Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Модель гібридної IoT-системи з підвищеним рівнем інформаційної безпеки»

Виконавець: студент IV курсу, групи КБ-41

_____ **Нікіта ОСТАПЧУК**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я, прізвище**
Керівник		Інна МИХАЛЬЧУК
Нормоконтроль		Юрій ЩЕБЛАНІН

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

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

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Остапчуку Нікіті Олександровичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Модель гібридної IoT-системи з підвищеним рівнем інформаційної безпеки

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Наявні IoT-системи та методи їх захисту

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Дослідження наявних IoT-систем та їх типових недоліків, аналіз наявних методів захисту, обґрунтування та розробка гібридної моделі IoT-системи

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблена модель гібридної IoT-системи, яка

забезпечує підвищений рівень захисту даних та безпечну взаємодію пристроїв

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ Інна МИХАЛЬЧУК
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Нікіта ОСТАПЧУК
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 14.01.2025	*виконано*
2	Аналіз літератури	15.01.2025 – 13.02.2025	*виконано*
3	Обґрунтування вибору рішення	14.02.2025 – 17.02.2025	*виконано*
4	Дослідження принципів IoT-систем	18.02.2025 – 03.03.2025	*виконано*
5	Аналіз наявних рішень та їх недоліків	02.03.2025 – 24.03.2025	*виконано*
6	Вибір та аналіз інструментів для інтеграції в гібридну систему	25.03.2025 – 02.04.2025	*виконано*
7	Створення схеми гібридної IoT-системи	03.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2025 – 28.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	29.05.2025 – 13.06.2025	*виконано*

Завдання видала _____ Інна МИХАЛЬЧУК
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Нікіта ОСТАПЧУК
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, додатків, має 83 сторінки основного тексту, 4 рисунка та 3 таблиці. Список використаних джерел містить 28 пунктів.

Метою роботи є розробка моделі гібридної IoT-системи з підвищеним рівнем інформаційної безпеки для захисту даних і надійної взаємодії пристроїв у критично важливих середовищах.

Об’єктом дослідження є Інтернет речей (IoT) як середовище обміну та обробки інформації в умовах сучасних кіберзагроз.

Предметом дослідження є архітектурні рішення, методи шифрування, автентифікації, контролю доступу та захисту даних у гібридних IoT-системах.

Методи дослідження:

- Аналіз наявних IoT-архітектур та загроз інформаційній безпеці;
- Аналіз наявних методів забезпечення безпеки;
- Моделювання гібридної IoT-архітектури з розмежуванням рівнів безпеки;
- Порівняння запропонованої архітектури з наявними рішеннями.

Практична цінність полягає в розробленій моделі гібридної IoT-системи, яка забезпечує підвищений рівень захисту даних та безпечну взаємодію пристроїв. Вона дозволяє ефективно протидіяти сучасним кіберзагрозам за рахунок використання багаторівневого захисту, криптографії та безпечної автентифікації, що робить її придатною для впровадження у сферах з підвищеними вимогами до інформаційної безпеки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 6
ВСТУП 9
РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПРОБЛЕМАТИКИ IOT 12
1.1 Актуальність теми, роль IoT у сучасних системах. 12
1.2 Визначення, архітектура та класифікація IoT-систем. 14
1.3 Загрози, вразливості, проблеми безпеки. 18
1.4 Нормативна база. 23
Висновки за розділом 1. 26
РОЗДІЛ 2 ОГЛЯД І КРИТИЧНИЙ АНАЛІЗ НАЯВНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ 27
2.1 Криптографічні методи, доступ, IDS/IPS, автентифікація. 27
2.2 Приклади рішень, фреймворків, архітектур. 32
2.3 Проблеми та обмеження наявних підходів. 34
2.4 Мотивація до створення нового підходу. 38
Висновки за розділом 2. 40
РОЗДІЛ 3 РОЗРОБКА ГІБРИДНОЇ СИСТЕМИ БЕЗПЕКИ IOT 41
3.1 Концепція і обґрунтування. 41
3.2 Архітектура. 44
3.3 Технології та механізми безпеки. 53
3.4 Управління ризиками. 58
Висновки за розділом 3. 61
РОЗДІЛ 4 ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОЇ СИСТЕМИ 63
4.1 Порівняння з аналогами. 63
4.2 Переваги і недоліки. 69
4.3 Перспективи розвитку. 72
Висновки за розділом 4. 76
ВИСНОВКИ 78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 80
ДОДАТОК А 84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ABAC	–	Attribute-Based Access Control
AES	–	Advanced Encryption Standard
AES-GCM	–	Advanced Encryption Standard - Galois/Counter Mode
AI	–	Artificial Inteligence
AIoT	–	Artificial Intelligence of Things
AMQP	–	Advanced Message Queuing Protocol
API	–	Application Programming Interface
CA	–	Certification Authority
CoAP	–	Constrained Application Protocol
CRL	–	Certificate Revocation List
D2D	–	Device-to-Device
DAC	–	Discretionary Access Control
DDoS	–	Distributed Denial of Service
DID	–	Decentralized Identifiers
DLT	–	Distributed Ledger Technology
DNS	–	Domain Name System
DoS	–	Denial of Service
DTLS	–	Datagram Transport Layer Security
ECC	–	Elliptic Curve Cryptography
FOTA	–	Firmware-Over-The-Ai
HIDS	–	Host-based Intrusion Detection Systems
HIPS	–	Host-based Intrusion Prevention Systems
HSM	–	Hardware Security Modules
HTTP	–	Hypertext Transfer Protocol
IaaS	–	Infrastructure as a Service

IAM	–	Identity and Access Management
IdM	–	Identity Management
IDS	–	Intrusion Detection Systems
IIoT	–	Industrial IoT
Intel SGX	–	Intel Software Guard Extensions
IoC	–	Indicators of Compromise
IoT	–	Internet of Things
IPsec	–	Internet Protocol Security
IPS	–	Intrusion Prevention Systems
JTAG	–	Joint Test Action Group
JWT	–	JSON Web Tokens
KMS	–	Key Management Systems
LoRaWAN	–	Long Range Wide Area Network
LPWAN	–	Low-Power Wide-Area Network
LWC	–	Lightweight Cryptography
M2M	–	Machine-to-machine
MAC	–	Mandatory Access Control
MFA	–	Multi-Factor Authentication
ML	–	Machine Learning
MQTT	–	Message Queuing Telemetry Transport
NAC	–	Network Access Control
NB-IoT	–	Narrowband IoT
NIDS	–	Network Intrusion Detection Systems
NIPS	–	Network Intrusion Prevention Systems
OCSP	–	Online Certificate Status Protocol
OMA DM	–	Open Mobile Alliance Device Management
OTA	–	Over-the-Air
PaaS	–	Platform as a Service
PAM	–	Privileged Access Management

PQC	–	Post-Quantum Cryptography
PSK	–	Pre-Shared Key
PUF	–	Physically Unclonable Functions
RBAC	–	Role-Based Access Control
SaaS	–	Software as a Service
SDN	–	Software-Defined Networking
SE	–	Secure Elements
SIEM	–	Security Information and Event Management
SOAR	–	Security Orchestration, Automation and Response
SOTA	–	Software-Over-The-Air
SSL	–	Secure Sockets Layer
TEE	–	Trusted Execution Environments
TLS	–	Transport Layer Security
TPM	–	Trusted Platform Modules
TR-069	–	Technical Report 069
UART	–	Universal Asynchronous Receiver-Transmitter
UEBA	–	User and Entity Behavior Analytics
VLAN	–	Virtual Local Area Network
VPN	–	Virtual Private Network
Wi-Fi	–	Wireless Fidelity
WIPS	–	Wireless Intrusion Prevention Systems
XSS	–	Cross-Site Scripting
ІБ	–	Інформаційна безпека
КБ	–	Кібербезпека

ВСТУП

Сучасний світ переживає епоху Четвертої промислової революції (Індустрії 4.0), рушійною силою якої є цифрові технології. Однією з ключових та найбільш динамічних технологій є Інтернет Речей (IoT), що представляє собою глобальну мережу фізичних об'єктів, оснащених сенсорами, програмним забезпеченням та іншими технологіями для підключення та обміну даними [1]. Кількість підключених IoT-пристроїв стрімко зростає, сягаючи десятків мільярдів одиниць, та відіграє значну роль у промисловості (IIoT), розумних містах, охороні здоров'я, сільському господарстві, енергетиці та побутовій сфері [5].

Разом з тим, стрімке поширення IoT-технологій супроводжується пропорційним зростанням загроз та вразливостей безпеки [2, 3]. IoT-системи часто характеризуються використанням пристроїв з обмеженими обчислювальними ресурсами, великою різнорідністю апаратного та програмного забезпечення, а також тривалим життєвим циклом, що робить їх привабливими цілями для зловмисників [6]. Наслідки успішних кібератак можуть бути руйнівними, включаючи фінансові збитки, порушення конфіденційності даних та навіть загрозу фізичній безпеці [3]. Наявні методи забезпечення безпеки часто виявляються недостатньо ефективними для IoT-середовища, оскільки традиційні підходи погано адаптовані до специфіки IoT, а централізовані системи мають суттєві недоліки, такі як єдина точка відмови та затримки. Наявні системи безпеки для IoT часто є статичними та нездатними швидко адаптуватися до нових видів атак.

Таким чином, актуальність даної роботи зумовлена нагальною потребою у розробці та дослідженні нових, більш гнучких, комплексних та ефективних підходів до забезпечення безпеки IoT-систем. Запропонована гібридна система безпеки, що поєднує сильні сторони різних технологій та архітектурних рішень, спрямована на подолання обмежень наявних підходів та забезпечення надійного

захисту на всіх рівнях IoT-інфраструктури. Дослідження та впровадження таких систем є критично важливим для подальшого безпечного розвитку технологій Інтернету Речей.

Метою роботи є розробка моделі гібридної IoT-системи з підвищеним рівнем інформаційної безпеки для захисту даних і надійної взаємодії пристроїв у критично важливих середовищах.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні завдання:

- провести аналіз предметної області, актуальних проблем та викликів у сфері безпеки Інтернету Речей;
- здійснити огляд і критичний аналіз наявних методів, архітектурних рішень та нормативної бази забезпечення безпеки IoT-систем, виявити їх обмеження;
- обґрунтувати концепцію та розробити багаторівневу архітектуру гібридної системи безпеки IoT, що охоплює рівні пристроїв, локальних обчислень/шлюзів, мережевої інфраструктури та хмарних технологій;
- визначити та описати ключові технології та механізми безпеки для кожного рівня запропонованої гібридної системи;
- розглянути підходи до управління ризиками в контексті розробленої гібридної системи;
- провести оцінку ефективності запропонованої системи шляхом порівняння з аналогами, визначення її переваг та недоліків, а також окреслення перспектив подальшого розвитку.

Об’єктом дослідження є Інтернет речей (IoT) як середовище обміну та обробки інформації в умовах сучасних кіберзагроз.

Предметом дослідження є архітектурні рішення, методи шифрування, автентифікації, контролю доступу та захисту даних у гібридних IoT-системах.

Методи дослідження:

- Аналіз наявних IoT-архітектур та загроз інформаційній безпеці;

- Методи криптографічного захисту та безпечної аутентифікації пристроїв;
- Моделювання гібридної IoT-архітектури з розмежуванням рівнів безпеки;
- Порівняння запропонованої архітектури з наявними рішеннями.

Практична цінність полягає в розробленій моделі гібридної IoT-системи, яка забезпечує підвищений рівень захисту даних та безпечну взаємодію пристроїв. Вона дозволяє ефективно протидіяти сучасним кіберзагрозам за рахунок використання багаторівневого захисту, криптографії та безпечної автентифікації, що робить її придатною для впровадження у сферах з підвищеними вимогами до інформаційної безпеки.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПРОБЛЕМАТИКИ IOT

1.1 Актуальність теми, роль IoT у сучасних системах

На тлі Четвертої промислової революції, Інтернет Речей вже сьогодні відіграє значну роль у численних аспектах людської діяльності та функціонуванні сучасних систем. Його вплив відчувається у:

– Промисловості (Industrial IoT - IIoT): автоматизація виробничих процесів, предиктивне обслуговування обладнання, оптимізація ланцюгів постачання, підвищення ефективності та зниження витрат. IIoT є одним із наріжних каменів концепції "розумного виробництва".

– Розумних містах (Smart Cities): інтелектуальні транспортні системи, управління енергоспоживанням та водними ресурсами, моніторинг стану навколишнього середовища, підвищення громадської безпеки та якості життя мешканців.

– Охороні здоров'я (Healthcare IoT): віддалений моніторинг стану пацієнтів, персоналізована медицина, оптимізація роботи медичних закладів, "розумні" медичні пристрої.

– Сільському господарстві (Smart Agriculture): моніторинг стану посівів та худоби, автоматизація процесів поливу та внесення добрив, підвищення врожайності та раціональне використання ресурсів.

– Енергетиці (Smart Grids): інтелектуальні мережі електропостачання, оптимізація розподілу та споживання енергії, інтеграція відновлюваних джерел енергії.

– Побутовій сфері (Smart Homes): автоматизація домашніх приладів, системи безпеки та комфорту, енергозбереження.

Тенденція до все глибшого проникнення IoT у різні сфери життя та економіки продовжується. Розвиток супутніх технологій, таких як штучний

інтелект (AI), машинне навчання (ML) [4], хмарні та туманні/граничні (fog/edge) обчислення [14, 15], ще більше розширює можливості та прискорює впровадження IoT-рішень. Зокрема, спостерігається тренд на перенесення частини обчислювальних потужностей та аналізу даних безпосередньо на "границю" мережі (edge computing), тобто ближче до джерела генерації даних, що дозволяє зменшити затримки та навантаження на централізовані ресурси [16].

Разом з тим, стрімке поширення IoT-технологій супроводжується пропорційним зростанням загроз та вразливостей безпеки. IoT-системи часто характеризуються використанням пристроїв з обмеженими обчислювальними ресурсами, великою різнорідністю апаратного та програмного забезпечення, а також тривалим життєвим циклом, протягом якого підтримка та оновлення безпеки можуть бути ускладнені або взагалі відсутні [2]. Це робить їх привабливими цілями для зловмисників. Типові вразливості зустрічаються на всіх рівнях архітектури IoT – від самих пристроїв, де можуть використовуватися слабкі механізми автентифікації або зберігатися незашифровані дані, до мережевого рівня, де поширені атаки типу "людина посередині" або передача незашифрованого трафіку, та хмарних платформ, вразливих до атак на API чи несанкціонованого доступу [25]. Наслідки успішних кібератак на IoT-системи можуть бути руйнівними, включаючи фінансові збитки, порушення конфіденційності та цілісності даних, відмову в обслуговуванні критично важливих сервісів, а в окремих випадках – навіть загрозу фізичній безпеці та життю людей.

Наявні методи та засоби забезпечення безпеки часто виявляються недостатньо ефективними для протидії сучасним загрозам в IoT-середовищі [3]. Традиційні підходи до інформаційної безпеки погано адаптовані до специфіки IoT, зокрема до обмежених ресурсів пристроїв та величезної масштабованості систем. Централізовані системи безпеки, хоч і пропонують зручне управління, мають суттєві недоліки, такі як вразливість до єдиної точки відмови, можливі затримки в передачі даних та залежність від постійного підключення, що

критично для багатьох IoT-застосунків. Наявні системи безпеки для IoT часто є статичними, нездатними швидко адаптуватися до нових видів атак, та мають обмежені можливості для інтеграції новітніх технологій, таких як штучний інтелект чи блокчейн [4, 13].

Таким чином, актуальність даної роботи зумовлена нагальною потребою у розробці та дослідженні нових, більш гнучких, комплексних та ефективних підходів до забезпечення безпеки IoT-систем. Запропонована гібридна система безпеки, що поєднує сильні сторони різних технологій та архітектурних рішень, спрямована на подолання обмежень наявних підходів та забезпечення надійного захисту на всіх рівнях IoT-інфраструктури. Дослідження та впровадження таких систем є критично важливим для подальшого безпечного розвитку та широкого впровадження технологій Інтернету речей у сучасному суспільстві.

1.2 Визначення, архітектура та класифікація IoT-систем

Інтернет речей (IoT) — це мережа фізичних об'єктів, з вбудованими сенсорами, програмним забезпеченням та технологіями, що дозволяють збирати та обмінюватися даними з іншими пристроями та системами через Інтернет. Ці пристрої можуть варіюватися від звичайних побутових приладів до складного промислового обладнання.

Основні властивості Інтернет речей:

1) Однією з головних властивостей є підключеність (Connectivity) — здатність пристроїв з'єднуватися з мережею та обмінюватися даними. Цей обмін відбувається за допомогою різноманітних технологій зв'язку, зокрема Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT та стільникових мереж [1].

2) Такі пристрої також оснащуються сенсорами та актуаторами (Sensors and Actuators). Сенсори призначені для збору інформації про стан навколишнього середовища, як-от температура, вологість, тиск, рух чи освітленість. Натомість актуатори виконують дії на основі отриманих даних:

вмикають чи вимикають прилади, регулюють їхню роботу або здійснюють переміщення [1].

3) Зібрана інформація обов'язково проходить обробку (Data Processing). Вона може аналізуватися як локально на самому пристрої, що відомо як edge computing, так і передаватися для подальшої, більш глибокої обробки та зберігання на хмарні сервіси чи сервери [14].

4) Для ефективного керування кожен пристрій у мережі потребує унікальної ідентифікації (Identification), що дозволяє його точно адресувати та розрізняти серед інших [1].

5) Нарешті, важливим елементом є взаємодія (Interaction). Пристрої IoT можуть комунікувати як між собою в режимі "машина-до-машини" (M2M), так і з користувачами через різноманітні інтерфейси, наприклад, веб- чи мобільні додатки [1].

Типова IoT-архітектура, має різні варіації залежно від специфіки застосування та масштабу системи, але вона завжди структурується за логічними рівнями. Такий поділ дозволяє розібрати складну систему на більш керовані частини, кожна з яких виконує визначені функції. Крім рівнів, архітектура IoT визначається набором ключових компонентів, що взаємодіють між собою, та різноманітними протоколами зв'язку, які забезпечують передачу даних та команд на кожному з цих рівнів [11].

Одна з базових моделей включає декілька таких рівнів. В її основі лежить рівень пристроїв (Device Layer), який складається з фізичних пристроїв IoT із сенсорами та/або актуаторами, що збирають дані та виконують дії. Ці пристрої можуть бути як простими, з обмеженими ресурсами, так і досить потужними.

Далі йде рівень мережі (Network Layer), що відповідає за передачу даних, які були зібрані пристроями, до наступного етапу. Цей рівень включає різні мережеві технології та протоколи, що забезпечують зв'язок, наприклад Wi-Fi, Bluetooth, Ethernet, стільникові мережі чи LPWAN [1, 11].

Після передачі дані потрапляють на рівень обробки (Processing Layer), де вони фільтруються, агрегуються та аналізуються. Як було зазначено раніше, це

може відбуватися як локально (edge computing), так і централізовано в хмарі або на серверах.

Над ним знаходиться рівень застосунків (Application Layer). Він представляє користувацькі інтерфейси та програми, які використовують оброблені дані для формування зручного звіту для користувача. Зазвичай це веб-панелі, мобільні застосунки, системи візуалізації даних та керування.

Усю цю структуру охоплює рівень управління (Management Layer), який відповідає за моніторинг, налаштування, оновлення та безпеку як окремих IoT-пристроїв, так і всієї системи загалом [1, 28].

Основні компоненти IoT-системи, що забезпечують її функціонування, показані в табл. 1.1.

Таблиця 1.1

Основні компоненти IoT-системи

Назва компонента:	Опис:
IoT-пристрої (IoT Devices)	Фізичні об'єкти з вбудованими сенсорами, актуаторами.
IoT-шлюзи (IoT Gateways)	Пристрої, головна ціль яких це забезпечення зв’язку між IoT-пристроями та хмарними платформами або локальними серверами. Вони можуть виконувати функції агрегації даних, перетворення протоколів, фільтрації та попередньої обробки.
IoT-платформи (IoT Platforms)	Хмарні або локальні платформи, які надають набір інструментів та сервісів для керування пристроями, збору, зберігання, обробки та аналізу даних, а також розробки та розгортання IoT-додатків.
Мережева інфраструктура (Network Infrastructure)	Сукупність мережевих пристроїв та технологій, що забезпечують передачу даних між компонентами IoT-системи.

Протоколи зв'язку, що використовуються на різних рівнях архітектури IoT, будуть узагальнені в табл. 1.2.

Таблиця 1.2

Протоколи зв’язку

Тип протоколів:	Опис:
Протоколи фізичного та канального рівнів	IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee, Thread), LoRaWAN, NB-IoT, LTE-M, Ethernet.
Мережеві протоколи	IP (IPv4, IPv6), CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), HTTP (Hypertext Transfer Protocol), AMQP (Advanced Message Queuing Protocol).
Протоколи управління пристроями	OMA DM (Open Mobile Alliance Device Management), TR-069.

IoT-пристрої класифікуються за різними критеріями, що відображають їхнє різноманіття та сфери застосування.

1) Класифікація за функціональним призначенням.

У цій категорії можна виділити побутові пристрої (Smart Home), такі як розумні лампочки, термостати, замки, камери спостереження та різноманітна побутова техніка, для яких характерні зручність, автоматизація процесів та енергоефективність [1]. Промислові пристрої (Industrial IoT, IIoT) це сенсори для моніторингу стану обладнання, системи керування виробничими процесами та роботизовані системи, де основними особливостями є надійність, точність, оптимізація виробництва та безпека [1]. Медичні пристрої (Healthcare IoT), до яких відносяться фітнес-трекери, системи моніторингу стану здоров'я та засоби дистанційної діагностики, вирізняються високою точністю, вимогою до безпеки даних та персоналізацією [1]. Транспортні засоби та інфраструктура (Connected

Vehicles & Infrastructure) охоплюють автомобілі з підключенням до Інтернету, системи управління дорожнім рухом та розумні паркомісця, орієнтовані на безпеку, ефективність та комфорт, як пішоходів так і водіїв[1]. Сільськогосподарські пристрої (Agriculture IoT), такі як сенсори вологості ґрунту, метеостанції та системи автоматичного поливу, спрямовані на оптимізацію врожайності та економію ресурсів [1]. Останніми в цій категорії є – пристрої для розумних міст (Smart Cities), до них входять системи освітлення, управління відходами, моніторингу якості повітря та громадського транспорту, сприяють сталому розвитку та покращенню якості життя містян [1].

2) Класифікація за обчислювальною потужністю.

Розрізняють обмежені пристрої (Constrained Devices), що мають невелику обчислювальну потужність, обмежений обсяг пам'яті та низьке енергоспоживання, до прикладу це можуть бути прості сенсори відкриття дверей, воріт чи вікон [18]. На противагу їм існують потужні пристрої (Resource-rich Devices), які мають значні обчислювальні ресурси, володіють великим обсягом пам'яті та розширеними можливостями підключення, до прикладу це можуть бути промислові контролери або сучасні розумні камери з датчиками руху, нічним баченням і тд.

3) Тип підключення до мережі.

Пристрої поділяються на ті, що мають пряме підключення, тобто володіють власною IP-адресою та можуть безпосередньо підключатися до Інтернету, та пристрої з непрямим підключенням, які підключаються до мережі через шлюзи або інші проміжні пристрої [1, 11].

1.3 Загрози, вразливості, проблеми безпеки

Загрози безпеки в IoT-системах можуть бути класифіковані за різними критеріями, що допомагає краще розуміти їхню природу та розробляти ефективні методи захисту [2, 3]. Найпростіше розподілення відбувається за об’єктом атаки, за методом її проведення та за наслідками для безпеки.

1) Класифікація за об'єктом атаки.

Один із ключових підходів — це аналіз загроз залежно від того, на яку частину системи вони спрямовані. Загрози на рівні пристроїв стосуються атак, націлених безпосередньо на кінцеві IoT-пристрої. Це можуть бути спроби фізичного втручання, вилучення конфіденційної інформації з пам'яті, а також використання вразливостей програмного чи апаратного забезпечення для отримання контролю над пристроєм.

Існують також загрози на рівні мережі, що спрямовані на інфраструктуру зв'язку між пристроями, шлюзами та платформами. До них належать перехоплення трафіку, підміна пакетів, атаки типу "відмова в обслуговуванні" (DoS/DDoS) та несанкціонований доступ до мережевого обладнання.

Загрози на рівні платформи, чи то хмарної, чи локальної, націлені на сервери, бази даних та програмне забезпечення. Зловмисники можуть намагатися отримати несанкціонований доступ до даних, модифікувати їх, видалити, або атакувати програмні інтерфейси (API) [25].

Окремо виділяють загрози на рівні додатків, які спрямовані на користувацькі програми для взаємодії з IoT-системою [25]. Прикладами можуть бути крадіжка облікових даних, міжсайтовий скриптинг (XSS) або SQL-ін'єкції. І, нарешті, загрози на рівні даних фокусуються на порушенні конфіденційності, цілісності та доступності інформації, яку система збирає, передає та зберігає[3].

2) Класифікація за методом атаки.

Інший спосіб класифікації — за методом, який використовують зловмисники. Пасивні атаки спрямовані на отримання інформації без прямого втручання в роботу системи, наприклад, через перехоплення мережевого трафіку. На противагу їм, активні атаки мають на меті змінити стан системи, порушити її функціональність або отримати несанкціонований доступ, як-от у випадках DoS/DDoS-атак або ін'єкцій шкідливого коду.

Фізичні атаки передбачають безпосереднє втручання в обладнання: його крадіжку, пошкодження (тамперинг) або аналіз побічних каналів

випромінювання [6]. Атаки з використанням програмного забезпечення полягають в експлуатації вразливостей у коді пристроїв, платформ або додатків. Не варто забувати й про соціальну інженерію — маніпулювання користувачами з метою отримання доступу до системи або конфіденційної інформації.

3) Класифікація за наслідками для безпеки.

Нарешті, загрози можна розглядати з погляду їхніх наслідків. Порушення конфіденційності — це несанкціоноване розкриття чутливої інформації, такої як персональні дані, медичні записи або комерційні таємниці.

Порушення цілісності означає несанкціоновану зміну, модифікацію або видалення даних чи програмного коду [3]. Це може призвести до некоректної роботи системи, прийняття хибних рішень і навіть фізичної шкоди, наприклад, через зміну параметрів медичного обладнання.

Порушення доступності, або відмова в обслуговуванні, унеможливлює легітимний доступ до пристроїв, даних чи сервісів, що часто є наслідком DoS/DDoS атак або дій програм-вимагачів [2].

Останнім важливим наслідком є порушення автентичності, що означає неможливість перевірити справжність джерела даних або особи користувача [3]. Це відкриває шлях для атак із підробкою ідентичності (spoofing).

У розділі 1.2 було описано різні рівні типової архітектури IoT, кожен із них має свої особливі характеристики, відповідно й вразливості:

1) Вразливості на рівні пристроїв.

На рівні пристроїв однією з найпоширеніших проблем є слабкі або відсутні механізми автентифікації та авторизації [2, 25]. Це проявляється у використанні стандартних, легко вгадуваних паролів, відсутності багатофакторної автентифікації та загалом ненадійних методах ідентифікації. До цього додається небезпечне зберігання даних, коли конфіденційна інформація, така як ключі шифрування чи облікові дані, зберігається у незашифрованому вигляді або з використанням застарілих алгоритмів.

Також значний ризик становлять вразливості програмного забезпечення — помилки в коді операційної системи, прошивці чи додатках, які зловмисники

можуть використати для виконання довільного коду. Не варто ігнорувати і фізичну незахищеність: легкий доступ до пристрою дозволяє втрутитися в його роботу, вилучити дані або змінити конфігурацію. Нарешті, існують вразливості апаратного забезпечення, тобто недоліки в дизайні чи виробництві мікросхем, які можуть бути використані для атак, наприклад, побічними каналами [7].

Ці фактори демонструють, що IoT-пристрої є первинною і часто найвразливішою ланкою в системі безпеки. Проте, навіть якщо окремий пристрій захищений, дані, які він генерує та передає, можуть стати об'єктом атаки під час їхнього руху мережею. Далі розглянемо типові вразливості, притаманні саме мережевому рівню.

2) Вразливості на рівні мережі.

Забезпечення безпеки мережевої інфраструктури є не менш критичним завданням. Однією з головних вразливостей тут є передача незашифрованого або слабо зашифрованого трафіку. Використання застарілих криптографічних протоколів або їх повна відсутність дозволяє зловмисникам легко перехоплювати та аналізувати інформацію [11]. Це, у свою чергу, створює умови для атак типу "людина посередині" (Man-in-the-Middle, MITM), під час яких зловмисники можуть не лише прослуховувати, а й модифікувати дані, що передаються.

Крім того, мережевий рівень вразливий до атак типу "відмова в обслуговуванні" (DoS/DDoS), коли ресурси перевантажуються величезною кількістю запитів, що паралізує роботу сервісів. Істотний ризик також становить неправильна конфігурація мережевого обладнання: ненадійні налаштування маршрутизаторів чи брандмауерів можуть створити лазівки для зловмисників [2, 25].

Вразливості на цьому рівні можуть призвести до перехоплення, модифікації або блокування важливих даних IoT. Після успішної передачі через мережу, дані зазвичай потрапляють на обробку та зберігання до хмарних платформ, які, в свою чергу, також мають специфічні аспекти безпеки.

3) Вразливості на рівні хмарної платформи.

На рівні хмарної платформи знову постає проблема слабких механізмів автентифікації та авторизації для користувачів та пристроїв. Також поширеним є небезпечне зберігання даних у хмарі, пов'язане з неправильним налаштуванням прав доступу або зберіганням інформації без належного шифрування.

Значний вектор атак пов'язаний із вразливостями API (програмних інтерфейсів), які забезпечують взаємодію між компонентами системи. Через них можуть здійснюватися ін'єкції коду, коли шкідливий код впроваджується в запити до баз даних або інших сервісів платформи.

Серйозною архітектурною проблемою є недостатня сегментація мережі всередині платформи. Відсутність належної ізоляції різних компонентів дозволяє зловмисникам, отримавши доступ до однієї частини системи, легко поширити свою атаку на інші. Зрештою, самі програмні компоненти хмарної платформи можуть містити помилки, які стають точками входу для потенційних атак.

Отже, представлений огляд типових вразливостей на рівнях пристроїв, мережі та хмарної платформи підкреслює багатошаровий характер загроз безпеці в IoT-системах. Кожен рівень архітектури має унікальні слабкі місця, які можуть бути експлуатовані зловмисниками. Це вимагає комплексного підходу до захисту, що охоплює всі компоненти системи та враховує їх взаємозв'язок.

Гучні атаки на IoT-системи продемонстрували руйнівні наслідки їх недостатньої захищеності. Відомим прикладом є ботнет Mirai (2016), створений через вразливості IoT-пристроїв (IP-камер, роутерів). Він використовувався для масштабних DDoS-атак, зокрема на DNS-провайдера Dyn, що спричинило значні фінансові втрати та перебої в роботі веб-сервісів.

У 2018 році атака на казино через розумний термостат в акваріумі дозволила зловмисникам проникнути у внутрішню мережу та викрасти дані клієнтів. Це демонструє, як некритичні IoT-пристрої можуть стати точкою входу для серйозних атак.

Кібератака на Mueller Water Products, яка відбувалася у жовтні 2023, виробника обладнання для водопостачання, зачепила операційні та IT-системи, спричинивши збої в бізнес-операціях та фінансові втрати. Цей інцидент ілюструє ризики для промислових IoT-систем (IIoT) та критичної інфраструктури.

Існують також серйозні побоювання щодо атак на підключені медичні IoT-пристрої (інсулінові помпи, кардіостимулятори), що загрожує здоров'ю та життю пацієнтів, навіть за відсутності поки що масштабних інцидентів такого роду, потенціал для них залишається високим.

1.4 Нормативна база

Нормативно-правова база у сфері безпеки Інтернету речей (IoT) є динамічною та продовжує формуватися у відповідь на швидкий розвиток технологій та зростання кіберзагроз. Незважаючи на відсутність єдиного, всеосяжного міжнародного законодавства, існує низка важливих стандартів, рекомендацій та законодавчих ініціатив на міжнародному, регіональному та національному рівнях, які спрямовані на підвищення рівня безпеки IoT-пристроїв

1) Міжнародні стандарти та рекомендації.

На міжнародному рівні існує низка стандартів та рекомендацій, що формують основу для безпечного проектування та функціонування IoT-систем. Фундаментальним для розуміння та проектування таких систем є нормативний документ ISO/IEC 30141, розроблений Міжнародною організацією зі стандартизації (ISO) [28]. Цей документ встановлює стандарти, характеристики та моделі для чітко визначеної та ефективної архітектури Інтернету Речей, описуючи різні аспекти, включаючи функціональні компоненти, їхні взаємозв'язки та принципи проектування. Такий системний підхід опосередковано сприяє підвищенню безпеки, адже розуміння еталонної

архітектури допомагає ідентифікувати потенційні точки вразливості на різних рівнях системи.

Важливі ресурси, інструменти та рекомендації щодо безпеки надає некомерційна організація OWASP (Open Web Application Security Project). Оскільки багато IoT-пристроїв та платформ використовують веб-технології та API для комунікації та управління, рекомендації OWASP, зокрема такі як OWASP Top Ten, є надзвичайно важливими для забезпечення їхньої безпеки. Ці рекомендації включають захист від поширених веб-атак, наприклад, SQL-ін'єкцій та міжсайтового скриптингу (XSS) [25].

Глобальна асоціація операторів мобільного зв'язку GSMA (Groupe Speciale Mobile Association) розробила комплексні рекомендації щодо безпеки в IoT-системах (IoT Security Guidelines), орієнтовані на весь життєвий цикл IoT-пристроїв та сервісів. Вони охоплюють аспекти проектування безпеки, розгортання, управління пристроями, захист даних та забезпечення конфіденційності. Враховуючи значну роль мобільних мереж у підключенні багатьох IoT-пристроїв, ці рекомендації є цінним ресурсом для операторів та виробників [26].

Національний інститут стандартів та технологій США (NIST) розробив фреймворк кібербезпеки (Cybersecurity Framework), який є гнучким та може бути адаптований для різних галузей та технологій, включно з IoT. Цей фреймворк складається з п'яти основних функцій: ідентифікація, захист, виявлення, реагування та відновлення, надаючи організаціям структурований підхід до управління кіберризиками, у тому числі пов'язаними з IoT-системами [23].

2) Регіональні та національні законодавчі ініціативи.

На рівні регіональних та національних законодавчих ініціатив також формуються важливі вимоги. Так, в Європейському Союзі Загальний регламент про захист даних (GDPR), хоч і є загальним документом, має значний вплив на безпеку IoT-пристроїв та сервісів, що збирають та обробляють персональні дані громадян ЄС. GDPR встановлює суворі правила щодо згоди на обробку даних,

прав суб'єктів даних, безпеки обробки та повідомлень про витоки даних, вимагаючи від компаній, які розробляють та розгортають IoT-рішення в ЄС або для громадян ЄС, враховувати ці норми [24].

У США подібні права споживачам щодо їхніх персональних даних надають Каліфорнійський закон про конфіденційність споживачів (CCPA) та Каліфорнійський закон про права конфіденційності (CPRA). Вони включають право знати, які дані збираються, право вимагати видалення даних та право відмовитися від продажу їхніх даних, що також впливає на безпеку IoT-пристроїв, оскільки компанії повинні вживати розумних заходів для захисту зібраних персональних даних.

Активність у розробці законодавств та регуляторних актів у сфері кібербезпеки загалом та безпеки IoT зокрема спостерігається і в інших країнах. Це може включати закони про кібербезпеку критичної інфраструктури, вимоги до безпеки споживчих IoT-пристроїв, а також ініціативи, спрямовані на підвищення обізнаності та відповідальності виробників та користувачів IoT-технологій. Як приклад, у Сінгапурі було розроблено "Code of Practice for Cybersecurity of IoT Devices".

3) Подальші тенденції та виклики.

З огляду на подальші тенденції та виклики у сфері Інтернету речей, очікується продовження розвитку галузевих стандартів та впровадження програм сертифікації. Передбачається, що ці стандарти ставатимуть дедалі специфічними, з урахуванням особливостей конкретних галузей застосування IoT, таких як промисловість, охорона здоров'я чи автомобільна промисловість.

Необхідність узгодження різноманітних міжнародних стандартів та регуляторних підходів залишається надзвичайно важливим і складним викликом. Вирішення цього питання є ключовим для забезпечення максимальної сумісності та належного рівня безпеки в IoT-системах, що стрімко розвиваються та розширюються.

Нормативно-правова база повинна демонструвати гнучкість та здатність швидко адаптуватися до стрімкого розвитку нових технологій та появи нових

загроз у сфері IoT. Це стосується, зокрема, інтеграції штучного інтелекту в IoT-рішення (AIoT) та все ширшого використання технології блокчейн для забезпечення безпеки та прозорості.

В кінці кінців, під час процесу розробки регуляторних вимог надзвичайно важливо знайти баланс. З одного боку, необхідно постійно підвищувати рівень безпеки IoT-систем та захисту даних, а з іншого – не створювати надмірних перешкод, які б стримували інноваційний розвиток у цій динамічній галузі.

Висновки за розділом 1

Аналіз предметної області підтверджує стрімке зростання Інтернету Речей та його все глибше проникнення у ключові сфери людської діяльності. Така широка інтеграція IoT-пристроїв, які часто мають обмежені ресурси та тривалий життєвий цикл, робить їх привабливими цілями для зловмисників. Наявні вразливості на всіх рівнях архітектури IoT можуть призвести до руйнівних наслідків, включаючи фінансові збитки та загрозу фізичній безпеці. Наявні підходи до захисту часто виявляються недостатньо адаптованими до специфіки IoT, а нормативно-правова база все ще перебуває на етапі активного формування. Таким чином, існує нагальна потреба у розробці комплексних та ефективних рішень для забезпечення безпечного функціонування та подальшого розвитку IoT-екосистем.

РОЗДІЛ 2
ОГЛЯД І КРИТИЧНИЙ АНАЛІЗ НАЯВНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

2.1 Криптографічні методи, доступ, IDS/IPS, автентифікація

1) Криптографічні методи.

В IoT-системах використовуються різні криптографічні схеми. Симетричні алгоритми використовують один і той самий ключ як для шифрування, так і для дешифрування даних, що робить їх швидкими та ефективними для обробки великих обсягів інформації [11]. Асиметричні алгоритми (криптографія з відкритим ключем) використовують пару ключів: відкритий ключ для шифрування та закритий (приватний) ключ для дешифрування. Це дозволяє безпечно обмінюватися ключами та реалізовувати цифрові підписи. Гібридні схеми поєднують переваги обох підходів: асиметрична криптографія використовується для безпечного обміну сеансовим симетричним ключем, а потім цей симетричний ключ застосовується для швидкого шифрування основної маси даних. Такий підхід забезпечує як безпеку, так і ефективність, що особливо важливо для IoT.

Специфіка IoT-пристроїв, зокрема їхні обмежені обчислювальні ресурси, малий обсяг пам'яті та низьке енергоспоживання, ускладнює застосування традиційних, ресурсоємних криптографічних алгоритмів і робить енергоефективність критичним фактором, оскільки інтенсивні обчислення швидко виснажують батареї автономних пристроїв [18]. Для подолання цих обмежень розробляються та впроваджуються полегшені криптографічні алгоритми (LWC), оптимізовані для мінімального споживання ресурсів при збереженні належного рівня безпеки. Серед них виділяють полегшені симетричні шифри та режими автентифікованого шифрування (AEAD), такі як AES в оптимізованих режимах (AES-GCM, AES-CCM), що забезпечують

конфіденційність, цілісність та автентичність, а також спеціалізовані LWC-шифри, наприклад, ASCON (переможець конкурсу NIST LWC) або ChaCha20.

Для перевірки цілісності даних та генерації цифрових підписів використовуються полегшені хеш-функції, такі як алгоритми з сімейства SHA-3 (наприклад, SHAKE) або компактніші варіанти SHA-256. У сфері асиметричної криптографії криптографія на еліптичних кривих (ECC) є ефективною альтернативою традиційним алгоритмам, як-от RSA, оскільки забезпечує еквівалентний рівень безпеки при значно менших розмірах ключів, що робить її придатною для IoT-пристроїв з обмеженими можливостями зберігання та обробки даних [11, 18].

2) Контроль доступу.

Контроль доступу в системах Інтернету Речей (IoT) є фундаментальним механізмом безпеки, що реалізується на основі політик, які чітко визначають права для різноманітних суб'єктів — це можуть бути користувачі, численні IoT-пристрої або сервіси [2]. Враховуючи масштабованість та гетерогенність IoT-середовищ, вибір та правильне впровадження моделі контролю доступу є критично важливим для захисту ресурсів та даних. Існує кілька ключових моделей, кожна з яких має свої особливості.

– Дискреційний контроль доступу (DAC) – дозволяє власнику ресурсу самостійно визначати, які суб'єкти та які операції мають дозвіл[2]. Такий підхід забезпечує гнучкість, але може ускладнити централізоване управління безпекою у великих IoT-системах.

– Мандатний контроль доступу (MAC) – доступ до об'єктів визначається централізовано на основі міток безпеки, присвоєних як суб'єктам, так і об'єктам [2]. MAC забезпечує жорсткий контроль над інформаційними потоками і часто використовується в середовищах з високими вимогами до конфіденційності, однак є менш гнучким в адмініструванні.

– Модель рольового контролю доступу (RBAC) – надає права доступу до ресурсів суб'єктам на основі заздалегідь визначених ролей, що відображають

їхні функції в системі [2]. RBAC популярний завдяки своїй гнучкості, масштабованості та спрощенню адміністрування, що сприяє реалізації принципу найменших привілеїв.

– Контроль доступу на основі атрибутів (ABAC) – є найбільш динамічною моделлю [2]. Тут дозволи надаються на основі поєднання атрибутів суб'єктів, об'єктів та умов оточення. Незалежно від обраної моделі, важливо дотримуватися принципу найменших привілеїв, надаючи суб'єктам лише ті права, які є абсолютно необхідними для виконання їхніх завдань.

3) Системи виявлення та запобігання вторгненням (IDS/IPS).

Системи виявлення та запобігання вторгненням є важливими компонентами для забезпечення безпеки IoT-інфраструктур, допомагаючи ідентифікувати та блокувати зловмисну активність.

Системи виявлення вторгнень (IDS – Intrusion Detection Systems):

Ці системи призначені для моніторингу мережевого трафіку або активності на хостах з метою виявлення підозрілих патернів або відомих сигнатур атак. У випадку виявлення потенційної загрози, IDS генерує сповіщення для адміністраторів безпеки, які потім можуть вжити відповідних заходів. IDS самі по собі не блокують атаки, а лише інформують про них. Існують різні типи IDS-систем:

– Мережеві IDS (NIDS – Network Intrusion Detection Systems) – проводять аналіз трафіку, що проходить через певний сегмент мережі, відстежуючи комунікації між пристроями.

– Хостові IDS (HIDS - Host-based Intrusion Detection Systems) – встановлюються на окремих пристроях (хостах) та аналізують їхню внутрішню активність, таку як системні журнали, зміни у файлах конфігурації, або незвичну поведінку програм.

– Статистичні IDS – визначають базовий рівень "нормальної" активності системи або мережі та виявляють будь-які аномальні відхилення від цього встановленого нормального стану.

Системи запобігання вторгненням (IPS - Intrusion Prevention Systems):

Є еволюційним розвитком IDS. Основна відмінність полягає в тому, що IPS не тільки виявляють загрози, але й автоматично вживають заходів для їхнього блокування або ізоляції в реальному часі. Наприклад, IPS може розірвати шкідливе з'єднання, блокувати IP-адресу джерела атаки або змінити правила міжмережевого екрана. IPS також поділяються на типи:

– Мережеві IPS (NIPS - Network Intrusion Prevention Systems) – розміщуються у стратегічних точках мережі (наприклад, на периметрі або перед важливими сегментами) для моніторингу всього трафіку, що проходить через них, та активного запобігання загрозам шляхом блокування шкідливого трафіку до того, як він досягне цілі.

– Хостові IPS (HIPS - Host-based Intrusion Prevention Systems) – встановлюються безпосередньо на окремих хостах (серверах, робочих станціях) для моніторингу активності на конкретному пристрої. Вони контролюють системні виклики, доступ до файлів, зміни конфігурації та локальний мережевий трафік, блокуючи шкідливі дії безпосередньо на хості.

– Бездротові IPS (WIPS - Wireless Intrusion Prevention Systems) – спеціально розроблені для захисту бездротових мереж. Вони здійснюють моніторинг радіоефіру для виявлення неавторизованих точок доступу, атак на бездротові протоколи (наприклад, спроби деаутентифікації) та інших загроз, характерних для бездротових середовищ, і можуть активно втручатися для їх нейтралізації.

4) Безпечна автентифікація пристроїв.

Автентифікація, як процес перевірки ідентичності пристрою або користувача для доступу до системи, є критично важливою в IoT для запобігання несанкціонованому доступу [2, 3]. Залежно від кількості та типу факторів перевірки, розрізняють декілька типів автентифікації: однофакторна автентифікація використовує один фактор, такий як попередньо встановлений ключ (PSK) або пароль, причому паролі часто є слабким місцем через

використання стандартних чи легко вгадуваних комбінацій [25]; двофакторна або багатофакторна аутентифікація (MFA) вимагає надання двох або більше незалежних факторів (наприклад, комбінація пароля/ключа, апаратного токена/сертифіката або біометричних даних, як-от ключ у поєднанні з тимчасовим токеном) для підтвердження ідентичності; та взаємна аутентифікація, що є двостороннім процесом, під час якого і пристрій, і сервер (або інший пристрій) перевіряють ідентичність один одного, запобігаючи атакам типу "людина посередині" та підміні легітимних компонентів системи.

Є декілька поширених методів автентифікації в IoT:

– Сертифікати X.509. Кожен пристрій та сервер можуть мати унікальні цифрові сертифікати, видані довіреним центром сертифікації (CA). Вони часто використовуються в системах з потужнішими пристроями, здатними обробляти операції з сертифікатами, особливо на основі ECC. Перевірка сертифікатів відбувається під час встановлення захищеного з'єднання (наприклад, TLS/DTLS handshake). Управління життєвим циклом великої кількості сертифікатів може бути складним.

– Попередньо розділені ключі (Pre-Shared Keys - PSK). Спільний секретний ключ встановлюється на пристрої та сервері під час виробництва або безпечної ініціалізації. Цей метод простіший для малопотужних IoT-пристроїв, але вимагає безпечного зберігання та управління ключами. PSK часто використовуються в шифронаборах TLS/DTLS.

– OAuth 2.0 та JSON Web Tokens (JWT). Ці технології часто застосовуються в IoT-платформах для авторизації доступу до API[2, 25]. Пристрої отримують тимчасовий токен доступу (JWT) від сервера автентифікації (наприклад, за протоколом OAuth 2.0) і пред'являють його для доступу до захищених ресурсів.

– Підхід "Нульової довіри" (Zero Trust). Це сучасна парадигма безпеки, яка базується на принципі "ніколи не довіряй, завжди перевіряй". Замість того, щоб довіряти пристроям чи користувачам лише на основі їхнього розташування в мережі (наприклад, у внутрішній мережі), підхід "Нульової довіри" вимагає

суворої перевірки ідентичності та авторизації для кожного запиту на доступ до ресурсів, незалежно від того, звідки він надходить. Це означає постійну автентифікацію, авторизацію та моніторинг активності.

Захист каналів автентифікації є важливим, щоб сам процес обміну автентифікаційними даними був захищеним, і для цього використовуються протоколи шифрування каналів зв'язку. TLS (Transport Layer Security) та DTLS (Datagram Transport Layer Security) забезпечують шифрування, цілісність даних та автентифікацію між двома сторонами; TLS використовується для протоколів на основі TCP, таких як HTTPS та MQTT over TLS, тоді як DTLS адаптований для датаграмних протоколів, як-от UDP, що поширений в CoAP. HTTPS (HTTP Secure), що є HTTP, який працює поверх TLS, забезпечує безпечну передачу даних для веб-інтерфейсів та API. Відповідно, популярні IoT-протоколи, такі як MQTT та CoAP, повинні використовувати TLS або DTLS для захисту своїх комунікацій.

2.2 Приклади рішень, фреймворків, архітектур

Ефективне забезпечення безпеки в Інтернеті Речей вимагає застосування комплексних підходів, що ґрунтуються на фундаментальних методах захисту, розглянутих у попередньому підрозділі, та узгоджуються з нормативними базами і стандартами, окресленими в аналізі предметної області[23, 24, 26, 28]. Нижче наведено приклади конкретних архітектурних рішень та типів систем, що впроваджуються для захисту IoT-інфраструктур, з акцентом на їх практичне застосування, а не повторне визначення вже згаданих фреймворків.

1) Архітектури безпеки з використанням граничних та туманних обчислень.

Перенесення частини обчислень, аналізу даних та прийняття рішень щодо безпеки ближче до IoT-пристроїв (на рівень шлюзів або локальних серверів) є основою безпекових архітектур на базі Edge та Fog Computing[14, 16]. Такі архітектури дозволяють зменшити затримки при виявленні та реагуванні на

локальні загрози, оскільки дані безпеки (наприклад, логи, аномалії трафіку) можуть аналізуватися безпосередньо на периферії. Це також знижує навантаження на хмарні ресурси та канали зв'язку. Наприклад, локальні IDS/IPS можуть швидше блокувати атаки, а механізми автентифікації та контролю доступу можуть частково виконуватися на шлюзах, забезпечуючи функціонування навіть при тимчасовій втраті зв'язку з хмарою [16]. Fog-вузли можуть агрегувати дані безпеки з кількох Edge-пристроїв для більш комплексного аналізу перед відправкою до центральної платформи.

2) Комплексні платформи безпеки IoT.

Це програмні або програмно-апаратні рішення, часто хмарного базування, які пропонують інтегрований набір інструментів для управління безпекою IoT-систем протягом усього їхнього життєвого циклу [5]. Типові функції таких платформ включають: управління ідентифікацією та життєвим циклом пристроїв, безпечне підключення та автентифікацію пристроїв, захищене оновлення програмного забезпечення "по повітрю" (Secure OTA), моніторинг стану безпеки пристроїв та мережі, виявлення загроз та аномалій (часто з використанням алгоритмів машинного навчання), управління вразливостями, а також шифрування даних під час передачі та зберігання [4, 26]. Такі платформи спрямовані на централізацію управління безпекою та спрощення адміністрування великої кількості різнорідних пристроїв.

3) Рішення для безпечного введення в експлуатацію та оновлення пристроїв.

Забезпечення безпеки IoT-пристрою починається з моменту його виробництва та першого підключення до мережі [26]. Рішення цього типу фокусуються на безпечному постачанні унікальних ідентифікаторів та криптографічних ключів в кожен пристрій (наприклад, за допомогою HSM на етапі виробництва) [8]. Процес безпечного підключення (onboarding) включає надійну автентифікацію пристрою перед тим, як йому буде дозволено доступ до мережі та сервісів, а також безпечне налаштування початкових параметрів. Важливою складовою є також механізми безпечного оновлення програмного

забезпечення та прошивок, що використовують цифрові підписи для перевірки автентичності та цілісності оновлень, запобігаючи встановленню шкідливого коду [26].

4) Спеціалізовані системи виявлення та запобігання вторгненням для IoT.

Хоча традиційні IDS/IPS можуть бути адаптовані, специфіка IoT (обмежені ресурси пристроїв, різноманітність протоколів, велика кількість пристроїв) вимагає розробки спеціалізованих рішень [2, 4]. Це можуть бути IDS/IPS агенти, які використовують малу кількість ресурсів, що працюють на самих IoT-пристроях або шлюзах, і які здатні виявляти аномалії в поведінці пристроїв або специфічні атаки на IoT-протоколи. Часто такі системи використовують поведінковий аналіз та методи машинного навчання для виявлення невідомих загроз, оскільки сигнатурний аналіз може бути не завжди ефективним для нових атак в IoT-середовищі. Зібрані дані можуть надсилатися на центральну платформу для кореляції та глибшого аналізу.

Застосування цих архітектур та рішень, разом із принципом "Безпека через проектування" (Security by Design), який передбачає врахування аспектів безпеки на всіх етапах розробки IoT-системи, допомагає створювати більш надійні та захищені IoT-екосистеми [24, 26].

2.3 Проблеми та обмеження наявних підходів

Незважаючи на розвиток методів, фреймворків та архітектурних рішень, забезпечення високого рівня безпеки в IoT-системах залишається складним завданням. Наявні підходи мають низку проблем та обмежень, які ускладнюють їх ефективне застосування.

1) Недоліки традиційних методів захисту для специфічних умов IoT.

Традиційні методи інформаційної безпеки, розроблені для корпоративних мереж та потужних комп'ютерних систем, часто виявляються невідповідними

або недостатньо ефективними для унікального середовища IoT через низку причин.

Обчислювальні ресурси - багато IoT-пристроїв характеризуються суттєво обмеженою обчислювальною потужністю, а також малим обсягом оперативної та постійної пам'яті [2, 18]. Це значно ускладнює або навіть унеможливлює використання на них складних криптографічних алгоритмів, повноцінних операційних систем з розширеними функціями безпеки, а також ресурсоємних програмних рішень, таких як антивірусні програми [18]. Наприклад, реалізація асиметричного шифрування або комплексних протоколів автентифікації на таких пристроях може бути надто повільною для практичного застосування або вимагати більше пам'яті, ніж є в наявності.

Енергоефективність - велика кількість IoT-пристроїв розрахована на тривалу автономну роботу від батарейного живлення. Інтенсивні обчислювальні операції, необхідні для реалізації деяких заходів безпеки, такі як постійне шифрування та дешифрування даних або часті сеанси автентифікації, можуть призводити до швидкого виснаження заряду батареї, що робить їх непрактичними для тривалого використання. Через це виникає постійна необхідність пошуку компромісу між бажаним рівнем безпеки та допустимою тривалістю автономної роботи пристрою [18].

Масштабованість - системи Інтернету Речей можуть складатися з величезної кількості пристроїв, іноді десятків тисяч або навіть мільйонів. Традиційні підходи до управління безпекою, що передбачають ручне налаштування, індивідуальне оновлення програмного забезпечення або моніторинг кожного пристрою окремо, стають абсолютно неможливими в таких масштабах. Виникає гостра потреба в автоматизованих, централізованих або децентралізованих, але узгоджених механізмах для ефективного управління безпекою такої великої кількості пристроїв, включаючи їх ідентифікацію, автентифікацію та оновлення [22, 26].

2) Проблеми централізованих систем безпеки та їх вразливості.

Централізовані системи безпеки, хоча й пропонують певні переваги у спрощенні управління, водночас породжують специфічні проблеми та вразливості, особливо в контексті масштабних та розподілених IoT-систем [16].

Єдина точка відмови (Single Point of Failure) - однією з головних проблем є ризик єдиної точки відмови. Вихід з ладу або успішна атака на центральний сервер чи хмарну платформу, що відповідає за управління безпекою, автентифікацію пристроїв або зберігання критично важливих даних, може призвести до паралізації всієї IoT-системи або її значної частини. Внаслідок цього може бути втрачена доступність до всіх пристроїв, що контролюються цією центральною системою.

Приваблива ціль для атак - централізовані сервери та платформи неминуче перетворюються на особливо привабливу ціль для зловмисників [2]. Це пов'язано з тим, що вони акумулюють великі обсяги даних, які часто мають конфіденційний характер, та контролюють значну кількість підключених пристроїв. Успішна атака на такий центральний вузол може мати катастрофічні наслідки, включаючи масовий витік даних, компрометацію великої кількості IoT-пристроїв або навіть отримання зловмисниками контролю над фізичними процесами, керованими відповідною IoT-системою [6].

Затримка та пропускна здатність - у масштабних IoT-системах, де відбувається постійний обмін даними між пристроями та центральним сервером для виконання операцій автентифікації, авторизації чи перевірки політик безпеки, можуть виникати суттєві затримки, що є неприпустимим для критично важливих додатків, які вимагають реакції в реальному часі.

Залежність від підключення - у випадку втрати IoT-пристроями зв'язку з центральним сервером, вони можуть втратити можливість функціонувати належним чином або приймати рішення щодо безпеки, що є критичним для багатьох застосунків.

3) Складність управління безпекою великої кількості різнорідних пристроїв.

Екосистема IoT характеризується величезним розмаїттям пристроїв від різних виробників, з різними апаратними платформами, операційними системами, протоколами зв'язку та життєвими циклами. Це створює значні труднощі в управлінні їхньою безпекою.

Різнорідність (гетерогенність) - відсутність єдиних стандартів безпеки для всіх типів IoT-пристроїв ускладнює впровадження уніфікованих політик та засобів захисту [5]. Те, що підходить для одного типу пристроїв, може бути абсолютно непридатним для іншого.

Управління життєвим циклом - ефективне управління безпекою вимагає постійного стеження за пристроями протягом усього їхнього життєвого циклу – від початку експлуатації та налаштування до оновлення прошивок та виведення з експлуатації. Це складно реалізувати для великої кількості пристроїв, особливо якщо вони розташовані далеко один від одного та мають тривалий термін служби.

Оновлення програмного забезпечення та прошивок - багато IoT-пристроїв не мають простого та безпечного механізму оновлення. Деякі пристрої взагалі можуть не оновлюватись після випуску, що залишає їх вразливими до відомих загроз протягом тривалого часу. Організація безпечного та надійного процесу оновлення для великої кількості різнорідних пристроїв є значним викликом.

Слабкі стандартні налаштування - багато пристроїв постачаються зі стандартними, легко вгадуваними логінами та паролями, які користувачі часто не змінюють. Це робить їх легкою мішенню для автоматизованих атак.

Інвентаризація та моніторинг - ефективне управління безпекою вимагає точної інвентаризації всіх підключених пристроїв та постійного моніторингу їх стану безпеки. У великих і динамічних IoT-середовищах це може бути складним завданням.

4) Недостатня гнучкість та адаптивність наявних систем безпеки до нових загроз.

Ландшафт кіберзагроз постійно змінюється, з'являються нові типи атак та вектори експлуатації вразливостей, націлені на IoT [2, 6]. Наявні системи безпеки IoT часто не встигають за цими змінами.

Статичність захисту - багато вбудованих систем безпеки розроблені для протидії вже відомим загрозам на момент випуску пристрою та не мають можливості оновлювати свої бази даних сигнатур або поведінкові моделі для виявлення нових атак.

Відсутність проактивного виявлення загроз - традиційні системи часто використовують реактивний підхід, тобто реагують на вже відомі загрози та аномальні активності, замість того, щоб проактивно виявляти аномальну поведінку або потенційні загрози на ранніх стадіях.

Повільний процес оновлення та виправлення вразливостей - навіть якщо вразливість виявлена, процес створення, тестування та розгортання виправлення для великої кількості різнорідних IoT-пристроїв може бути дуже тривалим, залишаючи системи вразливими протягом значного часу.

Складність інтеграції нових технологій безпеки - впровадження новітніх підходів до безпеки, таких як штучний інтелект та машинне навчання для аналізу поведінки та виявлення аномалій, або технологій блокчейн для децентралізованого управління довірою, вимагає значних змін в архітектурі наявних систем та може бути обмежене апаратними можливостями пристроїв в системі [13].

Недостатня обізнаність користувачів та виробників - часто як кінцеві користувачі, так і деякі виробники недостатньо обізнані про ризики безпеки IoT, не приділяють їм належної уваги, або ж взагалі нехтують ними, що призводить до випуску та використання незахищених продуктів та практик [3].

2.4 Мотивація до створення нового підходу

Критичний аналіз наявних методів забезпечення безпеки (розділ 2.1), прикладів рішень та архітектур (розділ 2.2), а також детальний розгляд проблем

та обмежень цих підходів (розділ 2.3) однозначно вказують на наявність суттєвих недоліків у сучасних стратегіях захисту Інтернету Речей. Виявлені проблеми створюють значні ризики та перешкоджають повноцінній та безпечній реалізації потенціалу IoT-технологій, що обґрунтовує нагальну потребу в розробці та впровадженні принципово нового, більш комплексного та адаптивного підходу до безпеки.

Мотивація до створення такого нового підходу випливає безпосередньо з обмежень, властивих наявним рішенням:

1) Необхідність подолання обмежень традиційних методів в умовах IoT.

Як було показано, традиційні методи інформаційної безпеки погано адаптуються до специфіки IoT через жорсткі обмеження в обчислювальних ресурсах багатьох кінцевих пристроїв, їхні вимоги до енергоефективності та величезну масштабованість самих IoT-систем. Це мотивує до пошуку та розробки нових легкоадаптованих алгоритмів безпеки, які були б одночасно ефективними та спроможними функціонувати в умовах обмежених ресурсів, а також архітектур, що забезпечують належну масштабованість управління безпекою без надмірного навантаження на окремі компоненти.

2) Потреба у мінімізації ризиків, пов'язаних із централізованими системами.

Виявлені проблеми централізованих систем безпеки, такі як вразливість до єдиної точки відмови, їхня привабливість як цілі для масштабних атак, потенційні затримки в передачі даних та критична залежність від постійного підключення, стимулюють до розробки архітектур, які можуть запропонувати більшу стійкість та надійність. Це обумовлює необхідність створення рішень, що інтегрують децентралізовані елементи, забезпечують швидке реагування на локальному рівні та знижують залежність від одного центрального вузла.

3) Вирішення проблеми управління безпекою в умовах надзвичайної різнорідності пристроїв.

Складність управління безпекою величезної кількості різнорідних IoT-пристроїв від різних виробників, з різними операційними системами, протоколами та життєвими циклами, включаючи проблеми з оновленням програмного забезпечення та слабкими стандартними налаштуваннями, вимагає створення уніфікованих, але гнучких платформ управління. Такий підхід має забезпечувати надійну ідентифікацію, автентифікацію, моніторинг та своєчасне оновлення всіх елементів системи, незалежно від їхньої природи.

4) Підвищення гнучкості та адаптивності систем безпеки до динамічних загроз.

Статичність багатьох наявних систем захисту, їхня нездатність до проактивного виявлення нових загроз та повільний процес адаптації до змін у ландшафті кіберзагроз є вагомим мотиватором для розробки більш динамічних та інтелектуальних рішень. Необхідні системи, що можуть навчатися, інтегрувати новітні технології, такі як штучний інтелект та машинне навчання для аналізу поведінки та виявлення аномалій, та швидко реагувати на нові вектори атак.

Отже, сукупність вищезазначених проблем та обмежень підкреслює, що ефективне забезпечення безпеки IoT вимагає відходу від ізольованих або надто спрощених рішень на користь комплексного підходу. Такий підхід повинен інтегрувати сильні сторони різних технологій та архітектурних моделей – централізованих, децентралізованих, граничних та хмарних – для створення гнучкої, масштабованої, стійкої та адаптивної системи безпеки. Саме розробка такої гібридної системи, що здатна комплексно адресувати виклики безпеки на всіх рівнях IoT-інфраструктури, є головною метою даної роботи та буде детально розглянута у наступному розділі.

Висновки за розділом 2

Огляд наявних методів забезпечення безпеки продемонстрував наявність широкого арсеналу криптографічних засобів, механізмів контролю доступу,

систем виявлення та запобігання вторгненням, а також різноманітних архітектурних рішень, включаючи граничні обчислення та спеціалізовані платформи безпеки IoT. Проте, критичний аналіз виявив суттєві обмеження цих підходів при застосуванні до специфічних умов Інтернету Речей, зокрема через проблеми з обчислювальними ресурсами пристроїв, енергоефективністю та масштабністю систем. Централізовані системи безпеки, незважаючи на зручність управління, страждають від вразливостей, таких як єдина точка відмови та затримки, тоді як управління великою кількістю різнорідних пристроїв та адаптація до нових динамічних загроз залишаються значними викликами.

РОЗДІЛ 3
РОЗРОБКА ГІБРИДНОЇ СИСТЕМИ БЕЗПЕКИ IOT

3.1 Концепція і обґрунтування

Забезпечення надійного захисту систем Інтернету речей, як було згадано в попередніх розділах, вимагає важких та комплексних рішень. Традиційні, монолітні підходи до безпеки часто виявляються недостатніми через унікальні виклики, пов'язані з IoT, такі як обмежені ресурси пристроїв, величезну кількість та різнорідність кінцевих точок, а також динамічний ландшафт загроз. У цьому контексті гібридний підхід до безпеки пропонує більш гнучке, стійке та ефективне рішення.

Гібридний підхід до безпеки IoT полягає у комбінуванні та інтеграції різноманітних методів, технологій та архітектурних рішень для створення багаторівневої, всеохоплюючої та гнучкої системи захисту. Замість того, щоб покладатися на один універсальний механізм, гібридна модель використовує сильні сторони різних підходів для компенсації їх індивідуальних слабкостей. Сутність гібридного підходу полягає у створенні ешелонованої оборони –

defense in depth, де кожен шар захисту доповнює інші, забезпечуючи більш надійний та стійкий загальний рівень безпеки.

Ключові аспекти гібридного підходу в безпеці IoT включають:

1) Комбінування методів виявлення загроз – поєднання сигнатурних методів з методами аналізу поведінки та виявлення аномалій, для ідентифікації нових, невідомих атак, включаючи атаки нульового дня. Часто це реалізується за допомогою гібридних систем виявлення вторгнень (IDS).

2) Поєднання традиційних та інноваційних технологій – інтеграція перевірених рішень, таких як міжмережеві екрани та списки контролю доступу, з новітніми технологіями, такими як штучний інтелект та машинне навчання для предиктивного аналізу загроз, блокчейн для безпечного зберігання даних та управління ідентифікаціями, а також полегшену криптографію, оптимізовану для пристроїв з обмеженими ресурсами.

3) Інтеграція різних архітектурних рівнів захисту – застосування заходів безпеки на всіх рівнях IoT-архітектури представлено у табл. 3.1.

Таблиця 3.1

Список архітектурних рівнів захисту

Рівень	Опис захисту
Рівень пристроїв	Вбудовані елементи безпеки (Secure Elements, TPMs, TEEs), безпечне завантаження, шифрування даних на пристрої.
Рівень мережі	Сегментація мережі, захищені протоколи зв'язку (TLS/DTLS, VPN), мережеві IDS/IPS.
Рівень шлюзів (Edge/Fog Computing)	Розподілена обробка даних та аналітика безпеки ближче до джерела, що зменшує затримки та навантаження на хмару, а також дозволяє реагувати на локальні загрози.

Рівень хмари	Безпечне зберігання та обробка даних, централізоване управління ідентифікацією та доступом, розширений моніторинг безпеки.

4) Поєднання централізованих та децентралізованих елементів – централізоване управління політиками безпеки та оновленнями може поєднуватися з децентралізованими механізмами автентифікації пристроїв або зберіганням даних за допомогою технології блокчейн.

5) Використання гібридної криптографії – поєднання симетричного та асиметричного шифрування для забезпечення як швидкості, так і безпечного обміну ключами.

Щодо переваг над іншими підходами – гібридний підхід пропонує низку суттєвих переваг над суто централізованими або суто децентралізованими моделями безпеки в IoT.

Він забезпечує підвищену стійкість до відмов. На відміну від централізованих систем, у яких збій центрального вузла може паралізувати всю систему, гібридна архітектура з елементами децентралізації, наприклад, обробка на рівні шлюзів або використання P2P-комунікацій для певних функцій здатна продовжувати функціонувати, хоча б частково, навіть при відмові деяких компонентів. Такий ефект посилюється завдяки розподілу функцій безпеки між різними рівнями та компонентами, що зменшує ризик виникнення єдиної точки відмови.

Гібридний підхід також забезпечує кращу масштабованість систем безпеки для великої кількості IoT-пристроїв. Це можливо завдяки можливості виконання попередньої обробки даних та фільтрації загроз на шлюзах, що зменшує навантаження на центральні хмарні сервери. До того ж, мікросервісна архітектура, яку можна розглядати як частину гібридного підходу, дозволяє незалежно масштабувати окремі компоненти безпеки відповідно до поточних потреб.

Гнучкість є ще однією важливою перевагою, оскільки гібридний підхід дозволяє адаптувати рішення безпеки до специфічних вимог різних IoT-додатків та пристроїв. Реалізується можливість вибирати та комбінувати ті методи й технології, які найкраще підходять для поточного сценарію, враховуючи обмеження пристроїв, типи загроз та вимоги до продуктивності. Це також передбачає здатність інтегрувати рішення від різних постачальників та використовувати як власні, так і загальнодоступні технології.

Висока адаптивність гібридних систем досягається шляхом комбінування різних методів виявлення загроз, таких як сигнатурні, поведінкові та засновані на штучному інтелекті й машинному навчанні. Це робить систему більш пристосованою до нових та невідомих атак, дозволяючи системам "навчатися" та покращувати свої захисні можливості з часом. Також, забезпечується здатність динамічно перерозподіляти ресурси та змінювати конфігурації безпеки у відповідь на зміну ландшафту загроз або операційних умов.

Поєднуючи сильні сторони різних підходів, гібридна модель забезпечує всебічне покриття безпеки, охоплюючи ширший спектр типів вразливостей та векторів атак.

Нарешті, гібридні рішення сприяють оптимізованому використанню ресурсів. Вони можуть бути розроблені таким чином, щоб враховувати обмежені обчислювальні можливості та енергоспоживання IoT-пристроїв, переносячи ресурсоємні завдання на більш потужні вузли, такі як шлюзи або хмарна платформа.

3.2 Архітектура

Запропонована гібридна система безпеки для Інтернету речей базується на багатошаровій архітектурі, яка інтегрує різноманітні механізми захисту на кожному рівні – від кінцевих пристроїв до хмарних сервісів. Такий підхід забезпечує глибоку ешелоновану оборону, defense-in-depth, де кожен компонент

робить свій внесок у загальну стійкість системи. Архітектура поєднує переваги централізованого управління та моніторингу з гнучкістю та швидкістю реагування локальних обчислень, а також надійністю децентралізованих технологій для критичних функцій. Архітектура запропонованої гібридної системи безпеки IoT складається з чотирьох основних логічних рівнів, кожен з яких має специфічні компоненти та функції безпеки:

1) Рівень IoT-пристроїв.

Об'єднує різноманітні IoT-пристрої, такі як сенсори, актуатори та контролери, оснащені мікроконтролерами, модулями зв'язку і, в ідеалі, вбудованими елементами безпеки. Функціональність безпеки тут спрямована на забезпечення захисту безпосередньо на кінцевій точці, враховуючи її обмежені ресурси:

– Апаратна безпека ядра (Hardware Root of Trust). Забезпечення довіри до пристрою на найнижчому рівні реалізується через декілька ключових технологій. Вбудовані елементи безпеки (Secure Elements - SE) є захищеними мікроконтролерами, призначеними для безпечного зберігання криптографічних ключів, сертифікатів та виконання криптографічних операцій ізольовано від основного процесора пристрою. Довірені платформні модулі (Trusted Platform Modules - TPM) є спеціалізованими мікросхемами, що надають захищене сховище для ключів, генерацію випадкових чисел, атестацію пристрою та захищене завантаження. Також використовуються фізично не клоновані функції (Physically Unclonable Functions - PUF), які застосовують унікальні фізичні характеристики мікросхеми для генерації унікальних ідентифікаторів або криптографічних ключів, що значно ускладнює клонування та підробку пристроїв.

– Безпечне завантаження та цілісність програмного забезпечення (Secure Boot and Software Integrity) - Гарантування того, що на пристрої виконується лише автентичне та незмінене програмне забезпечення, досягається шляхом перевірки цифрових підписів. Під час завантаження кожен компонент програмного забезпечення, включаючи завантажувач, ядро ОС та прошивку,

перевіряється на наявність валідного цифрового підпису від довіреного виробника. Важливим елементом також є захист від відкату версій (Anti-rollback), який запобігає завантаженню старіших, потенційно вразливих версій програмного забезпечення.

– Полегшена криптографія та захист даних. Застосування криптографічних алгоритмів, оптимізованих для пристроїв з обмеженими обчислювальними ресурсами та енергоспоживанням, є критично важливим. Шифрування даних на пристрої (Data-at-Rest) забезпечує захист конфіденційної інформації, що зберігається в пам'яті пристрою, з використанням полегшених симетричних алгоритмів, наприклад AES в оптимізованих режимах або спеціалізовані LWC-шифри. Для захисту даних під час передачі (Data-in-Transit) використовуються протоколи на кшталт DTLS, що застосовують полегшену еліптичну криптографію (ECC) або інші LWC-механізми.

– Мінімізація поверхні атаки здійснюється через відключення непотрібних сервісів та портів, залишаючи активними лише ті функції та мережеві інтерфейси, які є абсолютно необхідними для роботи пристрою. Також застосовується використання мінімалістичних операційних систем (ОС) для IoT, таких як FreeRTOS, Zephyr, RIOT OS, з мінімальним набором компонентів, та обмеження або захист фізичних інтерфейсів, наприклад JTAG або UART, які можуть бути використані для несанкціонованого доступу.

– Локальна автентифікація та авторизація. Перевірка ідентичності та прав доступу для локальних взаємодій або перед передачею контролю на вищий рівень включає захист локальних інтерфейсів керування через використання паролів або інших механізмів автентифікації для доступу до локальних налаштувань пристрою. Також реалізується базовий контроль доступу, що обмежує функції, доступні різним користувачам або процесам на самому пристрої.

– Фізичний захист та виявлення втручання забезпечується використанням захищених корпусів, що ускладнюють розкриття пристрою без видимих пошкоджень. Додатково застосовуються датчики втручання (Tamper Sensors) –

механізми, що виявляють спроби фізичного втручання, такі як розкриття корпусу або відключення від живлення, та можуть ініціювати захисні дії, наприклад, стирання ключів. Пристрої цього рівня взаємодіють з наступним рівнем (шлюзами або хмарою) через захищені протоколи зв'язку (наприклад, DTLS, TLS).

Блок-схема рівня IoT-пристроїв наведена на рис. 3.1.

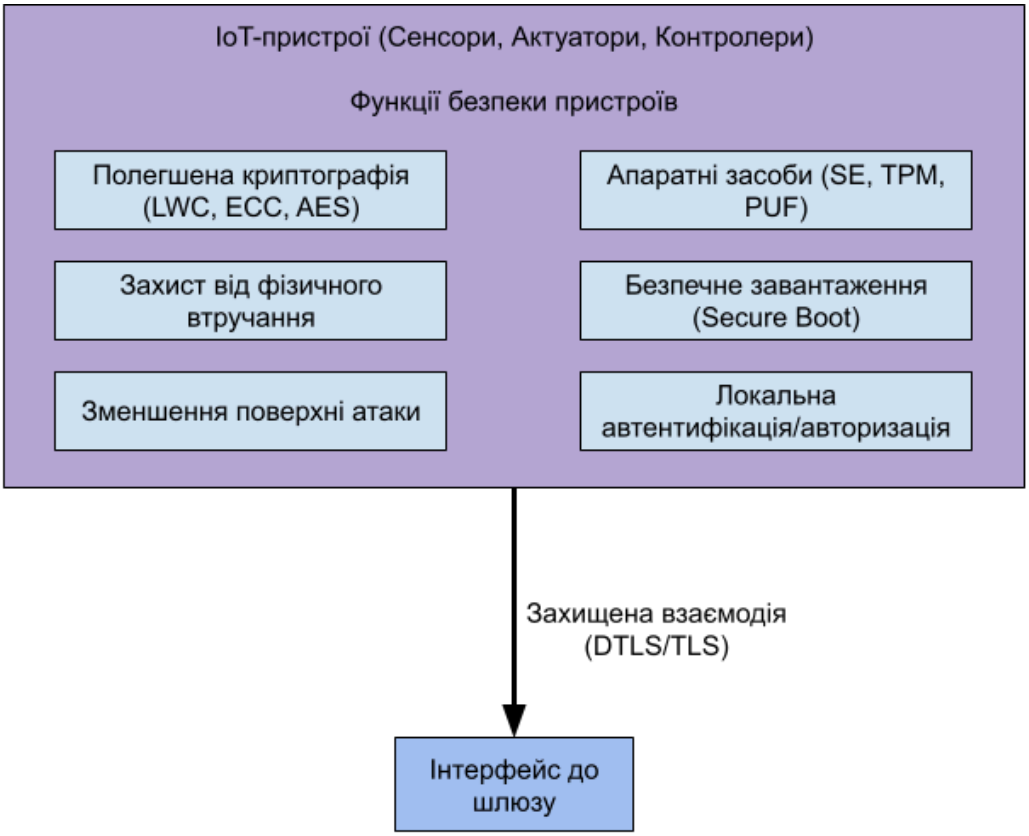


Рисунок 3.1 – Блок-схема першого рівня

2) Рівень локальних обчислень та шлюзів.

Включає IoT-шлюзи, периферійні сервери та прикордонні маршрутизатори з розширеними обчислювальними можливостями. Рівень локальних обчислень відіграє критично важливу, проміжну роль у гібридній архітектурі безпеки IoT, забезпечуючи низку ключових функцій:

– Розподілена аналітика безпеки реалізується через локальні системи виявлення та запобігання вторгненням (IDS/IPS), де шлюзи містять полегшені

версії цих систем, що аналізують трафік від підключених IoT-пристроїв і до них, дозволяючи швидко виявляти та блокувати локальні загрози без очікування реакції з хмари. Також сюди входить виявлення аномалій поведінки пристроїв шляхом моніторингу їхньої нормальної активності (наприклад, обсягу трафіку, типів з'єднань, періодичності передачі даних) та ідентифікації відхилень, що можуть свідчити про компрометацію або несправність. Крім того, здійснюється агрегація та фільтрація логів безпеки: збір та попередня обробка логів з IoT-пристроїв перед їх відправкою до централізованої SIEM-системи в хмарі, що зменшує навантаження на мережу та хмарні ресурси.

– Швидке реагування на інциденти забезпечується можливістю локального стримування загроз, коли у випадку виявлення атаки або компрометації пристрою шлюз автоматично ізолює його від решти мережі або обмежує його функціональність, запобігаючи поширенню загрози в системі. Також досягається зменшення затримки (Latency Reduction), оскільки критично важливі рішення щодо безпеки приймаються локально, без затримки, пов'язаної з передачею даних до хмари та назад.

– Розвантаження IoT-пристроїв, шлюзи можуть брати на себе виконання складних криптографічних операцій від імені ресурсообмежених IoT-пристроїв (проксіювання криптографічних операцій), а також здійснювати локальне управління сеансовими ключами для підключених пристроїв.

– Забезпечення приватності даних досягається шляхом анонімізації та псевдонімізації даних – обробки даних на шлюзі для видалення або маскування ідентифікаційної інформації перед передачею до хмари. Також застосовується федеративне навчання (Federated Learning), де моделі машинного навчання для безпеки можуть тренуватися локально на даних зі шлюзів, а в хмару передаються лише узагальнені оновлення моделі, зберігаючи сирі дані локально.

Окрім цих основних блоків функцій, шлюзи також відповідають за кешування та розподіл політик безпеки, отриманих з хмари, та їх застосування до локальних пристроїв, забезпечуючи дотримання правил навіть за тимчасової

відсутності зв'язку з хмарою. Також вони можуть брати участь у процесі безпечного підключення (Secure Onboarding) пристроїв, забезпечуючи безпечну реєстрацію та автентифікацію нових IoT-пристроїв у мережі.

Блок-схема рівня локальних обчислень та шлюзів наведена на рис. 3.2.

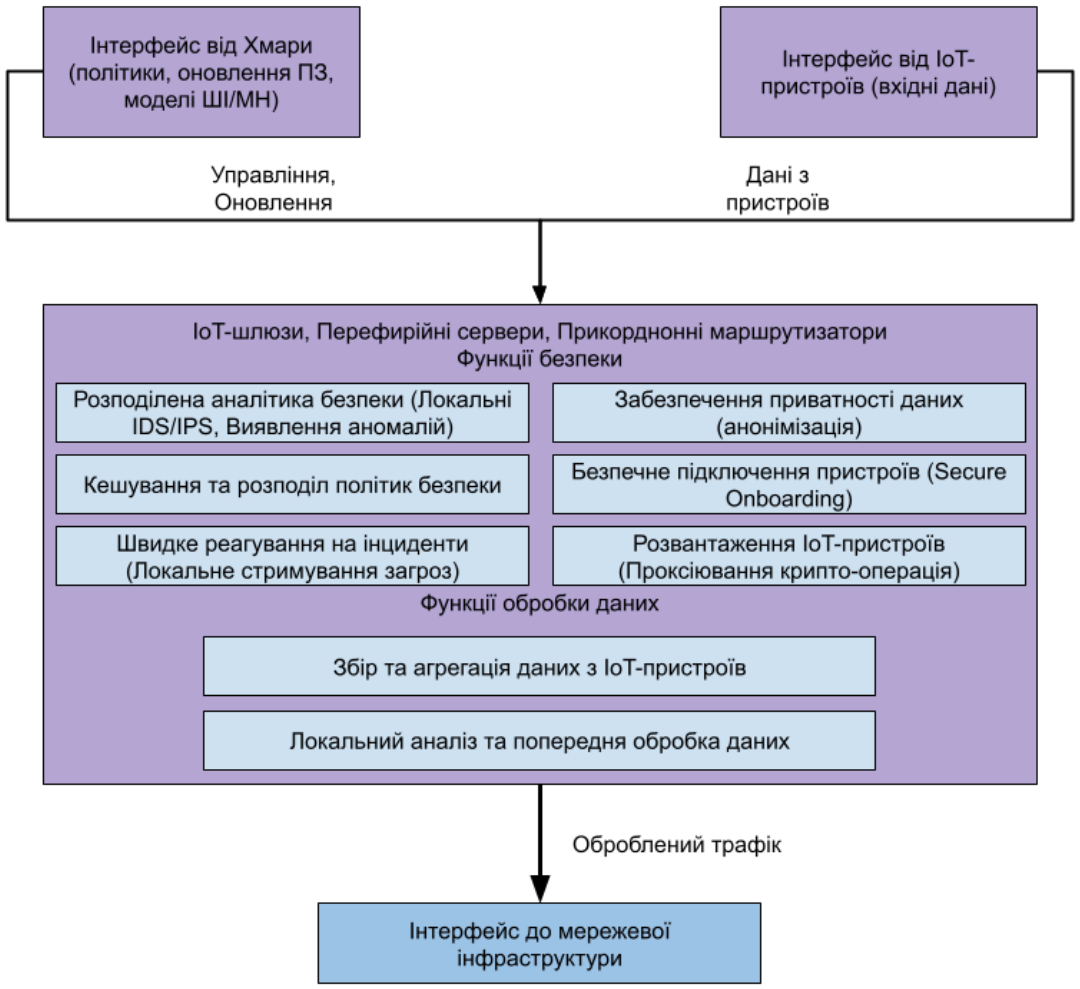


Рисунок 3.2 – Блок-схема другого рівня

3) Рівень мережевої інфраструктури.

Складається з маршрутизаторів, комутаторів, міжмережевих екранів, систем VPN та програмно-визначуваних мереж (SDN). Функціональність безпеки цього рівня зосереджена на захисті даних під час їх передачі між різними сегментами IoT-системи та контролі мережевого доступу:

– Сегментація та ізоляція мережі досягається через використання віртуальних локальних мереж (VLAN), які створюють логічно ізольовані

мережеві сегменти на базі наявної фізичної інфраструктури. Застосовується також мікросегментація, що є більш гранулярним підходом до ізоляції, дозволяючи створювати політики безпеки для окремих пристроїв або невеликих груп пристроїв, обмежуючи їх взаємодію лише необхідними комунікаціями. Для розміщення сервісів, що потребують доступу ззовні, таких як шлюзи, створюються делімітаризовані зони (DMZ), ізолюючи їх від внутрішньої критичної інфраструктури.

– Захист каналів передачі даних здійснюється через протоколи TLS/DTLS, які використовуються для шифрування трафіку між IoT-пристроями та шлюзами, а також між шлюзами та хмарними платформами. Для передачі даних між географічно розподіленими компонентами системи, такими як віддалені шлюзи та центральна хмарна інфраструктура, використовуються віртуальні приватні мережі (VPN), що створюють захищені тунелі, наприклад, з використанням IPsec або WireGuard.

– Мережеві системи виявлення та запобігання вторгненням займаються моніторинг мережевого трафіку на предмет шкідливої активності, відомих атак та аномалій включає аналіз трафіку в реальному часі, де перевіряються пакети даних, що проходять через ключові точки мережі, наприклад, на межі сегментів або перед доступом до хмари. Використовується сигнатурний та поведінковий аналіз для виявлення відомих загроз за сигнатурами та аномалій у мережевій поведінці, що можуть свідчити про нові атаки. У випадку NIPS реалізується автоматичне блокування загроз шляхом активного запобігання атакам через блокування шкідливого трафіку або ізоляцію джерел атаки.

– Перевірка відповідності пристроїв встановленим політикам безпеки перед наданням їм доступу до мережевих ресурсів є важливою функцією. Вона охоплює автентифікацію пристроїв, тобто перевірку ідентичності пристроїв, що намагаються підключитися до мережі, наприклад, за допомогою сертифікатів 802.1X. Також проводиться оцінка стану безпеки (Posture Assessment), що включає перевірку конфігурації пристрою, наявності оновлень безпеки, антивірусного ПЗ тощо. За результатами перевірки відбувається примусове

застосування політик, що може означати надання обмеженого доступу або повну ізоляцію пристроїв, які не відповідають політикам безпеки.

– Впровадження рішень для виявлення, фільтрації та пом'якшення DDoS-атак, спрямованих на перевантаження мережевих каналів або сервісів, є необхідним. Це досягається через системи аналізу трафіку, які виявляють аномальні сплески трафіку, характерні для DDoS-атак, та механізми фільтрації й очищення трафіку, що відділяють легітимний трафік від шкідливого.

– Використання можливостей SDN сприяє динамічному управлінню політиками безпеки, автоматизації реагування на інциденти та покращенню видимості мережевого трафіку, що підвищує загальний рівень захищеності мережевої інфраструктури. Цей рівень забезпечує захищене з'єднання між рівнем локальних обчислень/шлюзів та хмарним рівнем, а також між різними компонентами самої мережі.

Блок-схема рівня мережевої інфраструктури наведена на рис. 3.3.

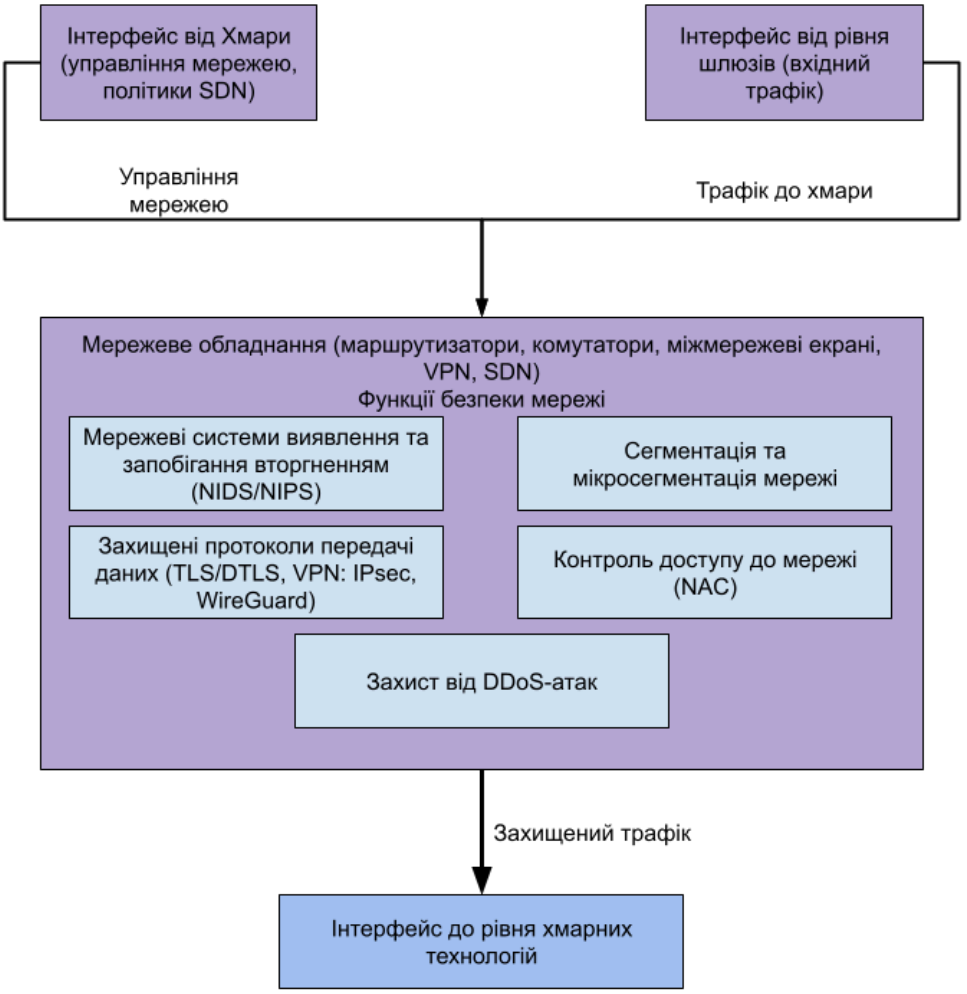


Рисунок 3.3 – Блок-схема третього рівня

4) Рівень хмарних технологій та додатків.

Представлений хмарними платформами (IaaS, PaaS, SaaS), серверами баз даних, аналітичними платформами, системами управління IoT-пристроями та додатками для користувачів.

– Здійснюється управління життєвим циклом ідентичностей IoT-пристроїв, користувачів та сервісів. Також відбувається визначення та застосування гранулярних політик доступу, таких як RBAC (рольова модель) та ABAC (модель на основі атрибутів), до ресурсів та даних IoT. Крім того, забезпечується багатофакторна автентифікація (MFA) для адміністраторів та користувачів.

– Розширена аналітика загроз та моніторинг

Використовуються системи управління інформаційною безпекою та подіями (SIEM), які забезпечують агрегацію, кореляцію та аналіз логів безпеки з усіх рівнів архітектури, включаючи пристрої, шлюзи, мережу та хмарні сервіси, з метою виявлення складних атак та інцидентів. Додатково застосовуються платформи оркестрації, автоматизації безпеки та реагування (SOAR), що дозволяють автоматизувати стандартні процедури реагування на інциденти, тим самим підвищуючи швидкість та ефективність відповіді. Важливу роль відіграє аналітика поведінки користувачів та сутностей (UEBA), яка використовує технології штучного інтелекту та машинного навчання для виявлення аномальної поведінки, що може свідчити про інсайдерські загрози або скомпрометовані облікові записи. Також для забезпечення системи актуальними даними про загрози здійснюється інтеграція з платформами аналізу загроз (Threat Intelligence Platforms), які надають інформацію про

актуальні загрози, вразливості та індикатори компрометації (IoC) із зовнішніх джерел.

– Здійснюється централізоване сканування на вразливості IoT-пристроїв, шлюзів та хмарних компонентів. Також реалізується управління життєвим циклом оновлень прошивок та програмного забезпечення (FOTA/SOTA), що включає процеси тестування, планування та безпечного розгортання оновлень.

– Забезпечується шифрування даних як під час їх зберігання, data-at-rest, так і під час передачі, data-in-transit, для чого використовуються надійні криптографічні алгоритми та системи управління ключами, KMS. Крім того, впроваджуються механізми резервного копіювання та відновлення даних.

– Централізоване визначення, розповсюдження та моніторинг дотримання політик безпеки на всіх рівнях системи.

Блок-схема рівня хмарних технологій та додатків наведена на рис. 3.4.

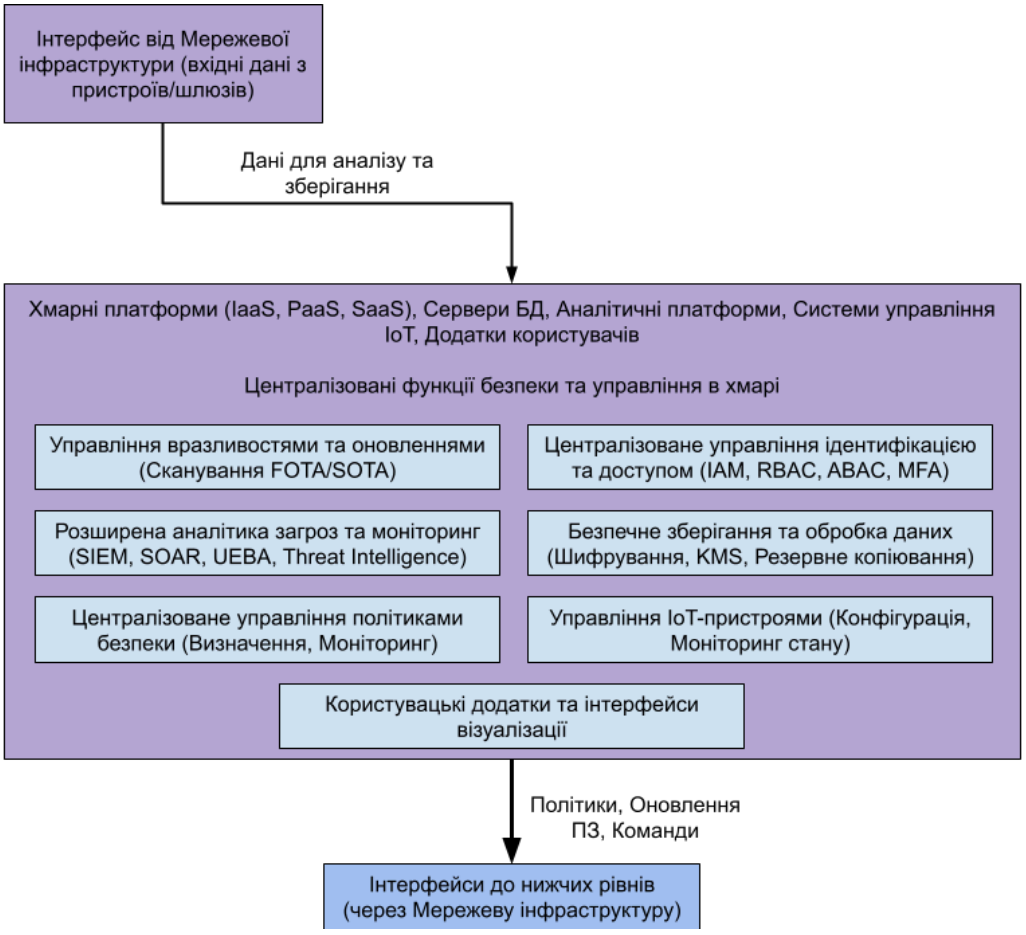


Рисунок 3.4 – Блок-схема четвертого рівня

3.3 Технології та механізми безпеки

Для забезпечення надійного захисту в запропонованій гібридній IoT-системі, з урахуванням обмежених ресурсів кінцевих пристроїв, будуть застосовані наступні ключові технології та механізми:

1) Криптографічний захист.

Для криптографічного захисту даних у запропонованій гібридній IoT-системі ключову роль відіграє полегшена криптографія (LWC), що є критично важливим з огляду на обмежені обчислювальні ресурси та енергоспоживання кінцевих IoT-пристроїв. Для ефективного шифрування та автентифікації даних безпосередньо на пристроях та в каналах зв'язку система використовуватиме перевірені симетричні шифри, такі як AES в оптимізованих режимах (зокрема, AES-GCM), а також спеціалізований LWC-алгоритм ASCON, який став переможцем конкурсу NIST LWC. Такий підхід забезпечить необхідний рівень конфіденційності, цілісності та автентичності даних при збереженні швидкодії та енергоефективності.

Для задач, що вимагають перевірки цілісності даних, генерації компактних цифрових підписів та автентифікації, особливо на пристроях з обмеженими можливостями, система покладатиметься на полегшені хеш-функції. Передбачається застосування алгоритмів з сучасного підсімейства SHA-3, зокрема універсальної функції SHAKE, яка дозволяє генерувати хеші різної довжини. Альтернативно, залежно від конкретних вимог до продуктивності та рівня безпеки окремих компонентів системи, можуть бути використані спеціалізовані полегшені хеш-функції, такі як PHOTON або SPONGENT.

2) Взаємна автентифікація компонентів.

У запропонованій гібридній системі безпеки, для гарантії легітимності кожного учасника взаємодії впроваджується багаторівнева взаємна

автентифікація. Це досягається шляхом комбінування різних методів, адаптованих до специфіки та можливостей кожного компонента системи.

Для надійної автентифікації між більш потужними елементами, такими як шлюзи та хмарна платформа, а також для захисту API, система покладається на сертифікати X.509, що базуються на еліптичній криптографії (ECC). Їхня автентичність та валідність перевіряються під час встановлення захищеного з'єднання (TLS/DTLS "рукостискання") за допомогою протоколів CRL або OCSP. Для IoT-пристроїв з обмеженими ресурсами, особливо у їх взаємодії зі шлюзами, перевага надається простішим, але ефективним попередньо розділеним ключам (PSK). Доступ до API хмарних сервісів авторизується за допомогою токенів доступу (наприклад, JWT через OAuth 2.0). Крім того, для доведення автентичності самих IoT-пристроїв та безпечного зберігання їхніх криптографічних ключів активно використовуються апаратні модулі безпеки, такі як Secure Elements (SE), Trusted Platform Modules (TPM) або Physically Unclonable Functions (PUF). Для прямої ж взаємодії між пристроями (D2D) передбачено використання спеціалізованих протоколів, що забезпечують взаємну автентифікацію без участі центрального сервера, наприклад, на основі групових ключів або децентралізованих механізмів довіри.

3) Технологія блокчейн.

У запропонованій гібридній IoT-системі технологія блокчейн інтегрується для вирішення ключових завдань безпеки та підвищення рівня довіри. Її застосування забезпечує незмінну цілісність критично важливих даних, таких як вимірювання з IoT-пристроїв та події безпеки, шляхом їх хешування та запису в розподілений реєстр. Це гарантує, що будь-які спроби несанкціонованої модифікації інформації будуть легко виявлені. Крім того, блокчейн створює надійний та прозорий аудиторський слід для всіх транзакцій та команд, забезпечуючи невідмовність та простежуваність дій у системі.

Технологія також сприяє децентралізованому управлінню ідентифікацією (DID) IoT-пристроїв, дозволяючи їм самостійно контролювати свої ідентифікаційні дані, та автоматизації політик контролю доступу через

смарт-контракти. Важливим аспектом є використання блокчейну для безпечного оновлення прошивок, де зберігання хешів прошивок та записів про оновлення забезпечує прозорість процесу та можливість перевірки автентичності джерела. З огляду на специфіку IoT, система передбачає використання полегшених, приватних або консорціумних блокчейнів, а також альтернативних технологій розподіленого реєстру (DLT) як-от IOTA чи Hashgraph, з інтеграцією вузлів на хмарній платформі та шлюзах для ефективної агрегації даних

4) Багаторівневе виявлення та запобігання загрозам.

Для забезпечення комплексного захисту від широкого спектра загроз, запропонована гібридна IoT-система впроваджує багаторівневу систему виявлення та запобігання вторгненням (IDS/IPS). На рівні самих IoT-пристроїв, де це дозволяють ресурси, полегшені HIDS/HIPS здійснюють моніторинг локальної активності, цілісності критичних файлів та аналізують системні виклики. Це дозволяє виявляти ознаки компрометації безпосередньо на кінцевій точці.

На рівні шлюзів та мережевої інфраструктури розгортаються системи NIDS/NIPS, які аналізують мережевий трафік між компонентами системи та її сегментами. Їхнє завдання – виявляти спроби сканування, використання відомих вразливостей, аномальний трафік (наприклад, DDoS-атаки, що походять з IoT-пристроїв), а також специфічні атаки, спрямовані на протоколи, що використовуються в IoT (MQTT, CoAP). Для цього поєднуються сигнатурний аналіз, глибокий аналіз протоколів та методи виявлення аномалій, часто із залученням технологій штучного інтелекту та машинного навчання. На хмарному рівні відбувається аналіз агрегованого трафіку, метаданих та журналів подій за допомогою SIEM/SOAR та більш складних аналітичних інструментів на основі ШІ/МН, що дозволяє ідентифікувати приховані та розподілені атаки. Ключовим елементом є кореляція подій: дані з IDS/IPS різних рівнів передаються до центральної SIEM/SOAR системи для отримання цілісної картини стану безпеки, зменшення кількості хибних спрацювань та

підвищення точності виявлення, а також для адаптації сигнатур та моделей поведінки до специфіки IoT.

5) Забезпечення приватності даних.

Для захисту великих обсягів конфіденційних та персональних даних, що генеруються IoT-системами, у запропонованій гібридній архітектурі застосовується комплексний підхід, що поєднує декілька передових методів збереження приватності. Насамперед, для ускладнення або унеможливлення ідентифікації конкретної особи чи пристрою, дані піддаються анонімізації та псевдонімізації. Ця обробка відбувається на рівні шлюзів або в хмарному середовищі перед тим, як дані будуть використані для аналізу або передані третім сторонам.

Для забезпечення можливості агрегованого аналізу даних без розкриття приватності окремих записів, система використовує диференційну приватність, додаючи контрольований "шум" до даних або результатів запитів. У випадках, коли для безпекових функцій (наприклад, виявлення аномалій) необхідне машинне навчання на чутливих даних, застосовується федеративне навчання: моделі тренуються локально на IoT-пристроях або шлюзах, а на центральний сервер передаються лише узагальнені оновлення моделі, а не сирі дані. Додатково, агрегація даних на рівні шлюзів не тільки зменшує обсяг інформації, що передається до хмари, але й сприяє збереженню локальної приватності. Для обробки особливо чутливої інформації в ізольованому та захищеному середовищі, навіть від адміністраторів системи, на серверах або потужних шлюзах використовуються апаратні захищені анклави (TEE), такі як Intel SGX або ARM TrustZone. Комбінація цих технік створює глибоко ешелонований захист даних та приватності в усій гібридній системі.

6) Безпечне оновлення прошивок та ПЗ.

Своєчасне та безпечне оновлення прошивок (Firmware-Over-The-Air – FOTA) та програмного забезпечення (Software-Over-The-Air – SOTA) є критично важливим процесом для виправлення вразливостей та додавання нових функцій безпеки в запропонованій гібридній IoT-системі. Для

забезпечення надійності цього процесу система дотримується ключових вимог: гарантується автентичність джерела оновлення через перевірку цифрових підписів, цілісність пакету оновлення за допомогою хеш-сум та цифрових підписів, а також, за потреби, конфіденційність оновлення шляхом шифрування пакету. На самих пристроях механізм безпечного завантаження (Secure Boot) гарантує запуск тільки автентичної та цілісної прошивки, а захист від відкату (Anti-rollback Protection) запобігає встановленню старіших, потенційно вразливих версій. На випадок невдалого оновлення передбачені механізми відновлення, наприклад, через використання подвійних банків пам'яті.

Роль компонентів гібридної системи в цьому процесі чітко розподілена. Хмарна платформа виступає як центральний вузол, що відповідає за безпечне зберігання пакетів оновлень, управління розкладом та процесом їх розгортання, а також за відстеження статусу оновлення підключених пристроїв. Шлюзи, що функціонують на рівні Edge, виконують роль проміжних ланок: вони можуть кешувати пакети оновлень для локальних пристроїв, що суттєво зменшує навантаження на зовнішні канали зв'язку та прискорює процес. Шлюзи також координують процес оновлення в локальному сегменті мережі та забезпечують додатковий рівень контролю. Нарешті, самі IoT-пристрої оснащені вбудованими механізмами для безпечного завантаження, ретельної перевірки автентичності та цілісності отриманих пакетів оновлень, а також для їх коректного встановлення.

3.4 Управління ризиками

Управління ризиками в контексті запропонованої гібридної IoT-системи – це фундаментальний, безперервний та ітеративний процес, спрямований на систематичну ідентифікацію, глибокий аналіз, всебічну оцінку та адекватну обробку ризиків безпеки з кінцевою метою їх зниження до заздалегідь визначеного прийнятного рівня для організації. Цей процес є невід'ємною

частиною життєвого циклу будь-якої IoT-системи, особливо такої комплексної, як запропонована гібридна архітектура.

1) Ідентифікація ризиків.

Цей початковий етап є основоположним і включає ретельне визначення всіх цінних активів в IoT-системі, таких як кінцеві IoT-пристрої (сенсори, актуатори), IoT-шлюзи, дані, що ними генеруються та обробляються (включаючи персональні дані, телеметрію, конфігураційні параметри), програмне забезпечення (прошивки, мобільні та веб-додатки), мережева та хмарна інфраструктура, а також нематеріальні активи, як-от репутація компанії. Далі відбувається детальне визначення потенційних загроз, які можуть вплинути на ці активи; це можуть бути технічні загрози (шкідливе ПЗ, DDoS-атаки, атаки на протоколи IoT), фізичні загрози (крадіжка пристроїв, тампериг), людський фактор (помилки користувачів, інсайдерські загрози) та відмови обладнання. Останнім кроком на цьому етапі є виявлення слабких місць, або вразливостей, в архітектурі системи, її конфігураціях, програмному та апаратному забезпеченні, а також у процесах управління та експлуатації, які можуть бути використані ідентифікованими загрозами для реалізації атаки. Цей процес включає регулярне автоматизоване сканування на наявність відомих вразливостей у програмному забезпеченні, проведення тестів на проникнення для імітації реальних атак, аналіз вихідного коду та аудит конфігурацій компонентів на всіх рівнях гібридної системи.

2) Оцінка ризиків.

Після ідентифікації ризиків проводиться їх оцінка, яка визначає рівень кожного з них шляхом комбінування ймовірності його реалізації та величини потенційних збитків (впливу) для активів. Аналізується, наскільки вірогідною є реалізація конкретної загрози через певну вразливість, враховуючи такі фактори, як привабливість активу для зловмисників, рівень наявних заходів захисту, складність експлуатації вразливості та історичні дані про інциденти. Одночасно оцінюється потенційний негативний вплив на організацію в разі реалізації ризику, що може включати прямі фінансові втрати, операційні збої,

репутаційні збитки, порушення нормативних вимог або навіть шкоду здоров'ю та безпеці людей, особливо у випадку критичних IoT-систем. Такий комплексний підхід дозволяє класифікувати ризики, наприклад, за допомогою матриці ризиків як низькі, середні або високі, для їх подальшої пріоритезації та визначення послідовності їх ефективної обробки, зосереджуючи ресурси на найбільш критичних напрямках. Можуть застосовуватись як якісні, так і кількісні методи оцінки, залежно від наявних даних та потреб організації.

3) Обробка ризиків.

Після всебічної оцінки ризиків настає етап їх обробки, що передбачає вибір та реалізацію одного або декількох підходів для кожного ідентифікованого ризику з метою досягнення прийнятного рівня залишкового ризику. Одним із основних підходів є зменшення ризику, яке полягає у впровадженні конкретних заходів безпеки, спрямованих на зниження ймовірності виникнення ризику або мінімізацію його потенційного впливу. Прикладами таких заходів в IoT-системі можуть бути встановлення надійних механізмів автентифікації на пристроях, шифрування каналів зв'язку між шлюзами та хмарою, або впровадження систем виявлення вторгнень на мережевому рівні. Іншим підходом є уникнення ризику, що означає свідому відмову від певних видів діяльності, використання специфічних технологій або продуктів, які генерують неприйнятно високий рівень ризику, що не може бути адекватно знижений (наприклад, відмова від використання IoT-пристроїв без підтримки оновлень безпеки). Також можлива передача ризику, коли частина фінансових наслідків від реалізації ризику перекладається на третю сторону, наприклад, через укладання договорів страхування від кіберризиків або аутсорсинг певних функцій безпеки спеціалізованим провайдерам з чіткими угодами про рівень обслуговування (SLA). Нарешті, існує стратегія прийняття ризику, яка передбачає свідоме та задокументоване рішення не вживати активних заходів щодо конкретного ризику, якщо його рівень оцінюється як низький, або якщо вартість впровадження контрзаходів значно перевищує потенційні збитки від його реалізації; таке рішення має бути обґрунтованим та схваленим керівництвом.

4) Моніторинг та перегляд ризиків.

Важливо усвідомлювати, що ризики безпеки не є статичними; вони постійно змінюються під впливом нових загроз, виявлених вразливостей, змін у бізнес-середовищі або в самій IoT-системі. Тому необхідно регулярно, а також у відповідь на значущі події, переглядати та оновлювати оцінку ризиків, ефективність впроваджених заходів їх обробки та загальну стратегію управління ризиками. Цей безперервний моніторинг може включати аналіз звітів про нові загрози (threat intelligence), результати тестів на проникнення, аудиторські висновки та зворотний зв'язок від системи моніторингу подій безпеки.

5) Управління ризиками в гібридній системі.

Запропонована гібридна архітектура має свою специфіку, яку необхідно враховувати при управлінні ризиками. Оцінка ризиків повинна враховувати складні взаємозв'язки та потенційні каскадні ефекти між різними рівнями системи – IoT-пристроями, локальними обчислювальними вузлами (шлюзами) та хмарною платформою. Специфічні ризики, пов'язані з обмеженістю ресурсів кінцевих пристроїв (що ускладнює впровадження надійних механізмів захисту), безпекою бездротових комунікаційних каналів (які можуть бути перехоплені), залежністю від сторонніх хмарних провайдерів (та пов'язаними з цим ризиками щодо доступності та конфіденційності даних), а також ризики, пов'язані з фізичною безпекою розподілених шлюзів, повинні бути ретельно проаналізовані та адресовані. Гібридна архітектура сама по собі може сприяти управлінню ризиками, наприклад, шляхом розподілу функцій безпеки та можливості локального реагування на інциденти на рівні шлюзу, що зменшує залежність від централізованих ресурсів. Використання визнаних міжнародних стандартів та фреймворків управління ризиками, таких як ISO/IEC 27005 або NIST Cybersecurity Framework, є доцільним для забезпечення структурованого, комплексного та послідовного підходу до управління ризиками в усій гібридній

IoT-системі, адаптуючи їхні рекомендації до специфіки кожного рівня та компонента.

Висновки за розділом 3

У відповідь на виявлені обмеження наявних підходів, було розроблено концепцію та детальну архітектуру гібридної системи безпеки для Інтернету Речей, яка базується на принципі ешелонованої оборони. Запропонована система інтегрує різноманітні технології та механізми захисту на чотирьох ключових рівнях: IoT-пристроїв, локальних обчислень та шлюзів, мережевої інфраструктури, а також хмарних технологій та додатків. На кожному рівні застосовуються специфічні засоби безпеки, починаючи від апаратної безпеки ядра та полегшеної криптографії на пристроях, через розподілену аналітику та швидке реагування на шлюзах, до розширеного моніторингу та централізованого управління в хмарі. Важливими компонентами системи є використання технології блокчейн для забезпечення цілісності даних та управління ідентифікацією, багаторівневі системи IDS/IPS, механізми безпечного оновлення ПЗ та технології збереження приватності, а також неперервний процес управління ризиками. Такий комплексний гібридний підхід дозволяє створити більш гнучку, стійку, масштабовану та адаптивну систему захисту, здатну ефективно протистояти сучасним та майбутнім загрозам в IoT.

РОЗДІЛ 4
ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОЇ СИСТЕМИ

4.1 Порівняння з аналогами

Забезпечення безпеки в Інтернеті Речей (IoT) є складним завданням, що вимагає інноваційних підходів, здатних адаптуватися до унікальних характеристик цього середовища, таких як обмежені ресурси пристроїв, величезна масштабованість та динамічний ландшафт загроз. Запропонована в даній роботі гібридна система безпеки IoT (детально описана в Розділі 3) позиціонується як більш комплексне та ефективне рішення порівняно з наявними аналогами, які часто страждають від низки обмежень, висвітлених у Розділі 2. Даний підрозділ проводить порівняльний аналіз запропонованої системи з цими аналогами, демонструючи її переваги.

Наявні підходи до безпеки IoT можна умовно розділити на кілька категорій, кожна з яких має свої недоліки, що їх намагається вирішити запропонована гібридна система:

1) Традиційні методи інформаційної безпеки, адаптовані для IoT - як зазначено в розділі 2.3, традиційні підходи часто виявляються невідповідними для специфіки IoT. Вони розроблені для потужних комп'ютерних систем і не враховують жорсткі обмеження в обчислювальних ресурсах, вимоги до енергоефективності та величезну масштабованість IoT-систем.

2) Суто централізовані системи безпеки IoT - хоча такі системи пропонують зручність управління, вони мають критичні вразливості, такі як єдина точка відмови, висока привабливість для атак, можливі затримки в передачі даних та залежність від постійного підключення.

3) Ізольовані або фрагментарні рішення безпеки - багато рішень фокусуються лише на окремих аспектах безпеки (наприклад, тільки на захисті

мережі або тільки на шифруванні даних), не забезпечуючи комплексного захисту на всіх рівнях IoT-архітектури.

4) Статичні системи безпеки - Такі системи часто не здатні адаптуватися до нових видів атак та мають обмежені можливості для інтеграції новітніх технологій.

Запропонована гібридна система безпеки IoT демонструє значні переваги порівняно з вищезгаданими аналогами завдяки своїй багатошаровій архітектурі та інтеграції різноманітних технологій та механізмів.

Порівняння запропонованої гібридної системи з аналогами:

1) Комплексність та багаторівневий захист ("Defense-in-Depth").

Порівняно з ізольованими рішеннями запропонована система забезпечує захист на всіх ключових рівнях IoT-архітектури. Це створює глибоко ешелоновану оборону, де кожен шар доповнює інші, на відміну від підходів, що захищають лише окремі компоненти. Безпека на рівні пристроїв забезпечується апаратними ядрами довіри (SE, TPM, PUF), безпечним завантаженням та полегшеною криптографією, тоді як мережевий рівень використовує сегментацію, захищені канали та NIDS/NIPS. Хмарний рівень доповнює це розширеною аналітикою загроз та централізованим управлінням.

2) Адаптація до обмежень IoT-пристроїв.

Порівняно з традиційними методами ІБ, система активно використовує технології, призначені для пристроїв з обмеженими ресурсами. Ключовим елементом є застосування алгоритмів полегшеної криптографії (LWC) для шифрування та автентифікації, що мінімізує навантаження на процесор та енергоспоживання. Крім того, архітектура передбачає розвантаження IoT-пристроїв шляхом перенесення складних обчислень, включаючи криптографічні операції та аналітику безпеки, на рівень шлюзів. Мінімізація поверхні атаки на пристроях також є важливим аспектом.

3) Підвищена стійкість та зменшення затримок.

Порівняно з суто централізованими системами, гібридна архітектура зменшує ризик єдиної точки відмови шляхом інтеграції децентралізованих

елементів та розподіленої обробки на рівні шлюзів (Edge/Fog computing). Локальна аналітика безпеки на шлюзах (наприклад, локальні IDS/IPS та виявлення аномалій) дозволяє швидко реагувати на інциденти без необхідності звернення до хмари, що критично для чутливих до затримок додатків. Навіть у разі тимчасової втрати зв'язку з хмарою, шлюзи можуть продовжувати забезпечувати базовий рівень безпеки та функціонування локальних пристроїв, кешуючи політики безпеки.

4) Гнучкість та адаптивність до нових загроз.

Порівняно зі статичними системами запропонована система використовує комбінацію методів виявлення загроз, включаючи сигнатурні методи та аналіз поведінки з використанням штучного інтелекту та машинного навчання (наприклад, UEBA на хмарному рівні, виявлення аномалій на рівні шлюзів та в NIDS/NIPS). Це дозволяє ідентифікувати не тільки відомі, але й нові, невідомі атаки. Система підтримує інтеграцію з платформами аналізу загроз (Threat Intelligence Platforms) та має розширені механізми безпечного оновлення програмного забезпечення та прошивок (FOTA/SOTA), що є критичним для своєчасного виправлення вразливостей.

5) Інтеграція інноваційних технологій безпеки.

Порівняно з багатьма наявними платформами, система передбачає використання передових технологій, таких як:

– Блокчейн - для забезпечення незмінності критичних даних, децентралізованого управління ідентифікацією (DID) та безпечного оновлення прошивок. При цьому враховуються обмеження традиційних блокчейнів для IoT, розглядаючи полегшені версії або DLT.

– Багаторівневі IDS/IPS - розгортання систем виявлення та запобігання вторгненням на рівнях пристроїв (HIDS/HIPS), шлюзів/мережі (NIDS/NIPS) та хмари, з кореляцією подій у SIEM/SOAR системах для комплексного аналізу.

– Техніки збереження приватності - такі як анонімізація/псевдонімізація даних, диференційна приватність та федеративне навчання для аналізу даних без розкриття конфіденційної інформації.

6) Централізоване управління та моніторинг з розподіленим виконанням.

Хоча система використовує розподілені елементи, вона зберігає переваги централізованого управління політиками безпеки, управління ідентифікацією та доступом (IAM), управління вразливостями та оновленнями, а також розширеного моніторингу (SIEM, SOAR) на хмарному рівні. Це дозволяє підтримувати узгоджений рівень безпеки в усій системі, тоді як шлюзи та пристрої забезпечують виконання цих політик та локальне реагування.

7) Структуроване управління ризиками.

Підхід до безпеки в запропонованій системі базується на безперервному процесі управління ризиками, що включає ідентифікацію, оцінку, обробку та моніторинг ризиків на всіх рівнях гібридної архітектури, враховуючи специфіку кожного компонента. Це забезпечує більш проактивний та обґрунтований підхід до захисту.

Сценарний аналіз:

1) Захист від DDoS-атак.

Розподілені атаки типу "відмова в обслуговуванні" (DDoS) спрямовані на перевантаження мережевих каналів або сервісів IoT-системи. Традиційні системи часто покладаються на хмарні сервіси очищення трафіку, що може бути ефективним для великих атак, але призводить до затримок і залежності від провайдера. Менші атаки або ті, що генеруються зсередини, наприклад, скомпрометованими IoT-пристроями, що стали частиною ботнету, можуть бути пропущені або виявлені із запізненням. Запропонована гібридна система реалізує багаторівневий захист. На рівні IoT-пристроїв превентивні заходи включають регулярні безпечні оновлення прошивок та ПЗ (FOTA/SOTA) та управління вразливостями, що значно зменшує ймовірність компрометації пристроїв і їх перетворення на ботнети. Мінімізація поверхні атаки також знижує ризики. На рівні локальних обчислень та шлюзів, шлюзи аналізують вихідний трафік від підключених IoT-пристроїв на предмет аномальної активності, характерної для участі в DDoS-атаці, наприклад, нетипово великий обсяг запитів до одного ресурсу. При виявленні такої активності шлюз може

локально ізолювати підозрілий пристрій або обмежити його трафік, запобігаючи його участі в атаці та інформуючи центральну систему. На рівні мережевої інфраструктури розгортаються мережеві IDS/NIPS та спеціалізовані рішення для захисту від DDoS-атак, які фільтрують відомі вектори атак та аномальний трафік ближче до джерела або цілі. Використання технологій SDN може забезпечити динамічне реагування та перенаправлення трафіку. Нарешті, на рівні хмарних технологій та додатків, хмарна платформа агрегує дані з усіх попередніх рівнів, використовуючи SIEM/SOAR та інтеграцію з Threat Intelligence для виявлення масштабних та складних атак, координації глобальних заходів захисту та аналізу трендів.

2) Безпечне оновлення програмного забезпечення та прошивок (FOTA/SOTA).

Необхідність оновлення ПЗ та прошивок для виправлення вразливостей та додавання функцій є критичною. Статичні та деякі традиційні системи часто не мають механізмів оновлення, або ці механізми небезпечні, наприклад, через ручне завантаження файлу без перевірки підпису, залишаючи пристрої вразливими на тривалий час. Запропонована гібридна система забезпечує надійний та керований процес оновлення. На рівні хмарних технологій реалізовано центральне управління: хмарна платформа слугує довіреним джерелом пакетів оновлень, де вони безпечно зберігаються, перевіряються та підписуються цифровим підписом. Платформа управляє процесом розгортання, дозволяючи поетапне впровадження та відстеження статусу оновлення кожного пристрою. Для ефективного розподілу оновлень на рівні локальних обчислень та шлюзів, останні можуть кешувати перевірені пакети оновлень для локальних пристроїв, що зменшує навантаження на зовнішні канали зв'язку, прискорює процес та дозволяє оновлювати пристрої навіть за умов обмеженого доступу до Інтернету. Шлюзи також можуть координувати послідовність оновлень на локальному рівні. На рівні IoT-пристроїв забезпечується надійне встановлення: пристрої оснащені механізмами для перевірки автентичності (цифровий підпис) та цілісності (хеш-суми) пакета оновлення перед встановленням; безпечного

завантаження (Secure Boot), що гарантує запуск лише автентичної та цілісної прошивки після оновлення; захисту від відкату (Anti-rollback Protection), що запобігає встановленню старих, потенційно вразливих версій прошивки; та механізмів відновлення (Recovery Mechanisms), наприклад, через використання подвійних банків пам'яті, для повернення до стабільної версії у випадку невдалого оновлення. Технологія блокчейн може додатково використовуватися для зберігання хешів прошивок та записів про оновлення, забезпечуючи прозорість та можливість перевірки автентичності джерела.

3) Реагування на компрометацію пристрою (наприклад, через Zero-Day вразливість).

Компрометація пристрою, особливо через невідому (Zero-Day) вразливість, може бути важко виявлена в традиційних або статичних системах. Якщо пристрій скомпрометований, він може тривалий час використовуватися зловмисниками для атак на інші системи або витоку даних без відома власника. Запропонована гібридна система реагує узгоджено на кількох рівнях. На рівні локальних обчислень та шлюзів відбувається виявлення аномальної поведінки та швидке стримування. Навіть якщо конкретна вразливість невідома, поведінка скомпрометованого пристрою може змінитися, наприклад, через нетипові з'єднання, зміну обсягів або типів трафіку, чи незвичну активність процесів. Локальна система виявлення аномалій на шлюзі, що базується на ШІ/МН та навчена на "нормальній" поведінці пристрою, фіксує такі відхилення. При виявленні підозрілої активності шлюз може автоматично ізолювати пристрій від мережі, як локальної, так і зовнішньої, або обмежити його функціональність згідно з попередньо налаштованими політиками. Такі дії миттєво обмежують потенційну шкоду та запобігають поширенню атаки, не вимагаючи команди з хмарного рівня. Полегшені HIDS/HIPS на самих пристроях, де це можливо, також можуть виявляти ознаки компрометації локально. На рівні хмарних технологій здійснюється глибокий аналіз та координація. Інформація про інцидент з локального шлюзу та інших джерел, таких як NIDS/NIPS та журнали пристроїв, передається до SIEM/SOAR системи в хмарі. Тут дані корелюються,

аналізуються з використанням UEBA та Threat Intelligence для визначення масштабу атаки, її природи та розробки комплексної стратегії реагування. Це включає розробку та розгортання необхідних виправлень через механізми FOTA/SOTA на всі вразливі пристрої.

4.2 Переваги і недоліки

Запропонована в Розділі 3 гібридна система безпеки для Інтернету Речей розроблена з метою подолання багатьох обмежень, властивих наявним підходам. Вона поєднує різноманітні технології та архітектурні рішення для створення комплексного та адаптивного захисту. Однак, як і будь-яка складна система, вона має свої переваги та потенційні недоліки, які варто розглянути.

Переваги запропонованої гібридної системи:

1) Комплексний та багаторівневий захист – система забезпечує глибоку ешелоновану оборону ("defense-in-depth"), охоплюючи всі рівні IoT-архітектури: від кінцевих пристроїв з апаратною безпекою ядра та полегшеною криптографією до рівня локальних обчислень та шлюзів з розподіленою аналітикою безпеки, рівня мережевої інфраструктури із сегментацією та захистом каналів і хмарного рівня з розширеною аналітикою загроз та централізованим управлінням. Такий підхід значно ускладнює завдання зловмисникам, оскільки вимагає подолання кількох бар'єрів безпеки.

2) Підвищена стійкість до відмов та атак – завдяки поєднанню централізованих, децентралізованих та розподілених елементів (Edge/Fog computing), система уникає проблеми єдиної точки відмови, характерної для суто централізованих архітектур. Локальні компоненти, такі як шлюзи, можуть продовжувати виконувати критичні функції безпеки навіть при тимчасовій втраті зв'язку з хмарою.

3) Покращена масштабованість – розподіл завдань обробки даних та аналітики безпеки, зокрема на рівні шлюзів, зменшує навантаження на

центральні хмарні сервери. Це дозволяє системі ефективно працювати з великою кількістю IoT-пристроїв та обсягами даних, що ними генеруються.

4) Гнучкість та адаптивність – гібридний підхід дозволяє інтегрувати різноманітні технології безпеки, включаючи традиційні та інноваційні, такі як штучний інтелект для аналізу поведінки, блокчейн для управління довірою та цілісністю даних, та полегшену криптографію для пристроїв з обмеженими ресурсами. Система може адаптуватися до специфічних вимог різних IoT-додатків та динамічно реагувати на нові загрози завдяки можливості оновлення політик та інтеграції з платформами Threat Intelligence.

5) Зменшення затримок при реагуванні на інциденти – обробка даних безпеки та прийняття рішень на локальному рівні (шлюзи) забезпечує швидке виявлення та реагування на локальні загрози, наприклад, ізоляцію скомпрометованого пристрою, що критично для запобігання поширенню атаки та мінімізації її наслідків.

6) Врахування обмежень IoT-пристроїв – система спеціально розроблена з урахуванням обмежених обчислювальних ресурсів та енергоспоживання багатьох IoT-пристроїв. Це досягається шляхом застосування полегшеної криптографії, мінімізації поверхні атаки на пристроях та перенесення ресурсоємних завдань на шлюзи або хмарну платформу.

7) Інтеграція передових механізмів безпеки – система включає сучасні підходи. До них належать багаторівневі системи виявлення та запобігання вторгненням (IDS/IPS), що працюють на рівнях пристроїв, шлюзів, мережі та хмари з кореляцією подій. Також передбачається використання технології блокчейн для забезпечення незмінності та простежуваності даних, децентралізованого управління ідентифікацією та безпечного оновлення прошивок. Окрім цього, впроваджуються комплексні механізми безпечного оновлення програмного забезпечення (SOTA/FOTA) з перевіркою автентичності, цілісності, захистом від відкату та механізмами відновлення. Нарешті, застосовуються технології збереження приватності даних, що

включають анонімізацію, псевдонімізацію, диференційну приватність та федеративне навчання.

Недоліки та виклики запропонованої гібридної системи:

1) Складність проектування та впровадження – інтеграція численних технологій (полегшена криптографія, блокчейн, ШІ/МН, IDS/IPS) та компонентів на різних архітектурних рівнях (пристрої, шлюзи, мережа, хмара) є складним інженерним завданням, що вимагає високої кваліфікації розробників та системних архітекторів.

2) Вища початкова вартість – розгортання комплексної гібридної системи може вимагати значних початкових інвестицій. Це стосується як закупівлі спеціалізованого обладнання (наприклад, IoT-пристроїв з вбудованими елементами безпеки, потужних шлюзів для локальної обробки даних), так і розробки або придбання відповідного програмного забезпечення та платформ.

3) Складність управління та обслуговування – управління гетерогенною системою, що складається з різнорідних пристроїв, протоколів та програмних компонентів, є викликом. Забезпечення узгодженої роботи всіх елементів, моніторинг їх стану, своєчасне оновлення та реагування на інциденти вимагають розвинених інструментів управління та кваліфікованого персоналу.

4) Потенційні проблеми сумісності та інтеграції – забезпечення безшовної взаємодії між компонентами від різних виробників або різними технологічними стеками (наприклад, інтеграція блокчейн-рішень з наявними хмарними платформами) може бути складним завданням та потребувати додаткових зусиль на розробку шлюзів та API.

5) Вимоги до продуктивності та безпеки шлюзів – шлюзи відіграють ключову роль в архітектурі, виконуючи функції агрегації даних, локальної аналітики безпеки та іноді криптографічного проксіювання. Це висуває підвищені вимоги до їх обчислювальної потужності, надійності та власної безпеки, оскільки компрометація шлюзу може вплинути на значний сегмент IoT-системи.

6) Необхідність безперервного оновлення знань та адаптації – ландшафт загроз та технології безпеки (ШІ, блокчейн, LWC) стрімко розвиваються. Підтримка ефективності гібридної системи вимагає постійного моніторингу нових тенденцій, оновлення знань персоналу та готовності до адаптації та модернізації компонентів системи.

7) Збалансування безпеки та функціональності – впровадження жорстких заходів безпеки на всіх рівнях, особливо на пристроях з обмеженими ресурсами, може потенційно вплинути на їхню основну функціональність, продуктивність або вартість. Знаходження оптимального балансу є важливим завданням.

Незважаючи на зазначені виклики, переваги запропонованої гібридної системи безпеки, зокрема її комплексність, адаптивність та стійкість, роблять її перспективним рішенням для захисту сучасних та майбутніх IoT-екосистем від широкого спектра кіберзагроз. Успішне впровадження вимагає ретельного планування, урахування специфіки конкретного застосування IoT та готовності до постійного вдосконалення системи.

4.3 Перспективи розвитку

Запропонована в даній роботі гібридна система безпеки для Інтернету Речей створює міцний фундамент для протидії сучасним кіберзагрозам. Однак, зважаючи на стрімкий розвиток IoT-технологій, постійну еволюцію загроз та появу нових викликів, подальший розвиток та вдосконалення як самої гібридної системи, так і підходів до безпеки IoT в цілому, є критично важливим. Перспективи розвитку охоплюють низку ключових напрямків, спрямованих на підвищення ефективності, адаптивності, стійкості та рівня довіри в IoT-екосистемах.

1) Поглиблена інтелектуалізація механізмів безпеки з використанням штучного інтелекту та машинного навчання (ШІ/МН) – як було зазначено, запропонована система вже передбачає використання ШІ/МН для аналізу поведінки та виявлення аномалій. Перспективним напрямком є подальше

розширення їх застосування. Це включає розробку більш досконалих моделей предиктивної аналітики, здатних прогнозувати потенційні атаки на основі аналізу слабких сигналів та глобальних даних про загрози (Threat Intelligence). Також важливим є розвиток систем автоматизованого реагування (SOAR), які зможуть не лише виявляти, але й самостійно вживати заходів для нейтралізації загроз в реальному часі, мінімізуючи людське втручання. Це особливо актуально для масштабних IoT-систем, де ручне управління інцидентами є неефективним. Крім того, ШІ/МН можуть використовуватися для створення адаптивних політик безпеки, які динамічно змінюються залежно від поточного контексту, рівня ризику та поведінки системи, що підвищить гнучкість захисту, яка є однією з переваг гібридної системи. Необхідно також досліджувати методи протидії атакам, що використовують сам ШІ (Adversarial AI), для забезпечення надійності інтелектуальних компонентів системи безпеки.

2) Стандартизація та посилення безпеки на граничних (Edge) та туманних (Fog) обчислювальних рівнях – архітектура запропонованої системи значною мірою покладається на переваги граничних та туманних обчислень для розподіленої аналітики безпеки та швидкого реагування. Майбутній розвиток повинен зосередитися на створенні стандартизованих протоколів безпеки для взаємодії між граничними вузлами та IoT-пристроями, а також між самими граничними вузлами. Це сприятиме інтероперабельності рішень від різних виробників та спростить розгортання безпечних граничних інфраструктур, що є одним із викликів. Важливим є також підвищення автономності граничних вузлів у прийнятті рішень щодо безпеки, розробка полегшених, але ефективних механізмів координації між ними для виявлення та стримування розподілених атак на локальному рівні. Потрібно посилити власну безпеку шлюзів, розробляючи для них спеціалізовані захищені операційні системи та апаратні модулі, оскільки компрометація шлюзу може мати серйозні наслідки. Розвиток технологій на кшталт федеративного навчання на граничних вузлах дозволить покращити моделі виявлення загроз, зберігаючи при цьому приватність даних.

3) Еволюція децентралізованих підходів на основі блокчейну та інших технологій розподіленого реєстру (DLT) – запропонована система розглядає використання блокчейну для таких завдань, як забезпечення цілісності даних, децентралізоване управління ідентифікацією та безпечне оновлення прошивок. Однак, наявні проблеми масштабованості та ресурсоємності традиційних блокчейнів стимулюють пошук нових рішень. Перспективи включають дослідження та впровадження полегшених блокчейн-архітектур, приватних та консорціумних блокчейнів, а також альтернативних DLT, таких як IOTA Tangle або Hashgraph, які є більш придатними для IoT-середовища. Майбутні розробки можуть бути спрямовані на створення децентралізованих ринків довірених IoT-даних, де блокчейн гарантуватиме прозорість та безпеку транзакцій. Також перспективним є використання смарт-контрактів для автоматизації складних політик безпеки та управління доступом в гетерогенних IoT-системах, що зменшить залежність від централізованих адміністраторів та підвищить стійкість системи. Подальші дослідження також необхідні для вирішення питань інтеграції блокчейн-рішень з наявними хмарними платформами та шлюзами.

4) Розробка та інтеграція постквантової криптографії для довгострокового захисту IoT-систем – з огляду на тривалий життєвий цикл багатьох IoT-пристроїв та потенційну загрозу з боку квантових комп'ютерів для наявних криптографічних алгоритмів на основі RSA та еліптичних кривих (ECC), надзвичайно важливим є завчасний перехід на постквантову криптографію (PQC). Хоча поточна гібридна система використовує сучасну полегшену криптографію (LWC), майбутні ітерації повинні передбачати інтеграцію PQC-алгоритмів, стійких до атак квантових комп'ютерів. Це особливо актуально для захисту довгостроково збережених даних, оновлень прошивок та каналів зв'язку в критично важливих IoT-інфраструктурах, таких як промислові системи чи медичні пристрої. Розробка саме полегшених версій PQC-алгоритмів, придатних для ресурсообмежених IoT-пристроїв, є одним із ключових

дослідницьких завдань у цьому напрямку, щоб забезпечити баланс між безпекою та функціональністю.

5) Удосконалення апаратних засобів безпеки та їх широке впровадження – апаратна безпека ядра (Hardware Root of Trust), що реалізується через вбудовані елементи безпеки (Secure Elements - SE), довірені платформні модулі (Trusted Platform Modules - TPM) та фізично не клоновані функції (Physically Unclonable Functions - PUF), є наріжним каменем безпеки на рівні пристроїв у запропонованій системі. Перспективи розвитку полягають у подальшій мініатюризації, зниженні вартості та підвищенні функціональності цих апаратних компонентів, що сприятиме їх масовому впровадженню навіть у найдешевші IoT-пристрої. Важливим є розробка нових типів PUF з покращеною стабільністю та надійністю, а також створення стандартизованих API для взаємодії програмного забезпечення з апаратними модулями безпеки. Інтеграція апаратних прискорювачів для полегшеної криптографії та постквантових алгоритмів також підвищить продуктивність та енергоефективність захищених IoT-пристроїв, що є критичним з огляду на вимоги до енергоефективності.

6) Створення всеосяжних стандартів безпеки, програм сертифікації та нормативно-правове регулювання – у документі підкреслюється фрагментарність та динамічність нормативно-правової бази у сфері безпеки IoT. Для забезпечення належного рівня безпеки та інтероперабельності IoT-рішень критично важливим є розробка та прийняття міжнародних та галузевих стандартів безпеки. Ці стандарти повинні охоплювати весь життєвий цикл IoT-пристроїв – від проектування та виробництва до виведення з експлуатації. Розвиток програм сертифікації IoT-пристроїв та платформ на відповідність вимогам безпеки допоможе користувачам робити усвідомлений вибір та підвищить відповідальність виробників. Необхідне подальше вдосконалення законодавства, зокрема щодо захисту персональних даних, відповідальності за інциденти безпеки та вимог до безпеки критичної IoT-інфраструктури, знаходячи баланс між безпекою та інноваціями.

7) Підвищення рівня обізнаності, зручності використання інструментів безпеки та фокус на "Безпеці через проектування" – людський фактор залишається однією з суттєвих проблем в безпеці IoT, включаючи недостатню обізнаність користувачів та виробників та використання слабких стандартних налаштувань. Майбутні зусилля мають бути спрямовані на розробку інтуїтивно зрозумілих інструментів управління безпекою IoT-систем, які не вимагатимуть від користувачів глибоких технічних знань. Принцип "Безпека через проектування" (Security by Design) має стати обов'язковим на всіх етапах розробки IoT-систем, що передбачає інтеграцію механізмів безпеки з самого початку, а не як додатковий функціонал. Це включає розробку безпечних за замовчуванням конфігурацій, спрощення процесу оновлення програмного забезпечення та надання користувачам чітких рекомендацій щодо безпечної експлуатації пристроїв. Освітні програми та кампанії з підвищення обізнаності про ризики та методи захисту в IoT також відіграватимуть важливу роль.

Запропоновані напрямки розвитку не є вичерпними, але вони окреслюють ключові вектори зусиль, необхідних для подальшого підвищення рівня безпеки Інтернету Речей. Успішна реалізація цих перспектив вимагатиме спільних зусиль дослідників, розробників, виробників, регуляторів та користувачів, а також постійних інвестицій в наукові дослідження та розробку нових технологій захисту. Розвиток гібридних підходів, подібних до запропонованого в даній роботі, залишатиметься актуальним для створення дійсно стійких, адаптивних та надійних IoT-екосистем майбутнього.

Висновки за розділом 4

Оцінка ефективності запропонованої гібридної системи безпеки IoT показала її суттєві переваги порівняно з наявними аналогами, зокрема завдяки комплексному багаторівневому захисту, підвищеній стійкості до відмов, покращеній масштабованості та адаптивності до нових загроз. Система ефективно враховує обмеження IoT-пристроїв та інтегрує передові механізми,

такі як ШІ, блокчейн та багаторівневі IDS/IPS, забезпечуючи швидке реагування на інциденти. Водночас, впровадження такої системи пов'язане з певними викликами, серед яких складність проектування та інтеграції, вища початкова вартість та потреба у кваліфікованому управлінні й постійній адаптації. Перспективи подальшого розвитку системи включають поглиблену інтелектуалізацію безпеки, стандартизацію на граничних рівнях, еволюцію децентралізованих підходів, впровадження постквантової криптографії та удосконалення апаратних засобів. Незважаючи на труднощі, запропонована гібридна модель є перспективним напрямком для створення надійних IoT-екосистем майбутнього.

ВИСНОВКИ

У кваліфікаційній роботі розв'язано актуальну науково-практичну задачу розробки моделі гібридної системи безпеки для Інтернету Речей (IoT) з підвищеним рівнем інформаційної безпеки, що є критично важливим в умовах стрімкого поширення IoT-технологій та зростання кількості кіберзагроз. Наявні підходи до захисту IoT-систем часто виявляються недостатньо адаптованими до їх специфіки, зокрема, до обмежених ресурсів пристроїв, великої масштабованості та гетерогенності систем, а також до динамічного характеру загроз. Метою роботи була розробка моделі гібридної IoT-системи, яка забезпечує підвищений рівень захисту даних і надійну взаємодію пристроїв у критично важливих середовищах.

Для досягнення поставленої мети було виконано наступні завдання:

1) Проведено комплексний аналіз предметної області Інтернету Речей, розглянуто актуальність теми, роль IoT у сучасних системах, його визначення, архітектуру та класифікацію. Детально досліджено загрози, вразливості та проблеми безпеки, притаманні IoT-системам на різних рівнях, а також проаналізовано наявну нормативну базу. Результати аналізу підтвердили нагальну потребу у розробці комплексних та ефективних рішень для безпеки IoT.

2) Здійснено огляд і критичний аналіз наявних методів забезпечення безпеки, включаючи криптографічні методи, засоби контролю доступу, системи виявлення та запобігання вторгненням (IDS/IPS), а також приклади рішень, фреймворків та архітектур. Виявлено проблеми та обмеження цих підходів, такі як невідповідність традиційних методів специфіці IoT, вразливості централізованих систем, складність управління різнорідними пристроями та недостатня адаптивність до нових загроз. Це обґрунтувало мотивацію до створення нового, більш комплексного підходу.

3) Розроблено модель та чотирирівневу архітектуру гібридної системи безпеки IoT, що базується на принципі ешелонованої оборони ("defense-in-depth"). На кожному рівні (IoT-пристроїв, локальних обчислень та шлюзів, мережевої інфраструктури, хмарних технологій та додатків) застосовуються специфічні технології та механізми безпеки, включаючи апаратну безпеку ядра, полегшену криптографію, взаємну автентифікацію, технологію блокчейн для цілісності даних, багаторівневі IDS/IPS, безпечне оновлення ПЗ (FOTA/SOTA), технології збереження приватності та безперервний процес управління ризиками.

4) Проведено оцінку ефективності запропонованої гібридної системи шляхом порівняння з наявними аналогами, виокремлено її переваги та недоліки. Визначено перспективи подальшого розвитку системи.

Ключовим результатом роботи є розроблена модель гібридної IoT-системи, яка забезпечує підвищений рівень захисту даних та безпечну взаємодію пристроїв. Запропонована система дозволяє ефективно протидіяти сучасним кіберзагрозам за рахунок інтеграції багаторівневого захисту, сучасних криптографічних методів, безпечної автентифікації, розподіленої аналітики безпеки та централізованого управління, що робить її придатною для впровадження у сферах з підвищеними вимогами до інформаційної безпеки, таких як промисловість, розумні міста та охорона здоров'я. Комплексний підхід, реалізований у гібридній архітектурі, забезпечує підвищену стійкість до відмов, кращу масштабованість, гнучкість та адаптивність до нових загроз, а також враховує обмеження IoT-пристроїв.

Таким чином, завдання кваліфікаційної роботи виконані у повному обсязі, а поставлена мета – досягнута. Розроблена модель гібридної системи безпеки IoT є внеском у вирішення проблеми забезпечення захищеності сучасних та майбутніх IoT-екосистем. Подальший розвиток запропонованих рішень, зокрема у напрямках поглибленої інтелектуалізації механізмів безпеки, стандартизації на граничних рівнях, еволюції децентралізованих підходів,

інтеграції постквантової криптографії та удосконалення апаратних засобів безпеки, дозволить створити ще більш надійні, стійкі та адаптивні IoT-системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7863703

2. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. Demystifying IoT Security: An Exhaustive Survey of Security Vulnerabilities and Defenses. IEEE Communications Surveys & Tutorials, 2019. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8643036

3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 2015. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S138912861400733X

4. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 2020. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8932732

5. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. Proceedings of the 10th International Conference on Information and Communication Systems (ICICS), 2019. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8769228 (або пошук у матеріалах конференції ICICS).

6. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 2018. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0167739X1730476X

7. Gupta, S. K., & Gentry, C. Physically Unclonable Functions (PUFs): A Tutorial. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7519201 (або пошук у матеріалах симпозіуму HOST).

8. Bringer, J., Chabanne, H., & Dottax, E. Secure Elements in the Internet of Things. Springer, 2016. – Режим доступу до ресурсу: https://link.springer.com/book/10.1007/978-3-319-33432-4 (інформація про книгу, доступ до повного тексту може бути обмежений).

9. Noorman, J., Van Herrewege, A., & Piessens, F. Trusted Execution Environments on Low-End Embedded Systems. ACM Transactions on Design Automation of Electronic Systems, 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://dl.acm.org/doi/10.1145/3060403

10. Wallgren, L., Raza, S., & Voigt, T. Routing Attacks and Countermeasures in the RPL-based Internet of Things. International Journal of Distributed Sensor Networks, 2013. – [Електронний ресурс] – Режим доступу до ресурсу: https://journals.sagepub.com/doi/10.1155/2013/794326

11. Granados, J., & Kammuller, F. Secure Communication Protocols for the Internet of Things - A Survey. Journal of Network and Computer Applications, 2020. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S108480451930313X

12. Hiller, M., & Hohl, A. A Survey of MQTT Security. International Journal of Internet Technology and Secured Transactions, 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.inderscienceonline.com/doi/abs/10.1504/IJITST.2017.087169

13. Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. Towards Blockchain-based Secure Message Exchange in the IoT. Proceedings of the ACM/IEEE Symposium on Edge Computing (SEC), 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://dl.acm.org/doi/10.1145/3132211.3134422

14. Stojmenovic, I., & Wen, S. The Fog Computing Paradigm: Scenarios and Security Issues. Proceedings of the IEEE Federated Conference on Computer Science and Information Systems, 2014. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/6935190

15. Yi, S., Li, C., & Li, Q. A Survey of Fog Computing: Concepts, Applications and Issues. Proceedings of the ACM Workshop on Mobile Big Data, 2015. – [Електронний ресурс] – Режим доступу до ресурсу: https://dl.acm.org/doi/10.1145/2757384.2757397

16. Roman, R., Lopez, J., & Mambo, M. Mobile edge computing, Fog computing and Internet of Things: A security perspective. Future Generation Computer Systems, 2018. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0167739X17302024

17. Ahmed, A. A., & Echi, M. O. A_Survey_of_Security_Issues_in_Fog_Computing. International Journal of Computer Applications, 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.ijcaonline.org/archives/volume161/number6/ahmed-2017-ijca-913312

18. McKay, K. A., Bassham, L., Turan, M. S., & Mouha, N. Report on Lightweight Cryptography. NISTIR 8114, National Institute of Standards and Technology, 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

19. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. The SIMON and SPECK Lightweight Block Ciphers. Design, Codes and Cryptography, 2015. – [Електронний ресурс] – Режим доступу до ресурсу: https://link.springer.com/article/10.1007/s10623-015-0040-4

20. Bernstein, D. J., & Lange, T. Post-quantum cryptography. Nature, 2017. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.nature.com/articles/nature23461

21. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Smith-Tone, A., & Yao, D.

Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309, 2020. – [Електронний ресурс] – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

22. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal, 2018. – [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8394380

23. National Institute of Standards and Technology (NIST). Cybersecurity for IoT Program. (Різні публікації, наприклад, NISTIR 8259 series). – [Електронний ресурс] – Режим доступу до ресурсу: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

24. European Union Agency for Cybersecurity (ENISA). Baseline Security Recommendations for IoT. 2017. (Та інші звіти). – [Електронний ресурс] – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications (пошук за назвою звіту).

25. OWASP Foundation. OWASP Internet of Things Project. (Настанови та інструменти). – [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-project-internet-of-things/

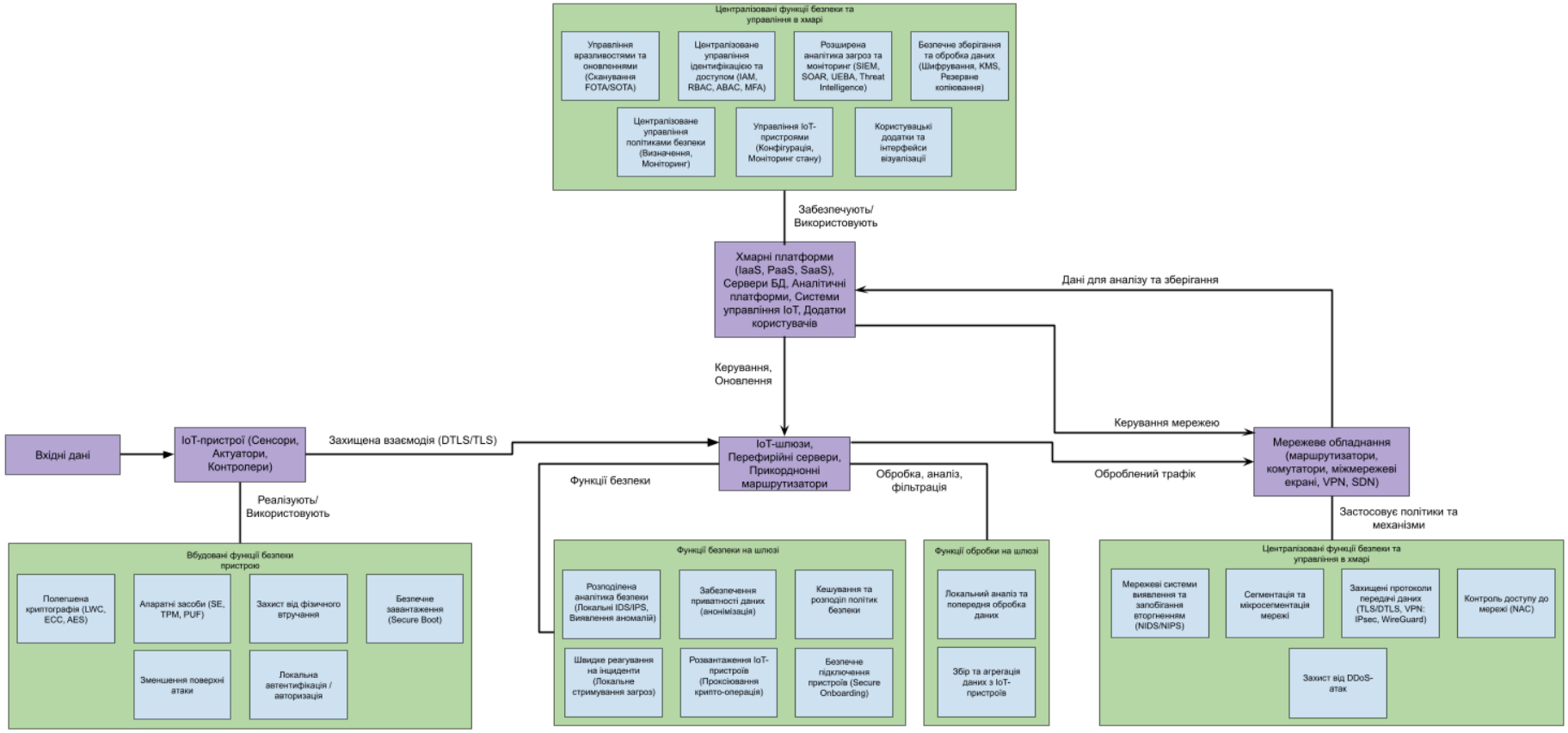
26. GSMA. IoT Security Guidelines & Assessment. (Документи для розробників та операторів). – [Електронний ресурс] – Режим доступу до ресурсу: https://www.gsma.com/iot/iot-security-guidelines/

27. ISO/IEC 27001. Information security management systems – Requirements. (Та пов'язані стандарти серії 27000). – Режим доступу до ресурсу: https://www.iso.org/standard/27001 (інформація про стандарт, повний текст зазвичай платний).

28. ISO/IEC 30141. Internet of Things (IoT) – Reference Architecture. 2018. – Режим доступу до ресурсу: https://www.iso.org/standard/65695.html (інформація про стандарт, повний текст зазвичай платний).

ДОДАТОК А

Блок-схема усієї моделі гібридної IoT-системи


Централізовані функції безпеки та управління в хмарі
Управління вразливостями та оновленнями (Сканування FOTA/SOTA)
Централізоване управління ідентифікацією та доступом (IAM, RBAC, ABAC, MFA)
Розширена аналітика загроз та моніторинг (SIEM, SOAR, UEBA, Threat Intelligence)
Безпечне зберігання та обробка даних (Шифрування, KMS, Резервне копіювання)
Централізоване управління політиками безпеки (Визначення, Моніторинг)
Управління IoT-пристроями (Конфігурація, Моніторинг стану)
Користувацькі додатки та інтерфейси візуалізації
Забезпечують/ Використовують
Хмарні платформи (IaaS, PaaS, SaaS), Сервери БД, Аналітичні платформи, Системи управління IoT, Додатки користувачів
Дані для аналізу та зберігання
Керування, Оновлення
Керування мережею
Вхідні дані
IoT-пристрої (Сенсори, Актуатори, Контролери)
Захищена взаємодія (DTLS/TLS)
IoT-шлюзи, Перефирійні сервери, Прикордонні маршрутизатори
Мережеве обладнання (маршрутизатори, комутатори, міжмережеві екрани, VPN, SDN)
Функції безпеки
Обробка, аналіз, фільтрація
Оброблений трафік
Реалізують/ Використовують
Застосовує політики та механізми
Вбудовані функції безпеки пристрою
Полегшена криптографія (LWC, ECC, AES)
Апаратні засоби (SE, TPM, PUF)
Захист від фізичного втручання
Безпечне завантаження (Secure Boot)
Зменшення поверхні атаки
Локальна автентифікація / авторизація
Функції безпеки на шлюзі
Розподілена аналітика безпеки (Локальні IDS/IPS, Виявлення аномалій)
Забезпечення приватності даних (анонімізація)
Кешування та розподіл політик безпеки
Швидке реагування на інциденти (Локальне стримування загроз)
Розвантаження IoT-пристроїв (Проксіювання крипто-операцій)
Безпечне підключення пристроїв (Secure Onboarding)
Функції обробки на шлюзі
Локальний аналіз та попередня обробка даних
Збір та агрегація даних з IoT-пристроїв
Централізовані функції безпеки та управління в хмарі
Мережеві системи виявлення та запобігання вторгненням (NIDS/NIPS)
Сегментація та мікросегментація мережі
Захищені протоколи передачі даних (TLS/DTLS, VPN: IPsec, WireGuard)
Контроль доступу до мережі (NAC)
Захист від DDoS-атак