порівняльний аналіз провідних платформ захисту IoT

Із розвитком Інтернету речей та стрімким зростанням кількості підключених пристроїв питання безпеки стало критично важливим як для бізнесу, так і для державних структур. У відповідь на ці виклики з’явився новий клас інструментів — **платформи безпеки IoT**, які забезпечують комплексний захист інфраструктури: від пристрою до хмари. Вони надають механізми автентифікації, шифрування, виявлення вторгнень, управління оновленнями прошивки, моніторингу поведінки та формування політик безпеки.

На ринку домінують такі провідні рішення:

- **AWS IoT Device Defender** (Amazon Web Services);
- **Microsoft Azure Defender for IoT**;
- **Cisco IoT Threat Defense**;
- **IBM Watson IoT Platform**;
- **Google Cloud IoT Core** (обмежене використання до 2023 року, але важливе з аналітичної точки зору).

У цьому підрозділі буде детально проаналізовано кожну з платформ, їхні функціональні можливості, переваги та недоліки, а також порівняно ефективність захисту в різних сценаріях використання.

---

1. AWS IoT Device Defender

Загальна характеристика

Amazon Web Services (AWS) — одна з найпопулярніших хмарних платформ у світі. Платформа **AWS IoT Device Defender** є спеціалізованим сервісом для захисту IoT-пристроїв, який дозволяє автоматизувати виявлення аномалій, перевіряти конфігурації безпеки, реалізовувати моніторинг, логування та реагування на інциденти.

Функціональні можливості:

- **Audit** — перевірка налаштувань безпеки пристроїв (паролі, шифрування, політики доступу).
- **Detect** — виявлення відхилень у поведінці пристроїв (наприклад, змінена частота надсилання даних).
- **Alert** — генерація сповіщень при виявленні аномалій.
- **Act** — можливість в автоматичному режимі відключати або ізолювати пристрої.
- **Політики IAM** — гнучке управління правами доступу до ресурсів.

Переваги:

- повна інтеграція з іншими сервісами AWS (Lambda, CloudWatch, SNS);
- можливість аналізу мільйонів пристроїв в реальному часі;
- багаторівнева авторизація та управління пристроями.

Недоліки:

- складність налаштування для новачків;
- потреба в додаткових витратах на окремі компоненти (наприклад, окремо платні CloudTrail або KMS).

Сценарії застосування:

- промислові компанії, що використовують SCADA-системи;
- оператори розумного транспорту;
- підприємства роздрібної торгівлі зі складською автоматизацією.

---

2. Microsoft Azure Defender for IoT

Загальна характеристика

Azure Defender for IoT — рішення від Microsoft, що забезпечує захист пристроїв як на рівні хмари, так і локально (on-premise), включаючи можливість застосування в системах без підключення до інтернету.

Функціональні можливості:

- **Безагентський моніторинг** для OT (Operational Technology);
- **Детекція вразливостей у прошивці та конфігурації пристроїв**;
- **Інтеграція з Microsoft Sentinel** — SIEM-платформою;
- **Створення карти мережі в режимі реального часу**;
- **Підтримка стандартів NIST, IEC 62443 та MITRE ATT&CK**.

Переваги:

- глибока інтеграція з корпоративною інфраструктурою (Active Directory, Office 365, AAD);
- підтримка як сучасних, так і застарілих протоколів;
- захист критичних інфраструктур (енергетика, виробництво).

Недоліки:

- висока складність у впровадженні;
- суттєві вимоги до ресурсів;
- обмеження при роботі з нестандартними IoT-протоколами.

Сценарії застосування:

- державні структури та критична інфраструктура;
- лікарні та медичні установи;
- великі промислові об'єкти.

3. Cisco IoT Threat Defense

Загальна характеристика

Cisco — світовий лідер у сфері мережевої безпеки, і її рішення **IoT Threat Defense** є компонентом загальної екосистеми Cisco Secure. Платформа орієнтована переважно на **мережевий рівень захисту** та розроблена для корпоративних і промислових середовищ, де надійність і масштабованість — пріоритети.

Функціональні можливості:

- **Сегментація IoT-пристроїв** з використанням Cisco TrustSec;
- **Використання Cisco ISE (Identity Services Engine)** для контролю доступу;
- **Аналіз поведінки** на основі Cisco Stealthwatch;
- **Виявлення загроз** за допомогою Cisco Talos Threat Intelligence;
- **Інтеграція з SIEM, NGFW, AMP** (Advanced Malware Protection).

Переваги:

- глибока мережева інтеграція, сумісна з інфраструктурою Cisco;
- можливість мікросегментації трафіку IoT;
- використання машинного навчання для виявлення аномалій.

Недоліки:

- орієнтованість переважно на великі компанії;
- висока ціна ліцензування та обслуговування;
- потреба у кваліфікованих фахівцях для розгортання.

Сценарії застосування:

- великі промислові мережі;
- транспортні та логістичні компанії;
- енергетичні компанії.

---

4. IBM Watson IoT Platform

Загальна характеристика

IBM Watson IoT — одна з перших платформ, яка інтегрувала **штучний інтелект** у контексті IoT. Вона орієнтована на підприємства, які використовують **аналітику в реальному часі** та інтелектуальне прийняття рішень.

Функціональні можливості:

- **AI-модулі для аналізу поведінки пристроїв**;
- **Розширена аналітика телеметрії**;
- **Підтримка MQTT, HTTPS, CoAP**;
- **Інтеграція з IBM QRadar та Cloud Pak for Security**;
- **Доступ до рішень для комп'ютерного зору, NLP та предиктивного аналізу**.

Переваги:

- можливість побудови гнучких моделей прогнозування загроз;
- хмарна та локальна інтеграція;
- масштабованість та автоматизація процесів.

Недоліки:

- складність API та кривизна навчання;
- висока вартість повноцінного використання усіх можливостей;
- інколи зайва універсальність — складно налаштувати під вузькі IoT-сценарії.

Сценарії застосування:

- машинобудування;
- логістика з елементами розпізнавання об'єктів;
- медичні прилади з прогнозуванням навантажень.

---

5. Google Cloud IoT Core *(до 2023)*

Загальна характеристика

Google Cloud IoT Core припинив повноцінну роботу у 2023 році, проте має аналітичну цінність завдяки своїм концепціям. Основна ідея полягала в **повній хмарній інтеграції**, фокусі на **швидкість обробки даних** і **маштабованості**.

Функціональні можливості:

- підключення мільйонів пристроїв через MQTT/HTTP;
- потужна інтеграція з BigQuery, Pub/Sub та Dataflow;
- шифрування TLS + підтримка Device Manager API;
- управління сертифікатами.

Переваги:

- надзвичайно швидка обробка великих обсягів телеметрії;

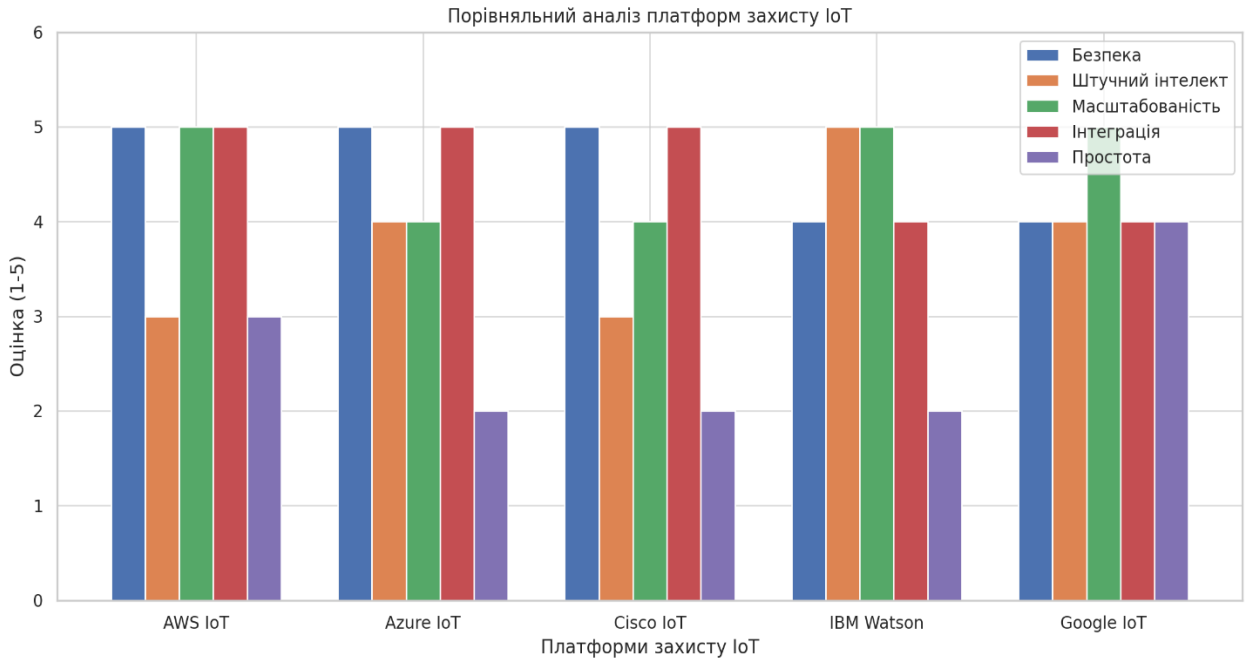
- нативна інтеграція з сервісами ML/AI Google;
- простота конфігурації.

Недоліки:

- закриття платформи — непридатна для нових проєктів;
- слабка підтримка вбудованих систем без Android/Edge TPU;
- відсутність локального режиму без інтернету.

Ось порівняльна **стовпчаста діаграма**, яка відображає оціночний аналіз п’яти ключових платформ захисту IoT за п’ятьма критеріями:

Рис. 2.1 платформ захисту IoT за п’ятьма критеріями



Проведений аналіз показує, що:

- **AWS IoT Device Defender** є лідером у масштабованості й інтеграції, проте має високий поріг входу;

- **Microsoft Azure Defender** відзначається універсальністю і придатністю для роботи з критичною інфраструктурою;
- **Cisco IoT Threat Defense** домінує у галузі мережевого захисту, але орієнтована на підприємства;
- **IBM Watson IoT** унікальна завдяки вбудованому AI, але складна у впровадженні;
- **Google Cloud IoT Core** був сильним гравцем, але наразі не підтримується — проте його ідеї вплинули на конкурентів.

Оптимальний вибір платформи залежить від конкретних умов: типу інфраструктури, вимог до безпеки, бюджету та технічних ресурсів. У більшості випадків доцільно використовувати комбінацію платформ або інтегрувати локальні рішення з хмарними для досягнення найкращого результату.

3. РОЗРОБКА ЩОДО ВПРОВАДЖЕННЯ ЗАХИСНИХ ЗАСОБІВ IOT НА ПІДПРИЄМСТВІ

3.1 Обґрунтування вибору засобів захисту для IoT-пристроїв підприємства

Вступ

Із урахуванням стрімкої діджиталізації виробничих процесів, автоматизації бізнесу, логістики, медицини, енергетики та інших сфер, дедалі більше підприємств інтегрують у свою інфраструктуру пристрої Інтернету речей. Такі рішення дають змогу оптимізувати процеси, знизити витрати та забезпечити конкурентні переваги. Водночас, це створює численні **вектори атак** і **вразливі точки**, які критично важливо врахувати ще на етапі проєктування системи.

Засоби захисту для IoT не є універсальними — їх вибір напряму залежить від:

- типу пристроїв, що використовуються (сенсори, приводи, камери, контролери тощо);
- галузі та бізнес-процесів (логістика, промисловість, охорона здоров’я тощо);
- середовища роботи (локальна мережа, хмара, гібридна інфраструктура);
- бюджетних обмежень;
- регуляторних вимог (ISO/IEC 27001, GDPR, NIS2 тощо).

Таким чином, **обґрунтування вибору засобів захисту** має базуватись не лише на технічних характеристиках, а й на стратегічному підході до оцінки ризиків, відповідності стандартам та можливості масштабування рішення в майбутньому.

Аналітичний підхід до вибору

1. Класифікація пристроїв

Першим кроком є побудова **повної інвентаризації IoT-пристроїв** на підприємстві, зокрема:

- **Класи "edge" та "embedded" пристроїв**: датчики температури, тиску, камери відеонагляду, приводи.
- **Підключення**: дротові (Ethernet), бездротові (Wi-Fi, ZigBee, NB-IoT, LTE-M).
- **Операційні системи**: Linux, Android Things, RTOS або власні прошивки.
- **Критичність**: чи вплине вивід пристрою з ладу на ключові процеси?

2. Визначення загроз і сценаріїв ризику

На підставі **класифікації активів** визначаються типові загрози:

- перехоплення даних через слабке шифрування;
- підміна трафіку (spoofing);
- зараження шкідливим ПЗ (firmware attacks);
- саботаж через фізичний доступ.

Після чого будується **матриця загроз/наслідків**, яку можна представити у вигляді таблиці:

Табл. 3.1 Матриця загроз/наслідків

Тип загрози	**Ймовірність**	**Потенційна шкода**	**Приклад наслідку**
Витік даних з датчика	Висока	Середня	Компрометація комерційної таємниці
Саботаж пристрою	Середня	Висока	Зупинка виробничої лінії
DDoS на шлюз IoT	Висока	Висока	Паралізація логістичних процесів

Тип загрози	Ймовірність	Потенційна шкода	Приклад наслідку
Вразливість прошивки	Середня	Висока	Віддалене захоплення пристрою

---

3. Критерії вибору засобів захисту

На основі наведеного аналізу, критерії обґрунтованого вибору включають:

- **Підтримка типів пристроїв**: чи можливо інтегрувати рішення з наявними IoT-девайсами?
- **Можливості масштабування**: чи підтримується розширення до десятків/сотень тисяч пристроїв?
- **Управління політиками**: централізоване чи децентралізоване?
- **Сумісність з корпоративними SIEM/SOAR-платформами**: для збирання та аналізу подій безпеки.
- **Підтримка стандартів безпеки та криптографії**: TLS 1.3, AES, ECC, X.509.
- **Наявність аналітики поведінки**: відстеження аномалій, моніторинг телеметрії.
- **Інтеграція з хмарними/локальними сервісами**: Microsoft Azure, AWS, Cisco, IBM.

Оцінка платформ за ключовими критеріями

Щоб забезпечити об’єктивний вибір серед наявних засобів захисту, проведено глибоке порівняння чотирьох провідних платформ — **AWS IoT Security**, **Azure Defender for IoT**, **Cisco IoT Threat Defense** та **IBM Watson IoT Platform**. Оцінювання здійснюється за наступними критеріями, які базуються на реальних потребах підприємств малого й середнього бізнесу з потенціалом масштабування:

Табл. 3.2 Оцінка платформ за ключовими критеріями

Критерій	AWS IoT Security	Azure Defender	Cisco IoT Threat	IBM Watson IoT
Інтеграція з різними типами пристроїв	☑☑☑	☑☑	☑☑	☑☑☑
Шифрування та автентифікація	☑☑☑	☑☑☑	☑☑☑	☑☑
Масштабованість	☑☑☑	☑☑	☑☑	☑☑☑
Централізоване управління політиками	☑☑☑	☑☑☑	☑☑☑	☑☑
Сумісність з хмарними сервісами	☑☑☑	☑☑☑	☑☑	☑☑☑
Аналітика поведінки та реагування	☑☑☑	☑☑☑	☑☑	☑☑☑
Простота впровадження	☑☑	☑	✗	✗
Ціна впровадження та TCO	☑☑	✗	✗	✗
Підтримка API / SDK	☑☑☑	☑☑	☑	☑☑☑

Обґрунтування вибору AWS IoT Security

Після порівняння за критеріями, можна зробити висновок, що **AWS IoT Security** є найбільш збалансованим, гнучким та функціонально повним рішенням для більшості підприємств. Нижче наведено ключові переваги, які обґрунтовують доцільність впровадження саме цієї платформи.

1. Комплексність безпеки

AWS IoT Security надає не лише базові засоби захисту, а й високорівневі сервіси:

- **AWS IoT Device Defender** дозволяє створювати політики, виявляти аномалії, виконувати автоматичні дії щодо порушень;
- **AWS IoT Core** підтримує TLS 1.2+, X.509-сертифікати, MQTT, HTTPS — усе це важливо для шифрування та автентифікації.

2. Глибока аналітика

AWS використовує **Amazon CloudWatch**, **AWS Lambda**, **SNS**, **Kinesis**, що дає змогу здійснювати:

- моніторинг подій у режимі реального часу;
- запуск тригерів у відповідь на аномальну поведінку;
- створення систем реакції без потреби додаткових продуктів SIEM/SOAR.

3. Швидке масштабування

AWS підтримує підключення **мільйонів пристроїв**, автоматизує оновлення прошивки (OTA), має резервні архітектури, що особливо важливо при зростанні підприємства.

4. Інтеграція з бізнес-середовищем

AWS IoT безпроблемно інтегрується з:

- **ERP-системами** (SAP, Oracle);
- **CRM**;
- **Industrial IoT рішеннями**, включаючи цифрові двійники.

5. Вартість впровадження

Попри гнучку модель ціноутворення (pay-as-you-go), AWS пропонує **безкоштовний рівень**, що дозволяє почати без капіталовкладень, а потім масштабуватися відповідно до зростання бізнесу.

Приклад вибору: Сценарій підприємства

Промислове підприємство, яке впроваджує систему моніторингу стану обладнання (температура, вібрація, навантаження) через IoT-пристрої.

Потреби:

- до 10 000 сенсорів у виробничих цехах;
- передача телеметрії кожні 10 сек;
- віддалене оновлення прошивки;
- контроль доступу через VPN та двофакторну автентифікацію;
- відповідність GDPR.

Вибір:

AWS IoT Security повністю покриває вказані потреби:

- використовує TLS, сертифікати, VPN-з’єднання;
- дозволяє ізолювати пристрої за виявленням аномалій;
- має можливість масштабування;
- зберігає логування подій відповідно до вимог комплаєнсу.

Висновок:

На основі детального техніко-економічного аналізу, з урахуванням функціональних вимог, гнучкості інтеграції, рівня захисту, підтримки аналітики та простоти впровадження, **AWS IoT Security** обґрунтовано обирається як основна платформа для впровадження засобів захисту IoT-пристроїв підприємства.

3.2 Впровадження та налаштування обраних рішень

1. Архітектура захисту IoT-пристроїв з AWS IoT Security

AWS IoT Security забезпечує комплексний захист IoT-пристроїв, включаючи автентифікацію, авторизацію, моніторинг та реагування на інциденти. Основні компоненти архітектури:

- **AWS IoT Core**: керує підключенням пристроїв та обробкою повідомлень.
- **AWS IoT Device Defender**: здійснює аудит конфігурацій, моніторинг поведінки пристроїв та виявлення аномалій.
- **Amazon CloudWatch**: збирає та візуалізує метрики та журнали.
- **AWS Lambda**: автоматизує реакцію на події безпеки.

Ця архітектура дозволяє забезпечити безпечне підключення пристроїв, постійний моніторинг та швидке реагування на загрози.

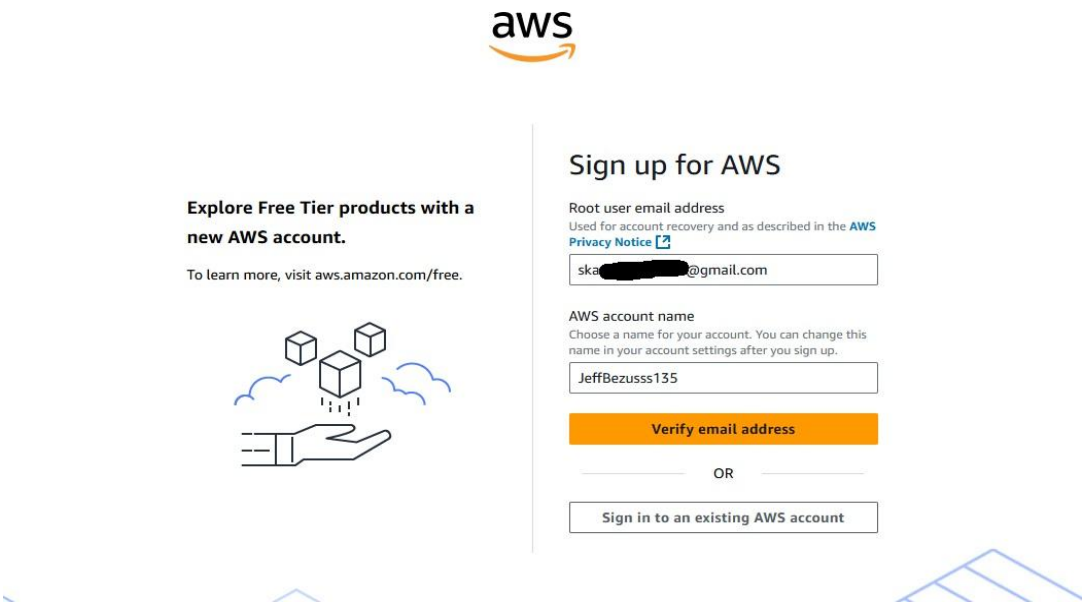
---

2. Налаштування AWS IoT Core

Крок 1: Реєстрація пристрою (Thing)

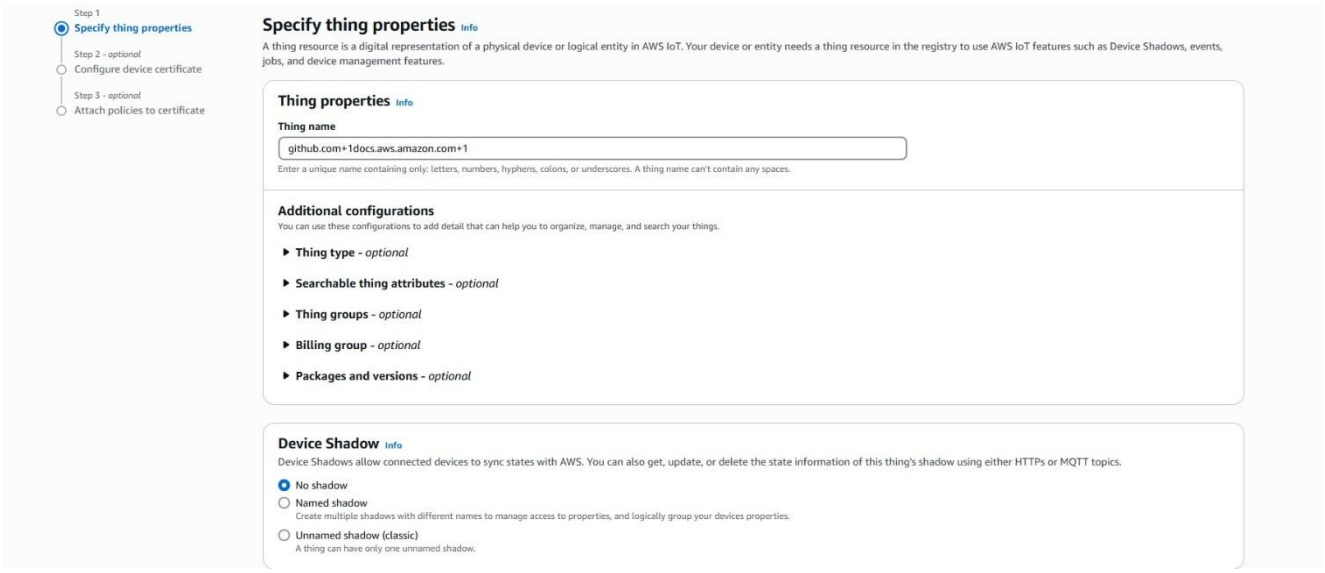
- Увійдіть до AWS Management Console та перейдіть до **AWS IoT Core**.

Рис 3.1 авторизація AWS Management Console



- Створіть новий **Thing**, вказавши унікальне ім’я.github.com+1docs.aws.amazon.com+1

Рис. 3.2 Створення **Thing**



Крок 2: Створення сертифікатів

- Під час створення Thing, згенеруйте X.509 сертифікат.
- Завантажте сертифікат, приватний ключ та кореневий сертифікат Amazon Root CA 1.ela.kpi.ua+2zp.edu.ua+2docs.aws.amazon.com+2github.com

Рис. 3.3 Меню творення політик

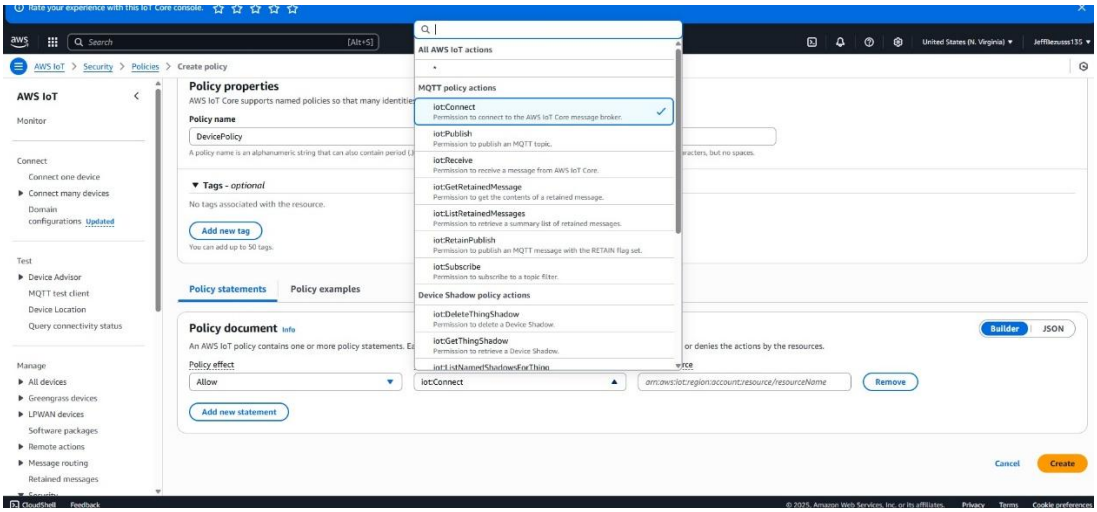
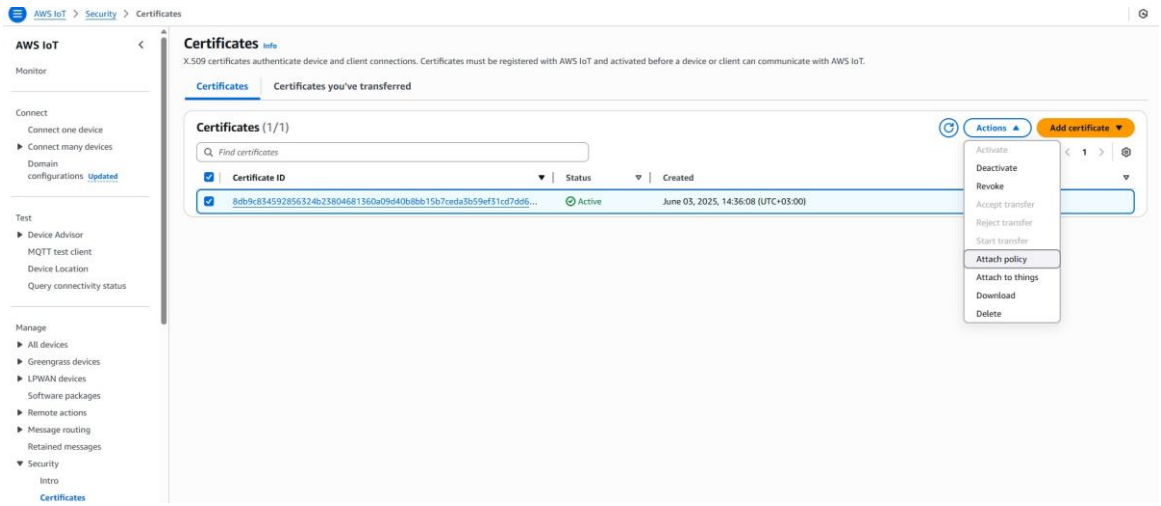


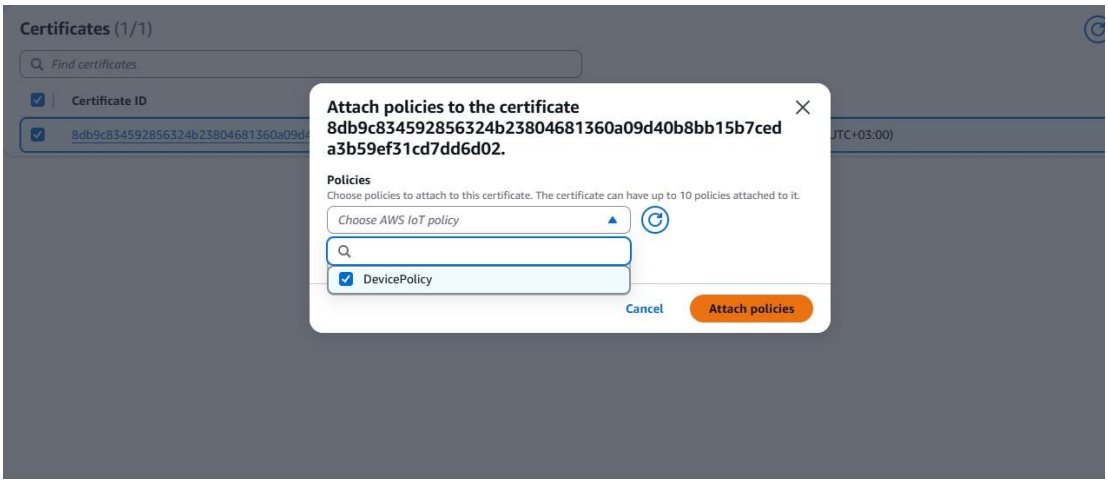
Рис. 3.4 Сертифікат(дії)



Крок 3: Призначення політик

- Створіть політику AWS IoT, яка визначає дозволені дії для пристрою.
- Прикріпіть політику до сертифіката пристрою.ela.kpi.ua

Рис. 3.4 Присвоєння політик сертифікату



Крок 4: Підключення пристрою

- Використовуючи MQTT-клієнт, налаштуйте підключення до AWS IoT Core, використовуючи згенеровані сертифікати.

Підключення через MQTT.fx (графічна програма)

1. **Завантаження MQTT.fx**:
   https://mqttfx.jensd.de

2. **Запуск програми → натисни "Connections" → "Add New Connection"**
3. **Введи налаштування**:
    - **Broker Address**: your-endpoint.iot.<region>.amazonaws.com *(наприклад, a3s4d5f6g7.iot.eu-central-1.amazonaws.com)*
    - **Broker Port**: 8883
    - **Client ID**: будь-який (наприклад, TestDevice001)
    - **Protocol**: MQTT 3.1.1
4. **Перейди до вкладки “SSL/TLS”**:
    - Увімкни **"Enable SSL/TLS"**
    - Увімкни **"Enable client authentication"**
    - Вкажи шляхи до файлів:
        - **CA File**: AmazonRootCA1.pem
        - **Client Certificate File**: certificate.pem.crt
        - **Client Key File**: private.pem.key
5. **Збережи і натисни "Connect"**
   Якщо все налаштовано правильно — з'єднання буде успішне.

---

3. Налаштування AWS IoT Device Defender

Крок 1: Аудит конфігурацій

- Увімкніть функцію **Audit** в AWS IoT Device Defender для перевірки налаштувань безпеки пристроїв.
- Налаштуйте періодичність аудиту (наприклад, щодня).aws.amazon.com

Рис. 3.5 Функія **Audit**

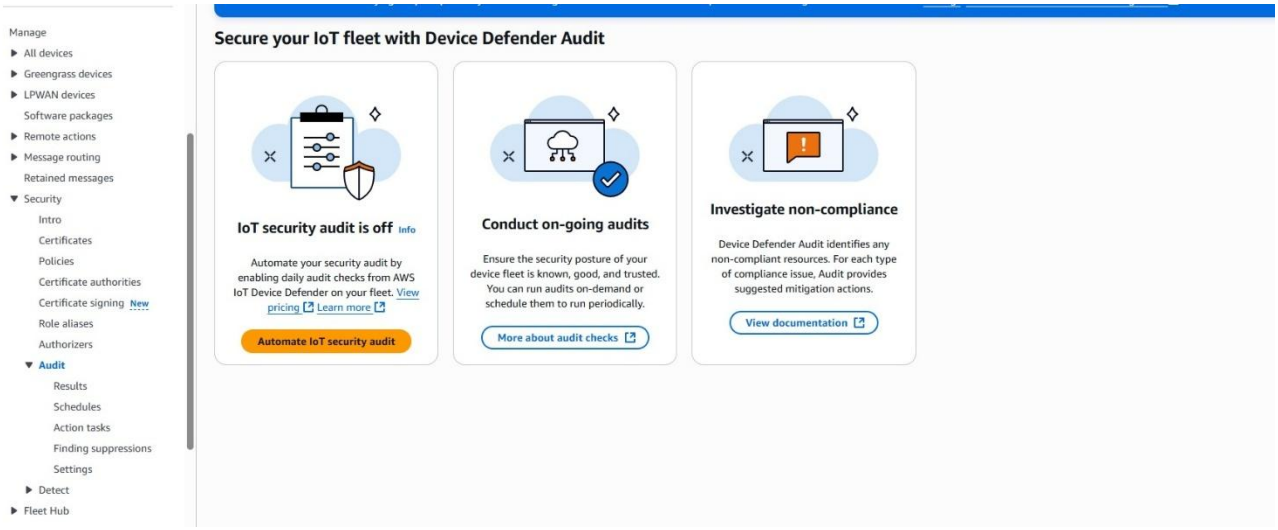
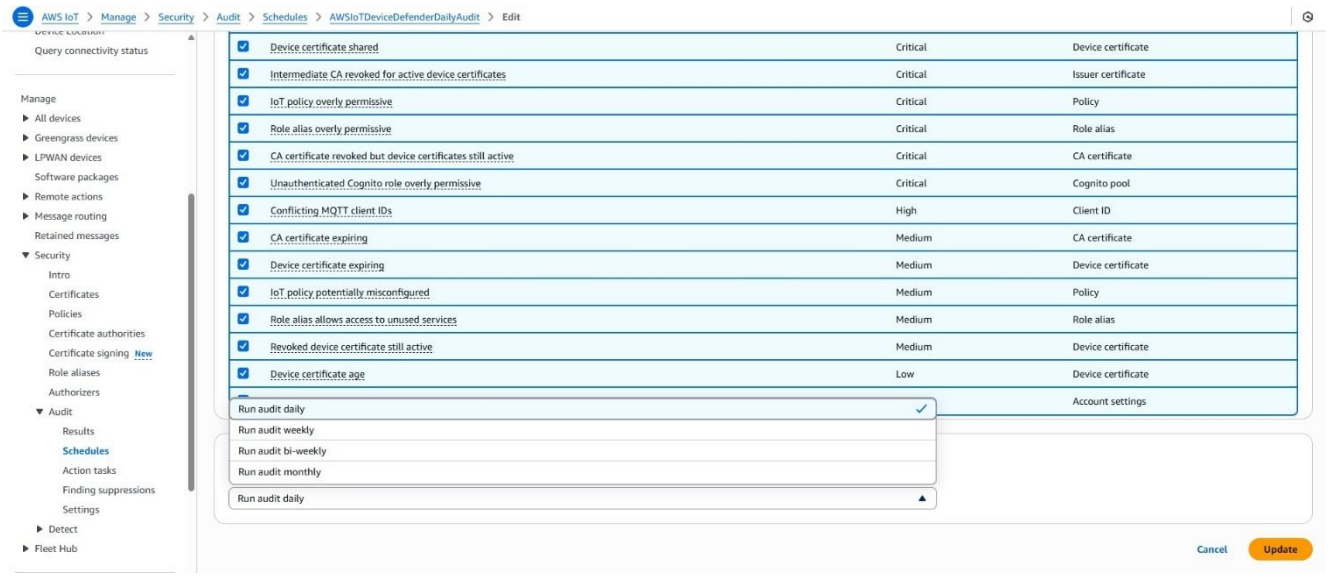


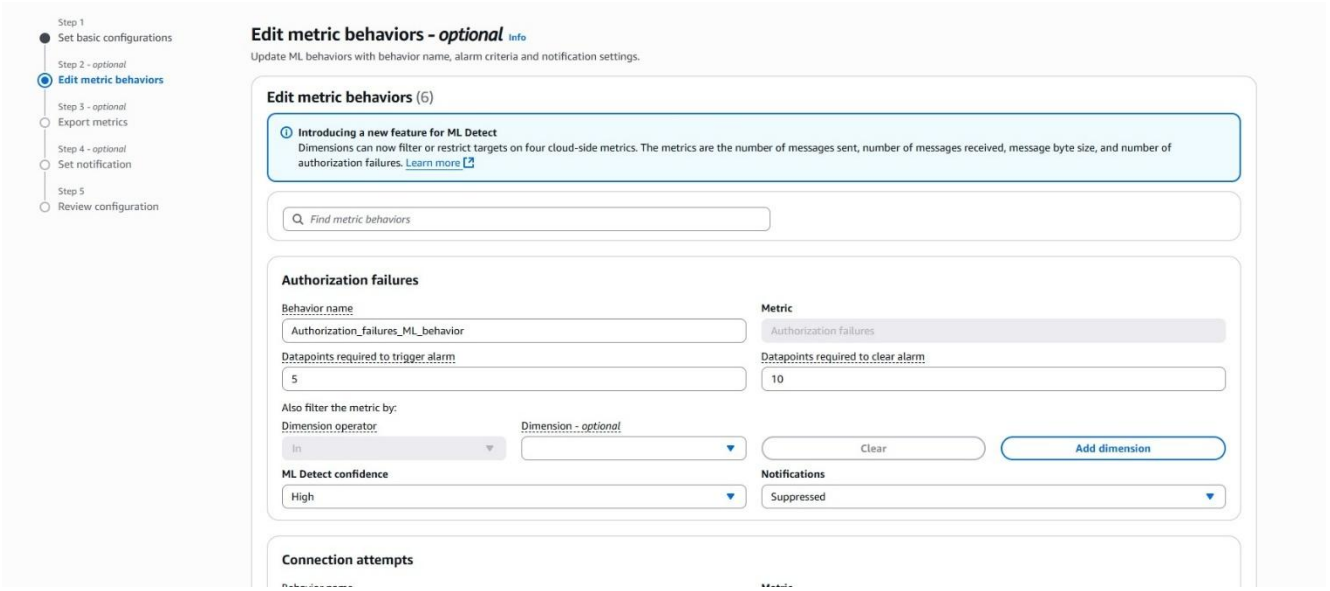
Рис. 3.6 Періодичність аудиту



Крок 2: Моніторинг поведінки

- Визначте нормальну поведінку пристроїв, встановивши метрики (наприклад, кількість підключень, обсяг переданих даних).
- Увімкніть функцію **Detect** для виявлення аномалій у поведінці пристроїв.

Рис. 3.7 Поведінка пристроїв



Що робить функція Detect?

Вона дозволяє відстежувати аномалії в поведінці пристроїв на основі визначених норм. Наприклад:

- Занадто багато підключень за короткий час
- Надмірна кількість опублікованих MQTT повідомлень
- Нетипова частота підписок або обсяг даних

Крок 3: Реагування на інциденти

- Налаштуйте сповіщення через **Amazon SNS** або **CloudWatch Alarms** для отримання повідомлень про виявлені аномалії.
- Використовуйте **AWS Lambda** для автоматичного виконання дій у відповідь на інциденти (наприклад, відключення пристрою).

Рис. 3.8 SNS concfig.

Що робимо:

Коли AWS IoT Device Defender виявляє аномалію, він надсилає повідомлення у **SNS Topic**, а звідти — на email, SMS або тригерить Lambda-функцію.

Як створити SNS Topic:

1. **Перейдіть у консоль SNS**: https://console.aws.amazon.com/sns
2. **Натисніть “Create topic”**
3. **Виберіть тип**: Standard
4. **Введіть назву**, наприклад:

КопироватьРедактировать
iot-alerts-topic

5. Натисніть **Create topic**

Підписка на сповіщення:

1. Перейдіть у створений **Topic** → вкладка **"Subscriptions" → "Create subscription"**
2. Виберіть:
   - **Protocol**: Email
   - **Endpoint**: свій email
3. Підтвердіть email (відкрий лист від AWS і натисни “Confirm subscription”)

Поверніться у AWS IoT Core → Defend → Detect → Security Profile

1. Відредагуйте свій профіль
2. У полі **Notifications**, виберіть **Send to SNS topic** → виберіть iot-alerts-topic

---

Частина 2: Автоматичне реагування через AWS Lambda

Наприклад: при виявленні аномалії — автоматично **відключити сертифікат пристрою**.

Кроки для реалізації:

1. Створіть Lambda-функцію

Перейдіть в AWS Lambda

- **Function name**: iot-disable-cert
- **Runtime**: Python 3.12 або Node.js 20
- **Permissions**: Додайте IAM роль з доступом до iot:UpdateCertificate

---

Код (Python) для відключення сертифікату:

python
КопироватьРедактировать

```
import json
import boto3

iot = boto3.client('iot')

def lambda_handler(event, context):
    # Отримуємо ARN сертифіката з події
    certificate_arn = event['detail']['violatingCertificateArn']

    # Отримуємо ID сертифіката з ARN
    cert_id = certificate_arn.split("/")[-1]

    # Відключаємо сертифікат
    response = iot.update_certificate(
        certificateId=cert_id,
        newStatus='INACTIVE'
    )

    print(f"Certificate {cert_id} has been deactivated")
    return {
        'statusCode': 200,
        'body': json.dumps('Certificate disabled')
    }
```

---

2. Підключіть Lambda до SNS

- У SNS Topic iot-alerts-topic → **Create subscription**
- Оберіть:
  - **Protocol**: Lambda
  - **Endpoint**: ваша функція iot-disable-cert

Важливо:

- Lambda повинна мати IAM-права:

```
json
КопироватьРедактировать
{
  "Effect": "Allow",
  "Action": [
    "iot:UpdateCertificate"
  ],
  "Resource": "*"
}
```

- Не забудь підтвердити дозволи SNS викликати Lambda (це робиться автоматично, якщо через консоль).

---

4. Приклад впровадження: Моніторинг температурних сенсорів

Сценарій:

Підприємство використовує температурні сенсори для моніторингу умов зберігання продукції. Необхідно забезпечити безпечне підключення сенсорів та моніторинг їхньої поведінки.

Реалізація:

- **Реєстрація сенсорів**: Кожен сенсор реєструється як окремий Thing в AWS IoT Core.
- **Підключення**: Сенсори підключаються до AWS IoT Core через MQTT, використовуючи X.509 сертифікати.
- **Моніторинг**: AWS IoT Device Defender відстежує кількість підключень та обсяг переданих даних кожного сенсора.
- **Реагування**: У разі виявлення аномалій (наприклад, надмірна кількість підключень), AWS Lambda автоматично відключає сенсор та надсилає сповіщення адміністратору.docs.aws.amazon.com

---

5. Висновки

Впровадження AWS IoT Security, зокрема AWS IoT Device Defender, дозволяє підприємствам забезпечити високий рівень безпеки IoT-пристроїв. Завдяки

гнучким можливостям налаштування, автоматичному моніторингу та реагуванню на інциденти, підприємства можуть ефективно захищати свою інфраструктуру та дані.

3.3 Розробка рекомендацій на прикладі платформи AWS IoT Security

На основі попередніх досліджень, аналізу вразливостей IoT, порівняння провідних рішень і практичного впровадження AWS IoT Security, виникає потреба у створенні **системи рекомендацій**, що дозволить підприємствам:

- стандартизувати безпеку IoT-інфраструктури;
- знизити ризики кіберінцидентів;
- забезпечити відповідність галузевим регламентам (GDPR, ISO/IEC 27001, NIS2 тощо).

AWS IoT Security — це не просто набір інструментів, а **архітектура довіри**, яку можна формалізувати через структуровані кроки. Нижче подано рекомендації щодо **організаційних**, **технічних** і **процедурних** аспектів захисту.

---

1. Організаційні рекомендації

1.1. Створення окремої політики IoT-безпеки

Підприємству рекомендовано створити **спеціалізовану політику безпеки IoT**, яка відрізняється від загальної політики IT-безпеки. Вона повинна включати:

- визначення критичних IoT-активів;
- правила підключення та автентифікації;
- процедури оновлення прошивок;
- регламент резервного копіювання IoT-конфігурацій.

1.2. Розподіл зон довіри

- Створити окремі **мережеві сегменти (VPC)** для IoT-пристроїв, щоб ізолювати їх від основної IT-інфраструктури.
- Налаштувати **AWS IoT policies** так, щоб кожен пристрій мав **мінімально необхідні права** — за принципом найменших привілеїв.

---

2. Технічні рекомендації

2.1. Використання X.509 сертифікатів

Забезпечення захищеної автентифікації пристроїв за допомогою сертифікатів:

- Генерація окремого сертифіката для кожного пристрою;
- Встановлення терміну дії сертифікатів;
- Відкликання сертифікатів при компрометації пристрою.

2.2. Аудит конфігурацій і виявлення аномалій

Рекомендовано активувати **Audit та Detect** у **AWS IoT Device Defender** для:

- перевірки політик доступу, правил шифрування, використання root-профілів;
- побудови моделей звичної поведінки пристроїв на основі їх трафіку та команд.

2.3. Автоматизація реагування

- Налаштувати **AWS Lambda** для автоматичної дезактивації пристрою або сповіщення у разі інциденту;
- Впровадити **CloudWatch Alarms** для реагування на критичні метрики (наприклад, spike у підключеннях).

Приклад реалізації рекомендацій на практиці

Розглянемо **реальний сценарій застосування** рекомендацій на прикладі впровадження AWS IoT Security на підприємстві, що використовує **індустріальні температурні сенсори** для контролю умов зберігання продукції у складських приміщеннях.

3.1. Передумови

- Понад 500 сенсорів температури на складі;
- Дані зчитуються кожні 30 секунд;
- Частина пристроїв встановлена у важкодоступних зонах;
- Потреба в автономному захисті, без людського втручання.

3.2. Етапи впровадження

Крок 1: Ідентифікація пристроїв

- Кожен сенсор отримує унікальне ім’я (Thing ID);
- Створюється окрема політика для кожної групи пристроїв.

Крок 2: Впровадження сертифікатів X.509

- Сертифікати створюються централізовано;
- Впроваджуються автоматично через AWS IoT Device Management;

- Підписуються та зберігаються у AWS Secrets Manager.

Крок 3: Сегментація трафіку

- Пристрої об'єднані у логічні групи;
- Налаштовано окремі правила для публікації даних лише у дозволені топіки MQTT;
- Мережеві ACL і Security Groups ізольовують сенсори від зовнішніх загроз.

Крок 4: Моніторинг та виявлення аномалій

- AWS IoT Device Defender збирає метрики по кожному сенсору;
- Побудована поведінкова модель нормального режиму;
- Аномальні дії (наприклад, часте підключення або відправка нестандартних пакетів) фіксуються.

Крок 5: Автоматизація реагування

- AWS Lambda вимикає пристрій із аномальною поведінкою;
- Адміністратор отримує push-сповіщення через SNS;
- Дані інциденту логуються в Amazon S3 для подальшого розслідування.

---

4. Модель життєвого циклу захисту IoT на AWS

Для стандартизації всіх рекомендацій доцільно використовувати **модель життєвого циклу безпеки IoT-пристроїв**, яку можна впровадити на будь-якому підприємстві, що працює з AWS:

Модель включає такі етапи:

1. **Ідентифікація**: формування інвентарю IoT-пристроїв, присвоєння атрибутів, реєстрація в AWS IoT Core.
2. **Автентифікація**: створення унікальних сертифікатів, застосування TLS 1.2+, ізоляція небезпечних пристроїв.
3. **Контроль доступу**: реалізація політик на основі ролей (IAM), мінімізація прав доступу.
4. **Моніторинг**: постійний аудит та побудова поведінкових моделей.
5. **Інцидент-менеджмент**: сповіщення, автоматичні реакції, аналіз подій.
6. **Оновлення та відновлення**: OTA-оновлення прошивок, відкликання сертифікатів, резервне копіювання.
7. **Деактивація**: безпечне виведення з експлуатації, очищення метаданих, знищення сертифікатів.

Схема моделі (розроблена у вигляді «цифрового колеса безпеки»):

[Ідентифікація] → [Автентифікація] → [Контроль доступу] →
[Моніторинг] → [Інцидент-менеджмент] → [Оновлення] → [Деактивація] →
[Ідентифікація]...

---

5. Висновки до підрозділу

У результаті впровадження та дотримання рекомендацій на базі **AWS IoT Security** підприємства отримують:

- Гнучку та масштабовану систему безпеки;
- Автоматизацію ключових процесів захисту;
- Контроль над поведінкою пристроїв у реальному часі;
- Зменшення впливу людського фактору;
- Підвищення рівня кібергігієни персоналу та відповідність міжнародним стандартам.

Платформа **AWS IoT Security** може служити еталонною для розгортання захищеної IoT-інфраструктури — як у великих корпораціях, так і в середньому бізнесі.

ВИСНОВКИ

У цій дипломній роботі було проведено всебічне дослідження засобів захисту інформації в системах Інтернету речей (IoT), що стають дедалі важливішими компонентами цифрової інфраструктури сучасного світу. Розгортання IoT-систем у різних галузях — від побутових смарт-пристроїв до критичних промислових мереж — висуває нові вимоги до інформаційної безпеки. Складність, гетерогенність, масштабованість та обмежені ресурси таких систем обумовлюють необхідність спеціалізованих рішень для забезпечення їх захисту.

У першому розділі було визначено фундаментальні поняття та принципи функціонування IoT, зокрема архітектуру, основні компоненти (пристрої, мережі, платформи, обробка даних), а також логіку обміну інформацією між вузлами. Особливу увагу приділено розумінню, як взаємодія пристроїв, обмежених у ресурсах, створює нові вектори атак, що не характерні для традиційних IT-систем.

У другому розділі було проведено глибоку класифікацію загроз безпеці IoT, серед яких виокремлено: несанкціонований доступ до пристроїв, DDoS-атаки, витоки конфіденційних даних, а також вразливості на рівні прошивки та програмного забезпечення. Проаналізовано конкретні приклади атак у 2023–2024 роках, включаючи інциденти зі смарт-будинками, медичними IoT-системами та критичною інфраструктурою. Це дало змогу побачити, як на практиці загрози можуть перетворитися на масштабні соціально-економічні ризики.

У третьому розділі розглянуто сучасні методи та рішення захисту IoT-систем. Розкрито переваги та недоліки традиційних підходів, таких як VPN, IDS/IPS, шифрування даних, а також новітніх засобів на основі AI/ML. Проведено порівняльний аналіз провідних хмарних платформ (AWS IoT Security, Azure Defender for IoT, Cisco IoT Threat Defense, IBM Watson, Palo Alto Prisma), що показав: хоча більшість рішень мають високий рівень інтеграції, лише AWS забезпечує повноцінну автоматизацію та гнучке масштабування у середовищі з великою кількістю пристроїв.

В останньому розділі на прикладі AWS IoT Security запропоновано стратегічну модель впровадження засобів захисту для підприємства з великою кількістю сенсорних пристроїв. Було описано життєвий цикл безпеки IoT — від автентифікації й контролю доступу до моніторингу, автоматизованого реагування та безпечної деактивації пристроїв. Представлено візуальні моделі впровадження та реальний сценарій, що доводить ефективність обраного підходу.

Основні висновки дипломної роботи:

- Інтернет речей є високоризиковим середовищем з точки зору кібербезпеки через масштаб, відкритість мереж, різноманітність платформ і обмеження ресурсів пристроїв.

- Найнебезпечнішими загрозами для IoT є DDoS-атаки, несанкціонований доступ та витоки конфіденційних даних.
- Традиційні IT-засоби безпеки часто не працюють ефективно в середовищі IoT; натомість потрібні спеціалізовані рішення з урахуванням обмежених можливостей пристроїв.
- Хмарні платформи, зокрема AWS IoT Security, забезпечують ефективний баланс між автоматизацією, адаптивністю, масштабуванням і зручністю адміністрування.
- Успішна безпека IoT — це не лише технічні засоби, а й стратегічний підхід, що охоплює політики, навчання персоналу, оновлення програмного забезпечення, управління ризиками та відновлення після інцидентів.

Перспективи подальших досліджень

Надалі доцільно дослідити:

- Використання моделей машинного навчання для раннього виявлення атак у реальному часі;
- Побудову стійких до атак IoT-мереж на основі Zero Trust принципів;
- Проблематику безпеки в IoT-пристроях з енергозалежною логікою;
- Законодавче регулювання та стандартизацію кіберзахисту IoT у різних юрисдикціях (зокрема в контексті NIS2, GDPR, ISO/IEC 27030).

ПЕРЕЛІК ПОСИЛАНЬ

Stallings W. *Cryptography and Network Security: Principles and Practice*, 8th Edition. Pearson, 2023.

Halabi, T. (2021). *Internet of Things Security: Challenges, Advances, and Analytics*. Springer.

Liu, C., Yu, J. *Cybersecurity for Industrial Control Systems and IoT*. Elsevier, 2023.

AWS Documentation – IoT Core: https://docs.aws.amazon.com/iot/latest/developerguide/

AWS Documentation – Device Defender: https://docs.aws.amazon.com/iot-device-defender/

Microsoft Defender for IoT: https://learn.microsoft.com/en-us/azure/defender-for-iot/

Cisco IoT Threat Defense: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html

IBM Watson IoT Platform: https://www.ibm.com/products/watson-iot-platform

OWASP IoT Top 10 Threats (2024): https://owasp.org/www-project-internet-of-things/

ENISA – Guidelines for Securing the Internet of Things (2023): https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

ISO/IEC 27030:2023 – Guidelines for IoT Security

Amazon Whitepapers – *Best Practices for AWS IoT Security*: https://docs.aws.amazon.com/whitepapers/latest/security-overview-aws-iot/

NIST SP 800-183 – *Networks of 'Things'* (2021): https://csrc.nist.gov/publications/detail/sp/800-183/final

IoT Security Foundation: https://www.iotsecurityfoundation.org/

ENISA Threat Landscape for the Internet of Things (2024): https://www.enisa.europa.eu/publications/threat-landscape-for-iot

Gartner Reports on IoT Security (2024) – [доступ через підписку]

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

Засоби захисту інформації для Інтернету речей

Інтернет речей (IoT) – одна з найдинамічніших і водночас найбільш вразливих сфер сучасних інформаційних технологій. За прогнозами дослідницької компанії Statista, до 2025 року кількість активних IoT-пристроїв у світі сягне понад 75 мільярдів одиниць, що формує безпрецедентну поверхню атаки для кіберзлочинців.

Ця робота присвячена комплексному аналізу сучасного стану безпеки Інтернету речей, вивченню ключових загроз, дослідженню найпоширеніших методів захисту та розробці практичних рекомендацій для підприємств.

Поняття та принципи роботи технології IoT

Визначення IoT

Інтернет речей – це глобальна інфраструктура, що забезпечує розширені сервіси шляхом взаємодії фізичних та віртуальних речей на основі інформаційно-комунікаційних технологій. Це не лише технологія, а й нова філософія побудови розумного простору.

Ключові принципи

- Принцип тотального з'єднання
- Принцип унікальної ідентифікації
- Принцип взаємодії у реальному часі
- Принцип автономного функціонування
- Принцип енергоефективності

Класифікація загроз та їх наслідки

Несанкціонований доступ

Перехоплення керування пристроєм, крадіжка або підміна даних. Більшість IoT-пристроїв мають уразливі інтерфейси — веб-панелі, відкриті порти, API, або працюють із заводськими паролями.

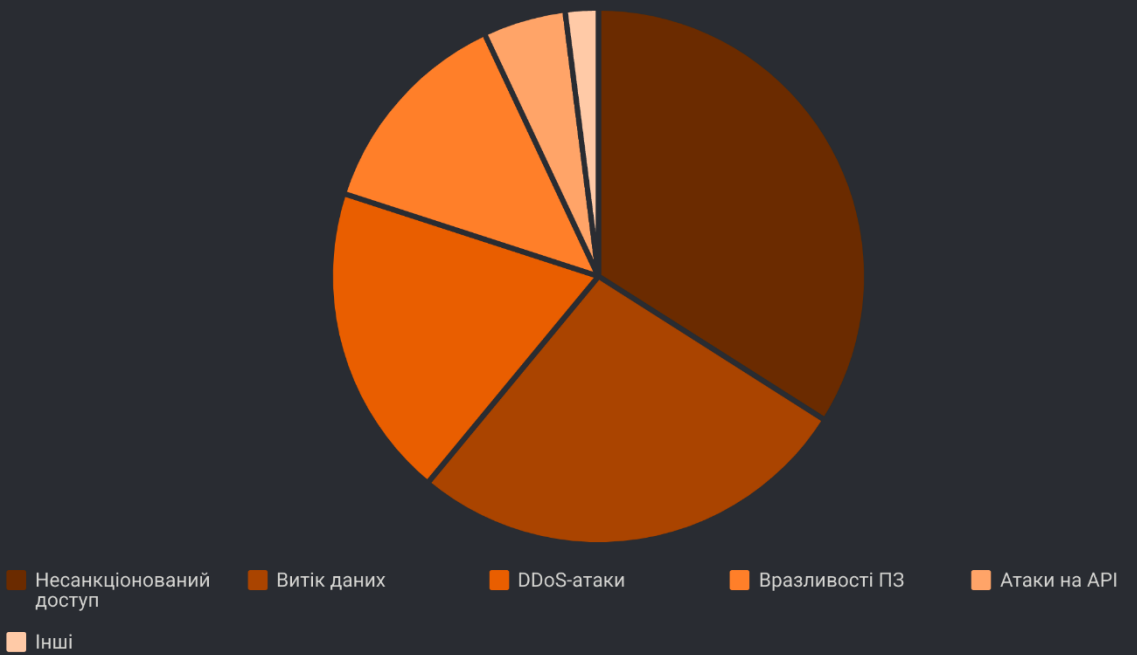
DDoS-атаки

Паралізація сервісів, фінансові втрати, відмова в обслуговуванні. Через слабкий захист, мільйони пристроїв можуть бути заражені шкідливим ПЗ, що об'єднує їх у мережу ботів.

Витоки конфіденційної інформації

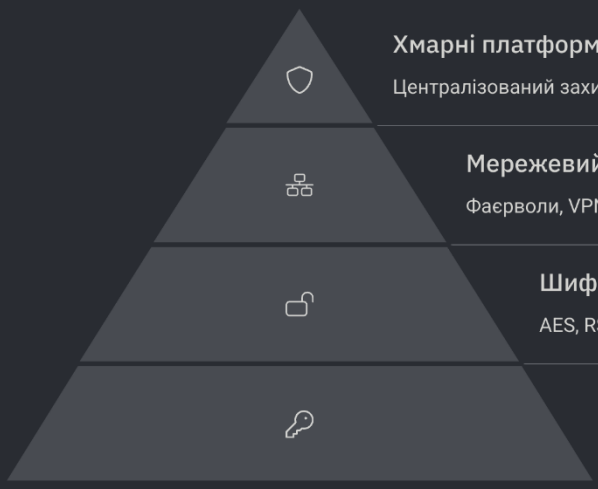
Порушення приватності, втрати персональних або корпоративних даних. Неналежне зберігання даних, передача незашифрованими каналами або відсутність механізмів автентифікації.

Аналіз статистики інцидентів кібербезпеки у сфері IoT



Статистика за 2023–2024 роки свідчить про поглиблення проблеми безпеки IoT. Найсерйознішою загрозою залишається несанкціонований доступ до пристроїв (34% усіх зареєстрованих інцидентів). На другому місці — витік даних (27%), на третьому — DDoS-атаки (19%). Також значну частку складають вразливості програмного забезпечення (13%).

Огляд сучасних методів та рішень захисту



Хмарні платформи безпеки

Централізований захист та моніторинг

Мережевий захист

Фаєрволи, VPN, сегментація, NAT

Шифрування даних

AES, RSA, ECC, TLS/SSL

Автентифікація та авторизація

Двофакторна, біометрія, PKI, OAuth 2.0

Сучасна практика захисту IoT базується на багаторівневому підході, що передбачає комбінацію технічних, програмних, мережевих і організаційних засобів. Кожен рівень захисту виконує свою функцію, а разом вони створюють комплексну систему безпеки.

Переваги та недоліки наявних засобів захисту

Автентифікація та контроль доступу

Переваги: захист від несанкціонованих підключень, гнучке налаштування, інтеграція з PKI-системами.

Недоліки: складність масштабування, обмеження старих пристроїв, небезпечні дефолтні налаштування.

Шифрування даних

Переваги: надійна конфіденційність, можливість використання хардварних прискорювачів, підтримка галузевих стандартів.

Недоліки: обмеження по ресурсах, складність ключового управління, відсутність шифрування за замовчуванням.

Хмарні платформи безпеки

Переваги: масштабованість, швидкий доступ до оновлень, висока аналітична здатність, автоматизація.

Недоліки: залежність від провайдера, юрисдикційні ризики, високі витрати, необхідність захисту каналів зв'язку.

Порівняльний аналіз провідних платформ захисту IoT

8.5

AWS IoT Security

Найкраща масштабованість та інтеграція з іншими сервісами

7.8

Azure Defender for IoT

Відмінна інтеграція з корпоративною інфраструктурою

7.5

Cisco IoT Threat Defense

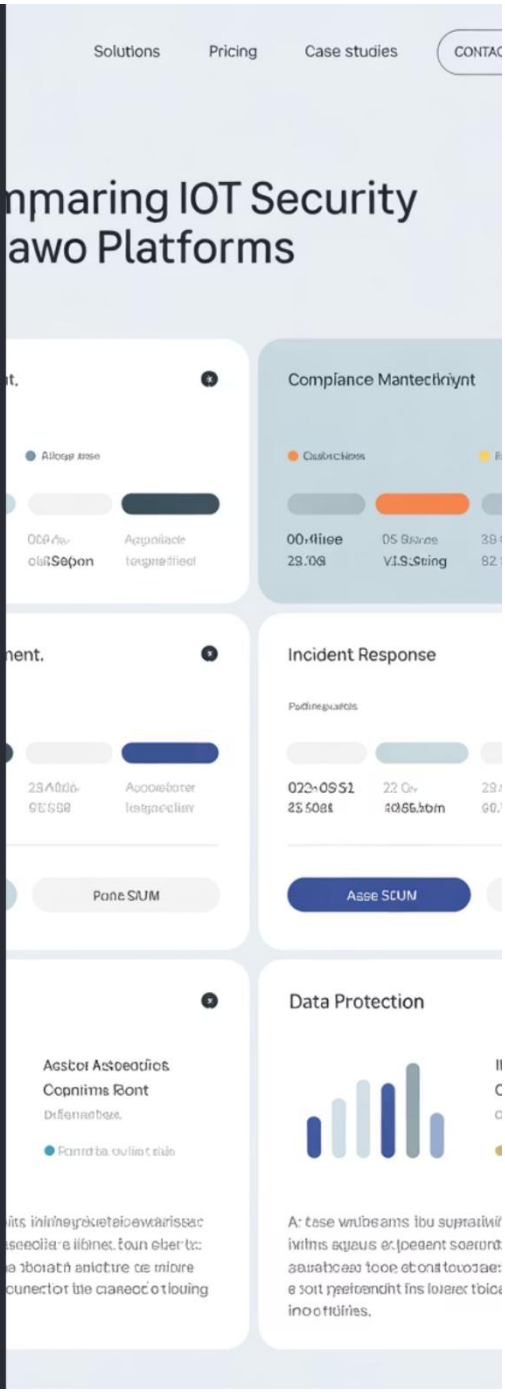
Лідер у галузі мережевого захисту

7.2

IBM Watson IoT

Унікальні можливості штучного інтелекту

Проведений аналіз показує, що AWS IoT Device Defender є лідером у масштабованості й інтеграції, Microsoft Azure Defender відзначається універсальністю для критичної інфраструктури, Cisco IoT Threat Defense домінує у галузі мережевого захисту, а IBM Watson IoT унікальна завдяки вбудованому AI.



Обґрунтування вибору засобів захисту для IoT-пристроїв підприємства

Класифікація пристроїв

Інвентаризація IoT-пристроїв, визначення типів підключення, операційних систем та критичності

Визначення загроз

Побудова матриці загроз/наслідків для конкретного підприємства

Критерії вибору

Оцінка підтримки типів пристроїв, масштабованості, управління політиками, сумісності з SIEM/SOAR

Вибір платформи

AWS IoT Security як найбільш збалансоване, гнучке та функціонально повне рішення

На основі детального техніко-економічного аналізу, з урахуванням функціональних вимог, гнучкості інтеграції, рівня захисту, підтримки аналітики та простоти впровадження, AWS IoT Security обґрунтовано обирається як основна платформа для впровадження засобів захисту IoT-пристроїв підприємства.

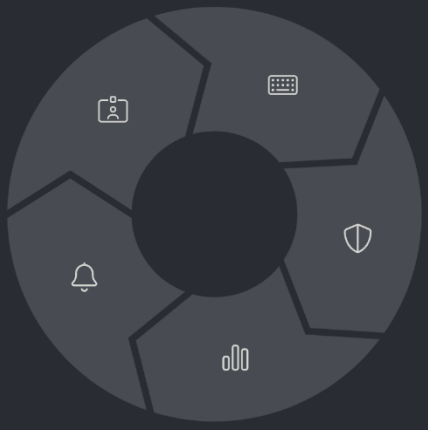
Впровадження та рекомендації на прикладі AWS IoT Security

Ідентифікація

Формування інвентарю IoT-пристроїв, присвоєння атрибутів, реєстрація в AWS IoT Core

Інцидент-менеджмент

Сповіщення через SNS, автоматичні реакції через Lambda, аналіз подій



Автентифікація

Створення унікальних X.509 сертифікатів, застосування TLS 1.2+, ізоляція небезпечних пристроїв

Контроль доступу

Реалізація політик на основі ролей (IAM), мінімізація прав доступу

Моніторинг

Постійний аудит та побудова поведінкових моделей через AWS IoT Device Defender

У результаті впровадження та дотримання рекомендацій на базі AWS IoT Security підприємства отримують гнучку та масштабовану систему безпеки, автоматизацію ключових процесів захисту, контроль над поведінкою пристроїв у реальному часі та підвищення рівня кібергігієни персоналу.

ВИСНОВОК

Комплексний підхід до захисту

Захист IoT-пристроїв вимагає комплексного підходу, який охоплює всі рівні інфраструктури. Впровадження сучасних методів захисту, зокрема на базі AWS IoT Security, дозволяє суттєво знизити ризики кіберінцидентів.

Системність заходів

Ключовим фактором успішного захисту є системність — від ідентифікації та автентифікації пристроїв до постійного моніторингу та своєчасного реагування на інциденти. Рекомендовано впроваджувати принципи багаторівневого захисту.

Постійне вдосконалення

Подальший розвиток технологій Інтернету речей вимагатиме постійного вдосконалення засобів захисту та регулярного аудиту безпеки для ефективної протидії новим кібер-загрозам.