МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ ПОБУДОВА МОДЕЛІ ЗАГРОЗ ТА ЗАХОДІВ ЗАХИСТУ ДЛЯ ІОТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Денис ПОБЕРЕЖЕЦЬ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Денис ПОБЕРЕЖЕЦЬ
Ім’я, ПРІЗВИЩЕ

Керівник: Євгенія ІВАНЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Побережець Денис Сергійович
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Побудова моделі загроз та заходів захисту для IoT-інфраструктури підприємства ”,
керівник кваліфікаційної роботи ІВАНЧЕНКО Євгенія, д.т.н., проф.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *IoT-інфраструктура підприємства, моделі загроз інформаційній безпеці, методи оцінки ризиків, засоби захисту IoT-пристроїв, міжнародні стандарти та нормативні документи у сфері кібербезпеки, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати особливості функціонування IoT-інфраструктури підприємства та пов'язані з нею загрози безпеці.
4.2. Дослідити підходи до побудови моделі загроз для IoT-середовища.
4.3. Розробити заходи та рекомендації щодо захисту IoT-інфраструктури підприємства.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	14.03.2026	
2.	Збір та аналіз літератури.	26.03.2026	
3.	Аналіз архітектури IoT-інфраструктури підприємства та сучасних кіберзагроз.	10.04.2026	
4.	Дослідження методів побудови моделей загроз для IoT-систем, аналіз підходів до виявлення потенційних вразливостей	19.04.2026	
5.	Аналіз сучасних засобів і методів забезпечення кібербезпеки IoT-інфраструктури підприємства	24.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	03.05.2026	
7.	Оформлення кваліфікаційної роботи.	09.05.2026	
8.	Підготовка презентації та доповіді.	13.05.2026	
9.	Отримання рецензії на роботу.	07.06.2026	
10.	Захист в ЕК.	10.06.2026	

Здобувач вищої освіти _____ Денис ПОБЕРЕЖЕЦЬ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(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 Побережець Д.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Побудова моделі загроз та заходів захисту для IoT-інфраструктури підприємства"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ПОБЕРЕЖЕЦЬ Денис у кваліфікаційній **роботі** проаналізував сучасний стан безпеки IoT-інфраструктури підприємства та актуальні вектори кіберзагроз, дослідив існуючі методології побудови моделей загроз, розробив структуровану модель загроз для IoT-середовища з урахуванням апаратного, мережевого та програмного рівнів, а також реалізував програмний застосунок що демонструє комплекс заходів захисту IoT-системи.

ПОБЕРЕЖЕЦЬ Денис показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований та відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ПОБЕРЕЖЕЦЯ Дениса на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Побережець Д.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ПОБЕРЕЖЦЯ Дениса
на тему “Побудова моделі загроз та заходів захисту для IoT-інфраструктури підприємства”

Актуальність. У сучасному світі кількість підключених IoT-пристроїв стрімко зростає і вже перевищує десятки мільярдів одиниць. Підприємства активно впроваджують IoT-рішення у виробничі та бізнес-процеси, однак більшість пристроїв проектувались без належного врахування вимог інформаційної безпеки — вони мають слабку автентифікацію, незашифрований зв'язок та рідко оновлюються. Кожен такий пристрій є потенційною точкою входу для зловмисника в корпоративну мережу.

З огляду на зазначене побудова моделі загроз та розробка заходів захисту для IoT-інфраструктури підприємства є актуальним науковим завданням.

Позитивні сторони.

1. У роботі проведено комплексний аналіз архітектури IoT-систем, типів пристроїв та протоколів передачі даних, що формує міцну теоретичну основу для подальшого дослідження.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення представлено у вигляді таблиць і рисунків.
3. Здобувач опрацював значну джерельну базу: понад 40 публікацій, в тому числі англомовних наукових статей з провідних видань у сфері кібербезпеки IoT.
4. Практична цінність роботи підтверджується розробкою програмного застосунку який імітує реальну систему безпеки IoT-інфраструктури з реалізованими механізмами автентифікації, шифрування, сегментації мережі та моніторингу загроз.

Недоліки.

Доцільно було б приділити більше уваги порівняльному аналізу існуючих комерційних рішень для захисту IoT-інфраструктури підприємств та детальнішому обґрунтуванню вибору між методологіями STRIDE і PASTA. Однак вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувач ПОБЕРЕЖЕЦЬ Денис заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню побудови моделі загроз та заходів захисту для IoT-інфраструктури підприємства. Робота складається зі вступу, трьох розділів, що містять 8 рисунків, 4 таблиці, висновків і списку використаних джерел із 42 найменувань. Загальний обсяг роботи становить 94 аркуша

Метою роботи є розробка моделі загроз та комплексу заходів захисту для IoT-інфраструктури підприємства на основі аналізу сучасних кіберзагроз та методологій оцінки ризиків.

Об'єктом дослідження є IoT-інфраструктура підприємства як сукупність пристроїв, мереж передачі даних, протоколів взаємодії та програмного забезпечення, що функціонують в єдиному інформаційному середовищі.

Предмет дослідження – методи та підходи до ідентифікації, класифікації загроз інформаційній безпеці та формування комплексу заходів захисту IoT-інфраструктури підприємства.

Методи дослідження. Для вирішення означеного наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до управління інформаційною безпекою, методологія моделювання загроз STRIDE.

Як результат у роботі проведено аналіз архітектури та компонентів IoT-інфраструктури підприємства, досліджено сучасні кіберзагрози для IoT-систем. Виконано інвентаризацію критичних активів та ідентифікацію потенційних порушників. Побудовано модель загроз, розроблено комплекс заходів захисту що включає механізми автентифікації та авторизації, криптографічний захист, сегментацію мережі та систему моніторингу й виявлення атак.

Галузь застосування. Розроблена модель загроз та запропонований комплекс заходів захисту можуть бути безпосередньо впроваджені у процеси управління інформаційною безпекою підприємств що використовують IoT-рішення.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, ІОТ-ІНФРАСТРУКТУРА, МОДЕЛЬ ЗАГРОЗ , STRIDE, ЗАХОДИ ЗАХИСТУ, СЕГМЕНТАЦІЯ МЕРЕЖІ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AES — Advanced Encryption Standard — стандарт симетричного шифрування

AI — Artificial Intelligence — штучний інтелект

API — Application Programming Interface — інтерфейс програмування застосунків

APT — Advanced Persistent Threat — передова постійна загроза

AWS — Amazon Web Services — хмарна платформа Amazon

BLE — Bluetooth Low Energy — Bluetooth з низьким енергоспоживанням

BMS — Battery Management System — система керування акумулятором

DDoS — Distributed Denial of Service — розподілена атака «відмова в обслуговуванні»

DMZ — Demilitarized Zone — демілітаризована зона мережі

ECC — Elliptic Curve Cryptography — криптографія на еліптичних кривих

ERP — Enterprise Resource Planning — система планування ресурсів підприємства

GDPR — General Data Protection Regulation — загальний регламент захисту даних

GPS — Global Positioning System — глобальна система позиціонування

HMI — Human-Machine Interface — інтерфейс людина–машина

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

ICS — Industrial Control System — промислова система керування

IDS — Intrusion Detection System — система виявлення вторгнень

IIoT — Industrial Internet of Things — промисловий Інтернет речей

IoMT — Internet of Medical Things — Інтернет медичних речей

IoT — Internet of Things — Інтернет речей

IP — Internet Protocol — інтернет-протокол

ВСТУП

Актуальність теми. У сучасному світі кількість підключених IoT-пристроїв стрімко зростає і вже перевищує десятки мільярдів одиниць. Підприємства активно впроваджують IoT-рішення у виробничі та бізнес-процеси, однак більшість пристроїв проектувались без належного врахування вимог інформаційної безпеки — вони мають слабку автентифікацію, незашифрований зв'язок та рідко оновлюються. Поєднуючи периферійні датчики, шлюзи та хмарні ресурси, IoT-інфраструктура стає безпрецедентною ціллю через велику кількість потенційних поверхонь атаки та вразливостей. Кожен підключений пристрій є потенційною точкою входу для зловмисника в корпоративну мережу, що може призвести до витоку даних, зупинки виробництва або загрози безпеці людей. Без системного підходу до аналізу загроз навіть досвідчена команда фахівців з безпеки може несвідомо залишати відкриті вразливості в IoT-інфраструктурі підприємства.

З огляду на зазначене побудова моделі загроз та розробка заходів захисту для IoT-інфраструктури підприємства є актуальним науковим і практичним завданням.

Мета роботи полягає у розробці моделі загроз та комплексу заходів захисту для IoT-інфраструктури підприємства на основі аналізу сучасних кіберзагроз та методологій оцінки ризиків.

Об'єкт дослідження – IoT-інфраструктура підприємства як сукупність пристроїв, мереж передачі даних, протоколів взаємодії та програмного забезпечення, що функціонують в єдиному інформаційному середовищі.

Предмет дослідження – методи та підходи до ідентифікації, класифікації загроз інформаційній безпеці та формування комплексу заходів захисту IoT-інфраструктури підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання:**

1. Провести аналіз сучасного стану безпеки IoT-систем та визначити актуальні вектори атак на інфраструктуру підприємства.
2. Дослідити існуючі методології побудови моделей загроз (STRIDE) та обґрунтувати вибір підходу для IoT-середовища.
3. Виконати інвентаризацію та категоризацію компонентів типової IoT-інфраструктури підприємства.
4. Розробити модель загроз для IoT-інфраструктури з урахуванням особливостей апаратного, мережевого та програмного рівнів.
5. Визначити та систематизувати заходи захисту відповідно до виявлених загроз та ризиків.
6. Провести оцінку ефективності запропонованих заходів захисту та верифікацію моделі.

Методи дослідження. Для вирішення означеного наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до управління інформаційною безпекою, а також методологія моделювання загроз STRIDE.

***Практичне значення одержаних результатів*.** Розроблена модель загроз та запропонований комплекс заходів захисту можуть бути безпосередньо впроваджені у процеси управління інформаційною безпекою підприємств що використовують IoT-рішення. Результати роботи також можуть слугувати основою для проведення аудитів безпеки IoT-систем та розробки корпоративних політик кібербезпеки у сфері Інтернету речей.

РОЗДІЛ 1 .АНАЛІЗ ІОТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА ТА СУЧАСНИХ КІБЕРЗАГРОЗ

1.1 Поняття та особливості IoT-інфраструктури підприємства

Інфраструктура Інтернету речей (IoT) — це фізична та цифрова система взаємопов’язаних компонентів, таких як датчики, мережі, хмарні платформи та програмне забезпечення, які дозволяють пристроям збирати, обробляти та реагувати на дані з мінімальним втручанням людини. Вона формує основу для інтелектуальних застосувань у різних галузях, від розумних будинків до промислової автоматизації та управління містом.

Ключові компоненти інфраструктури Інтернету речей включають:

Шар сприйняття (датчики та виконавчі механізми): це пристрої, які взаємодіють з навколишнім середовищем, збираючи необроблені дані (наприклад, температуру, рух) та виконуючи фізичні дії на основі цих даних.

Рівень зв'язку (мережевий рівень) - цей рівень передає дані від пристроїв до інших систем та хмари. Він включає різноманітні мережеві технології, такі як Wi-Fi, Bluetooth, стільникові мережі (4G, 5G) та протоколи, такі як Zigbee та LoRa.

Шлюзи діють як посередники, перетворюючи дані з пристроїв та підключаючи їх до ширших мереж або Інтернету.

Хмарні платформи та периферійні обчислення - пристрої та шлюзи підключаються до хмарних платформ або периферійних серверів для зберігання, обробки та аналітики даних. Периферійні обчислення обробляють дані ближче до їх джерела для швидшого реагування.

Рівень обробки та аналітики даних - цей рівень використовує програмне та апаратне забезпечення для обробки, аналізу та інтерпретації необроблених даних з пристроїв, вилучення змістовних висновків та

підтримки прийняття рішень за допомогою таких інструментів, як алгоритми машинного навчання.

Рівень додатків - це інтерфейс для користувачів, щоб візуалізувати дані, отримувати сповіщення, керувати пристроями та користуватися аналітикою, що генерується системою.

Інфраструктура Інтернету речей зазвичай дотримується такого операційного процесу:

Збір даних - датчики збирають дані з навколишнього середовища.

Передача даних - дані надсилаються на шлюзи або периферійні пристрої за допомогою різних бездротових або дротових протоколів.

Обробка даних - дані потім надсилаються в хмару або на периферію для зберігання та складного аналізу.

Генерація аналітики - інструменти аналітики та машинного навчання обробляють ці дані, щоб знаходити закономірності та генерувати практичні висновки.

Дія та керування - на основі отриманих даних система може запускати автоматизовані дії за допомогою виконавчих механізмів або надавати користувачам інформацію для прийняття рішень.

Рівень сприйняття є базовим рівнем у стеку інфраструктури Інтернету речей. Він відповідає за сприйняття та отримання даних з фізичного середовища за допомогою таких пристроїв, як датчики, виконавчі механізми, RFID-мітки та камери. Ці компоненти відстежують реальні змінні, включаючи температуру, рух, вологість, освітлення та інші параметри, перетворюючи фізичні явища на цифрові сигнали. Якість та надійність даних, що генеруються на рівні сприйняття, значно впливають на продуктивність наступних рівнів у стеку Інтернету речей.

Правильне розгортання та калібрування пристроїв рівня сприйняття є критично важливими, оскільки неточні або недостатні дані призводять до недосконалої аналітики та прийняття неефективних рішень. Цей рівень

може працювати в різноманітних, а іноді й суворих умовах, вимагаючи від пристроїв надійності та низького енергоспоживання. Масштабованість та простота обслуговування також є центральними міркуваннями, оскільки розгортання Інтернету речей може включати тисячі або навіть мільйони кінцевих точок, розподілених по великих географічних районах.

Рівень з’єднання сприяє передачі даних від пристроїв рівня сприйняття до центральних систем обробки або зберігання. Він охоплює поєднання дротових (Ethernet, оптоволокно) та бездротових протоколів зв’язку, таких як Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT та стільниковий зв’язок 5G. Вибір протоколу залежить від вимог до дальності, пропускної здатності, енергоспоживання та середовища розгортання. Надійне з’єднання забезпечує своєчасну та точну передачу даних між пристроями IoT, шлюзами та ширшою мережею.

Стільниковий зв'язок відіграє вирішальну роль у розгортанні Інтернету речей, особливо для застосувань, які потребують зв'язку на великі відстані, мобільності та покриття у віддалених районах. Такі технології, як LTE-M, NB-IoT та 5G, оптимізовані для випадків використання Інтернету речей, пропонуючи низьке енергоспоживання, безпечний зв'язок та широке географічне охоплення.

Стільникові мережі особливо корисні в таких галузях, як логістика, сільське господарство та розумні міста, де фіксована інфраструктура є непрактичною або недоступною. Ці мережі також мають переваги надійності операторського рівня, централізованого управління та інтеграції з автентифікацією пристроїв на основі SIM-картки, що робить їх добре придатними для масштабованих та безпечних впроваджень Інтернету речей.

Шлюзовий рівень слугує мостом між периферійними пристроями, що збирають дані, та системами вищого рівня, такими як хмарні платформи або локальні сервери. Шлюзи агрегують дані з численних датчиків і пристроїв,

за потреби перетворюючи протоколи, фільтруючи непотрібну інформацію та іноді виконуючи початкову обробку даних перед передачею даних вгору. Цей рівень часто обробляє засоби безпеки, автентифікацію пристроїв і гарантує, що лише авторизовані та відформатовані дані надходять далі в систему Інтернету речей.

Розгортання шлюзових пристроїв покращує масштабованість, зменшуючи кількість прямих підключень пристроїв, необхідних для серверної інфраструктури, усуваючи вузькі місця в комунікації. Шлюзи особливо важливі під час розгортання Інтернету речей у середовищах з різними типами пристроїв і протоколів, забезпечуючи сумісність. Вони також пропонують можливості для реалізації локальної обробки, що може зменшити затримку для чутливих до часу програм і зменшити пропускну здатність, необхідну для передачі великих обсягів даних у хмару.

Хмарні платформи забезпечують масштабовані можливості зберігання, обчислень та аналітики, необхідні для управління та інтерпретації даних Інтернету речей. Сучасний Інтернет речей спирається на хмарні сервіси для агрегації та обробки величезних потоків інформації, застосування алгоритмів машинного навчання та забезпечення віддаленого керування пристроями. Хмарні платформи, такі як AWS IoT, Microsoft Azure IoT, пропонують інструменти для обробки реєстрації пристроїв, отримання даних, обробки подій, візуалізації та інтеграції з бізнес-додатками.

Периферійні обчислення доповнюють хмару, наближаючи обчислення до джерела даних, часто в межах шлюзів або спеціалізованих периферійних серверів. Це зменшує затримку, підтримує аналітику в режимі реального часу та зменшує навантаження на централізовану хмарну інфраструктуру. Периферійні обчислення мають вирішальне значення для чутливих до часу або ресурсомістких програм, де локальне прийняття рішень може уникнути затримок, властивих хмарним передачам даних.

Балансування завдань обробки між хмарою та периферією є важливим для адаптивної, стійкої та ефективної інфраструктури Інтернету речей.

Рівень обробки та аналітики даних перетворює необроблені вхідні дані від датчиків і пристроїв на практичну інформацію. Цей рівень займається нормалізацією, агрегацією, очищенням та зберіганням даних, готуючи великі обсяги інформації для подальшого аналізу. Розширена аналітика, включаючи виявлення подій у режимі реального часу, машинне навчання та прогнозне моделювання, дозволяє організаціям отримувати цінність від розгортання своїх IoT-систем, виявляючи тенденції, аномалії та можливості оптимізації.

Своєчасна та ефективна обробка даних є важливою в Інтернеті речей, оскільки затримки або помилки можуть призвести до втрачених бізнес-можливостей і навіть до фізичних ризиків для безпеки. Цей рівень повинен підтримувати масштабованість для обробки даних як з малих, так і з масивних розподілених сенсорних мереж. Він також вимагає інтеграції з інструментами панелей інструментів, системами сповіщень та API, щоб аналітичні дані могли надаватися туди і тоді, коли вони найбільше потрібні, надаючи користувачам можливість швидко діяти на основі актуальної інформації.

Рівень додатків – це найвищий рівень інфраструктури Інтернету речей, який відповідає за відображення даних у користувацьких додатках або інтеграцію аналітики пристроїв у системи робочих процесів бізнесу. Він надає інтерфейси, такі як панелі інструментів, мобільні додатки або API, які дозволяють кінцевим користувачам керувати пристроями, аналізувати дані або автоматизувати процеси. Застосування варіюються від систем промислового управління та панелей моніторингу охорони здоров’я до споживчих додатків для розумного дому та інструментів управління муніципальною інфраструктурою.

Цей рівень повинен задовольняти різноманітні вимоги зацікавлених сторін, забезпечуючи зручність використання, доступність та налаштовувані функції. Безпека та конфіденційність даних тут мають першочергове значення, оскільки програми часто надають конфіденційні операційні дані зовнішнім користувачам. Розширюваність також необхідна; у міру розвитку рішень Інтернету речей виникатимуть нові функції, типи пристроїв та вимоги до інтеграції. Ефективність рівня додатків часто визначає відчутну бізнес-цінність, отриману від розгортання Інтернету речей.

1.2 Архітектура IoT-систем та основні компоненти

Корпоративний Інтернет речей (Enterprise IoT) – це технологія Інтернету речей (IoT) у великих організаціях для підключення пристроїв, систем та датчиків IoT, збору даних у режимі реального часу, автоматизації та прийняття інтелектуальних рішень. Йдеться про інтеграцію багатьох пристроїв, включаючи вбудовані обчислювальні пристрої, в екосистемі IoT, в одну мережу .

Ідея полягає в тому, щоб дозволити підприємствам краще контролювати, керувати та оптимізувати свої процеси. Компанії можуть автоматизувати робочі процеси, зменшити ручне втручання та підвищити операційну ефективність, використовуючи підключені технології. Інтернет речей у підприємствах є ключовою частиною цифрової трансформації та підтримки конкурентоспроможності, дозволяючи приймати більш розумні бізнес-рішення за допомогою розширеної аналітики.

Інтернет речей для підприємств стає дедалі важливішим для великих компаній, оскільки зростає потреба в адаптивності, стійкості та цифровій інтеграції в конкурентному світі. Оскільки бізнес перебуває під тиском щодо покращення обслуговування клієнтів, спрощення операцій та

автоматизації робочих процесів, рішення для бізнесу в галузі Інтернету речей стають основою для досягнення цієї мети.

Перехід до даних у режимі реального часу, прогнозної аналітики та підключених систем зумовлений необхідністю бути гнучким та проактивним у світі, що змінюється. Зі складнішими ланцюгами поставок та вищими очікуваннями клієнтів, Інтернет речей є ключем до прозорості, оперативності реагування та випередження конкурентів, забезпечуючи при цьому ефективне управління пристроями Інтернету речей. Не кажучи вже про те, що в довгостроковій перспективі бізнес працює ефективніше і, отже, заощаджує гроші.

Однією з найбільших переваг пристроїв Інтернету речей є підвищення операційної ефективності та зниження експлуатаційних витрат. Використовуючи інтелектуальні датчики, аналіз даних у режимі реального часу та машинне навчання, підприємства можуть автоматизувати рутинні завдання, оптимізувати споживання енергії, зменшити кількість відмов обладнання та оптимізувати логістику. Результатом є не лише економія коштів, але й краще управління запасами та зменшення простоїв. Така операційна ефективність оптимізує кожну частину бізнесу, від ланцюгів поставок до внутрішніх робочих процесів, забезпечуючи значні інвестиції в довгострокове підвищення продуктивності.

Системи Інтернету речей дозволяють контролювати умови праці в режимі реального часу, що дозволяє виявляти та пом'якшувати потенційні ризики. Наприклад, у промисловому середовищі промислові програми Інтернету речей можуть виявляти несправності обладнання та зміни умов навколишнього середовища, а також забезпечувати дотримання правил охорони праці та техніки безпеки. Однак інтеграція цих систем також створює новий ризик для безпеки, що вимагає надійних заходів безпеки для підприємств Інтернету речей. Проактивний підхід до Інтернету речей

означає менше нещасних випадків, безпечніших працівників, кращі умови праці, а також зниження відповідальності та витрат.

Прийняття рішень на основі даних

За допомогою Інтернету речей (IoT) можна збирати та аналізувати величезні обсяги конфіденційних даних з різних джерел, щоб приймати рішення на основі даних. Дані в режимі реального часу надають критично важливу інформацію для прогнозування тенденцій, виявлення проблем та оптимізації процесів. Це дозволяє коригувати свою стратегію на ходу та бути гнучким у світі, що змінюється. Крім того, корпоративні IoT-додатки підтримують прогнозне обслуговування, виявляючи проблеми до того, як вони стануть серйозними, що дозволяє зменшити час простою та витрати.

Впровадження рішень Інтернету речей може дати значну конкурентну перевагу . Завдяки підвищенню ефективності, кращому управлінню ресурсами та пропонуванні нових моделей обслуговування ви можете надавати кращі продукти та краще реагувати на потреби клієнтів. На швидкозмінному ринку компанії, які впроваджують технології Інтернету речей, мають кращі можливості для досягнення успіху, оскільки вони є більш гнучкими та можуть надавати рішення в режимі реального часу, що відповідають вимогам ринку.

Виробництво – це сектор, де машинобудування з'явилося вже давно.

Кожна виробнича компанія відрізняється. У них є власні машини та процеси, тому існує величезне поле для автоматизації на замовлення та підключення фізичних об'єктів і машин таким чином, щоб можна було аналізувати дані згодом. Під даними я маю на увазі, наприклад, журнали пристроїв для отримання статистики. Наявність даних – це дуже важливо. Дані допомагають приймати кращі рішення, які можуть або оптимізувати ваш прибуток, або призвести до нових потоків доходів.

Приклад екосистеми Інтернету речей для виробничих корпоративних пристроїв

Отже, спочатку потрібно змусити машини спілкуватися. Тут важко говорити про стандарти, але деякі пристрої мають можливість підключатися до локальної мережі через кабель Ethernet, а потім передавати дані через протокол, такий як OPC UA або MQTT.

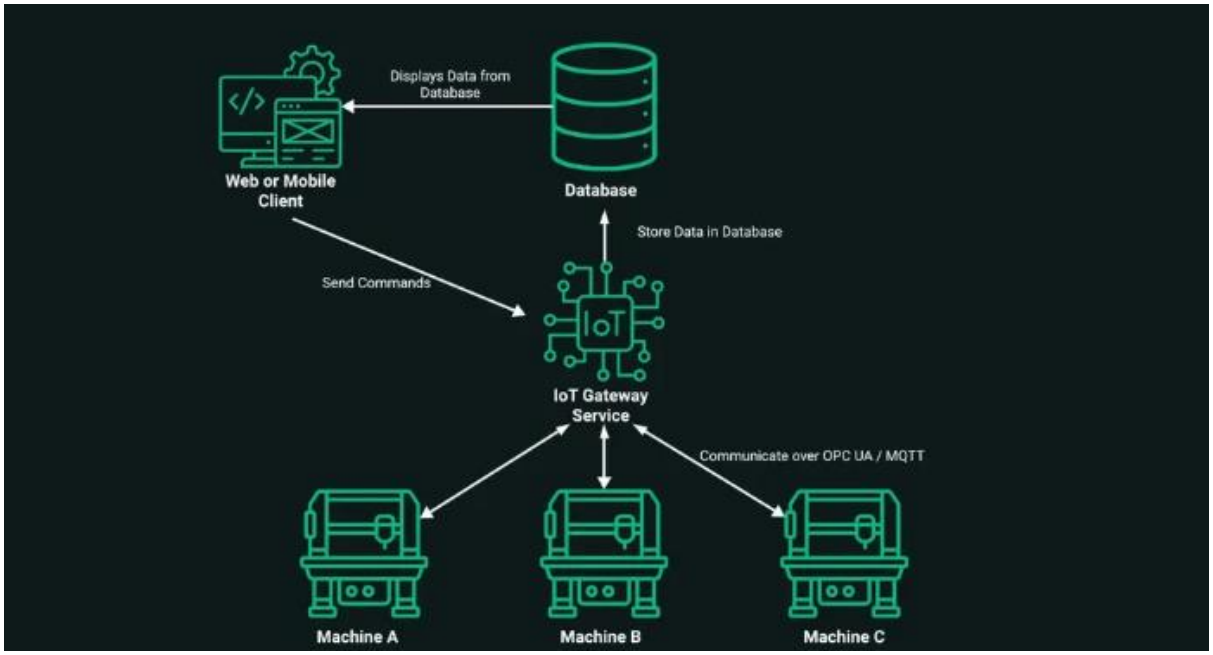

Рис. 1.1. Стандартизована архітектура IoT

Інтернет речей у сфері охорони здоров'я часто описують як IoMT (Інтернет медичних речей) . Це використання розумних пристроїв для моніторингу здоров'я пацієнтів та оптимізації медичних процесів. Прикладами є пристрої Інтернету речей для дистанційного моніторингу пацієнтів та портативні медичні пристрої. Такі підключені фізичні продукти дозволяють покращити догляд за пацієнтами[1].

Прикладом IoMT є монітор життєво важливих параметрів пацієнта . Ця система збирає дані в режимі реального часу про життєво важливі показники, такі як частота пульсу та рівень кисню, і надсилає їх безпосередньо медичним працівникам для моніторингу та аналізу. Це

приклад того, як IoT може покращити догляд за пацієнтами, виявляючи стани здоров'я на ранній стадії, підтримуючи своєчасне медичне втручання та оптимізуючи загальну медичну допомогу в клінічних умовах.

Інтернет речей у сільському господарстві використовує розумні пристрої для оптимізації ведення сільського господарства, економії енергії та зменшення споживання ресурсів. Прикладами є датчики вологості ґрунту на базі Інтернету речей та метеостанції, які відстежують умови в режимі реального часу. Ці пристрої дозволяють фермерам автоматизувати зрошення, забезпечуючи використання води лише за необхідності, що значно зменшує споживання енергії.

Прикладом сільськогосподарських технологій Інтернету речей є система точного зрошення. Аналізуючи дані ґрунтових та погодних датчиків, вона автоматизує графіки поливу, щоб мінімізувати втрати енергії та води, підвищуючи сталий розвиток та збільшуючи врожайність сільськогосподарських культур. Такі рішення підкреслюють трансформаційний вплив Інтернету речей на сучасне сільське господарство.

Інтернет речей (IoT) на підприємстві вимагає чіткого розуміння бізнес-потреб та стратегії, яка узгоджує технологію IoT з бізнес-цілями. Організації повинні забезпечити, щоб їхні IoT-проекти приносили відчутну цінність, вирішували ключові проблемні питання та сприяли досягненню загальних бізнес-цілей.

Масштабованість та сумісність важливі під час розгортання платформи Інтернету речей, особливо у великих організаціях. Рішення Інтернету речей повинні мати можливість розвиватися разом з бізнесом, а нові пристрої повинні бути сумісними з існуючими системами. Підприємствам слід вибирати платформи Інтернету речей, які можуть інтегруватися з широким спектром пристроїв та мереж Інтернету речей, щоб вони могли бути гнучкими відповідно до розвитку своїх потреб.

Впровадження Інтернету речей може бути дорогим на початку, враховуючи інвестиції в апаратне та програмне забезпечення, підключення та інтеграцію з існуючими системами. Підприємства повинні провести аналіз витрат і вигод, щоб зрозуміти рентабельність інвестицій та визначити, де Інтернет речей може принести найбільшу економію коштів з часом.

Технологія Інтернету речей може бути перешкодою для багатьох організацій. Впровадження Інтернету речей передбачає інтеграцію багатьох пристроїв, обробку кількох протоколів зв'язку та управління величезними обсягами даних. Щоб подолати ці труднощі, підприємствам слід співпрацювати з досвідченими постачальниками рішень Інтернету речей та інвестувати в навчання співробітників, щоб зробити впровадження більш плавним.

Обсяг даних, що генеруються пристроями Інтернету речей, є серйозною проблемою безпеки та конфіденційності. Для багатьох компаній це може бути причиною нових ризиків безпеці. Підприємства повинні впроваджувати найкращі практики шифрування даних, безпечної автентифікації пристроїв та конфіденційності користувачів, щоб їхні пристрої Інтернету речей не були вразливими до кібератак. Захист пристроїв та даних, які вони генерують, є ключем до зменшення нових ризиків безпеки , зміцнення довіри та дотримання правил конфіденційності.

Інтернет речей генерує величезні обсяги даних, які потрібно зберігати, керувати ними та аналізувати. Успішна стратегія Інтернету речей включає надійну інфраструктуру управління даними та передові інструменти аналітики для перетворення необроблених даних на практичну інформацію. Підприємствам слід інвестувати в хмарні рішення

для зберігання даних та платформи аналітики даних, які можуть витягувати цінну інформацію з потоку даних Інтернету речей.

Міжплатформна інтеграція стає ключовою тенденцією, оскільки пристрої Інтернету речей повинні безперешкодно взаємодіяти один з одним. Підприємства рухаються до відкритих стандартів, які дозволяють різним пристроям і системам Інтернету речей безперешкодно інтегруватися, щоб дані могли передаватись, а дії можна було координувати між кількома програмами та платформами.

Периферійні обчислення використовуються разом з Інтернетом речей (IoT) для обробки даних ближче до місця їх генерації, щоб зменшити затримку та забезпечити прийняття рішень у режимі реального часу. Поєднання Інтернету речей зі штучним інтелектом відкриває нові можливості для прогнозної аналітики та автономних операцій, роблячи корпоративні процеси розумнішими та ефективнішими.

Сталий розвиток стає ключовою частиною проектів Інтернету речей. Підприємства використовують Інтернет речей для зменшення споживання енергії, мінімізації відходів та моніторингу впливу на навколишнє середовище. Рішення Інтернету речей можуть допомогти компаніям досягти своїх цілей сталого розвитку, надаючи дані для оптимізації використання ресурсів та зменшення їхнього вуглецевого сліду[2].

1.3 Типи IoT-пристроїв та сфери їх використання

У розумних містах інфраструктура Інтернету речей відіграє вирішальну роль в оптимізації транспортного потоку, управлінні вуличним освітленням, моніторингу стану навколишнього середовища та підвищенні громадської безпеки. Датчики, вбудовані в дороги та світлофори, збирають дані про рух транспортних засобів та пішоходів у режимі реального часу, що дозволяє динамічно регулювати світлофори для зменшення заторів.

Системи управління відходами використовують сміттєві баки на базі Інтернету речей, які сигналізують про необхідність їх вивезення, зменшуючи споживання палива та підвищуючи ефективність санітарії в міських регіонах.

Окрім операційних удосконалень, інфраструктура Інтернету речей розумного міста підтримує стале використання ресурсів та реагування на надзвичайні ситуації. Датчики погоди, якості повітря та шуму надають дані, що використовуються для інформування мешканців, формування міської політики та вжиття заходів щодо пом'якшення наслідків у разі несприятливих умов. Застосунки громадської безпеки, такі як камери спостереження та підключені аварійні сигналізації, покращують час реагування правоохоронних органів та готовність до стихійних лих. Усі ці системи покладаються на стійку, масштабовану інфраструктуру Інтернету речей для координації та аналізу величезних потоків інформації на благо громадян.

Інфраструктура Інтернету речей (IoT) є центральною для сучасного виробничого середовища, де вона дозволяє здійснювати моніторинг обладнання в режимі реального часу, проводити прогнозне обслуговування та оптимізувати процеси. Машини та роботи, оснащені датчиками, генерують дані про продуктивність, температуру, вібрацію та обсяг виробництва, які можна аналізувати для прогнозування збоїв до виникнення простоїв. Використовуючи ці дані, виробники знижують витрати на обслуговування та збільшують час безвідмовної роботи.

Інфраструктура IIoT також підтримує забезпечення якості та видимість ланцюга поставок. Підключені пристрої контролюють стан виробничої лінії, допомагаючи швидко виявляти дефекти або аномалії та автоматизувати коригувальні дії. Інтеграція з ERP (системами планування ресурсів підприємства) та MES (системами виконання виробництва)

гарантує, що інформація з виробничого цеху доступна для ширшої бізнес-аналітики.

Інфраструктура Інтернету речей трансформує ланцюги поставок та логістичні операції, забезпечуючи відстеження в режимі реального часу, моніторинг статусу та автоматизований контроль запасів. Підключені мітки, GPS-трекери та датчики навколишнього середовища, прикріплені до вантажів, дозволяють компаніям контролювати місцезнаходження, температуру, вологість та удари під час транспортування. Це дозволяє проактивно реагувати на затримки або екологічні ризики, підвищуючи надійність доставок та захищаючи товари від втрати або пошкодження.

Таблиця 1.1.

Порівняльна характеристика побутових, промислових та медичних IoT-пристроїв

Тип пристрою	**Приклади**	**Сфера застосування**	**Протоколи зв'язку**	**Особливості**
Побутова сфера (Smart Home)				
Датчики середовища	Термостати, датчики вологості, CO_2, руху	Розумний будинок, енергозбереження	Zigbee, Z-Wave, Wi-Fi	Низьке енергоспоживання, автономна робота
Розумні замки та камери	IP-камери, смарт-замки, відеодзвінки	Безпека, контроль доступу	Wi-Fi, Bluetooth, RTSP	Обробка відео, хмарне зберігання
Побутова техніка	Смарт-холодильники	Автоматизація побуту	Wi-Fi, Matter, Thread	Голосове керування (Alexa, Google)

Продовження таблиці 1.1.

Тип пристрою	Приклади	Сфера застосування	Протоколи зв'язку	Особливості
Промисловий IoT (IIoT)				
Промислові датчики	Датчики тиску, температури, вібрації	Виробництво, моніторинг обладнання	Modbus, OPC-UA, MQTT	Висока надійність, захист IP67+
Промислові контролери (PLC)	Siemens S7, Allen-Bradley, Mitsubishi	Автоматизація ліній, робототехніка	EtherNet/IP, PROFINET	Реальний час, детермінованість
Промислові шлюзи	Edge-комп'ютери, IoT-шлюзи	Локальна обробка даних	4G/LTE, Ethernet, Wi-Fi	Edge-обчислення, протокол-конверсія
Медицина та охорона здоров'я				
Носимі пристрої	Смарт-годинники, фітнес-трекери, патчі	Моніторинг здоров'я, спорт	Bluetooth LE, ANT+	Тривале живлення від батареї
Медичні імплантати	Кардіостимулятори, інсулінові помпи, CGM	Критична медицина	NFC, MICS-діапазон	Надійність life-critical, сертифікація FDA
Медичне обладнання	МРТ, ЕКГ-монітори, ШВЛ-апарати	Лікарні, телемедицина	HL7, DICOM, Wi-Fi	Медичні стандарти, захист даних

Таблиця 1.2.

Порівняльна характеристика IoT-пристроїв для міста, транспорту та сільського господарства

Тип пристрою	**Приклади**	**Сфера застосування**	**Протоколи зв'язку**	**Особливості**
Розумне місто (Smart City)				
Датчики інфраструктури	Датчики рівня води, стану доріг, мостів	Моніторинг інфраструктури	LoRaWAN, NB-IoT	Дальній зв'язок, роки автономної роботи
Розумне освітлення	Адаптивні вуличні ліхтарі	Енергоефективність міста	Zigbee, DALI, LoRa	Датчики руху, авто-димування
Сміттєві контейнери	Смарт-урни з датчиком наповнення	Комунальні послуги	NB-IoT, Sigfox	Оптимізація маршрутів вивезення
Транспорт та логістика				
Системи моніторинг у авто	OBD-трекери, GPS-маяки, телематика	Логістика, страхування	4G/LTE, CAN-bus, GPS	Геолокація, стиль водіння
RFID/NFC-теги	Теги для вантажу, смарт-палети	Склад, ланцюг постачання	RFID (UHF/HF), NFC	Пасивні теги, не потребують батареї

Продовження таблиці 1.2.

Тип пристрою	**Приклади**	**Сфера застосування**	**Протоколи зв'язку**	**Особливості**
Сенсори дронів/роботів	LiDAR, камери, IMU-датчики	Доставка, інспекція	Wi-Fi 6, 5G, MAVLink	Обробка в реальному часі
Сільське господарство (AgriTech)				
Ґрунтові датчики	Вологість ґрунту, pH, температура	Точне землеробство	LoRaWAN, Sigfox, 4G	Автономна робота до 5 років
Метеостанції	Агрометеостанції, прогноз заморозків	Управління врожаєм	LoRa, Wi-Fi, GSM	Мікроклімат, агрономічні сповіщення
Автоматизований полив	Смарт-зрошення, дрони для обприскування	Ефективність водних ресурсів	Zigbee, Z-Wave, Wi-Fi	Інтеграція з прогнозом погоди

Аналітичні платформи обробляють дані цих датчиків для оптимізації маршрутизації, прогнозування термінів доставки та автоматизації складських операцій. Системи управління запасами на базі Інтернету речей автоматично визначають рівень запасів та ініціюють поповнення запасів, зменшуючи накладні витрати та мінімізуючи випадки відсутності товару на

складі. Прозорий потік інформації через логістичну мережу покращує координацію між виробниками, складами та роздрібними торговцями.

В охороні здоров'я інфраструктура Інтернету речей дозволяє безперервно контролювати життєво важливі показники пацієнтів за допомогою портативних пристроїв та підключених медичних пристроїв. Потоки даних у режимі реального часу від моніторів серцевого ритму, датчиків глюкози та манжет для вимірювання артеріального тиску передаються на хмарні платформи, де лікарі можуть аналізувати тенденції та швидко втручатися за необхідності. Дистанційний моніторинг дозволяє пацієнтам залишатися вдома, отримуючи високоякісну допомогу, зменшуючи кількість візитів до лікарні та забезпечуючи раннє втручання при хронічних захворюваннях.

Інтернет речей також є основою критично важливих процесів у лікарнях, таких як відстеження активів та моніторинг навколишнього середовища. Розумні медичні пристрої повідомляють про свій робочий стан та використання, що забезпечує ефективне обслуговування та використання. Інтеграція з електронними медичними картками (EHR) та системами аналітики підтримує персоналізований догляд, управління здоров'ям населення та дотримання правил охорони здоров'я. Надійна та безпечна інфраструктура Інтернету речей є основою для реалізації переваг цифрової трансформації охорони здоров'я.

Інфраструктура Інтернету речей формує основу для багатьох критично важливих функцій у сучасній економіці. Ось кілька критично важливих елементів, які забезпечують безпеку архітектур Інтернету речей.

Автентифікація пристроїв та управління ідентифікацією формують першу лінію захисту в безпеці Інтернету речей. Кожен пристрій, що підключається до мережі Інтернету речей, повинен підтвердити свою ідентичність, щоб запобігти несанкціонованому доступу та забезпечити цілісність даних. Це включає цифрові сертифікати, безпечне надання

ключів, а іноді й апаратні модулі безпеки, які зберігають криптографічні секрети. Централізовані платформи ідентифікації керують реєстрацією, відкликанням та постійною перевіркою пристроїв, забезпечуючи основу для довіреної взаємодії між пристроями.

Впровадження надійних заходів ідентифікації пристроїв є складним завданням через величезну кількість пристроїв та їхні різноманітні можливості. Для датчиків з обмеженими ресурсами часто потрібні легкі протоколи автентифікації, а рішення має бути масштабованим для управління життєвим циклом від виробництва до виведення з експлуатації. Слабке управління ідентифікацією наражає організації на ризики спуфінгу, витоку даних та атак типу «відмова в обслуговуванні», що підкреслює важливість надійних, адаптивних систем автентифікації.

Шифрування є важливим для захисту даних під час їх переміщення між пристроями Інтернету речей, шлюзами та хмарними платформами. Наскрізне шифрування гарантує, що дані не можуть бути перехоплені або змінені під час передачі, а надійні алгоритми шифрування захищають файли, що зберігаються локально або в хмарі. TLS (безпека транспортного рівня) зазвичай використовується для шифрування транспорту, тоді як дані, що зберігаються в базах даних або сховищах, часто захищені за допомогою AES-256 або аналогічних стандартів[4].

Впровадження шифрування в гетерогенному середовищі Інтернету речей створює проблеми, пов'язані з управлінням ключами, сумісністю пристроїв та обчислювальним навантаженням. Легка криптографія, адаптована для Інтернету речей, – це галузь, що швидко розвивається та підтримує пристрої з обмеженими ресурсами. Автоматична ротація ключів, безпечне виділення ресурсів та централізовані системи управління є життєво важливими для підтримки послідовного стану шифрування в міру зростання та змін мережі Інтернету речей, що зменшує ризики в інфраструктурі.

Безпечні оновлення прошивки та програмного забезпечення є критично важливими для зменшення вразливостей у міру появи нових загроз. Інфраструктура Інтернету речей повинна підтримувати механізми автентифікації та перевірки оновлень, гарантуючи, що на пристроях встановлюється лише надійний код. Зазвичай це включає підписання коду, контрольні суми та безпечні процеси завантаження, а також механізми оновлення, які можуть надійно працювати через переривчасті або низькопропускні з’єднання[5].

Збої в процесах оновлення можуть призвести до компрометації пристроїв або операційних збоїв, що підкреслює необхідність надійних та безвідмовних механізмів оновлення. Оновлення по бездротовій мережі (OTA) зазвичай використовуються для масштабних розгортань Інтернету речей, що дозволяє дистанційно встановлювати виправлення без переривання роботи пристроїв. Централізована видимість та контроль над станом оновлень у поєднанні з можливостями відкату необхідні для підтримки безпеки та відповідності вимогам у системах Інтернету речей у міру їх масштабування та розвитку.

Брандмауери захищають критично важливі компоненти інфраструктури Інтернету речей від несанкціонованого зв'язку та атак. Їх можна розгортати в різних точках, включаючи граничні шлюзи, хмарні платформи або навіть на самих пристроях, залежно від можливостей. Сегментація мережі, білий список та мікросегментація допомагають обмежити поширення вторгнень та стримати потенційну шкоду у разі порушення. Брандмауери часто адаптуються для середовищ з низьким енергоспоживанням та вбудованих середовищ у розгортаннях Інтернету речей.

Системи виявлення вторгнень (IDS) забезпечують моніторинг у режимі реального часу на предмет ознак компрометації або аномальної поведінки, таких як неочікувані моделі трафіку, аномальні команди або

спроби використання відомих вразливостей. Сучасні рішення IDS використовують машинне навчання для підвищення точності виявлення та зменшення кількості хибнопозитивних результатів. Інтеграція з централізованими центрами операцій безпеки (SOC) дозволяє швидко отримувати сповіщення та скоординовано реагувати на загрози, що розвиваються[6].

Інфраструктура Інтернету речей часто працює в галузях із суворими нормативними вимогами щодо збору, зберігання та обробки даних. Стандарти відповідності, такі як GDPR, HIPAA або галузеві рекомендації, диктують контроль за особистою або конфіденційною інформацією. Організації повинні впроваджувати заходи контролю доступу, ведення журналу аудиту та мінімізації даних, щоб залишатися дотриманими вимог та уникати суттєвих штрафів. Забезпечення прозорості в практиці обробки даних також є обов'язковим згідно з багатьма нормативними актами[7].

Конфіденційність даних стосується не лише юридичних вимог, а й підтримки довіри користувачів. Програми Інтернету речей збирають величезні обсяги конфіденційної інформації, і будь-яке порушення може мати серйозні наслідки для репутації та експлуатації. Конфіденційність на етапі проектування – вбудовування засобів контролю конфіденційності в дизайн пристроїв та інфраструктури з самого початку – є надзвичайно важливою. Надійні процедури управління згодою користувачів, анонімізації даних та реагування на порушення є критично важливими елементами архітектури конфіденційності будь-якого розгортання Інтернету речей.

1.4 Основні протоколи передачі даних в IoT

Прикладний рівень – це верхній рівень моделі OSI. На цьому рівні протоколи виконують найбільш ресурсоємні процеси, що відповідають за

обмін повідомленнями між кінцевими пристроями та програмними застосунками. [8]

AMQP — це протокол відкритого стандарту, що використовується для обміну повідомленнями та управління чергами. Він забезпечує надійну та впорядковану доставку повідомлень, підтримує різноманітні схеми зв'язку та пропонує високий ступінь сумісності. AMQP широко впроваджується у фінансовому секторі та корпоративних комунікаціях.

HTTP – це широко використовуваний протокол для передачі веб-сторінок і даних через Інтернет. Ця технологія проста у впровадженні та використовує існуючу веб-інфраструктуру. HTTP часто розгортається в системах розумного дому, які потребують інтеграції з веб-сервісами.

Протокол WebSocket забезпечує низьку затримку та ефективну передачу даних. Він ідеально підходить для програм реального часу, таких як онлайн-ігри, платформи фінансової торгівлі та програми чату.

Протокол LwM2M спеціально розроблений для керування пристроями Інтернету речей. Він є ресурсоефективним та забезпечує ефективне дистанційне налаштування та моніторинг енергетичних та комунальних програм.

XMPP (Розширюваний протокол обміну повідомленнями та присутності)

Протокол розширюваного обміну повідомленнями та присутності (Extensible Messaging and Presence Protocol) – це технологія керування обміном повідомленнями та присутністю. Керування присутністю дозволяє партнерам по зв'язку вказувати свою доступність у месенджері. XMPP є гнучким, безпечним, широко розгорнутим та розширюваним. Протокол зазвичай використовується для чат-додатків та соціальних мереж, а також для зв'язку між пристроями в мережах Інтернету речей (IoT).

Протокол SMS добре відомий для надсилання коротких повідомлень через стільникові мережі. SMPP – це стандарт для обміну SMS-

повідомленнями між центрами служби коротких повідомлень та зовнішніми серверами обміну повідомленнями. Обидві технології є надійними та широко розповсюдженими, оскільки вони забезпечують зв'язок між пристроями Інтернету речей через стільникові мережі. Ці технології також широко використовуються в телематиці та управлінні автопарком[9] .

Стандарт USSD – це протокол для зв’язку між мобільними пристроями та серверами додатків операторів мобільного зв’язку. Він швидкий, забезпечує безпечний зв’язок у режимі реального часу, не потребує постійного підключення до Інтернету та не зберігає повідомлення. Протокол Інтернету речей також використовується для мобільних платежів.

Технологія SSI — це простий протокол зв'язку для передачі даних у режимі реального часу між датчиками та комп'ютерами. SSI легко впроваджується та підтримує пряме підключення датчиків та систем керування. Цей протокол Інтернету речей часто використовується в промислових застосуваннях, які потребують ефективної передачі даних датчиків.

CoAP розроблено спеціально для локально обмежених пристроїв та мереж. Він легкий, ефективний, надійний та може бути інтегрований з існуючими веб-сервісами. Протокол Інтернету речей ідеально підходить для систем розумного міста та розумного будинку, які зазвичай обмежені певною територією та потребують ресурсоефективних технологій[10].

Технологія DDS – це протокол для надійного обміну даними в режимі реального часу між пристроями Інтернету речей. Цей стандарт часто використовується для критично важливих для безпеки застосувань в аерокосмічній, оборонній та промисловій автоматизації.

MQTT – це надійний протокол доставки повідомлень. Він простий у впровадженні та підходить для пристроїв Інтернету речей з обмеженою пропускною здатністю та потужністю. Технологія MQTT широко

використовується в домашній автоматизації, моніторингу стану та промисловому моніторингу.

Транспортний рівень – це четвертий рівень у моделі OSI, який забезпечує надійну передачу даних між кінцевими системами. Протоколи цього рівня контролюють потік даних і гарантують, що пакети даних надходять правильно та в правильному порядку[11].

Стандарт TCP – це протокол, орієнтований на з'єднання. Він використовує повідомлення підтвердження, щоб гарантувати надходження пакетів даних у правильному порядку та без втрат. Протокол в основному використовується в промисловій автоматизації, охороні здоров'я та критично важливих для безпеки додатках. Цілісність даних, яка стосується правильності, повноти та безпеки даних, є критично важливою в цих сферах Інтернету речей.

UDP — це протокол без встановлення з'єднання, який надсилає пакети даних безпосередньо одержувачу без попереднього встановлення з'єднання. Технологія забезпечує низьку затримку та швидку передачу даних, а також використовується для некритичних застосувань, таких як потокове відео та передача голосу через Інтернет-протокол (VoIP), де випадкові простої не обов'язково впливають на цілісність даних.

Мережевий рівень – це третій рівень моделі OSI. Він відповідає за пересилання пакетів даних між різними мережами. Відповідні протоколи визначають, яким маршрутом пакети даних ефективно досягають пункту призначення.

IP – це широко використовуваний протокол для адресації та маршрутизації пакетів даних в Інтернеті. Він гнучкий і сумісний практично з будь-яким типом мережі та пристрою. Стандарт IP реалізовано майже у всіх додатках Інтернету речей, включаючи розумні будинки, носимі пристрої та промислову автоматизацію.

Протокол 6LoWPAN сприяє ефективному використанню пропускної здатності та потужності. Він спеціально розроблений для бездротових мереж з низьким енергоспоживанням і забезпечує безперешкодну інтеграцію невеликих пристроїв Інтернету речей (IoT) в Інтернет з мінімальним споживанням енергії. Технологія широко застосовується для розумних міст, домашньої автоматизації та промислових сенсорних мереж, де енергоефективність та низька вартість володіння є критично важливими.

Канальний рівень – це другий рівень моделі OSI. Технології цього рівня забезпечують безпомилкову передачу даних між двома безпосередньо підключеними пристроями.

Інститут інженерів з електротехніки та електроніки (IEEE) розробляє та підтримує кілька стандартів передачі даних. Вони є надійними, сумісними з багатьма типами мереж та взаємодіють між пристроями та постачальниками. Одним із таких протоколів є IEEE 802.15.4, базовий стандарт для ZigBee, енергоефективного протоколу Інтернету речей для низькоенергетичних пристроїв та інших бездротових мереж. IEEE 802.15.4 в основному використовується в домашній автоматизації, промисловому моніторингу та сенсорних мережах[11].

Технологія LPWAN включає кілька протоколів, таких як LoRaWAN та NB-IoT. Стандарт LoRaWAN підтримує передачу даних на великі відстані, тоді як NB-IoT ідеально підходить для пристроїв з низьким енергоспоживанням. LPWAN не тільки пропонують як велику дальність дії, так і енергоефективність, вони також з'єднують пристрої на великі відстані та подовжують термін служби їх батареї. Застосування включають розумні міста, сільське господарство, моніторинг навколишнього середовища та цифровізацію логістики.

Фізичний рівень – це найнижчий рівень моделі OSI. Протоколи на цьому рівні керують передачею бітів через середовище передачі, таке як мідний дріт, оптоволоконний кабель або радіохвилі.

Bluetooth — це бездротова технологія для передачі даних на короткі відстані. BLE — це версія Bluetooth з низьким енергоспоживанням, яка ідеально підходить для пристроїв з живленням від батарейок. Обидва протоколи є недорогими та простими варіантами передачі даних. Носимі пристрої, пристрої розумного дому та медичні програми часто використовують Bluetooth та BLE[12].

Технологія Ethernet є поширеним стандартом для дротових мереж. Як протокол Інтернету речей, Ethernet забезпечує надійну та швидку передачу даних, ідеально підходить для Індустрії 4.0 та розумних будівель, де потрібна висока пропускна здатність.

Стандарти мобільного зв'язку забезпечують бездротовий зв'язок на великих відстанях. LTE та 5G забезпечують високу швидкість передачі даних та низьку затримку, тоді як 2G, GPRS та 3G, навпаки, мають нижчу продуктивність, але широко використовуються. Застосування Інтернету речей включають розумні міста, автономне водіння та мобільні пристрої Інтернету речей.

Протокол NFC підтримує бездротовий зв'язок на дуже коротких відстанях, зазвичай кілька сантиметрів. NFC простий у використанні, забезпечує швидку передачу даних і не вимагає сполучення пристроїв, як Bluetooth. Технологія використовується в безконтактних платіжних системах та для обміну інформацією між пристроями.

Стандарт ПЛК використовує існуючі лінії електропередач для передачі даних, що забезпечує економічно ефективне мережеве рішення без необхідності додаткової проводки. ПЛК ідеально підходить для передачі даних усередині будівель і часто використовується для систем «розумного будинку» та автоматизації будівель.

Протокол LPWAN LoRaWAN — це бездротова технологія для зв'язку на великі відстані, що дозволяє передати дані на великі відстані з низьким

енергоспоживанням. Вона ідеально підходить для пристроїв з живленням від батарей на великих площах, таких як сільське господарство.

Бездротовий мережевий протокол Sigfox оптимізовано для низьких швидкостей передачі даних та великих відстаней. Sigfox є енергоефективним, економічно ефективним та простим у розгортанні. Ця технологія використовується для програм відстеження активів та інтелектуального обліку.

Стандарт Neocortec — це надійне та масштабоване рішення для підключення багатьох пристроїв Інтернету речей. Він забезпечує гнучкий та енергоефективний зв'язок для Індустрії 4.0 та розумних будівель.

Протокол Weightless IoT підходить для бездротового зв'язку на великих відстанях з низькою швидкістю передачі даних. Він призначений для застосувань, які мають періодичні потреби в передачі даних, таких як інтелектуальне вимірювання або відстеження активів[13].

Технологія RFID використовує радіохвилі для ідентифікації та відстеження об'єктів. Вона швидка, надійна, безконтактна та може застосовуватися в різних середовищах, включаючи логістику 4.0 , управління запасами та системи контролю доступу.

Широко поширена технологія Wi-Fi створює локально обмежені мережі. Її легко розгорнути, вона сумісна з багатьма пристроями та програмами, а також забезпечує швидку передачу даних. Розумні будинки, офісні будівлі та громадські точки доступу – усі вони використовують Wi-Fi.

Протокол Z-Wave розроблений для домашньої автоматизації. Він енергоефективний, простий в установці та підтримує високий рівень сумісності між пристроями різних виробників. Z-Wave в основному використовується в системах розумного дому, таких як освітлення, безпека та системи моніторингу.

Технологія ZigBee — це низькоенергетичний протокол Інтернету речей. Він ідеально підходить для пристроїв з живленням від батарейок у системах розумного будинку, промислової автоматизації та охорони здоров'я[14].

1.5 Аналіз сучасних кіберзагроз для IoT-систем

Критичною проблемою в мережах Інтернету речей є безпечний розподіл групових ключів між різними пристроями з обмеженими обчислювальними ресурсами. Таким чином, дослідники попереднього дослідження розробили централізовану систему управління, побудовану на програмно-визначених мережах (SDN), та включили модифікований протокол одностороннього дерева функцій (MOFT) для вирішення цієї проблеми. Представлений підхід захищає від атак змови та досягає значного підвищення ефективності, зменшуючи накладні витрати на зв'язок на 39% порівняно з традиційними методами OFT. Дослідники підтвердили своє рішення за допомогою формального аналізу безпеки, продемонструвавши ефективну стійкість до змови, зберігаючи при цьому оптимальну обчислювальну ефективність [15].

Для підвищення безпеки зв'язку між транспортним засобом та інфраструктурою (V2I) було розроблено новий метод автентифікації для Інтернету транспортних засобів. Цей метод використовує криптографію з відкритим ключем, але підвищує ефективність шляхом інтеграції криптографії еліптичних кривих (ECC), нечітких екстракторів та фізичних неклонованих функцій (PUF), що дозволяє уникнути обчислювально ресурсоємних білінійних пар. Протокол розроблено таким чином, щоб витримувати атаки по бічних каналах та спроби захоплення, здійснені дорожнім блоком (RSU). Крім того, включення значень Діффі-Хеллмана досягає ідеальної прямої секретності. Результатом є демонстративно

безпечний протокол, перевірений за моделлю випадкового оракула, який пропонує знижені обчислювальні вимоги та накладні витрати на зв'язок порівняно з аналогічними схемами автентифікації [16].

Критична потреба в безпечних та ефективних протоколах автентифікації в підводних акустичних мережах (UAN) була задоволена завдяки новим дослідженням. UAN, які використовуються для управління морськими ресурсами, були визначені як вразливі до атак через обмеження енергії та схильність до захоплення. Було запропоновано легкий протокол автентифікації для UAN з метою захисту від захоплення датчиків та шлюзів під час атак. Підвищена безпека та ефективність, порівняно з існуючими схемами, були досягнуті завдяки протоколу, розробленому на основі фізичних неклонованих функцій (PUF) та хаотичних карт. Безпека запропонованого протоколу була офіційно доведена в моделі випадкового оракула, і його продуктивність продемонструвала свою придатність для обмеженого ресурсами характеру UAN. Було підкреслено наслідки для ширшої безпеки Інтернету речей, оскільки проблеми, з якими стикаються підводні сенсорні мережі, відображають ті, що виникають у багатьох пристроях Інтернету речей з обмеженими ресурсами, розгорнутих у несприятливих середовищах. Представлений підхід до автентифікації в обмежених середовищах можна вважати цінним для інформування про проекти безпеки в різних застосуваннях Інтернету речей, де пристрої піддаються подібним обмеженням та загрозам [17].

Для вирішення зростаючих проблем безпеки в мережах Інтернету речей (IoT), зокрема потреби в ефективному виявленні вторгнень, було представлено нову систему спільного виявлення вторгнень (CIDS). Запропонована CIDS розроблена для ієрархічної структури IoT, використовуючи архітектуру «периферія-туман-хмара» в поєднанні з федеративним навчанням (FL). Дослідження демонструє значні переваги завдяки розподіленому навчанню системи за допомогою федеративного

навчання на частині набору даних CICIoT2023 (зокрема, на позначеній ненезалежній та ідентично розподіленій (не-IID) підмножині). CIDS досягає зменшення затримки та меншого використання ресурсів, зберігаючи при цьому точність виявлення вторгнень. Дослідження також надає контрольний показник продуктивності, демонструючи, що цей підхід призводить до кращих результатів, таких як коротший час навчання та зменшення мережевого трафіку, порівняно з традиційними моделями виявлення вторгнень на основі централізованого навчання [18].

Через широке використання пристроїв Інтернету речей (IoT) у повсякденному та професійному житті, наголошується на необхідності забезпечення їхньої безпеки. Було створено автоматизовану систему для створення детальної бази даних під назвою VARIoT, щоб задовольнити потребу в кращій інформації про вразливості для пристроїв IoT. Ця система використовує обробку природної мови, машинне навчання та спеціалізовані фільтри для автоматичного збору описів вразливостей та їх зв'язування з кодом експлойтів з різних неструктурованих джерел. Система ефективно класифікує вразливості та призначає оцінки достовірності, що дозволяє користувачам виявляти критичні недоліки безпеки, навіть коли деталі продукту незрозумілі або відсутні [19].

Ще одним контекстом застосування систем Інтернету речей є Інтернет речей (WoT). Було проведено детальний аналіз для ретельного вивчення безпеки WoT. Цей аналіз включав створення моделей загроз, визначення різних типів атак — від атак типу «відмова в обслуговуванні» та «людина посередині» до атак методом ін'єкцій та фізичних атак — та пропонування захисних стратегій. Ці засоби захисту включають надійну автентифікацію, шифрування даних та методи ізоляції. Архітектура системи та потенційні ситуації атак візуалізуються за допомогою UML та діаграм послідовностей. Результатом цієї роботи є запропонована

архітектура безпеки, яка може служити орієнтиром для середовищ WoT [20].

Ще одна проблема, що досліджується в контексті Інтернету речей, полягає в тому, як люди емоційно реагують на порушення кібербезпеки, що впливають на різні пристрої розумного дому. За допомогою онлайн-дослідження та реального польового експерименту дослідники використовували спеціальну анкету для вимірювання сили емоцій, схильності людей до дій та типу реакцій (когнітивні/мотиваційні проти суто емоційних). Ключові результати дослідження показують, що у разі порушення безпеки розумні камери викликають найпотужніші емоційні реакції. Крім того, дослідження показує, що усвідомлення порушень безпеки впливає на інтенсивність емоційних реакцій [21].

Висновки до розділу 1

Розробка нових послуг в рамках Інтернету речей значною мірою залежить від вирішення проблем безпеки та пошуку нових рішень для різних застосувань. Представлені дослідження розглядають ключові питання, досліджуючи обмеження ресурсів та децентралізовані системи, а також пропонуючи програмно-визначений мережевий підхід для ефективного управління груповими ключами. Також представлені вдосконалені методи автентифікації для зв'язку між транспортним засобом та інфраструктурою, використовуючи ефективну криптографію та фізично неклоновані функції. Крім того, проактивна безпека вдосконалюється за допомогою спільної системи виявлення вторгнень на основі федеративного навчання разом з автоматизованою базою даних вразливостей для покращеного виявлення загроз. Нарешті, людський аспект безпеки Інтернету речей розглядається шляхом дослідження емоційних реакцій

користувачів на інциденти безпеки, з акцентом на ширших наслідках кібербезпеки в підключених середовищах.

РОЗДІЛ 2.ПОБУДОВА МОДЕЛІ ЗАГРОЗ ДЛЯ IOT-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

2.1 Формування структури IoT-інфраструктури підприємства

SM забезпечує вдосконалений режим виробництва, заснований на глибокій інтеграції передових виробничих технологій та інформаційних технологій нового покоління. Ці технології проходять через увесь життєвий цикл продукту, від проектування, виробництва, продажів, логістики та послуг [9]. SM має характеристики самосприйняття, самостійного прийняття рішень, самовиконання, самоадаптації та самонавчання, і його метою є покращення якості, ефективності та гнучкості виробничої галузі.

Інфраструктура IIoT відіграє вирішальну роль у SM. Вона забезпечує допоміжні можливості. Щодо SM, можна вважати, що IIoT являє собою критичну основу, на якій можна будувати наступні кроки [10]. Інфраструктура IIoT не призначена лише для підтримки SM, а й для інших застосувань або галузей. Однак існує сильний перетин між «IIoT» та «SM» з точки зору публічного визнання з боку світових організацій-розробників стандартів (SDO) у сфері передового виробництва та Інтернету речей, організацій та інших зацікавлених груп [11].

Ми пропонуємо концептуальну основу інфраструктури IIoT з точки зору Інтернету речей та SM, як показано на рисунку 2.1. Вона в основному базується на еталонній моделі Інтернету речей та SM [6 , 7]. Досліджуючи та розробляючи спільні засоби на різних рівнях, модель збагачується об'єднанням різних поглядів в один погляд для використання впроваджувачами та іншими зацікавленими сторонами [1,2 ,3,4,5].

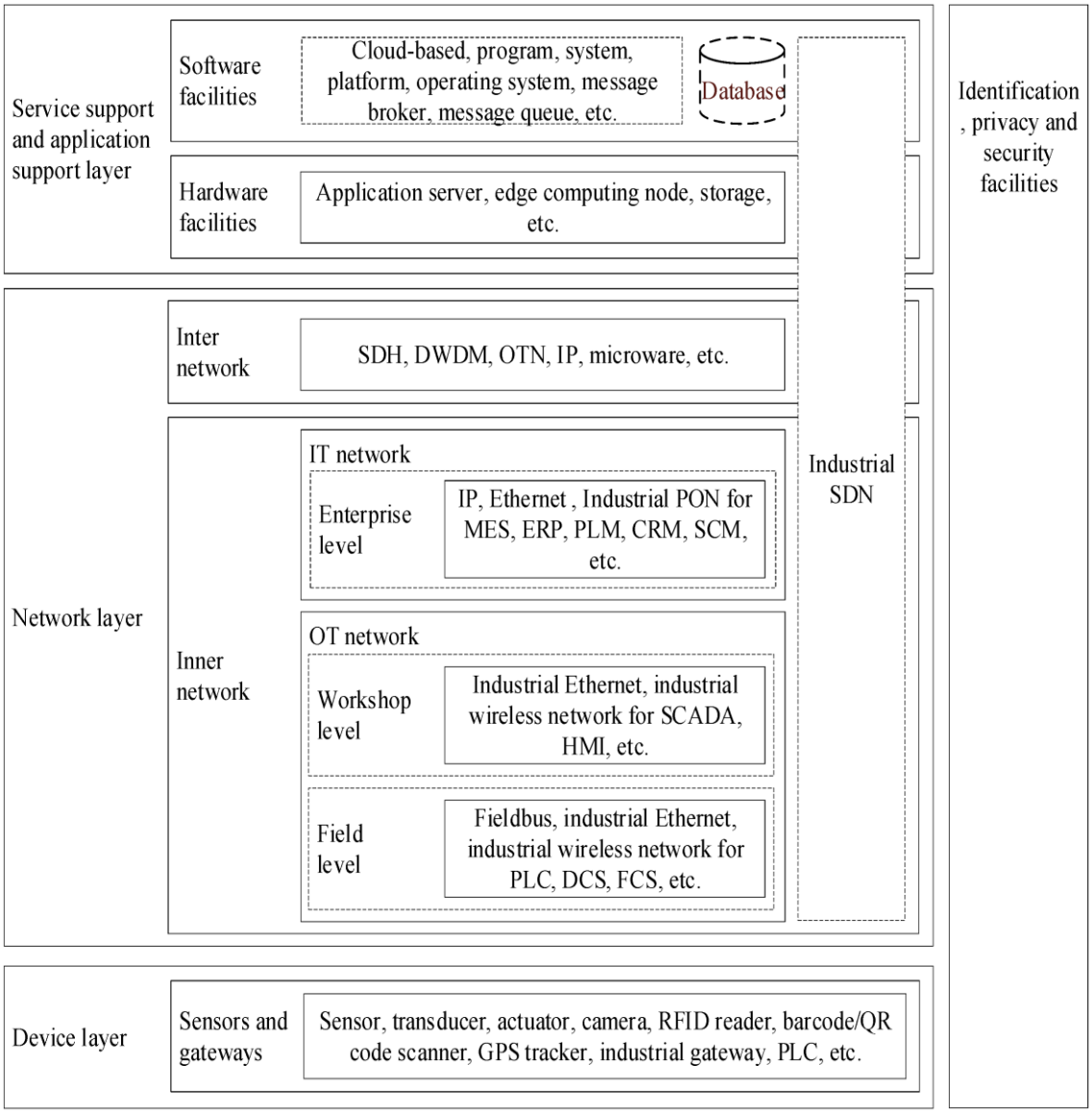

Рис. 2.1. Концептуальна основа інфраструктури IIoT з точки зору IoT та SM

Через велику кількість комунікаційних технологій у промисловій мережі, відповідні комунікаційні середовища на фізичному рівні інфраструктури IIoT є дуже різноманітними [12]. Пристрої, підключені до промислової мережі, – це не лише звичайне мережеве та IT-обладнання (таке як комутатори, маршрутизатори, брандмауери, ПК, принтери та інше обладнання), але й промислове обладнання для керування та управління (таке як промислові ПК, інтерфейс людина-машина (HMI), програмовані

логічні контролери (ПЛК), контролери руху, віддалені термінали та обладнання радіочастотної ідентифікації (RFID)).

Ці пристрої працюють на різних рівнях або на кількох рівнях еталонної моделі OSI, надають дані у стандартизованому або нестандартизованому форматі, отримують сигнали керування та регулювання від верхніх рівнів, а також виконують комплексне зондування та керування відповідним обладнанням і процесами в середовищі промислового виробництва [13].

Пристрої цього рівня можна розділити на датчики та шлюзи, які безпосередньо взаємодіють з машинами, робототехнікою, екологічним обладнанням та іншими польовими засобами для виробництва SM, з метою підвищення продуктивності та результатів [14].

Датчики поділяються на різні категорії, такі як датчики ресурсів, безпеки, присутності, освітлення, руху, навколишнього середовища та положення, які встановлюються на фізичних об'єктах для SM. Ці пристрої дозволяють збирати та відстежувати стан машин SM, робототехніки, операцій, навколишнього середовища тощо, щоб допомогти об'єктам верхніх рівнів збирати, обробляти, аналізувати та зрештою генерувати цінну інформацію для послуг SM.

Спеціалізовані на виробництві шлюзи з'єднують виробничі об'єкти, такі як датчики, ПЛК, машини та робототехніка [15], які мають відкриті інтерфейси даних. Це робиться для того, щоб сприймати та ідентифікувати дані з різних ресурсів, а також допомагати контролювати та виконувати потоки рішень з об'єктів верхнього рівня. Шлюзи перетворюють та перетворюють інформацію, що надходить від пристроїв та датчиків, у формати та структури, придатні для застосувань та систем верхнього рівня, та транспортують її за допомогою відповідних мережевих протоколів, і навпаки.

У розвиненому промисловому середовищі сервіси не лише розгортаються в хмарі, але й, ймовірно, будуть розгортатися як у промисловій сфері, так і в хмарі [16]. Промислове польове обладнання та машини вироблятимуть великий обсяг даних на периферії мережі, а обладнання периферійної мережі, таке як шлюзи в промисловій сфері, вимагатиме сумісних можливостей обробки даних та гнучких можливостей передачі та переадресації послуг.

Мережа забезпечує комплексний взаємозв'язок людей, машин та речей для передачі даних між ними, що є основною функцією для виконання вимог промислових застосувань [17]. Вона сприяє безперебійному потоку та інтеграції різноманітних промислових даних.

Мережеві з'єднання IIoT охоплюють різні технічні галузі всередині та поза заводом. Багато мережевих технологій використовуються в промисловій сфері з відповідними перевагами продуктивності [18] у певних сценаріях. Однак ці технології зі специфічними можливостями (такі як багато видів промислових польових шин) розроблені та застосовуються лише в певних сценаріях і не можуть задовольнити вимоги IIoT щодо сумісності даних та безперешкодної інтеграції.

Загальна мета мережевого підключення полягає у сприянні взаємозв'язку між системами, розблокуванні даних з ізольованих систем або мереж та підвищенні цінності даних для галузевих та міжгалузевих застосувань.

Мережевий рівень складається з двох підрівнів: внутрішньої мережі та міжмережевого, а також промислової програмно-визначеної мережі (SDN) [19], яка перетинає як мережевий рівень, так і рівень підтримки послуг та рівень підтримки додатків.

Внутрішня мережа — це мережа всередині заводу або закритої виробничої зони, яка використовується для з'єднання персоналу (такого як виробничий персонал, конструктори та зовнішній персонал), машин (таких

як обладнання та офісні прилади), матеріалів (таких як сировина, незавершене виробництво та готова продукція), середовища (такого як прилади та обладнання для моніторингу) тощо. Через внутрішню мережу вони взаємопов'язані з центром обробки даних підприємства та серверами додатків для підтримки бізнес-додатків на заводі [20].

З точки зору SM, внутрішня мережа охоплює мережу OT та мережу IT [21]. Вони з'єднані між собою через промислові шлюзи (такі як брандмауери, діоди даних та системи захисту від вторгнення (IPS)) для реалізації взаємозв'язку та фізичної ізоляції мережі. Мережу OT можна розділити на польовий рівень та рівень майстерні, тоді як мережа IT належить до рівня підприємства.

Польовий рівень мережі OT;

На польовому рівні мережі OT, зазвичай використовуваними комунікаційними технологіями в галузі промислового управління є: промислова польова шина, промисловий Ethernet та промислова бездротова мережа.

Промислова польова шина;

Технології промислових польових шин [22] (такі як Profibus, Modbus, HART, CANopen, LonWorks, DeviceNet, ControlNet, CC-Link та RS232/RS485) широко використовуються для підключення датчиків виявлення польових сигналів, виконавчих механізмів та промислових контролерів. Промислова польова шина в основному забезпечує підтримку передачі даних від польового датчика до контролера; від контролера до виконавчого механізму; або між контролером та кожною підстанцією керування вводом/виводом (наприклад, ПЛК та РСУ/СУК).

Порівняно з іншими комунікаційними технологіями, технологія промислових польових шин має деякі недоліки, такі як низька комунікаційна здатність, коротка відстань, погана стійкість до перешкод тощо [23]. Її вразливість до сильних струмових перешкод, низька

надійність, застарілий режим обслуговування, обмеження пропускної здатності та відстані, а також висока вартість прокладання кабелю призводять до суттєвих обмежень у використанні. Однак промислова оптична шина може бути використана під керуванням ПЛК, який базується на технології оптичного зв'язку, у поєднанні з можливостями оптичного розділення та доступу кількох терміналів через оптичну розподільчу мережу. Промислова оптична шина забезпечує конкурентні показники продуктивності для польових шин, а також забезпечує вищу пропускну здатність та зменшує затримку передачі.

Промисловий Ethernet;

Промислові технології Ethernet (такі як EtherNet/IP, PROFINET, Modbus TCP, Powerlink та EtherCAT) – це налаштовані та оптимізовані комунікаційні технології на основі Ethernet, які впроваджуються в галузь промислового управління. Багато промислових протоколів Ethernet поступово увійшли в застосування керування та зв'язку в різних промислових системах управління [24]. Їхня низька вартість, ефективна комунікаційна здатність та гнучкість у розширенні топології мережі заклали основу для покращення рівня промислового управління.

Промислова бездротова мережа.

Промислова бездротова мережа в основному використовується в деяких некритичних промислових застосуваннях, таких як транспортування матеріалів, управління запасами, патрульна перевірка, технічне обслуговування та інші випадки [25]. Промислові бездротові технології [26] (такі як Wi-Fi, Bluetooth, WirelessHART, WPAN, WIA-PA, WIA-FA, RFID, NB-IoT, ZigBee, ISA100.11a, 4G/5G та MulteFire) з'єднують мобільне обладнання на заводі, де кабельне підключення ускладнене або неможливе.

З розвитком 5G, такі показники продуктивності, як затримка, надійність та зв'язок, можуть вимагати гарантії для екстремальних

застосувань промислового керування [27]. Завдяки цим покращеним можливостям мережа 5G може розширити масштаб застосування промислових бездротових мереж для більш гнучких сценаріїв промислового застосування, а промислова бездротова мережа може працювати разом з промисловою фіксованою мережею для досягнення комплексного взаємозв'язку.

Рівень майстерні мережі ОТ;

На рівні цеху мережі ОТ вона в основному забезпечує з'єднання між контролерами; між контролерами та локальними або віддаленими системами моніторингу; а також між контролерами та системами операційного рівня (такими як система диспетчерського керування та збору даних (SCADA) та інтерфейс людини-машини (HMI)). Цей рівень переважно використовує промисловий Ethernet та промислові бездротові мережі, тоді як деякі виробники використовують власні протоколи зв'язку для зв'язку між промисловими контролерами та системами.

2.2 Визначення критичних активів системи

На рівні IT-мережі підприємства, поширеними комунікаційними технологіями для мережевого з'єднання між системами корпоративного рівня є високошвидкісний Ethernet, TCP/IP, промислова PON [28] тощо. Системи корпоративного рівня - це системи управління виробництвом (MES), планування ресурсів підприємства (ERP), управління життєвим циклом продукту (PLM), управління взаємовідносинами з клієнтами (CRM), управління ланцюгами поставок (SCM) тощо.

Мережеві пристрої на цьому рівні допомагають з'єднувати промислових користувачів, системи, сервери додатків та сховища даних з високою швидкістю та надійністю, включаючи комутатори, маршрутизатори та інші мережеві пристрої. Ці пристрої можуть бути

частиною промислової SDN, допомагаючи побудувати віртуалізовану мережеву архітектуру, з метою подальшого надання мережевих послуг за допомогою передових мережевих технологій (таких як SDN та віртуалізація мережевих функцій (NFV)), які можуть мати різні угоди про рівень обслуговування (SLA) на різних логічних рівнях мережі. Ці мережеві послуги можна швидко розгортати, налаштовувати та повторно використовувати з гарантією високої якості обслуговування (QoS).

Міжмережа – це мережа поза заводом, яка використовується для з’єднання таких об’єктів, як розумні заводи, філії підприємств, кооперативні підприємства, що працюють вище та нижче за течією, центри обробки даних загальнодоступних промислових хмар, розумні продукти (такі як розумна сімейна техніка, розумні медичні інструменти, розумні автомобілі та розумне інженерне обладнання) та користувачі [29].

Сервери додатків центру обробки даних всередині розумного заводу взаємопов'язані з промисловими хмарними центрами обробки даних поза заводом через міжмережеву мережу. Філії підприємств, кооперативні підприємства, розумні продукти та користувачі також підключаються до промислових хмарних центрів обробки даних або корпоративних центрів обробки даних через міжмережеву мережу відповідно до вимог.

Міжмережеві мережі використовують такі мережеві технології, як SDH, DWDM, OTN, IP та мікрохвильовий зв'язок через стільниковий або супутниковий зв'язок. З точки зору промислових підприємств, міжмережеві мережі забезпечують виділені лінії (такі як виділена лінія для Інтернету, виділена лінія для корпоративного взаємозв'язку та виділена лінія для хмари) для задоволення потреб галузевого та міжгалузевого зв'язку [30].

Виділена лінія Інтернету забезпечує з'єднання між розумною фабрикою та Інтернетом. Вона також може забезпечити доступ користувачів або розумних продуктів до розумної фабрики. Це базова виділена лінія промислових підприємств. Користувачі або розумні

продукти підключаються до розумної фабрики через Інтернет, а потім з'єднуються з публічними промисловими хмарними центрами обробки даних. Це основа для промислових підприємств для реалізації інтелектуальних послуг для SM.

Виділена лінія корпоративного з'єднання забезпечує безпечне та надійне з'єднання між «розумними» заводами, філіями підприємств та кооперативними підприємствами. Вона зазвичай використовується великими та середніми підприємствами.

Виділена лінія хмарного зв'язку забезпечує взаємозв'язок між розумною фабрикою та загальнодоступними промисловими хмарними центрами обробки даних [31]. Зазвичай це виділена лінія від підприємства до постачальника послуг загальнодоступної хмари.

Частина інфраструктури IIoT на рівні підтримки послуг та підтримки додатків складається з апаратних та програмних засобів, а також міжрівневої промислової SDN.

Ці засоби, як інфраструктура на цьому рівні, забезпечують можливості інтеграції користувачів та ресурсів (таких як дані та послуги) всередині та/або за межами заводів, а також забезпечують можливості аналізу інтеграції промислових даних для підтримки різних промислових застосувань [32]. Вони є критично важливою основою для побудови промислових екосистем для SM.

Апаратні засоби цього рівня включають різні типи обладнання, такі як сервери додатків, вузли периферійних обчислень та сховища. Це зроблено для того, щоб допомогти у побудові апаратної інфраструктури для подальшої побудови програмної інфраструктури (програмні засоби цього рівня) та забезпечити багатоцільові рішення для SM, такі як промислові послуги та додатки.

Апаратні засоби сприяють взаємозв'язку між пристроями, системами, інтелектуальними продуктами та людьми, що дозволяє збирати історичні

дані та дані в режимі реального часу [33]. Вони також можуть взаємодіяти з різними платформами, що надають дані, з метою покращення комплексного збору даних та інтелектуального аналізу.

Програмні засоби цього рівня включають різні типи програмного забезпечення, такі як системи, платформи, операційні системи, брокери повідомлень, черги повідомлень та бази даних.

Таблиця 2.1.

Критичні активи підприємства

Критичний актив	**Призначення активу**	**Можливі загрози**	**Потенційні наслідки**	**Рівень критичності**	**Основні заходи захисту**
IoT-пристрої (датчики, контролери, камери)	Збір та передача даних, автоматизація процесів	Несанкціонований доступ, шкідливе ПЗ, фізичне пошкодження	Втрата контролю над системою, витік даних, збій роботи	Високий	Аутентифікація, оновлення прошивки, сегментація мережі
Сервер управління IoT	Централізоване керування пристроями та обробка інформації	DDoS-атаки, компрометація облікових записів, експлуатація вразливостей	Повне порушення роботи інфраструктури	Критичний	Firewall, IDS/IPS, резервне копіювання, багатофакторна автентифікація
База даних системи	Зберігання телеметрії та службової інформації	SQL-ін’єкції, викрадення даних, пошкодження БД	Втрата або підміна інформації	Критичний	Шифрування даних, контроль доступу, резервування
Мережева інфраструктура	Передача даних між IoT-пристроями та серверами	Перехоплення трафіку, MITM-атаки, перевантаження мережі	Порушення зв’язку та витік інформації	Високий	VPN, TLS-шифрування, VLAN-сегментація

Продовження таблиці 2.1.

Критичний актив	**Призначення активу**	**Можливі загрози**	**Потенційні наслідки**	**Рівень критичності**	**Основні заходи захисту**
Хмарні сервіси IoT	Віддалене зберігання та обробка даних	Несанкціонований доступ, витік даних, збій сервісу	Втрата доступу до сервісів та інформації	Високий	Контроль доступу, шифрування, аудит безпеки
Автентифікації користувачів	Контроль доступу до компонентів системи	Викрадення паролів, brute-force атаки	Несанкціоноване керування системою	Високий	MFA, складні паролі, журналювання подій
Канали бездротового зв’язку	Передача даних між пристроями	Перехоплення сигналу, spoofing, jam-атаки	Втрата конфіденційності та доступності	Середній	WPA3, шифрування, моніторинг трафіку
Програмне забезпечення IoT-платформи	Управління функціями системи	Вразливості ПЗ, malware, помилки конфігурації	Порушення роботи сервісів	Високий	Регулярні оновлення, тестування безпеки
Конфігураційні файли та ключі доступу	Зберігання параметрів системи та криптографічних ключів	Викрадення ключів, несанкціонована зміна конфігурації	Повна компрометація системи	Критичний	Захищене зберігання, шифрування, контроль доступу
Система резервного копіювання	Відновлення даних після інцидентів	Видалення резервних копій, ransomware	Неможливість відновлення системи	Високий	Ізольовані резервні копії, регулярне тестування

На цьому рівні хмарне програмне забезпечення надає віртуалізовані обчислення, сховище та мережеві ресурси [34], а також фундаментальні хмарні можливості (такі як Hadoop, OpenStack та Cloud Foundry), можливості зберігання даних (такі як розподілена файлова система Hadoop, хмарні бази даних, сховище BLOB-об'єктів), обчислювальні можливості (такі як MapReduce та SPARK) та можливості інформаційної системи, щоб забезпечити допоміжні можливості для промислових послуг та додатків.

Користувачі та промислові додатки можуть використовувати ці ресурси та допоміжні можливості.

Промислова SDN, яка використовується на мережевому рівні, а також на рівні підтримки послуг і підтримки додатків, є досить складною для мережевих операторів та системних адміністраторів. Через традиційні методи управління IT-системами та мережами комунікаційних технологій (КТ), відповідний управлінський персонал кваліфікований лише в галузі IT або КТ, але не зобов'язаний знати обидві, тоді як промислова SDN, оскільки має так багато переваг, також має набагато вищі вимоги до адміністраторів, які достатньо добре знають ІКТ. Промислова SDN використовує мережеві контролери для рівномірного управління мережевими ресурсами [35] на заводі, щоб забезпечити якість обслуговування мережі, необхідну ключовим підприємствам.

IT- та OT-мережі на заводі традиційно працюють незалежно одна від одної, обидві топології мережі є жорсткими, а взаємодія та управління інформацією між мережами дуже складні [36]. Промислова SDN дозволяє глибоку інтеграцію IT- та OT-мереж для побудови гнучкої та гнучкої промислової мережі.

Промислова SDN складається з термінального обладнання з кількома протоколами, програмованих промислових програмно-визначених мережевих пристроїв та централізованих промислових SDN-контролерів. Термінальне обладнання передає характеристики потоку даних та вимоги до передачі до промислового SDN-контролера через північний інтерфейс, а промисловий SDN-контролер генерує правила переадресації відповідно до отриманих характеристик потоку даних та вимог до передачі. Ці правила переадресації реалізуються в промислових програмно-визначених мережевих пристроях через стандартизований південний інтерфейс.

Промислова SDN може мати один або кілька мережевих контролерів. Через різні типи північних інтерфейсів (таких як RESTful) та південних

інтерфейсів (таких як OpenFlow, Netconf, YANG, BGP-LS, BGP Flowspec, сегментна маршрутизація та PCEP) мережевих пристроїв, різні мережеві контролери керують різними типами мережевих пристроїв (таких як промислові комутатори, маршрутизатори, шлюзи, брандмауери, IPS, відкриті віртуальні комутатори (OVS), промислові PON та OTN) або мережевими пристроями від різних постачальників. Важко об'єднати багато протоколів північних та південних інтерфейсів в один єдиний мережевий контролер для досягнення сумісності, тому можна використовувати кілька мережевих контролерів, які можна класифікувати як контролер домену та суперконтролер. Кожен контролер домену керує частиною мережі (доменом), тоді як суперконтролер керує всіма контролерами домену. Ці мережеві контролери можуть бути сформовані як вертикальна деревоподібна топологія або горизонтальна багатошарова топологія без використання суперконтролера, щоб реалізувати міжрівневе та/або міждоменне управління та координацію мережевих пристроїв.

Ключовим механізмом промислової SDN є керування та налаштування мережевих пристроїв, таких як комутатори, за допомогою програмного забезпечення. Вона також може підтримувати орієнтовані на майбутнє пристрої, чутливі до часу, мережі (TSN). Промислова SDN може підтримувати уніфікований доступ та гнучке мережеве об'єднання обладнання в IT- та OT-мережі, забезпечувати гарантію високої пропускної здатності передачі та гарантію надання послуг у режимі реального часу від початку до кінця. Обладнання та трафік в обох мережах можуть бути однаково моніторинговані та керовані.

Засоби безпеки для інфраструктури IIoT на всіх трьох рівнях повинні забезпечувати відповідні можливості безпеки не лише на незалежних рівнях, але й, що найголовніше, надавати наскрізні механізми безпеки для сервісів та застосунків SM на всіх периферійних пристроях, мережах, апаратному та програмному забезпеченні.

Як один із компонентів інфраструктури IIoT для SM, засоби ідентифікації, конфіденційності та безпеки забезпечують можливості ідентифікації, безпеки та захисту для різних функцій заводу [37], включаючи ідентифікацію та автентифікацію пристроїв, захист конфіденційності, фізичну безпеку, функціональну безпеку та інформаційну безпеку. Ці засоби в основному використовуються для захисту різних фізичних або віртуальних інфраструктурних ресурсів, служб аналізу даних, комплектів розробки, промислових застосувань тощо. Вони проходять через усі три рівні інфраструктури IIoT та охоплюють різні виміри безпеки IIoT, включаючи надійність, конфіденційність, цілісність, доступність, конфіденційність та захист даних.

На рівні пристроїв унікальний ідентифікатор (ID) може використовуватися для реєстрації та ідентифікації різних типів пристроїв, служб і програм. На мережевому рівні мережевий зв'язок на основі ідентифікаторів може бути використаний для забезпечення можливостей автентифікації та авторизації, щоб гарантувати цілісність і безпеку обміну інформацією. На рівні підтримки послуг і підтримки програм ідентифікатор може використовуватися як запис для визначення атрибутів, можливостей і служб, пов'язаних з відповідними пристроями.

2.3 Ідентифікація потенційних порушників

Екосистема Інтернету речей складається з кількох співіснуючих та конкуруючих платформ і продуктів, а також різноманітних бізнес-гравців, які взаємодіють один з одним. У зв'язку з цим ми виявили, що певні моделі, представлені ITU, можуть бути відправною точкою, придатною для дослідження та подальшої адаптації. Інформативний додаток I до Рекомендації ITU-T Y.4000 [5] представляє приклад визначених бізнес-

ролей в екосистемі Інтернету речей та їхніх взаємозв'язків. Оскільки цей приклад не представляє всіх можливих відповідних ролей у розгортанні бізнесу Інтернету речей, ми маємо намір розширити його, включивши вплив нових обчислювальних парадигм. Ми також розглядаємо Рекомендацію ITU-T Y. 4100 [6], оскільки вона надає загальні вимоги до Інтернету речей на основі загальних випадків використання Інтернету речей та учасників Інтернету речей. З огляду на очікування, що кількість підключених пристроїв буде настільки величезною, що дані Інтернету речей становитимуть переважну частину даних, що передаються мережами, у цьому дослідженні також враховуються Рекомендація ITU-T Y.4114 [7] та представлені ключові можливі зіставлення бізнес-ролей Інтернету речей [5] з ролями даних Інтернету речей.

Бізнес-ролі, визначені в Інформативному додатку до Рекомендації ITU-T Y.4000 [5], є такими:

Постачальник пристроїв надає пристрої постачальнику мережі та постачальнику додатків;

Мережевий постачальник здійснює доступ та інтеграцію ресурсів інших постачальників, надає можливості Інтернету речей (IoT) та їх підтримку та управління їхньою інфраструктурою, а також надає мережеві можливості та ресурси різним постачальникам;

Постачальник платформи надає постачальникам додатків такі можливості, як зберігання даних, обробка даних, керування пристроями, можливості інтеграції та відкриті інтерфейси;

Постачальник застосунків надає IoT-застосунки клієнтам застосунків, використовуючи можливості або ресурси мережевого постачальника, постачальника пристроїв та постачальника платформи;

Клієнт застосунку – це користувач застосунків Інтернету речей, що надаються постачальником застосунків

Аналізуючи ці відповідність між учасниками Інтернету речей та бізнес-ролями у вибраних рекомендаціях ITU, а також враховуючи визначення для «Менеджера даних», наведені в ITU-T Y.4100 [6], «Постачальника пристроїв» та «Постачальника додатків», наведені в ITU-T Y.4000 [5], визначені як відповідні бізнес-ролі менеджера даних, ми вважаємо, що менеджер даних як учасник Інтернету речей потребує більш детального визначення. З більшою деталізацією загальний потік даних та відповідні обов'язки стають більш зрозумілими та чіткими.

Актор «Менеджер даних» відповідає постачальнику пристроїв, коли надаються пристрої, які включають деякі функції керування даними [6]. Залежно від наданих можливостей обробки пристроїв, відповідний актор «Менеджер даних» потрібно гранулювати як «Менеджер даних роси», «Менеджер даних туману», «Менеджер даних периферії», «Менеджер даних туману» та «Менеджер даних хмари».

Актор «Менеджер даних» відповідає постачальнику застосунків, коли надані застосунки включають деякі функції керування даними [6]. Оскільки постачальник застосунків використовує ресурси або можливості постачальника пристроїв, постачальника мережі та постачальника платформи, відповідний актор «Менеджер даних» має бути гранульований як «Менеджер мережевих даних», «Менеджер даних платформи» та «Менеджер даних застосунків».

Різноманітність варіантів пристроїв та варіантів використання в поєднанні з різноманітними застосуваннями Інтернету речей робить ланцюжок створення вартості Інтернету речей складною екосистемою, яка може мати незліченну кількість партнерств між учасниками.

Крім того, призначення, виробництво та розповсюдження пристроїв Інтернету речей можуть здійснюватися за несумісними стандартами в різних юрисдикціях. Така ж ситуація спостерігається і з учасниками

Інтернету речей, тобто багато з них знаходяться поза межами юрисдикції, в якій надається послуга Інтернету речей.

2.4 Аналіз можливих каналів атак

Усі пристрої Інтернету речей зазвичай демонструють певну вразливість або слабкість, яка послаблює їхню здатність безпроблемно функціонувати. Ці вразливості зазвичай дозволяють користувачам отримати доступ до даних, використовуючи слабкість для проникнення в пристрій, або ж їх можна використовувати для відстеження та маніпулювання пристроєм. У будь-якому випадку це шкодить пристрою та його функціональності. Деякі зі способів, якими зловмисники можуть отримати доступ до цього, - це мережеві вразливості, вразливості програмного забезпечення або навіть вразливості апаратного забезпечення, як показано нижче (Рис.2.2).

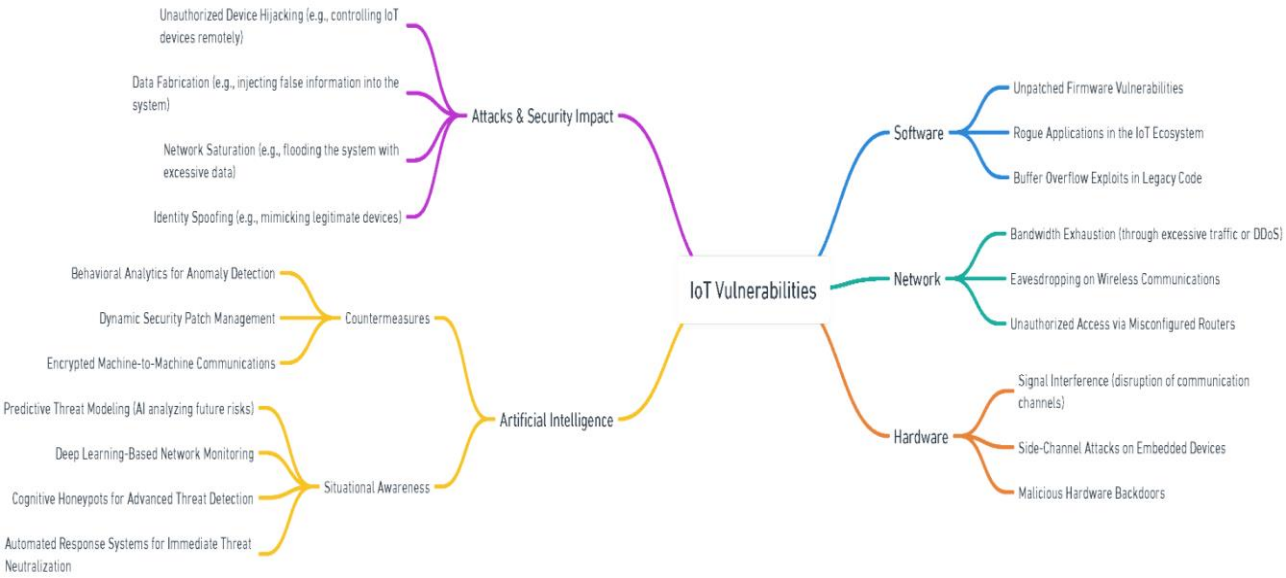

Рис. 2.2. Канали атак на пристрої

Способи використання цих вразливостей представлені іншою половиною рівня атаки. Зловмисник може досить легко атакувати будь-який пристрій Інтернету речей через будь-яку з вразливостей, і таким чином він може вирішити атакувати цілісність даних, конфіденційність, автентифікацію або навіть доступність. Конфіденційність призначена для захисту пристроїв та інформації Інтернету речей від несанкціонованого доступу та зазвичай забезпечується за допомогою шифрування, контролю доступу, а також автентифікації користувача та даних. Через будь-яку з цих вищезгаданих вразливостей ми можемо побачити витік інформації, який може призвести до розголошення будь-яких даних будь-кому, незалежно від того, чи це зловмисник, чи звичайна людина. Цілісність зазвичай гарантує захист від несанкціонованих модифікацій апаратного або програмного забезпечення пристрою шляхом забезпечення шифрування, перевірки вхідних даних, моніторингу та обмежень інтерфейсу тощо [58]. Вони розроблені для того, щоб запобігти вразливості будь-якої частини пристрою. Однак, знову ж таки, на етапі проектування пристрою зазвичай не враховуються дрібні речі, які дозволяють зловмиснику використовувати цей пристрій для власних зловмисних цілей. Підзвітність являє собою ідею відстеження дій та завдань, щоб переконатися, що пристрій виконує те, що повинен робити. Тобто, вона контролює все, що робить пристрій, і обмежує пристрій певними завданнями. Зловмисник може використовувати вразливості виробника, щоб проникнути в пристрій та змінити шлях подій. Вони можуть використовувати це, щоб змінити призначення пристроїв або навіть перенаправити дані на них для моніторингу даних. Нарешті, у нас є ідея доступності. Доступність – це ідея того, що пристрій завжди доступний для використання, коли користувачеві це потрібно. Коли зловмисник націлюється на ці вразливості, він може затримати пристрій або навіть вивести його з офлайн-режиму, що послабить доступність. Усі ці впливи на безпеку є результатом типів атак, які може здійснити зловмисник. Чи то

фізична, програмна чи навіть мережева атака. Пристрій Інтернету речей на іншому кінці атаки може впливати на один або часто на багато аспектів, показаних вище.

Більшість, якщо не всі, пристрої Інтернету речей працюють без нагляду та зазвичай мають обмежені властивості захисту від несанкціонованого доступу, що надзвичайно полегшує зловмиснику отримання доступу до пристрою . Зловмисник може модифікувати пристрій Інтернету речей щодо послуг, які він надає, а також отримати дані, до яких він не повинен мати доступу, і які можуть завдати серйозної шкоди багатьом людям . Наприклад, якщо хакер отримає доступ до розумного дверного дзвінка, він зможе змінити всі налаштування всередині, переглянути дані всередині або навіть видалити їх. Тепер давайте зробимо цей крок далі, у дуже делікатне середовище. Якби зловмисник якимось чином отримав доступ до камери військової бази, він міг би використати цей доступ, щоб відстежити, куди надсилаються дані. У цьому випадку він би знайшов сервер з великою кількістю інших даних з камер. Потім він міг би вимкнути камери та атакувати або навіть розголошувати військові таємниці, які були зафіксовані на камеру.

Хакер може отримати доступ до пристрою на апаратному рівні за допомогою різних методів, причому атака «людина посередині» є найпоширенішим підходом. Як правило, обговорення атак «людина посередині» зосереджені на експлуатації на мережевому рівні — перехопленні даних через дротові або бездротові з'єднання. Однак ця перспектива охоплює лише частину потенціалу цієї техніки. Набагато підступнішим є використання радіочастотного (РЧ) випромінювання, яке за своєю суттю виробляють усі електронні пристрої. Це випромінювання, яке можна виявити за допомогою таких інструментів, як аналізатори спектру або програмно-визначені радіоприймачі (наприклад, HackRF, пристрої Ettus Research або навіть недорогі пристрої RTL-SDR), пропонує

зловмисникам можливість спостерігати та маніпулювати зв'язком пристроїв на фундаментальному рівні.

Процес починається з ідентифікації сигналу. Кожен пристрій випромінює радіочастотні сигнали, що характеризуються унікальними атрибутами, які зловмисник може проаналізувати, щоб визначити їхню природу. Ці атрибути включають пропускну здатність (спектральний слід сигналу), частоту (його положення, наприклад, 2,4 ГГц для Bluetooth або 5 ГГц для Wi-Fi), силу сигналу (його амплітуду) та поведінкові моделі (наприклад, стрибки частоти, періодичні сплески або безперервна передача). Візуалізована на аналізаторі спектру форма хвилі сигналу — чи то різкий імпульс, чи модульована крива — додатково розкриває його ідентичність. Маючи цю інформацію, зловмисник може класифікувати сигнал — будь то Bluetooth, Zigbee чи власний протокол — та оцінити його вразливості. Бездротові протоколи за своєю природою мають притаманні слабкі місця, такі як недостатнє шифрування, передбачувані часові інтервали або механізми рукостискання, які можна використовувати. Використовуючи ці недоліки, зловмисник може порушити сигнал, взяти під контроль його або непомітно змінити його вміст.

Одним із ефективних захистів від цих типів атак є використання надійних механізмів шифрування, таких як AES-128/256-бітове шифрування та криптографія еліптичних кривих (ECC) . Завдяки шифруванню даних перед передачею, навіть якщо зловмисник успішно перехопить сигнал, він не зможе розшифрувати його вміст. Крім того, такі методи, як ковзні коди та автентифікація на основі одноразового коду, запобігають атакам повторного відтворення, гарантуючи, що раніше перехоплені передачі не можуть бути використані повторно. Також слід застосовувати протоколи безпечного обміну ключами, такі як Diffie-Hellman або ECDH, щоб гарантувати, що навіть перехоплені повідомлення залишаються нерозшифрованими.

Атаки типу «людина посередник» на основі радіочастот виходять за рамки простого порушення зв'язку, дозволяючи як перехоплювати, так і маніпулювати комунікаціями. Зловмисник може позиціонувати себе як посередника між двома пристроями, скажімо, смартфоном та бездротовим периферійним пристроєм, передаючи повідомлення, таємно контролюючи обмін. Крім того, вони можуть повністю видати себе за один пристрій, перенаправляючи сигнал на себе. У цьому сценарії пристрій-джерело передає дані зловмиснику, який потім може переслати їх цільовому одержувачу, змінити їх або зберегти для подальшого використання. Наприклад, зловмисник може вводити шкідливі команди, змінювати передані дані або просто підслуховувати — і все це без виявлення вторгнення пристроями зв'язку. Радіочастотне середовище безперешкодно сприяє цьому обману, оскільки сигнали зберігаються у своїх очікуваних шаблонах, не залишаючи жодних явних слідів перешкод. Без спеціалізованого обладнання для моніторингу, такого як SDR, яким володіє пильний захисник, атака залишається непомітною .

Для пом'якшення цих атак можна використовувати методи поширення спектру зі стрибкоподібною перебудовою частоти (FHSS) та поширення спектру прямої послідовності (DSSS), щоб запобігти ізоляції певної передачі зловмисником. Ці методи забезпечують динамічне зміщення сигналу між кількома частотами, що значно ускладнює для зловмисника визначення, захоплення або маніпулювання зв'язками. Крім того, дотримання суворих політик оновлення прошивки може усунути відомі вразливості в бездротових протоколах, запобігаючи використанню зловмисниками застарілих заходів безпеки .

2.5 Побудова моделі загроз IoT-середовища

На основі вивченої інформації побудуємо таблицю в якій розміщуватимуться моделі загроз пристроїв табл. 2.2.

Таблиця 2.2.

Моделі загроз IoT-середовища

№	Тип загрози	Джерело загрози	Об'єкт впливу	Основні методи реалізації	Можливі наслідки	Рівень небезпеки	Методи захисту
1	Несанкціонований доступ	Зовнішній зловмисник	IoT-пристрої, сервери	Підбір паролів, експлуатація вразливостей	Захоплення контролю над системою	Критичний	MFA, контроль доступу, складні паролі
2	DDoS-атака	Ботнети, хакери	Мережеві ресурси, сервери	Масове надсилання запитів	Недоступність сервісів	Високий	IDS/IPS, фільтрація трафіку
3	Перехоплення трафіку (MITM)	Кіберзловмисник	Канали передачі даних	Підміна вузлів мережі, sniffing	Витік конфіденційної інформації	Високий	TLS/SSL, VPN, шифрування трафіку
4	Шкідливе програмне забезпечення	Malware, віруси	IoT-пристрої, сервери	Завантаження заражених файлів, експлойти	Порушення роботи системи	Високий	Антивірусний захист, оновлення ПЗ

Продовження таблиці 2.2.

№	Тип загрози	Джерело загрози	Об’єкт впливу	Основні методи реалізації	Можливі наслідки	Рівень небезпеки	Методи захисту
5	Підміна IoT-пристрою	Внутрішній або зовнішній порушник	Датчики, контролери	Spoofing MAC/IP-адрес	Передача неправдивих даних	Середній	Сертифікація пристроїв, автентифікація
6	Витік конфіденційних даних	Інсайдер, хакер	Бази даних, хмарні сервіси	Викрадення облікових даних, SQL-ін’єкції	Компрометація інформації	Критичний	Шифрування БД, аудит доступу
7	Фізичне пошкодження пристроїв	Людський фактор, зловмисник	IoT-обладнання	Демонтаж, руйнування, крадіжка	Зупинка роботи системи	Середній	Контроль фізичного доступу, відеоспостереження
8	Jam-атаки	Радіоелектронний вплив	Бездротові канали	Генерація радіоперешкод	Втрата зв’язку між пристроями	Середній	Захищені канали зв’язку, резервні канали
9	Компрометація прошивки	Кіберзловмисник	Firmware IoT-пристроїв	Впровадження модифікованої прошивки	Повний контроль над пристроєм	Критичний	Secure Boot, цифровий підпис прошивки
10	Помилки конфігурації	Адміністратор, персонал	Уся IoT-інфраструктура	Неправильні налаштування системи	Вразливість до атак	Високий	Політики безпеки, аудит конфігурацій
11	Соціальна інженерія	Кіберзловмисник	Персонал підприємства	Фішинг, психологічний вплив	Отримання доступу до системи	Високий	Навчання персоналу, контроль доступу

Прожовження таблиці 2.2.

№	Тип загрози	Джерело загрози	Об’єкт впливу	Основні методи реалізації	Можливі наслідки	Рівень небезпеки	Методи захисту
12	Відмова обладнання	Технічні несправності	Сервери, датчики, мережа	Зношення або збій компонентів	Переривання функціонування системи	Середній	Резервування обладнання, технічне обслуговування

Функціональність пристроїв Інтернету речей (IoT) охоплює широкий спектр, який формується не лише їхнім апаратним забезпеченням, а й програмним забезпеченням, вбудованим у їхні мікроконтролери. Візьмемо, наприклад, три однакові пристрої IoT, кожен з яких оснащений модулем Bluetooth і не відрізняються за зовнішнім виглядом. Їхня поведінка залежить від прошивки наступним чином: один може бути запрограмований виключно на передачу сигналів Bluetooth, інший — на отримання сигналів лише від авторизованих користувачів, а третій — на перемикання між ролями залежно від контексту. Ця програмно-орієнтована гнучкість визначає адаптивність IoT, але водночас виявляє критичну ахіллесову п'яту. Коли це програмне забезпечення скомпрометовано — чи то через розкриття, модифікацію чи експлуатацію — пристрій стає каналом для витоків даних, шкідливих імплантацій або повного контролю, і все це потенційно невідомо його оператору.

Програмні вразливості в пристроях Інтернету речей проявляються в різних формах, кожна з яких має різні шляхи експлуатації .

Поширеним типом є переповнення буфера, коли погано керований розподіл пам'яті дозволяє зловмиснику вводити дані, що перевищують ємність призначеного буфера . Ці надлишкові дані можуть перезаписувати

сусідню пам'ять, що дозволяє впроваджувати шкідливий код або змінювати потік виконання програми. Для пристрою Інтернету речей це може означати захоплення процесу оновлення прошивки для виконання несанкціонованих команд. Пом'якшення вразливостей переповнення буфера вимагає безпечних практик кодування та механізмів захисту пам'яті. Розробники повинні використовувати перевірку меж та валідацію вводу, щоб запобігти переповненню буферів пам'яті надлишковими даними. Використання стекових «канарейок» — невеликих значень безпеки, розміщених у стеку для виявлення пошкоджень — може допомогти виявити та заблокувати спроби експлуатації. Крім того, оновлення прошивки повинні бути криптографічно підписані та перевірені для забезпечення автентичності, запобігаючи виконанню несанкціонованих модифікацій.

Ще однією поширеною вразливістю є слабка автентифікація, коли неадекватні або жорстко закодовані облікові дані — часто ім'я користувача та пароль за замовчуванням, такі як «admin/admin» — надають зловмисникам легкий доступ. Потрапивши всередину, вони можуть маніпулювати роботою пристрою або перекачувати конфіденційні дані, такі як ключі сполучення для з'єднання Bluetooth. Щоб протидіяти слабкій автентифікації, пристрої Інтернету речей повинні застосовувати надійні політики паролів, вимагаючи унікальних та складних облікових даних під час першого використання. Багатофакторну автентифікацію слід впроваджувати, де це можливо, додаючи додатковий рівень безпеки, окрім простого пароля. Крім того, виробники пристроїв повинні відмовитися від жорстко закодованих облікових даних та натомість впроваджувати динамічні ключі автентифікації для кожного пристрою, щоб запобігти широкому використанню витоку облікових даних.

Незахищений зв'язок становить ще один серйозний ризик, оскільки незашифровані або погано зашифровані передачі даних, наприклад, пакети Bluetooth у відкритому тексті, наражають інформацію на ризик

перехоплення. Зловмисник із програмно-визначеним радіо може підслуховувати ці сигнали, реконструюючи команди або введені користувачем дані, навіть не торкаючись пристрою. Для зменшення ризику незахищеного зв'язку потрібне наскрізне шифрування з використанням надійних криптографічних протоколів, таких як AES для передачі даних та TLS для мережевого зв'язку. Пристрої повинні уникати передачі конфіденційних даних у відкритому тексті та впроваджувати механізми безпечного обміну ключами для захисту ключів шифрування від перехоплення. Крім того, ввімкнення методів розширеного спектру зі стрибкоподібною перебудовою частоти в бездротових протоколах може значно ускладнити пасивне підслуховування.

Фізичний доступ посилює ці ризики, пропонуючи прямі шляхи для використання недоліків програмного забезпечення. Зловмисник може підключити пристрій до комп'ютера або дослідити його контакти, щоб витягти прошивку з мікроконтролера. В ідеальному сценарії вони отримують вихідний код та файли конфігурації, оголюючи логіку пристрою. Найчастіше вони отримують лише машинний код — скомпільований двійковий файл. Однак це далеко не глухий кут. Такі інструменти, як Ghidra, IDA Pro або шістнадцятковий редактор, дозволяють зловмиснику аналізувати цей код, відстежуючи його інструкції для відображення функціональності пристрою, від обробки сигналів до перевірок безпеки. Складна декомпіляція може навіть перетворити цей двійковий файл на редагований код C, відкриваючи двері для індивідуальних модифікацій. Завдяки цьому розумінню зловмисник виявляє все, включаючи операційні слабкі місця, приховані функції або поведінку, шкідливу для власника пристрою, наприклад, схильність до трансляції ідентифікованих даних у відкритому вигляді. Щоб запобігти вилученню прошивки та зворотному проектуванню, виробники повинні впроваджувати механізми шифрування прошивки та захисту від

зчитування, запобігаючи несанкціонованому доступу до пам'яті мікроконтролера. Слід забезпечити безпечні процеси завантаження, гарантуючи, що на пристрої може виконуватися лише автентифікована та непідроблена прошивка. Крім того, методи обфускації коду можуть значно ускладнити зворотне проектування, маскуючи критичну логіку та механізми безпеки.

Примітно, що фізичне володіння цільовим пристроєм не завжди є необхідним. Пристрої Інтернету речей, часто доступні за ціною та частково з відкритим вихідним кодом, заохочують до непрямого використання. Зловмисник може отримати ідентичний пристрій, витягти його шістнадцяткові дані та провести зворотну розробку прошивки, щоб відобразити поведінку цілі. Хоча це може не розкрити специфічні для користувача налаштування, наприклад, власні ключі шифрування, це розкриває основну архітектуру програмного забезпечення. Окрім простого розуміння, цей доступ дозволяє зловмиснику створювати шкідливі зміни, такі як вбудовування бекдорів для моніторингу активності, додавання логіки для дистанційного керування або маскування своєї присутності за допомогою прихованих процедур. Ці зміни, які часто потребують лише кількох рядків коду, можна швидко повторно завантажити, перетворюючи пристрій на скомпрометований актив. Щоб запобігти шкідливим модифікаціям прошивки, слід використовувати безпечні механізми оновлення прошивки, які вимагають криптографічного підпису та перевірки оновлень перед встановленням. Також має бути передбачений захист від відкату, щоб запобігти зниженню версії пристроїв до старішої, вразливої прошивки зловмисниками. Крім того, виявлення поведінкових аномалій у системах Інтернету речей може допомогти визначити, коли пристрій починає демонструвати неочікувану активність, що свідчить про втручання.

Інші вразливості, такі як впровадження коду, наприклад, через неправильно сформовані вхідні дані до веб-інтерфейсу, або ескалація привілеїв, коли зловмисник використовує недосконалі перевірки дозволів, ще більше розширюють поверхню атаки, дозволяючи зловмисникам перейти від обмеженого доступу до повного домінування. У кожному випадку, властива програмованість програмного забезпечення — його найбільша сила — стає стрижнем його руйнування, наражаючи екосистеми Інтернету речей на багатогранний спектр загроз.

Висновки до розділу 2

Оскільки Інтернет речей продовжує розширюватися в різні сектори, проблеми безпеки, які він створює, стають все більш очевидними та актуальними. Це дослідження показало, що системи Інтернету речей за своєю суттю вразливі на багатьох рівнях, включаючи апаратне забезпечення, програмне забезпечення, мережі та хмарну інфраструктуру. Ці вразливості створюють можливості для зловмисників використовувати пристрої Інтернету речей, що призводить до потенційних витоків даних, збоїв у роботі системи та несанкціонованого контролю критично важливих операцій. Зростаюча залежність від Інтернету речей підкреслює нагальну необхідність вирішення цих проблем безпеки за допомогою проактивних механізмів захисту та структурованих стратегій пом'якшення наслідків.

Аналіз, проведений у цій роботі, підкреслює необхідність посилення безпеки Інтернету речей шляхом впровадження найкращих практик, таких як безпечні оновлення прошивки, надійні методи автентифікації, зашифровані канали зв'язку та постійний моніторинг аномалій. Завдяки вживанню цих заходів безпеки можна значно зменшити ризик експлуатації, забезпечуючи цілісність та надійність екосистем Інтернету речей. Крім того, це дослідження підкреслює важливість постійних досліджень та

розробок у сфері безпеки Інтернету речей для протидії новим загрозам та адаптації до мінливого ландшафту кібератак.

Оскільки технологія Інтернету речей продовжує розвиватися та інтегруватися в критично важливі інфраструктури, відповідальність за безпеку цих систем має залишатися головним пріоритетом. Майбутні дослідження повинні бути зосереджені на вдосконаленні існуючих заходів безпеки, вивченні інноваційних рішень для зменшення нових векторів атак та підвищенні стійкості мереж Інтернету речей до складних загроз. Проактивно вирішуючи ці проблеми, ми як спільнота можемо працювати над створенням більш безпечного та надійного середовища Інтернету речей, яке зможе відповідати вимогам сучасних технологій та їх широкого застосування.

РОЗДІЛ 3.РОЗРОБКА ТА РЕАЛІЗАЦІЯ ЗАХОДІВ ЗАХИСТУ ІОТ-ІНФРАСТРУКТУРИ

3.1 Розробка комплексу заходів захисту IoT-системи

Критично важливим кроком до захисту пристроїв Інтернету речей є їх посилення за допомогою захисту кінцевих точок Інтернету речей. Посилення захисту кінцевих точок передбачає усунення вразливостей у портах високого ризику, таких як протокол керування передачею (TCP) та протокол користувацьких дейтаграм (UDP) , бездротові з'єднання та незашифрований зв'язок. Також життєво важливо захистити пристрої від впровадження шкідливого коду.

Захист кінцевих точок дозволяє організаціям захистити свої мережі від складних атак, таких як новітні штами шкідливих програм та програм-вимагачів . Він також захищає пристрої на межі мережі, дозволяючи командам безпеки отримувати повний контроль над своєю мережею, отримувати інформацію про те, які пристрої до неї підключені в режимі реального часу, та зменшувати площу атаки .

Підприємства також можуть захистити свої пристрої Інтернету речей за допомогою шлюзу безпеки Інтернету речей, який забезпечує дотримання політик доступу до Інтернету та запобігає доступу небажаного програмного забезпечення, такого як шкідливе програмне забезпечення, до підключень користувачів.

Безпечний веб-шлюз (SWG) включає такі життєво важливі функції, як контроль програм, глибока перевірка протоколу передачі гіпертексту (HTTPS) та рівня захищених сокетів (SSL), ізоляція віддаленого браузера та фільтрація URL-адрес (Uniform Resource Locator) . Це має вирішальне значення, оскільки організації мігрують у хмару та забезпечують віддалені

підключення. Це допомагає запобігти ризикам безпеки для веб-трафіку та захищає пристрої Інтернету речей від зовнішніх та внутрішніх кібератак.

З’єднання також можуть бути захищені за допомогою рішень для моніторингу загроз, які запобігають витоку даних , та віртуальних приватних мереж (VPN) , які шифрують дані перегляду та запобігають перехопленню інтернет-активності користувачів хакерами.

Інтерфейси хмарного прикладного програмування (API) дозволяють програмам і системам Інтернету речей взаємодіяти та інтегруватися. Вони відіграють важливу роль у зв'язку служб і передачі даних. Це означає, що зламаний або зламаний API може призвести до масового витоку даних. Тому життєво важливо захистити хмарні API за допомогою автентифікації , шифрування , токенів та шлюзів API.

Наприклад, безпека веб-API захищає дані під час їх передачі через Інтернет, а REST API шифрують дані та інтернет-з’єднання для захисту даних, що передаються між серверами та пристроями.

Розробка безпечного мережевого з’єднання забезпечує належний контроль доступу . Це гарантує, що до мережі дозволено підключатися лише безпечним, автентифікованим або перевіреним пристроям.

Безпека мережі починається з налаштування безпечного брандмауера. Потім важливо розгорнути інструменти та методи безпеки, такі як багатофакторна автентифікація (MFA) , які захищають пристрої щоразу, коли користувачі намагаються підключитися до мережі. Також важливо зберігати ключі автентифікації в безпеці, встановлювати оновлене антивірусне та антивірусне програмне забезпечення , а також постійно контролювати мережеву активність, щоб забезпечити безпеку пристроїв та користувачів.

Шифрування має вирішальне значення для захисту даних під час їх передачі між пристроями або в Інтернеті. Шифрування Інтернету речей зазвичай здійснюється за допомогою асиметричних та симетричних методів

шифрування. Симетричне шифрування використовує один криптографічний ключ для шифрування та розшифрування даних, тоді як асиметричне шифрування використовує відкриті та закриті ключі та пропонує підвищений рівень безпеки.

Пристрої та датчики Інтернету речей створюють постійно зростаючі обсяги конфіденційних даних, від фінансової та особистої інформації до біометричних даних, що зберігаються на хмарних або апаратних сховищах. Тому вкрай важливо мати засоби безпеки, щоб гарантувати безпеку цієї інформації під час зберігання або передачі.

Захист сховища даних включає ефективні, оновлені антивірусні рішення та інструменти моніторингу та сканування, які захищають мережу від загроз Інтернету речей у режимі реального часу. Важливо мати такі функції, як гнучка звітність та сканування, а також системи сповіщень, захист від шкідливого програмного забезпечення та централізовану консоль керування, яка забезпечує глибокий контроль мережевої активності.

3.2 Реалізація механізмів автентифікації та авторизації

```
# ============================================================
# USERS DATABASE
# ============================================================

USERS = {
    "admin": {
        "password": hashlib.sha256("admin123".encode()).hexdigest(),
        "role": "Administrator"
    },
    "operator": {
        "password": hashlib.sha256("operator123".encode()).hexdigest(),
        "role": "Operator"
    },
    "guest": {
        "password": hashlib.sha256("guest123".encode()).hexdigest(),
        "role": "Guest"
    }
}

# ============================================================
# NETWORK SEGMENTS
# ============================================================
```

```
NETWORK_SEGMENTS = {
    "IoT Devices": [
        "Camera-01",
        "Sensor-Temp",
        "DoorLock-01",
        "SmartLight-01"
    ],
    "Corporate Network": [
        "Workstation-01",
        "Server-DB",
        "Admin-PC"
    ],
    "DMZ": [
        "WebGateway",
        "Firewall"
    ]
}

# ============================================================
# ACCESS RULES
# ============================================================

ACCESS_RULES = {
    "Administrator": ["IoT Devices", "Corporate Network", "DMZ"],
    "Operator": ["IoT Devices"],
    "Guest": []
}

# ============================================================
# GLOBAL VARIABLES
# ============================================================

CURRENT_USER = None
CURRENT_ROLE = None
MONITORING = False
```

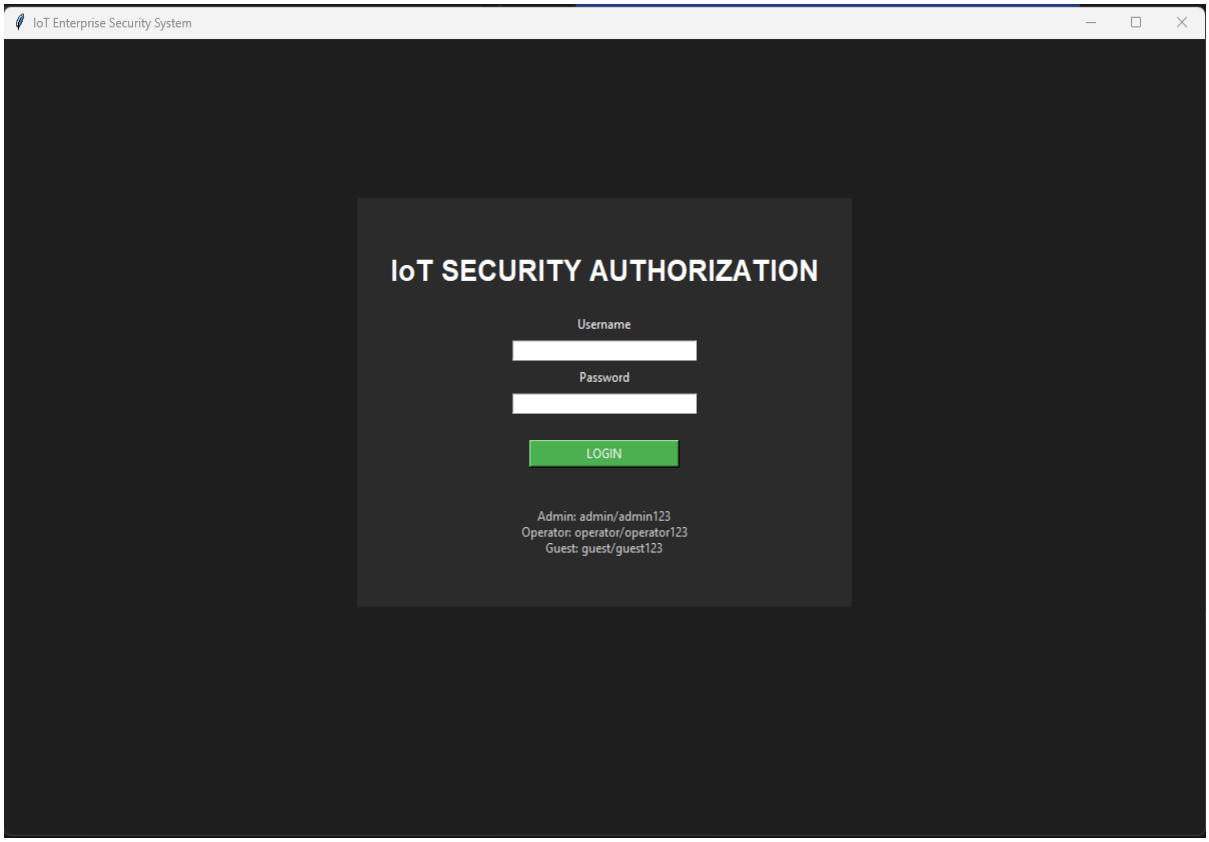

Рис. 3.1. Форма авторизації

3.3 Використання криптографічного захисту даних

```
def generate_key():
    return secrets.token_bytes(16)

SECRET_KEY = generate_key()

def encrypt_data(data):
    """
     XOR-шифрування
    """

    data_bytes = data.encode()

    encrypted = bytearray()

    for i in range(len(data_bytes)):
        encrypted.append(data_bytes[i] ^ SECRET_KEY[i % len(SECRET_KEY)])

    return base64.b64encode(encrypted).decode()

def decrypt_data(encrypted_data):

    encrypted_bytes = base64.b64decode(encrypted_data)

    decrypted = bytearray()
```

```
    for i in range(len(encrypted_bytes)):
        decrypted.append(
            encrypted_bytes[i] ^ SECRET_KEY[i % len(SECRET_KEY)]
        )

    return decrypted.decode()
```

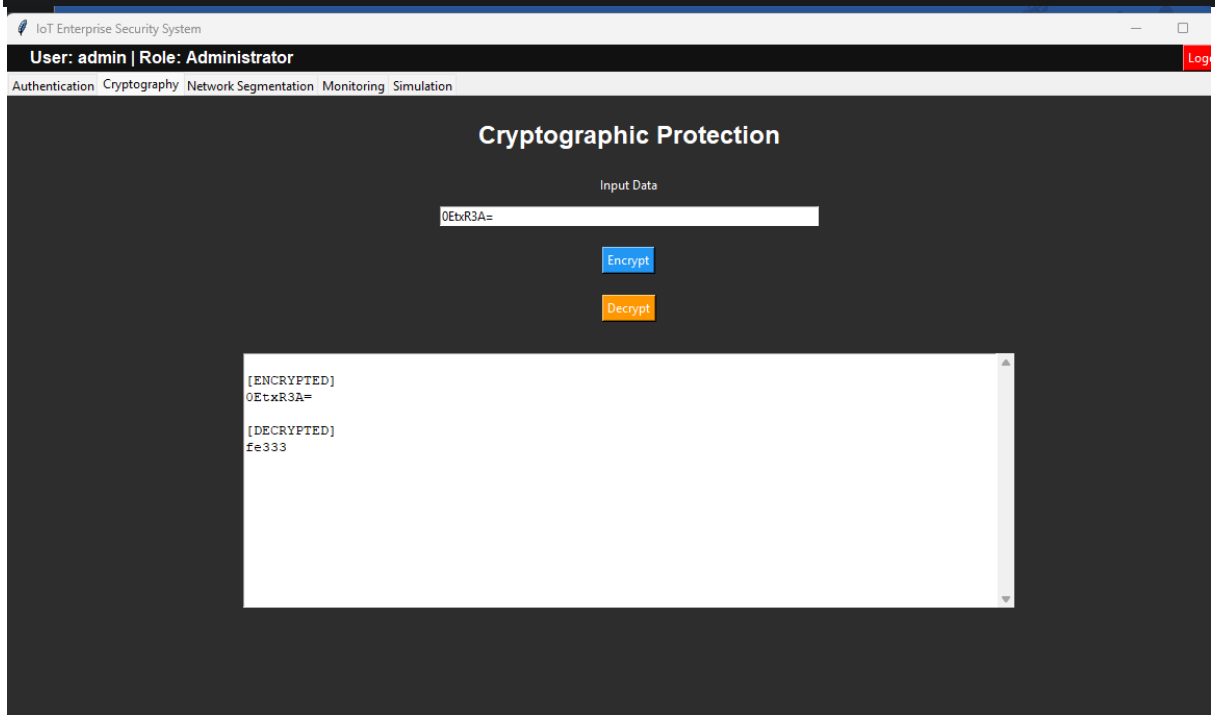

Рис. 3.2. Криптографічний захист данних

3.4 Сегментація мережі та контроль доступу

```
NETWORK SEGMENTS
# ============================================================

NETWORK_SEGMENTS = {
    "IoT Devices": [
        "Camera-01",
        "Sensor-Temp",
        "DoorLock-01",
        "SmartLight-01"
    ],
    "Corporate Network": [
        "Workstation-01",
        "Server-DB",
        "Admin-PC"
    ],
    "DMZ": [
        "WebGateway",
        "Firewall"
    ]
}

ACCESS_RULES = {
```

```
    "Administrator": ["IoT Devices", "Corporate Network", "DMZ"],
    "Operator": ["IoT Devices"],
    "Guest": []
}
```

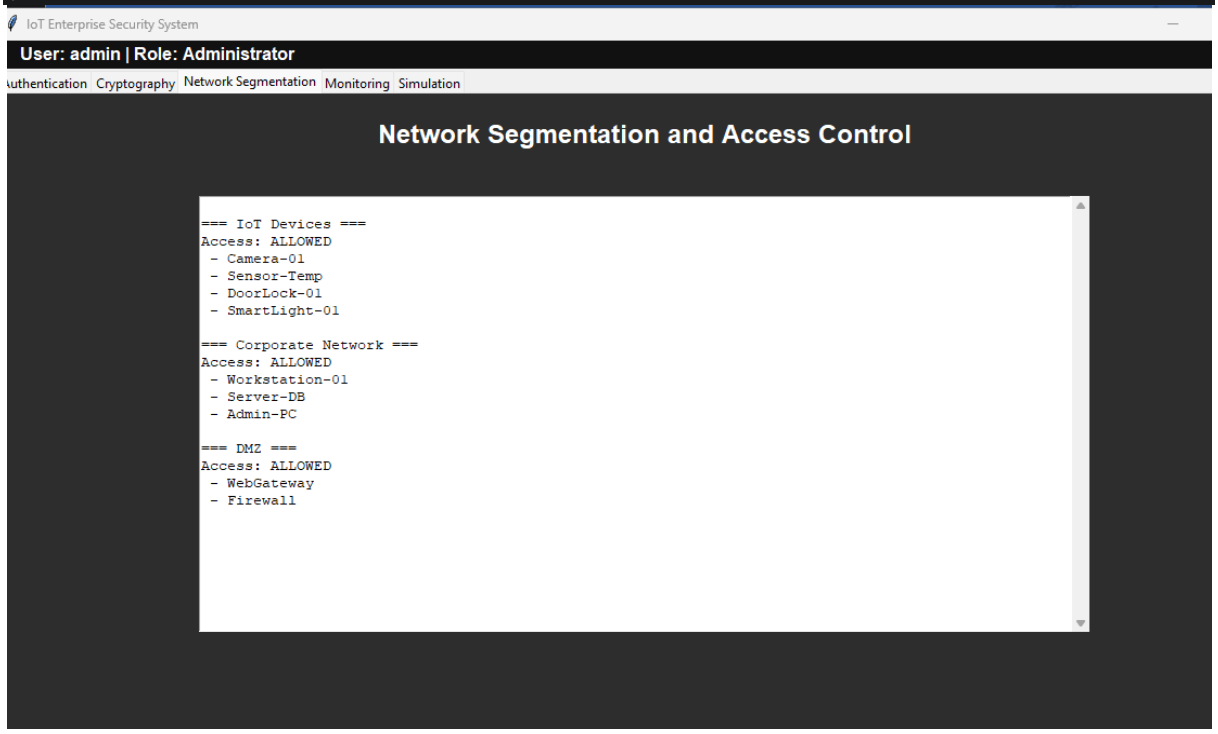

Рис. 3.3. Сегменти мережі

3.5 Система моніторингу та виявлення атак

```
# MONITORING TAB
# ============================================================

def build_monitor_tab(self):

    title = tk.Label(
        self.monitor_tab,
        text="Attack Monitoring and Detection",
        font=("Arial", 18, "bold"),
        fg="white",
        bg="#2D2D2D"
    )

    title.pack(pady=20)

    start_btn = tk.Button(
        self.monitor_tab,
        text="Start Monitoring",
        bg="#4CAF50",
        fg="white",
        command=self.start_monitoring
    )

    start_btn.pack(pady=10)
```

```
    stop_btn = tk.Button(
        self.monitor_tab,
        text="Stop Monitoring",
        bg="red",
        fg="white",
        command=self.stop_monitoring
    )

    stop_btn.pack(pady=10)

    self.monitor_text = scrolledtext.ScrolledText(
        self.monitor_tab,
        width=120,
        height=25
    )

    self.monitor_text.pack(pady=20)
```

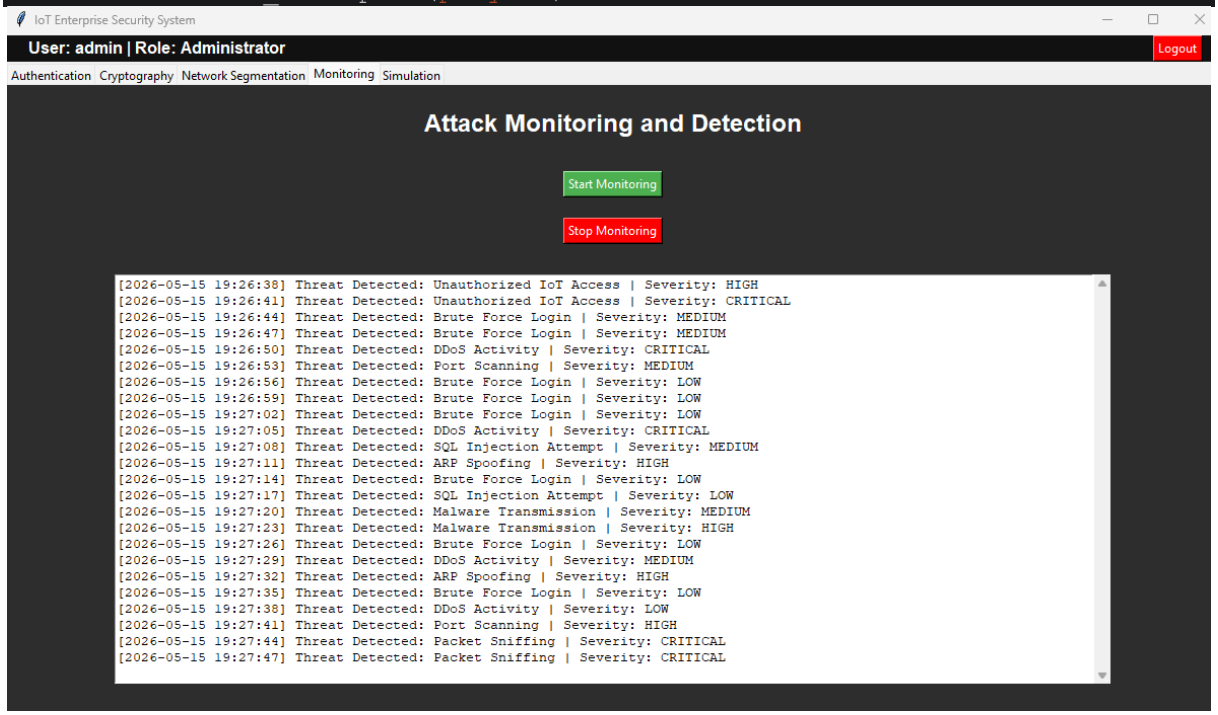

Рис. 3.4. Вікно моніторингу загроз

3.6 Розробка програмного або імітаційного середовища моделі

```
# ============================================================
# SIMULATION TAB
# ============================================================

def build_simulation_tab(self):

    title = tk.Label(
        self.simulation_tab,
        text="IoT Threat Model Simulation",
        font=("Arial", 18, "bold"),
```

```
        fg="white",
        bg="#2D2D2D"
    )

    title.pack(pady=20)

    simulate_btn = tk.Button(
        self.simulation_tab,
        text="Run Simulation",
        bg="#9C27B0",
        fg="white",
        command=self.run_simulation
    )

    simulate_btn.pack(pady=20)

    self.sim_text = scrolledtext.ScrolledText(
        self.simulation_tab,
        width=110,
        height=25
    )

    self.sim_text.pack(pady=20)

# ============================================================
# LOGIN
# ============================================================

def login(self):

    global CURRENT_USER
    global CURRENT_ROLE

    username = self.username_entry.get()
    password = self.password_entry.get()

    if authenticate(username, password):

        CURRENT_USER = username
        CURRENT_ROLE = USERS[username]["role"]

        messagebox.showinfo(
            "Success",
            "Authentication successful"
        )

        self.create_dashboard()

    else:
        messagebox.showerror(
            "Error",
            "Invalid username or password"
        )

# ============================================================
# ENCRYPT
# ============================================================

def encrypt_action(self):

    text = self.crypto_input.get()
```

```
    encrypted = encrypt_data(text)

    self.crypto_output.insert(
        tk.END,
        f"\n[ENCRYPTED]\n{encrypted}\n"
    )

# ============================================================
# DECRYPT
# ============================================================

def decrypt_action(self):

    text = self.crypto_input.get()

    try:

        decrypted = decrypt_data(text)

        self.crypto_output.insert(
            tk.END,
            f"\n[DECRYPTED]\n{decrypted}\n"
        )

    except:
        messagebox.showerror(
            "Error",
            "Invalid encrypted data"
        )
```

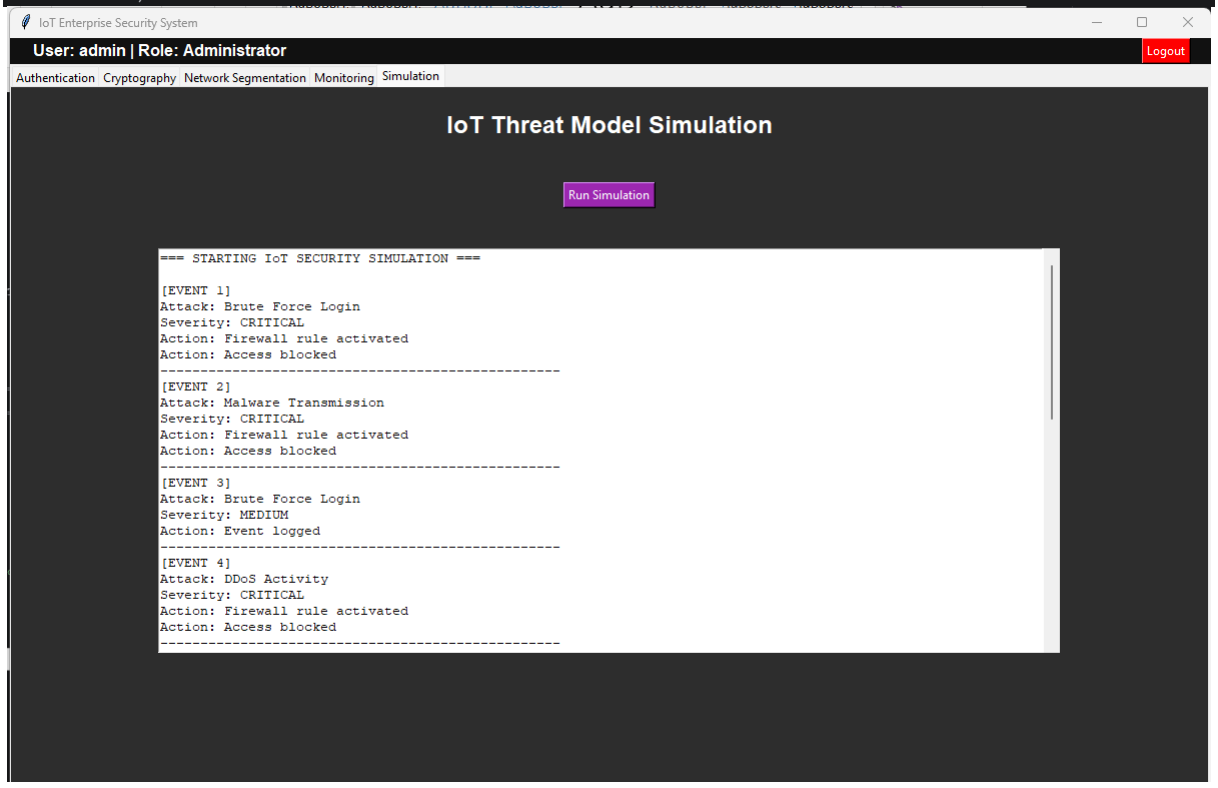

Рис. 3.5. Симуляцій загроз в мережі

Висновки до розділу 3

Дотримання найкращих практик безпеки пристроїв Інтернету речей (IoT) є критично важливим для постійного забезпечення безпеки користувачів, пристроїв і даних. Безпека IoT починається зі створення та документування стратегії, яка інтегрується із загальною IT-стратегією та загальним бізнес-планом організації. Вона повинна охоплювати кожну бізнес-сферу, яка використовує мережу IoT організації.

Ефективна стратегія безпеки Інтернету речей повинна визначати заходи безпеки, які необхідно впровадити, та як вони будуть моніторитися або переглядатися з часом. Вона також повинна пропонувати глибоке розуміння IT-архітектури організації та кінцевих точок, щоб забезпечити захист усього бізнесу від загроз Інтернету речей.

В кінцевому результаті на основі вивченої інформації було розроблено програмний застосунок який моделює інтерфейс системи керування IoT пристроями.В ній кожен користувач має свої повноваження та не може робити більше ніж цього потрібно відповідно до ролі.

Програма демонструє симуляцію загроз та захист пристроїв.

ВИСНОВКИ

Розробка нових послуг в рамках Інтернету речей значною мірою залежить від вирішення проблем безпеки та пошуку нових рішень для різних застосувань. Представлені дослідження розглядають ключові питання, досліджуючи обмеження ресурсів та децентралізовані системи, а також пропонуючи програмно-визначений мережевий підхід для ефективного управління груповими ключами. Також представлені вдосконалені методи автентифікації для зв'язку між транспортним засобом та інфраструктурою, використовуючи ефективну криптографію та фізично неклоновані функції. Крім того, проактивна безпека вдосконалюється за допомогою спільної системи виявлення вторгнень на основі федеративного навчання разом з автоматизованою базою даних вразливостей для покращеного виявлення загроз. Нарешті, людський аспект безпеки Інтернету речей розглядається шляхом дослідження емоційних реакцій користувачів на інциденти безпеки, з акцентом на ширших наслідках кібербезпеки в підключених середовищах.

Оскільки Інтернет речей продовжує розширюватися в різні сектори, проблеми безпеки, які він створює, стають все більш очевидними та актуальними. Це дослідження показало, що системи Інтернету речей за своєю суттю вразливі на багатьох рівнях, включаючи апаратне забезпечення, програмне забезпечення, мережі та хмарну інфраструктуру. Ці вразливості створюють можливості для зловмисників використовувати пристрої Інтернету речей, що призводить до потенційних витоків даних, збоїв у роботі системи та несанкціонованого контролю критично важливих операцій. Зростаюча залежність від Інтернету речей підкреслює нагальну необхідність вирішення цих проблем безпеки за допомогою проактивних механізмів захисту та структурованих стратегій пом'якшення наслідків.

Аналіз, проведений у цій роботі, підкреслює необхідність посилення безпеки Інтернету речей шляхом впровадження найкращих практик, таких як безпечні оновлення прошивки, надійні методи автентифікації, зашифровані канали зв'язку та постійний моніторинг аномалій. Завдяки вживанню цих заходів безпеки можна значно зменшити ризик експлуатації, забезпечуючи цілісність та надійність екосистем Інтернету речей. Крім того, це дослідження підкреслює важливість постійних досліджень та розробок у сфері безпеки Інтернету речей для протидії новим загрозам та адаптації до мінливого ландшафту кібератак.

Оскільки технологія Інтернету речей продовжує розвиватися та інтегруватися в критично важливі інфраструктури, відповідальність за безпеку цих систем має залишатися головним пріоритетом. Майбутні дослідження повинні бути зосереджені на вдосконаленні існуючих заходів безпеки, вивченні інноваційних рішень для зменшення нових векторів атак та підвищенні стійкості мереж Інтернету речей до складних загроз. Проактивно вирішуючи ці проблеми, ми як спільнота можемо працювати над створенням більш безпечного та надійного середовища Інтернету речей, яке зможе відповідати вимогам сучасних технологій та їх широкого застосування.

Дотримання найкращих практик безпеки пристроїв Інтернету речей (IoT) є критично важливим для постійного забезпечення безпеки користувачів, пристроїв і даних. Безпека IoT починається зі створення та документування стратегії, яка інтегрується із загальною IT-стратегією та загальним бізнес-планом організації. Вона повинна охоплювати кожну бізнес-сферу, яка використовує мережу IoT організації.

Ефективна стратегія безпеки Інтернету речей повинна визначати заходи безпеки, які необхідно впровадити, та як вони будуть моніторитися або переглядатися з часом. Вона також повинна пропонувати глибоке

розуміння IT-архітектури організації та кінцевих точок, щоб забезпечити захист усього бізнесу від загроз Інтернету речей.

В кінцевому результаті на основі вивченої інформації було розроблено програмний застосунок який моделює інтерфейс системи керування IoT пристроями.В ній кожен користувач має свої повноваження та не може робити більше ніж цього потрібно відповідно до ролі.

Програма демонструє симуляцію загроз та захист пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A Survey. *Comput. Netw.* 2010, *54*, 2787–2805.

2. Weber, R.H. Internet of Things—New Security and Privacy Challenges. *Comput. Law Secur. Rev.* 2010, *26*, 23–30.

3. Khanam, S.; Shapla, S.; Ali, M.S.; Hossain, M.S.; Ahamad, M.S.; Rahman, M.M. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE Access* 2020, *8*, 219709–219743.

4. Baker, S.A.; Nori, A.S. Internet of Things Security: A Survey. In *Advances in Cyber Security, Proceedings of the Second International Conference, ACeS 2020, Penang, Malaysia, 8–9 December 2020*; Revised Selected Papers 2; Springer: Singapore, 2021; pp. 95–117.

5. Campos, E.M.; Saura, P.F.; González-Vidal, A.; Hernández-Ramos, J.L.; Bernabé, J.B.; Baldini, G.; Skarmeta, A. Evaluating Federated Learning for Intrusion Detection in Internet of Things: Review and Challenges. *Comput. Netw.* 2022, *203*, 108661.

6. Katagi, M.; Moriai, S. *Lightweight Cryptography for the Internet of Things*; Sony Corporation: Tokyo, Japan, 2008; pp. 7–10.

7. Summerville, D.H.; Zach, K.M.; Chen, Y. Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices. In Proceedings of the 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), Nanjing, China, 14–16 December 2015; pp. 1–8.

8. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards Decentralized IoT Security Enhancement: A Blockchain Approach. *Comput. Electr. Eng.* 2018, *72*, 266–273.

9. Hellaoui, H.; Koudil, M.; Bouabdallah, A. Energy-Efficient Mechanisms in Security of the Internet of Things: A Survey. *Comput. Netw.* 2017, *127*, 173–189.

10. Ishaq, I.; Carels, D.; Teklemariam, G.K.; Hoebeke, J.; Van den Abeele, F.; De Poorter, E.; Demeester, P. IETF Standardization in the Field of the Internet of Things (IoT): A Survey. *J. Sens. Actuator Netw.* 2013, *2*, 235–287.

11. Bothra, P.; Karmakar, R.; Bhattacharya, S.; De, S. How Can Applications of Blockchain and Artificial Intelligence Improve Performance of Internet of Things?—A Survey. *Comput. Netw.* 2023, *224*, 109634.

12. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet Things J.* 2017, *4*, 1250–1258.

13. Elmassik, Z. Edge Computing in the Internet of Things: A Survey. *Authorea Prepr.* 2023.

14. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* 2020, *9*, 44.

15. Taurshia, A.; Kathrine, J.W.; Andrew, J.; Eunice R, J. Securing Internet of Things Applications Using Software-Defined Network-Aided Group Key Management with a Modified One-Way Function Tree. *Appl. Sci.* 2024, *14*, 2405.

16. Xie, Q.; Huang, J. Improvement of a Conditional Privacy-Preserving and Desynchronization-Resistant Authentication Protocol for IoV. *Appl. Sci.* 2024, *14*, 2451.

17. Wardana, A.A.; Kołaczek, G.; Sukarno, P. Lightweight, Trust-Managing, and Privacy-Preserving Collaborative Intrusion Detection for Internet of Things. *Appl. Sci.* 2024, *14*, 4109.

18. Felkner, A.; Adamski, J.; Koman, J.; Rytel, M.; Janiszewski, M.; Lewandowski, P.; Pachnia, R.; Nowakowski, W. Vulnerability and Attack Repository for IoT: Addressing Challenges and Opportunities in Internet of Things Vulnerability Databases. *Appl. Sci.* 2024, *14*, 10513.

19. Albarrak, K.M. Securing the Future of Web-Enabled IoT: A Critical Analysis of Web of Things Security. *Appl. Sci.* 2024, *14*, 10867.

20. Budimir, S.; Fontaine, J.R.J.; Huijts, N.M.A.; Haans, A.; IJsselsteijn, W.A.; Oostveen, A.-M.; Stahl, F.; Heartfield, R.; Loukas, G.; Bezemskij, A.; et al. We Are Not Equipped to Identify the First Signs of Cyber–Physical Attacks: Emotional Reactions to Cybersecurity Breaches on Domestic Internet of Things Devices. Applied Sciences, 2024.

21. IEC 61158-1 Ed.2.0. Industrial Communication Networks—Fieldbus Specifications—Part 1: Overview and Guidance for the IEC 61158 and IEC 61784 Series. IEC: Geneva, Switzerland, 2019.

22. Lu, Y.; Xu, X.; Wang, L. Smart manufacturing process and system automation—A critical review of the standards and envisioned scenarios. J. Manuf. Syst. 2020, 56, 312–325.

23. Abubakr, M.; Abbas, A.T.; Tomaz, I.; Soliman, M.S.; Luqman, M.; Hegab, H. Sustainable and Smart Manufacturing: An Integrated Approach. Sustainability 2020, 12, 2280.

24. Yu, H.; Zeng, P.; Xu, C. Industrial Wireless Control Networks: From WIA to the Future. Engineering. 2022, 8, 18–24.

25. Cao, W.; Jiang, P.; Fu, Y. Ubiquitous data computing and information using in a smart factory with wireless manufacturing. Eng. Sci. 2013, 11, 2–9.

26. Suvarna, M.; Büth, L.; Hejny, J.; Mennenga, M.; Li, J.; Ng, Y.; Herrmann, C.; Wang, X. Smart Manufacturing for Smart Cities—Overview, Insights, and Future Directions. Adv. Intell. Syst. 2020, 2, 2000043.

27. European Telecommunications Standards Institute (ETSI). Fifth Generation Fixed Network (F5G), F5G Technology Landscape. 2021. URL:
https://www.etsi.org/deliver/etsi_gs/F5G/001_099/003/01.01.01_60/gs_F5G003v010101p.pdf
(дата звернення: 19.05.2026).

28. Lenz, J.; MacDonald, E.; Harik, R.; Wuest, T. Optimizing smart manufacturing systems by extending the smart products paradigm to the beginning of life. J. Manuf. Syst. 2020, 57, 274–286.

29. Li, B.; Zhang, L.; Chai, X. Smart Cloud Manufacturing (Cloud Manufacturing 2.0)—A New Paradigm and Approach of Smart Manufacturing. ISPE CE 2014, 26.

30. Mittal, S.; Khan, M.A.; Romero, D.; Wuest, T. Smart manufacturing: Characteristics, technologies and enabling factors. Proc. Inst. Mech. Eng. Part B J. Eng. Manuf. 2019, 233, 1342–1361.

31. Moghaddam, M.; Cadavid, M.N.; Kenley, C.R.; Deshmukh, A.V. Reference architectures for smart manufacturing: A critical review. J. Manuf. Syst. 2018, 49, 215–225.

32. Yao, X.; Zhou, J.; Lin, Y.; Li, Y.; Yu, H.; Liu, Y. Smart manufacturing based on cyber-physical systems and beyond. J. Intell. Manuf. 2017, 30, 2805–2817.

33. Ghahramani, M.; Qiao, Y.; Zhou, M.C.; O'Hagan, A.; Sweeney, J. AI-based modeling and data-driven evaluation for smart manufacturing processes. IEEE/CAA J. Autom. Sin. 2020, 7, 1026–1037.

34. Jiang, J.; Lin, C.; Han, G.; Abu-Mahfouz, A.M.; Shah, S.B.H.; Martínez-García, M. How AI-Enabled SDN Technologies Improve the Security and Functionality of Industrial IoT Network: Architectures, Enabling Technologies, and Opportunities. Digit. Commun. Netw. 2022.

35. Parhi, S.; Joshi, K.; Akarte, M. Smart manufacturing: A framework for managing performance. Int. J. Comput. Integr. Manuf. 2021, 34, 227–256.

36. Tuptuk, N.; Hailes, S. Security of smart manufacturing systems. J. Manuf. Syst. 2018, 47, 93–106.

37. Zenisek, J.; Wild, N.; Wolfartsberger, J. Investigating the Potential of Smart Manufacturing Technologies. Procedia Comput. Sci. 2021, 180, 507–516.

38. Cheng, J.; Chen, W.; Tao, F.; Lin, C.L. Industrial IoT in 5G environment towards smart manufacturing. J. Ind. Inf. Integr. 2018, 10, 10–19.

39. Kim, H.; Shon, T. Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. J Supercomput 2022, 78, 13554–13563.

40. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. Sensors 2021, 21, 3654.

41. Lu, Y.; Asghar, M.R. Semantic communications between distributed cyber-physical systems towards collaborative automation for smart manufacturing. J. Manuf. Syst. 2020, 55, 348–359.

42. Xia, K.; Sacco, C.; Kirkpatrick, M.; Saidy, C.; Nguyen, L.; Kircaliali, A.; Harik, R. A digital twin to train deep reinforcement learning agent for smart manufacturing plants: Environment, interfaces and intelligence. J. Manuf. Syst. 2021, 58, 210–230.

ДОДАТКИ

Додаток А.Лістинг

```
import tkinter as tk
from tkinter import ttk, messagebox, scrolledtext
import hashlib
import secrets
import base64
import random
import time
import threading
from datetime import datetime

# ============================================================
# USERS DATABASE
# ============================================================

USERS = {
    "admin": {
        "password": hashlib.sha256("admin123".encode()).hexdigest(),
        "role": "Administrator"
    },
    "operator": {
        "password": hashlib.sha256("operator123".encode()).hexdigest(),
        "role": "Operator"
    },
    "guest": {
        "password": hashlib.sha256("guest123".encode()).hexdigest(),
        "role": "Guest"
    }
}

# ============================================================
# NETWORK SEGMENTS
# ============================================================

NETWORK_SEGMENTS = {
    "IoT Devices": [
        "Camera-01",
        "Sensor-Temp",
        "DoorLock-01",
        "SmartLight-01"
    ],
    "Corporate Network": [
        "Workstation-01",
        "Server-DB",
        "Admin-PC"
    ],
    "DMZ": [
        "WebGateway",
        "Firewall"
    ]
}

# ============================================================
# ACCESS RULES
# ============================================================

ACCESS_RULES = {
```

```
    "Administrator": ["IoT Devices", "Corporate Network", "DMZ"],
    "Operator": ["IoT Devices"],
    "Guest": []
}

# ============================================================
# GLOBAL VARIABLES
# ============================================================

CURRENT_USER = None
CURRENT_ROLE = None
MONITORING = False

# ============================================================
# CRYPTOGRAPHIC FUNCTIONS
# ============================================================

def generate_key():
    return secrets.token_bytes(16)

SECRET_KEY = generate_key()

def encrypt_data(data):
    """
     XOR-шифрування
    """

    data_bytes = data.encode()

    encrypted = bytearray()

    for i in range(len(data_bytes)):
        encrypted.append(data_bytes[i] ^ SECRET_KEY[i % len(SECRET_KEY)])

    return base64.b64encode(encrypted).decode()

def decrypt_data(encrypted_data):

    encrypted_bytes = base64.b64decode(encrypted_data)

    decrypted = bytearray()

    for i in range(len(encrypted_bytes)):
        decrypted.append(
            encrypted_bytes[i] ^ SECRET_KEY[i % len(SECRET_KEY)]
        )

    return decrypted.decode()

# ============================================================
# AUTHENTICATION
# ============================================================

def authenticate(username, password):

    if username in USERS:

        hashed_password = hashlib.sha256(
            password.encode()
        ).hexdigest()
```

```
        if USERS[username]["password"] == hashed_password:
            return True

    return False

def authorize(role, segment):

    allowed = ACCESS_RULES.get(role, [])

    return segment in allowed

# ============================================================
# ATTACK SIMULATION
# ============================================================

ATTACKS = [
    "SQL Injection Attempt",
    "Brute Force Login",
    "Port Scanning",
    "DDoS Activity",
    "Unauthorized IoT Access",
    "ARP Spoofing",
    "Malware Transmission",
    "Packet Sniffing"
]
```