Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складний П.М.

_____
(підпис)
« ___» _____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
Дослідження та вироблення рекомендацій щодо забезпечення безпеки системи "розумний дім/розумне місто"

Виконав

студент групи БІКСм-1-24-1.4д

Криволап Андрій Олександрович

(прізвище, ім'я, по батькові)

(підпис)

Науковий керівник

к.т.н., доцент

Козачок Валерій Анатолійович

(прізвище, ініціали)

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
Імені професора Володимира Бурячка

Освітньо-кваліфікаційний рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складний П.М.

_____
(підпис)
«___»_____20__р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Криволапу Андрію Олександровичу

1. Тема роботи: Дослідження та вироблення рекомендацій щодо забезпечення безпеки системи «розумний дім/розумне місто»; керівник Козачок Валерій Анатолійович к.т.н., доцент, затверджені наказом ректора від «___»____ 20___ року №__.
2. Термін подання студентом роботи «10» грудня 2025 р.
3. Вихідні дані до роботи:
   - 3.1 науково-технічна та нормативна література з теми дослідження: Закон України «Про основні засоби забезпечення кібербезпеки України», стандарти NIST SP 800-213, ETSI EN 303 645, NIST SP 800-207, рекомендації ENISA, специфікації протоколів MQTT v5.0 та CoAP (RFC 7252);
   - 3.2 методи: Меточжи системного аналізу, моделювання загроз (STRIDE), сканування вразливостей, експериментального тестування (Penetration Testing), порівняльного аналізу ефективності захисту системи;
   - 3.3 технології: Інтернету речей (IoT), мікросегментації мережі (VLAN), криптографічного захисту (TLS 1.3/SSL), міжмережевого екранування (Firewall), віртуалізації мережі;
   - 3.4 алгоритми: Словникового підбору паролів (Brute-force), шифрування даних (AES-256), хешування, автентифікації клієнтів у брокерських повідомленнях;

3.5 мова програмування: Python (для написання скриптів тестування безпеки та автоматизації атак);

3.6 математичні моделі та методи: методика оцінювання вразливостей CVSS v3.1 (Common Vulnerability Scoring System), методика розрахунку повернення інвестицій у безпеку (ROSI).

4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):

4.1 Дослідити сучасний стан, архітектуру та вектори кіберзагроз у системах «розумний дім» та «розумне місто», проаналізувати нормативну базу.

4.2 Провести аналіз вразливостей протоколів IoT (MQTT, CoAP), розробити методику тестування захищеності та змінити сценарії атаки на мережеву інфраструктуру.

4.3 Розробити практичні рекомендації щодо забезпечення безпеки досліджуваних систем, обґрунтувати їх ефективність за допомогою кількох метрик ризику та економічних розрахунків.

5. Перелік графічного матеріалу:

5.1Презентація доповіді, виконана в Microsoft PowerPoint.

5.2 Типові схеми архітектури IoT-системи, схеми реалізації атак (MITM), діаграми результатів сканування та ефективності захисту.

6. Дата видачі завдання «15» лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	05.03.2025-11.03.2025	Виконано
2.	Аналіз літератури	12.03.2025-18.03.2025	Виконано
3.	Обґрунтування вибору рішення	18.03.2025-22.03.2025	Виконано
4.	Збір даних	22.09.2025-19.10.2025	Виконано
5.	Виконання та оформлення розділу 1.	20.10.2025-28.10.2025	Виконано
6.	Виконання та оформлення розділу 2.	29.10.2025-08.11.2025	Виконано
7.	Виконання та оформлення розділу 3.	10.11.2025-18.11.2025	Виконано
8.	Виконання та оформлення розділу 4	18.11.2025-23.11.2025	Виконано
9.	Виконання та оформлення розділу 5	23.11.2025-28.11.2025	Виконано
10.	Вступ, висновки, реферат	20.10.2025-01.11.2025	Виконано
11.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції	05.11.2025	Виконано
12.	Оформлення та друк текстової частини роботи	10.12.2025	Виконано
13.	Оформлення презентацій	08.12.2025-12.12.2025	Виконано
14.	Отримання рецензій	02.12.2025	Виконано
15.	Попередній захист роботи	30.11.2025	Виконано
16.	Захист в ЕК	16.12.2025-18.12.2025	Виконано

Студент _____ Криволап Андрій Олександрович
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Козачок Валерій Анатолійович
(підпис) (прізвище, ім’я, по батькові)

Реферат

Кваліфікаційна робота присвячена технологіям використання засобів та методів забезпечення інформаційної безпеки в системах «розумний дім/розумне місто».

Робота складається зі вступу, п’яти розділів, що містять 5 рисунків та 5 таблиць, висновків та списку використаних джерел, що містить 30 найменування. Загальний обсяг роботи становить 87 сторінок, з яких 18 сторінки займають ілюстрації і таблиці на окремих аркушах, а також додатки, перелік умовних скорочень та список використаних джерел.

Об’єктом дослідження в роботі є процес забезпечення інформаційної безпеки в системах «розумний дім/розумне місто».

Предметом дослідження є метод аналізу загроз, вразливостей та розроблення рекомендацій щодо підвищення рівня захищеності IoT-інфраструктури.

Метою роботи є підвищення рівня безпеки систем «розумний дім/розумне місто» шляхом дослідження кіберзагроз та вироблення практичних рекомендацій щодо їх нейтралізації.

Для досягнення поставленої мети у роботі:

проведено аналіз існуючих підходів до побудови та захисту систем «розумний дім» та «розумне місто»,

досліджено особливості функціонування протоколів та компонентів IoT-інфраструктури та їх вразливостей,

обґрунтовано комплекс рекомендацій щодо покращення архітектури безпеки та впровадження технічних і організаційних заходів захисту.

Наукова новизна одержаних результатів полягає в тому, що в роботі запропоновано удосконалену математичну модель оцінки ризиків безпеки систем «розумний дім/розумне місто», розроблено метод формування рекомендацій із урахуванням результатів аналізу загроз та вразливостей та отримано кількісні показники ефективності запропонованих заходів.

Галузь застосування. Запропоновані підходи можуть бути використані для створення та модернізації систем «розумний дім» та «розумне місто», а також при проектуванні безпечних IoT-рішень для житлової та міської інфраструктури.

Ключові слова: БЕЗПЕКА, ЗАГРОЗА, ІНФОРМАЦІЯ, ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА, ОБ’ЄКТ БЕЗПЕКИ, ПОРУШНИК, СИСТЕМА ЗАХИСТУ

Зміст

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС – автоматизована система
БД – база даних
IoT – Інтернет речей (Internet of Things)
КЗЗ – комплекс заходів захисту
МЗ – модель загроз
ПЗ – програмне забезпечення
СЗІ – система захисту інформації
СУБД – система управління базою даних
AES − Advanced Encryption Standard – симетричний алгоритм блокового шифрування
API − Application Programming Interface – прикладний програмний інтерфейс
CoAP − Constrained Application Protocol – протокол прикладного рівня для обмежених пристроїв
CVSS − Common Vulnerability Scoring System – загальна система оцінювання вразливостей
DDoS − Distributed Denial of Service – розподілена атака на відмову в обслуговуванні
ENISA − European Union Agency for Cybersecurity – Агентство Європейського Союзу з кібербезпеки
HTTP − HyperText Transfer Protocol – протокол передачі гіпертексту
IDS − Intrusion Detection System – система виявлення вторгнень
IP − Internet Protocol – міжмережевий протокол
MITM − Man-in-the-Middle – атака «людина посередині»
MQTT − Message Queuing Telemetry Transport – мережевий протокол для обміну повідомленнями
NIST − National Institute of Standards and Technology – Національний інститут стандартів і технологій США
OWASP − Open Web Application Security Project – відкритий проект безпеки веб-застосунків
ROSI − Return on Security Investment – коефіцієнт повернення інвестицій у безпеку
TCP − Transmission Control Protocol – протокол керування передачею
TLS − Transport Layer Security – протокол захисту транспортного рівня
UDP − User Datagram Protocol – протокол користувацьких датаграм
Wi-Fi − Wireless Fidelity – технологія бездротової передачі даних (IEEE 802.11

ВСТУП

Актуальність теми. За даними аналітичних звітів, кількість підключених IoT-пристроїв у світі вже перевищила 15 мільярдів, а до 2030 року цей показник може подвоїтися. Експоненційний розвиток цих технологій супроводжується зростанням кількості кіберінцидентів: у 2023 році кількість атак на IoT-сегмент зросла на 400% порівняно з попереднім періодом. Вразливі пристрої «розумного дому» та «розумного міста» стають точками входу для зловмисників, що загрожує не лише витоком понад мільярдів записів персональних даних, а й стабільності функціонування критичної міської інфраструктури (водопостачання, енергетика, транспорт). Особливо на даному етапі, коли цифровізація міст відбувається в умовах гібридних загроз, проблема захисту інформації є першочерговою і потребує постійного удосконалення.

В якості системної методології захисту виділяють підхід, пов’язаний з комплексною оцінкою архітектурних вразливостей та управлінням ризиками. Більшість користувачів та операторів муніципальних систем зіштовхуються з низкою проблемних питань у сфері IoT-безпеки, зокрема:

1. гетерогенність протоколів та відсутність єдиних стандартів безпеки;
2. обмеженість обчислювальних ресурсів пристроїв, що унеможливлює використання «важких» алгоритмів шифрування;
3. масове використання заводських налаштувань (default credentials) та слабких парольних політик;
4. відсутність сегментації мережі, що дозволяє зловмисникам вільно переміщуватися між компонентами системи;
5. складність процесу оновлення програмного забезпечення (firmware) на кінцевих пристроях;
6. низька обізнаність користувачів щодо методів протидії соціальній інженерії та фішингу.

Якісний підхід за допомогою моделювання загроз (STRIDE) та кількісний підхід, який включає експериментальне сканування вразливостей (Penetration Testing) і розрахунок метрик CVSS — це фундамент для побудови ешелонованої

системи захисту, який є необхідним для мінімізації ризиків. У процесі дослідження пропонується використання автоматизованих скриптів для перевірки стійкості системи. Вище перелічене підтверджує актуальність даного дослідження.

Мета роботи полягає у підвищенні рівня захищеності систем «розумний дім» та «розумне місто» шляхом розробки практичних рекомендацій на основі експериментального аналізу вразливостей та оцінки ризиків.

Для досягнення цієї мети в роботі необхідно вирішити такі завдання:

1. проаналізувати архітектуру IoT-систем та нормативне забезпечення їх захисту на основі міжнародних стандартів (NIST, ETSI);
2. дослідити основні сценарії атак (DoS, MITM, Brute-force) та методики їх виявлення;
3. здійснити експериментальне моделювання атак та оцінку ефективності засобів захисту (шифрування, мікросегментація);
4. розробити та обґрунтувати комплекс рекомендацій щодо забезпечення безпеки з урахуванням економічної ефективності (ROSI).

Виходячи з цього, **об'єктом дослідження** є технології Інтернету речей (IoT), що є основою побудови систем «розумного дому» та «розумного міста».

Предмет дослідження — методи та засоби захисту, що забезпечують конфіденційність, цілісність і доступність даних у системах «розумного дому» і «розумного міста».

Методи дослідження. Для вирішення вищезгаданих завдань у роботі використано наступні методи: структурний аналіз (для архітектури), моделювання загроз, метод експериментального тестування (імітація атак за допомогою Nmap, Wireshark, Python), методи кількісної оцінки ризиків (CVSS v3.1) та метод системного синтезу (для формування рекомендацій).

Наукова новизна одержаних результатів. Наукова новизна полягає у поєднанні експериментального методу аналізу вразливостей протоколів MQTT/CoAP та математичного моделювання ризиків для створення адаптивної

моделі захисту IoT-інфраструктури, яка враховує специфіку обмежених ресурсів пристроїв.

Теоретичне та практичне значення полягає в обґрунтуванні необхідності переходу до архітектури «нульової довіри» (Zero Trust) в IoT-мережах та розробці прикладних сценаріїв налаштування безпеки, які можуть бути безпосередньо імплементовані.

Галузь застосування. Результати роботи можуть бути використані для модернізації систем житлової автоматизації («розумний дім») та захисту критичних підсистем муніципальної інфраструктури («розумне місто»), а також як матеріал для використання у навчальному процесі при підготовці фахівців з кібербезпеки.

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

1) в тезах доповіді на Студентській науковій конференції «Безпека інформаційно-комунікаційних систем» (Київ: Київський столичний університет імені Бориса Грінченка, 24 листопада 2025 року)

Розділ 1. ТЕОРЕТИЧНІ ЗАСАДИ БЕЗПЕКИ СИСТЕМ «РОЗУМНИЙ ДІМ» ТА «РОЗУМНЕ МІСТО»

1.1 Поняття та принципи побудови систем «Розумний дім» та «Розумне місто»

У сучасному технічному дискурсі концепція «розумний дім» (smart home) інтерпретується як інтегрована екосистема, що забезпечує автоматизацію побутових процесів через синергію апаратних та програмних компонентів. Згідно з визначенням Національного інституту стандартів і технологій США, наведеним у спеціальній публікації NIST SP 1800-15[1], архітектура розумного дому визначається як сукупність гетерогенних пристроїв, об'єднаних мережевою інфраструктурою, що взаємодіють за допомогою спеціалізованих сервісів. Ключовою детермінантою даного визначення є функціонування сенсорів, контролерів та виконавчих механізмів у рамках єдиного інформаційного простору, метою якого є оптимізація ресурсоспоживання, підвищення рівня фізичної безпеки та забезпечення комфорту експлуатації житлового середовища.

Відповідно до стандартів IEEE[2] та рекомендацій NIST[3], функціональний профіль систем розумного дому класифікується за трьома пріоритетними векторами: автоматизація рутинних операцій, забезпечення енергоефективності та імплементація механізмів фізичного й інформаційного захисту. Емпіричні дані досліджень Американської ради з енергоефективної економіки (ACEEE) демонструють кореляцію між впровадженням інтелектуальних систем терморегуляції та зниженням енерговитрат, фіксуючи середній показник економії на рівні 12–15% для систем опалення та кондиціонування[4]. Інтеграція підсистем відеоспостереження та контролю доступу дозволяє мінімізувати ризики несанкціонованого проникнення шляхом автоматизації сценаріїв реагування на інциденти безпеки.

Систематизація ключових параметрів розумного дому, базована на аналізі нормативної документації міжнародних інституцій, наведена у Таблиці 1.1.

Таблиця 1.1

Ключові параметри розумного дому за міжнародними стандартами

Аспект	**Характеристика**	**Джерело**
Базове визначення	Інтегрована сукупність мережевих пристроїв та сервісів	NIST SP 1800-15
Архітектура	Багаторівнева структура (Device, Network, Edge, Cloud, Application layers)	IEEE Standards
Цільові вектори	Автоматизація, енергозбереження, безпека	NIST, IEEE
Енергоефективність	12–15% економія на системах HVAC	ACEEE Research
Принципи безпеки	Security by Design, Privacy by Design	ENISA

Концепція «розумне місто» (smart city) є екстраполяцією принципів цифровізації на рівень урбаністичної інфраструктури, що передбачає інтеграцію інформаційно-комунікаційних технологій (ІКТ) у процеси муніципального управління. Згідно з дефініцією Європейської комісії[11], розумне місто визначається як середовище, в якому ефективність традиційних мереж та послуг підвищується завдяки імплементації цифрових рішень. Дане визначення підкреслює трансформацію міста у складний соціотехнічний комплекс, функціонування якого базується на безперервному зборі телеметрії з розподіленої мережі IoT-сенсорів, агрегації даних у реальному часі та їх подальшій аналітичній обробці для підтримки прийняття управлінських рішень.

Вектори розвитку систем типу smart city, регламентовані рекомендаціями міжнародних організацій[11], включають автоматизацію критичної інфраструктури, оптимізацію надання муніципальних послуг та забезпечення сталого урбаністичного розвитку. Комплексний характер даної парадигми передбачає конвергенцію підсистем життєзабезпечення (водо- та

енергопостачання), транспортної логістики, екологічного моніторингу та громадської безпеки в єдину керовану платформу.

Систематизація нормативних документів NIST, ENISA[3,6] та Європейської комісії дозволяє формалізувати набір фундаментальних принципів, що детермінують архітектурну цілісність, експлуатаційну ефективність та кіберстійкість систем інтелектуального житла та урбаністичних агломерацій. Дані принципи відображають консенсус експертної спільноти щодо методології проектування IoT-інфраструктур в умовах цифрової трансформації.

Принцип масштабованості та модульності визначає здатність системи до еволюційного розвитку шляхом інкрементального нарощування функціональних можливостей без необхідності кардинальної реінжинірингу існуючої архітектури. В умовах експоненційного зростання кількості підключених вузлів даний підхід забезпечує економічну доцільність модернізації інфраструктури відповідно до бюджетних обмежень. Модульна парадигма проектування, регламентована стандартами NIST[3], передбачає інтеграцію нових сенсорних мереж та сервісних підсистем з мінімальним впливом на операційну стабільність розгорнутої екосистеми, гарантуючи гнучкість адаптації до технологічних змін.

Критичним фактором ефективності є інтероперабельність, що інтерпретується як здатність гетерогенних апаратних платформ та програмних середовищ до коректного обміну даними та синтаксичної сумісності. Згідно з рекомендаціями Європейської комісії та консорціуму OASC[6], запобігання ефекту прив'язки до конкретного постачальника (vendor lock-in) досягається виключно через використання відкритих стандартів, уніфікованих моделей даних (NGSI-LD, SAREF) та публічних API. Забезпечення наскрізної сумісності дозволяє реалізувати конвергенцію даних між різними функціональними доменами — від транспортних систем до сектору охорони здоров'я, формуючи єдиний інформаційний простір міста.

Принцип орієнтації на користувача (User-Centricity) передбачає проектування цифрових сервісів на основі аналізу реальних потреб кінцевих бенефіціарів та забезпечення інклюзивності інтерфейсів взаємодії. У контексті

концепції smart city технологічні рішення розглядаються як інструментарій оптимізації якості життя, що вимагає прозорості алгоритмів надання послуг та наявності ефективних механізмів зворотного зв'язку. Для систем розумного будинку це реалізується через ергономічність керування, тоді як на муніципальному рівні — через уніфікацію доступу до адміністративних та комунальних сервісів.

Концепція Security by Design та Privacy by Design[6] імперативно вимагає інтеграції механізмів інформаційної безпеки та захисту персональних даних на етапі архітектурного проектування системи. Відповідно до директив NIST[3] та вимог GDPR, реалізація даного принципу передбачає впровадження системного ризик-менеджменту, застосування криптографічних протоколів, багаторівневої автентифікації та мінімізації обсягу оброблюваних даних. Проведення регулярних оцінок впливу на захист даних (DPIA)[5] є обов'язковою умовою легітимізації функціонування систем збору телеметрії у публічному просторі.

Відкритість даних та стандартизація API розглядаються як каталізатор інноваційного розвитку екосистеми. Політика Європейської комісії наголошує на необхідності публікації неперсоналізованих наборів міських даних у машиночитних форматах для стимулювання розробки сторонніх додатків та сервісів. Наявність уніфікованих платформ обміну даними створює передумови для формування ринку вторинних цифрових послуг, залучення приватного капіталу та розвитку локального IT-сектору.

Принцип стійкості (Resilience) та енергоефективності визначає здатність інфраструктури зберігати критичний функціонал в умовах деструктивних впливів, техногенних аварій або кібератак, одночасно оптимізуючи ресурсоспоживання. Стандарти smart city[6] передбачають впровадження відмовостійких архітектур з гарячим резервуванням компонентів та підтримкою режимів деградованої функціональності. На рівні розумного будинку це реалізується через інтеграцію з інтелектуальними енергомережами (smart grids), тоді як муніципальні системи (освітлення, транспорт) повинні забезпечувати

автономність роботи периферійних вузлів при втраті зв'язку з центром управління.

Підсумовуючи, зазначені принципи формують концептуальний базис проектування сучасних IoT-систем. Їх системна імплементація дозволяє створити масштабовану, інтероперабельну та захищеною інфраструктуру, що відповідає вимогам сталого розвитку та забезпечує баланс між технологічною ефективністю та захистом прав користувачів[3, 6].

Принципи масштабованості та модульності виступають фундаментальними детермінантами архітектурної стійкості систем «розумний дім» та «розумне місто», визначаючи їхній потенціал до еволюційного розвитку та адаптації в умовах динамічного технологічного ландшафту. Реалізація даних принципів передбачає проектування систем, здатних підтримувати інкрементальне нарощування обчислювальних потужностей та функціонального наповнення без необхідності реінжинірингу базової інфраструктури. Критичною вимогою є забезпечення інтеграції нових сенсорних вузлів та сервісних модулів з мінімальною латентністю та відсутністю негативного впливу на операційну стабільність діючих компонентів, що досягається шляхом застосування слабко зв'язаних архітектур (loosely coupled architectures)[3].

У контексті великомасштабних урбаністичних систем, де життєвий цикл впровадження IoT-рішень є тривалим, масштабованість забезпечується переходом від монолітних платформ до розподілених мікросервісних архітектур. Це дозволяє незалежно масштабувати окремі функціональні блоки (наприклад, підсистему обробки даних відеоспостереження або модуль керування вуличним освітленням) відповідно до поточного навантаження. Для побутового сегменту модульність реалізується через стандартизацію інтерфейсів взаємодії (API), що дозволяє користувачеві поетапно розширювати функціонал житла, інтегруючи пристрої різних поколінь та виробників у єдиний контур управління[6].

Технічна реалізація масштабованості також спирається на ієрархічну структуру обробки даних, що включає рівні хмарних обчислень (Cloud Computing) та периферійних обчислень (Edge/Fog Computing). Децентралізація

обчислень дозволяє знизити навантаження на магістральні канали зв'язку та центральні сервери, забезпечуючи горизонтальне масштабування системи за рахунок додавання нових периферійних шлюзів. Такий підхід регламентований стандартами NIST SP 800-183[3] (Networks of 'Things') та рекомендаціями ENISA[6], які визначають модульність як ключовий фактор забезпечення відмовостійкості: вихід з ладу одного модуля не призводить до каскадної відмови всієї екосистеми.

Таким чином, дотримання принципів модульності та масштабованості гарантує створення гнучких, економічно ефективних та довговічних IoT-екосистем, здатних інтегрувати інноваційні технології без порушення цілісності архітектури безпеки [31-42].

Забезпечення інтероперабельності — здатності гетерогенних апаратних та програмних компонентів до коректної взаємодії — є критичною умовою функціонування розподілених систем класу «розумний дім» та «розумне місто». Реалізація даного принципу базується на імплементації уніфікованих комунікаційних протоколів та стандартизованих моделей даних, що дозволяє подолати фрагментарність IoT-ландшафту та нівелювати ризики технологічної залежності від пропрієтарних рішень окремих вендорів (vendor lock-in). Відкрита архітектура взаємодії гарантує можливість безшовної інтеграції нового обладнання в існуючу інфраструктуру, забезпечуючи синтаксичну та семантичну сумісність на всіх рівнях моделі OSI[2].

Стратегічні директиви Європейської комісії визначають пріоритетність використання відкритих стандартів як каталізатора розвитку цифрових екосистем. Технічна реалізація інтероперабельності досягається шляхом застосування протоколів прикладного рівня, таких як MQTT[15], CoAP[16] та AMQP, які забезпечують ефективний обмін телеметрією в умовах обмеженої пропускної здатності каналів зв'язку. Для забезпечення семантичної сумісності, тобто однозначного тлумачення даних різними підсистемами, застосовуються онтологічні моделі та стандарти, зокрема NGSI-LD, розроблений ETSI[5], та еталонна архітектура IEEE P2413[2].

Згадані стандарти регламентують структуру інформаційних потоків, забезпечуючи уніфікацію інтерфейсів взаємодії між вертикальними доменами розумного міста (транспорт, енергетика, безпека). Такий підхід дозволяє реалізувати концепцію "системи систем" (System of Systems)[11], де дані, згенеровані в одному домені, можуть бути вільно використані в іншому для створення нових крос-функціональних сервісів. Імплементація принципів відкритості та стандартизації сприяє зниженню капітальних витрат (CAPEX) на інтеграцію та операційних витрат (OPEX) на підтримку інфраструктури, створюючи передумови для побудови стійкої, адаптивної та інноваційної цифрової платформи урбаністичного середовища[6].

Принцип орієнтації на користувача (User-Centric Approach) є визначальним фактором успішної інтеграції IoT-систем у соціальне середовище. Проектування інтерфейсів взаємодії «людина-машина» (HMI) у системах розумного дому та міста повинно базуватися на методології Human-Computer Interaction (HCI), що передбачає мінімізацію когнітивного навантаження на оператора та забезпечення інтуїтивної зрозумілості алгоритмів керування. Критичною вимогою є забезпечення інклюзивності цифрових сервісів, що досягається шляхом адаптації інтерфейсів відповідно до стандарту веб-доступності WCAG (Web Content Accessibility Guidelines) для користувачів з обмеженими можливостями та різним рівнем цифрової грамотності.

Технічна реалізація даного принципу передбачає мультимодальність каналів взаємодії: підтримку графічних інтерфейсів (GUI) через мобільні та веб-додатки, голосових інтерфейсів (VUI) на базі обробки природної мови (NLP), а також тактильних панелей керування. Така варіативність дозволяє адаптувати сценарії використання під контекст ситуації та індивідуальні преференції користувача. Забезпечення прозорості функціонування алгоритмів автоматизації є необхідною умовою для формування довіри до технології та подолання бар'єру відчуження інновацій (technology rejection).

У контексті урбаністичних систем орієнтація на користувача трансформується у концепцію «громадянин як сенсор» (Citizen-as-a-Sensor)[11],

де мешканці стають активними учасниками екосистеми, надаючи зворотний зв'язок через цифрові платформи. Системна імплементація принципів юзабіліті та доступності є передумовою для подолання цифрового розриву (digital divide), гарантуючи рівний доступ до переваг смарт-технологій для всіх демографічних груп населення.

Згідно з директивами Європейського агентства з мережевої та інформаційної безпеки (ENISA), імплементація механізмів захисту інформації повинна здійснюватися на превентивній основі, інтегруючись у всі етапи життєвого циклу розробки систем (SDLC)[6]. Парадигма Security by Design постулює відмову від реактивної моделі безпеки на користь проактивної архітектури, де захищеність є невід'ємною властивістю кожного компонента системи. Технічна реалізація даного підходу передбачає забезпечення наскрізного шифрування (End-to-End Encryption) каналів передачі даних з використанням протоколів TLS 1.2/1.3, а також застосування симетричних (AES-256) та асиметричних алгоритмів для захисту даних у стані спокою (Data at Rest)[3]. Критичним елементом є впровадження суворих політик контролю доступу (IAM) на основі рольової моделі (RBAC) та обов'язкової багатофакторної автентифікації (MFA) для адміністративних інтерфейсів[24].

Паралельно, принцип Privacy by Design регламентує алгоритми роботи з персональними даними (PII), базуючись на концепції мінімізації даних (Data Minimization)[5]. Це означає, що збір телеметрії повинен обмежуватися виключно обсягом, необхідним для виконання цільової функції сервісу. Архітектура системи має передбачати механізми псевдонімізації та анонімізації даних на етапі їх генерації (Edge Processing), що знижує ризики деанонімізації суб'єктів даних у разі витоку. Відповідність регламенту GDPR забезпечується наданням користувачеві повного контролю над власним цифровим профілем, включаючи технічну можливість реалізації прав на доступ, експорт та забуття даних (Right to be Forgotten)[6]. Інтеграція зазначених принципів формує фундамент довіреного середовища (Trusted Environment)[22], необхідного для легітимного функціонування систем розумного міста та житла.

Стратегія відкритих даних (Open Data Strategy) та уніфікація програмних інтерфейсів (API) виступають каталізаторами інноваційного розвитку екосистем розумного міста та житла, трансформуючи сирі масиви телеметрії у додану вартість. Архітектура муніципальних платформ повинна передбачати наявність публічного шлюзу API, реалізованого на базі архітектурних стилів RESTful або GraphQL, що забезпечує стандартизований доступ до агрегованих потоків даних з сенсорних мереж, геоінформаційних систем (GIS) та аналітичних модулів[11]. Такий підхід дозволяє стороннім розробникам та технологічним стартапам інтегруватися в цифрову інфраструктуру міста без необхідності побудови власної мережі збору даних, що суттєво знижує бар'єр входу та прискорює Time-to-Market для нових цифрових сервісів.

Публікація наборів даних (datasets) у машиночитних форматах (JSON, CSV, XML) на спеціалізованих порталах відкритих даних сприяє підвищенню прозорості муніципального управління та реалізації концепції Data-Driven Decision Making. Це створює передумови для розвитку Civic Tech проектів, де громадськість бере безпосередню участь у моніторингу ефективності міських служб[11]. Стандартизація API згідно з рекомендаціями Open API Specification (OAS) забезпечує синтаксичну сумісність та спрощує інтеграцію різнорідних систем, формуючи конкурентне середовище постачальників послуг та запобігаючи монополізації ринку smart-рішень. Імплементація даних принципів відповідає глобальним трендам цифрової трансформації, перетворюючи дані на стратегічний актив міської агломерації[25].

Забезпечення операційної стійкості (Operational Resilience) до деструктивних впливів техногенного, природного та кібернетичного характеру визначено пріоритетним вектором розвитку IoT-систем у стандартах ENISA[6] та IEEE[2]. Архітектура критичних підсистем розумного міста та житла повинна реалізовувати принципи відмовостійкості (Fault Tolerance) шляхом впровадження N+1 резервування апаратних компонентів та географічної диверсифікації центрів обробки даних. Ключову роль у забезпеченні безперервності надання сервісів (Business Continuity) відіграє технологія

периферійних обчислень (Edge Computing)[3], яка дозволяє локалізувати процеси прийняття рішень на рівні кінцевих шлюзів. Це гарантує автономне функціонування систем життєзабезпечення (енергопостачання, контроль доступу) навіть в умовах повної ізоляції від центральних хмарних платформ або деградації каналів зв'язку.

Паралельно, імперативом сучасного проектування є максимізація енергоефективності згідно з парадигмою Green IoT. Інтелектуальні алгоритми керування навантаженням (Demand Response) у системах Smart Grid дозволяють оптимізувати профілі енергоспоживання, згладжуючи пікові навантаження та інтегруючи розподілені джерела відновлюваної енергії. Впровадження адаптивних систем керування освітленням та кліматом на базі аналізу патернів поведінки користувачів сприяє суттєвому зниженню вуглецевого сліду урбаністичних агломерацій та операційних витрат (OPEX)[4]. Синергія механізмів кіберфізичної стійкості та енергетичної оптимізації формує фундамент для досягнення цілей сталого розвитку, забезпечуючи баланс між надійністю, економічною доцільністю та екологічною відповідальністю[6].

1.2 Архітектура IoT-системи: рівні, пристрої та протоколи

Концептуалізація архітектури систем Інтернету речей (IoT) виступає фундаментальною передумовою для проведення комплексного аналізу їх експлуатаційної надійності, інформаційної безпеки та потенціалу масштабування. Архітектурна модель детермінує принципи інтерконекту компонентів, специфікації каналів передачі даних та розподіл функціонального навантаження між вузлами гетерогенної мережі. Системне розуміння структурної ієрархії є необхідним інструментом для ідентифікації векторів загроз, оптимізації вибору технологічного стеку та проектування ешелонованих систем захисту.

На основі аналізу нормативної документації NIST SP 800-213[3] та стандартів IEEE[2], у роботі імплементовано п'ятирівневу референтну модель архітектури IoT, яка є де-факто стандартом у сучасній науково-технічній

літературі. Дана модель відображає повний цикл обробки даних: від первинної генерації телеметрії на периферії мережі, через етапи транзиту та агрегації, до фінальної аналітичної обробки та візуалізації у прикладних інтерфейсах. Кожен рівень архітектури характеризується унікальним набором функціональних вимог, обмежень ресурсів та специфічних вразливостей.

П'ятирівнева модель включає наступні стратифікаційні шари:

1. Рівень пристроїв (Device Layer) — фізичні сенсори та актуатори.
2. Мережевий рівень (Network Layer) — протоколи та канали комунікації.
3. Рівень периферійних обчислень (Edge/Fog Layer) — локальна попередня обробка даних.
4. Хмарний рівень (Cloud Layer) — централізоване зберігання та глибока аналітика.
5. Прикладний рівень (Application Layer) — інтерфейси взаємодії та бізнес-логіка.

Детальний аналіз функціональної взаємодії та протоколів кожного рівня є критично важливим для побудови стійкої екосистеми, здатної забезпечити цілісність, конфіденційність та доступність даних в умовах динамічного кіберпростору[3].

Рівень пристроїв, також відомий як рівень сприйняття (Perception Layer), становить фундамент архітектури Інтернету речей, забезпечуючи інтерфейс взаємодії між фізичним світом та цифровим середовищем. Функціональне призначення даного рівня полягає у конвертації фізичних величин у цифрові сигнали за допомогою перетворювачів (сенсорів) та зворотному перетворенні керуючих сигналів у механічні дії за допомогою виконавчих механізмів (актуаторів). Номенклатура компонентів включає датчики параметрів середовища (температури, вологості, газоаналізатори), інтелектуальні прилади обліку ресурсів (Smart Meters), системи відеоспостереження та електромеханічні реле[1].

Ключовою характеристикою обладнання даного рівня є суттєві апаратні обмеження (Constrained Devices)[3] у частині обчислювальної потужності (CPU), обсягу оперативної пам'яті (RAM) та енергоємності джерел живлення. Зазначені лімітації диктують необхідність використання оптимізованих протоколів комунікації персональних мереж (WPAN), таких як Zigbee (IEEE 802.15.4), Z-Wave та Bluetooth Low Energy (BLE). Згідно з технічними специфікаціями IEEE[2], дані стандарти реалізують енергоефективні алгоритми передачі даних, що забезпечує тривалий термін автономного функціонування пристроїв (до 5–10 років) від інтегрованих джерел живлення.

Специфіка апаратних обмежень формує унікальний ландшафт загроз на рівні пристроїв. Недостатність обчислювальних ресурсів ускладнює імплементацію стійких асиметричних криптографічних алгоритмів (RSA, ECC) та протоколів TLS, що призводить до використання спрощених схем автентифікації або передачі даних у відкритому вигляді[8]. Окрім кібернетичних векторів атак (експлуатація дефолтних облікових записів, перехоплення радіоефіру), критичним фактором ризику є фізична незахищеність периферійних вузлів (Physical Tampering), розміщених у публічному просторі, що створює загрозу несанкціонованого доступу до інтерфейсів налагодження (JTAG/UART) та екстракції прошивки[9].

Функціональне призначення мережевого рівня полягає у забезпеченні маршрутизації та надійного транспортування потоків даних між периферійними вузлами, концентраторами (шлюзами) та централізованими платформами обробки. Вибір комунікаційного стеку детермінується сукупністю технічних критеріїв, включаючи радіус покриття (Coverage Range), бюджет енергоспоживання (Power Budget), пропускну здатність каналу (Bandwidth) та вимоги до латентності (Latency). Коректна оцінка зазначених параметрів є передумовою для проектування ефективної мережевої топології гетерогенних систем[2].

Систематизація критеріїв вибору протоколів наведена у (Таблиці 1.2):

Таблиця 1.2

Порівняльна характеристика протоколів мережевого рівня

Критерій вибору	**Вплив на архітектуру**	**Релевантні протоколи**
Дальність передачі	Визначає топологію: PAN (Personal Area Network) vs WAN (Wide Area Network)	PAN:Zigbee, BLE, Wi-Fi WAN:LoRaWAN, NB-IoT, Sigfox
Енергоефективність	Критичний для автономних сенсорів (Battery-powered devices)	Висока:LoRaWAN, NB-IoT (10+ років) Низька:Wi-Fi, Cellular (LTE)
Пропускна здатність	Обмежує тип передаваних даних (відеопотік vs телеметрія)	Висока:Wi-Fi 6, 5G Низька:MQTT, CoAP over UDP
Модель взаємодії	Синхронна (Request-Response) vs Асинхронна (Pub/Sub)	Pub/Sub:MQTT Request-Response:CoAP, HTTP

Домінуючими протоколами прикладного рівня в екосистемі IoT є MQTT та CoAP. Протокол MQTT (Message Queuing Telemetry Transport), що функціонує поверх TCP/IP, реалізує асинхронну модель «видавець-підписник» (Publish/Subscribe)[15]. Згідно з рекомендаціями NIST[3], MQTT є стандартом де-факто для смарт-систем завдяки підтримці різних рівнів якості обслуговування (QoS 0/1/2), що гарантує доставку повідомлень навіть в умовах нестабільного з'єднання. Протокол CoAP (Constrained Application Protocol) базується на транспорті UDP і призначений для пристроїв з екстремальними обмеженнями ресурсів, надаючи RESTful-інтерфейс з мінімальним оверхедом заголовків пакетів[16].

Для організації фізичного рівня передачі даних у межах домогосподарств використовуються технології Mesh-мереж (Zigbee, Z-Wave, Thread), що забезпечують самоорганізацію та самовідновлення маршрутів[2]. У масштабах розумного міста застосовуються технології класу LPWAN (Low-Power Wide-Area Network), такі як LoRaWAN та NB-IoT, що дозволяють передавати невеликі обсяги телеметрії на відстані до 15–20 км з високою проникаючою здатністю у щільній міській забудові[11].

Ландшафт загроз мережевого рівня включає атаки типу Man-in-the-Middle (MITM), прослуховування трафіку (Sniffing) та підміну пакетів (Spoofing)[9]. Забезпечення конфіденційності та цілісності даних вимагає імплементації протоколів шифрування транспортного рівня (TLS/DTLS) та механізмів взаємної автентифікації вузлів[5].

Еволюція архітектурних парадигм IoT призвела до інтеграції проміжного рівня обробки даних, що реалізується через концепції Edge Computing (граничні обчислення) та Fog Computing (туманні обчислення), регламентовані стандартом IEEE 1934[2]. Функціональне призначення даного рівня полягає у децентралізації обчислювальних процесів, що дозволяє перенести навантаження з хмарних платформ безпосередньо до джерел генерації даних. Основні операції рівня включають нормалізацію протоколів (protocol translation), фільтрацію шумових даних, агрегацію телеметрії та локальну аналітику. Такий підхід забезпечує суттєву оптимізацію пропускної здатності магістральних каналів зв'язку (Backhaul bandwidth optimization) та мінімізацію мережевої латентності[3].

Для критично важливих систем розумного міста (інтелектуальні транспортні системи, моніторинг енергомереж) та систем фізичної безпеки житла, здатність до прийняття рішень у режимі реального часу (Real-time decision making) є визначальним фактором надійності[11]. Використання інтелектуальних шлюзів (Edge Gateways) забезпечує автономність функціонування локальних сегментів мережі: у випадку втрати з'єднання з центральною хмарною платформою, периферійні вузли зберігають здатність виконувати базові керуючі алгоритми. Це підвищує загальну кіберстійкість (Resilience) інфраструктури, нівелюючи ризики повної відмови сервісів (Single Point of Failure) при деградації глобальної мережі[6].

Ландшафт загроз рівня периферійних обчислень характеризується підвищеними ризиками компрометації шлюзів, які виступають точками концентрації потоків даних. Вразливість шлюзу може призвести до перехоплення чутливої інформації, несанкціонованої ін'єкції керуючих команд у

локальну мережу сенсорів або використання обчислювальних потужностей для організації ботнетів[9]. Забезпечення безпеки на даному рівні вимагає впровадження механізмів апаратної автентифікації (Secure Boot, TPM), шифрування локальних сховищ даних та сегментації мережевого трафіку для ізоляції скомпрометованих вузлів.

Хмарний рівень виконує роль центрального концентратора обчислювальних ресурсів, забезпечуючи агрегацію, довгострокове зберігання (Storage) та глибоку аналітичну обробку масивів даних (Big Data Analytics), згенерованих розподіленою сенсорною мережею. Згідно з архітектурними паттернами NIST[3], функціональне навантаження хмарної платформи охоплює реалізацію складних алгоритмів машинного навчання (ML) для виявлення кореляцій у гетерогенних потоках даних (наприклад, предиктивна аналітика транспортних заторів або моделювання пікових навантажень на енергомережу). Крім того, даний рівень забезпечує централізовану оркестрацію (Orchestration) IoT-пристроїв, управління життєвим циклом оновлень (OTA Updates) та інтеграцію зі сторонніми сервісами через стандартизовані API[11].

Архітектурна централізація робить хмарну платформу критичним елементом з точки зору інформаційної безпеки, оскільки вона агрегує найбільш чутливі дані та керуючі функції. Відповідно до класифікації ризиків ENISA[6] та NIST SP 800-213[3], порушення тріади CIA (конфіденційність, цілісність, доступність) на даному рівні здатне спричинити каскадну відмову всієї екосистеми розумного міста, включаючи параліч критичної інфраструктури та масовий витік персональних даних (Data Breach).

Стратегія захисту хмарного сегмента вимагає імплементації ешелонованої оборони (Defense-in-Depth). Обов'язковими заходами є впровадження суворої політики контролю доступу на основі ролей (RBAC), використання багатофакторної автентифікації (MFA) для адміністративного персоналу та застосування криптографічного захисту даних як у транзиті (TLS), так і у стані спокою (AES-256)[24]. Забезпечення високої доступності (High Availability) досягається через географічно розподілене резервування центрів обробки даних

(Geo-redundancy) та балансування навантаження. Постійний моніторинг аномалій у мережевому трафіку за допомогою SIEM-систем дозволяє оперативно виявляти та нейтралізувати спроби несанкціонованого доступу або DDoS-атаки[9,25].

Прикладний рівень, що займає найвищу позицію в ієрархії референтної моделі IoT, виконує функцію інтерфейсу взаємодії між користувачем та кіберфізичною системою. Його призначення полягає у візуалізації телеметричних даних, забезпеченні механізмів оперативного управління та реалізації бізнес-логіки автоматизації. Функціональний спектр рівня охоплює генерацію аналітичних звітів, відображення стану периферійних пристроїв у реальному часі через графічні інтерфейси (GUI) веб-порталів та мобільних додатків, а також інтеграцію зі сторонніми сервісами для реалізації крос-платформних сценаріїв[3].

Незважаючи на абстрагування від апаратних процесів, прикладний рівень є критичним вектором загроз. Згідно з даними досліджень ACM та звітів галузевих консорціумів, до 80% успішних атак на IoT-інфраструктуру ініціюються саме на цьому рівні через експлуатацію вразливостей програмного забезпечення та людський фактор[13]. Домінуючими загрозами є вразливості, класифіковані у OWASP Top 10[9] (наприклад, ін'єкції коду, міжсайтовий скриптинг XSS, незахищені API), а також атаки методами соціальної інженерії та фішингу, спрямовані на компрометацію облікових даних (Credential Theft). Відсутність надійної автентифікації та недоліки в механізмах авторизації (Broken Access Control) дозволяють зловмисникам отримати несанкціонований адміністративний доступ до всієї екосистеми[24].

Узагальнена характеристика п'ятирівневої архітектури із зазначенням компонентної бази, протоколів та специфічних ризиків наведена у (Таблиці 1.3):

Таблиця 1.3

Структурно-функціональна характеристика рівнів IoT-архітектури та вектори загроз

Рівень архітектури	**Основні компоненти**	**Типові протоколи**	**Ключові ризики безпеки**
Device Layer	Сенсори, актуатори, мікроконтролери	Zigbee, Z-Wave, BLE, NFC	Фізичний злом (Tampering), експлуатація дефолтних паролів
Network Layer	Маршрутизатори, комутатори, базові станції	MQTT, CoAP, Wi-Fi, LoRaWAN, NB-IoT	Eavesdropping (прослуховування), Man-in-the-Middle, Spoofing
Edge/Fog Layer	Інтелектуальні шлюзи, локальні сервери	OPC UA, Modbus TCP, Edge-native protocols	Компрометація вузлів агрегації, ін'єкція шкідливого коду
Cloud Layer	ЦОД, кластери баз даних, аналітичні платформи	REST,gRPC, AMQP, Kafka	Data Breach, DDoS-атаки, незахищені API endpoints

1.3 Загрози, вразливості та типи атак на IoT-системи

Комплексна ідентифікація векторів загроз та механізмів реалізації кібератак є фундаментальною умовою проектування стійких систем класу «розумний дім» та «розумне місто». Специфіка архітектури Інтернету речей детермінує формування екстенсивної та фрагментованої поверхні атак (Attack Surface), що охоплює гетерогенний парк кінцевих пристроїв[7]. Аналіз звітів провідних аналітичних агентств за період 2024–2025 років демонструє зростання кількості інцидентів безпеки в сегменті IoT на 107%, із фіксацією середньодобового показника спроб компрометації на рівні 820 000 подій[14]. Наведені емпіричні дані свідчать про ескалацію рівня кіберзагроз та необхідність імплементації багаторівневих стратегій захисту.

Ландшафт загроз (Threat Landscape) визначається сукупністю структурних факторів. По-перше, домінування парадигми Time-to-Market у виробничих процесах призводить до нехтування вимогами безпеки на користь функціональності (Security by Obscurity). По-друге, технологічна гетерогенність екосистеми — варіативність апаратних платформ, операційних систем та комунікаційних протоколів — унеможливлює застосування уніфікованих паттернів захисту[3]. По-третє, складність управління життєвим циклом (Patch Management) у розподілених інфраструктурах створює передумови для тривалої експлуатації відомих вразливостей (N-day vulnerabilities)[13].

У даному підрозділі здійснено систематизацію ключових загроз відповідно до рівнів референтної архітектури IoT. Класифікація вразливостей базується на таксономіях OWASP IoT Top 10[9], NIST SP 800-213[3] та рекомендаціях ENISA[6]. Такий підхід дозволяє структурувати знання про вектори атак та визначити пріоритетні контрзаходи для забезпечення цілісності, конфіденційності та доступності критичних систем.

Стратифікація загроз відповідно до архітектурних рівнів є методологічною основою для розробки цільових стратегій мінімізації ризиків. Аналіз векторів атак дозволяє ідентифікувати специфічні вразливості компонентів та застосувати диференційовані контрзаходи.

Рівень пристроїв (Device Layer) характеризується домінуванням загроз, пов'язаних з фізичною та логічною незахищеністю кінцевого обладнання.

- Hardcoded Credentials: Експлуатація статичних облікових записів адміністратора (наприклад, admin/admin), інтегрованих у прошивку виробником, залишається критичним вектором атак, що дозволяє отримати root-доступ без застосування методів перебору паролів.
- Firmware Extraction: Фізичний доступ до інтерфейсів налагодження (JTAG, UART, SPI) дозволяє здійснити дамп пам'яті пристрою, декомпілювати код та вилучити криптографічні ключі або сертифікати, що компрометує всю серію пристроїв.

- Insecure Defaults: Наявність відкритих мережевих портів (Telnet, SSH) та увімкнених служб налагодження (UPnP) за замовчуванням створює умови для автоматизованого сканування та інфікування пристроїв ботнет-мережами (наприклад, Mirai).

Мережевий рівень (Network Layer) піддається атакам на цілісність та конфіденційність каналів зв'язку.

- Eavesdropping / Sniffing: Передача телеметрії та керуючих команд у незашифрованому вигляді (HTTP, MQTT без TLS) дозволяє пасивно перехоплювати чутливі дані.
- Man-in-the-Middle (MITM): Активне втручання у сесію зв'язку шляхом ARP-спуфінгу або підробки DNS-записів дозволяє модифікувати дані "на льоту" або здійснювати підміну команд.
- Distributed Denial of Service (DDoS): Використання ресурсів скомпрометованих IoT-пристроїв для генерації аномальних обсягів трафіку (UDP Flood, SYN Flood), спрямованих на виведення з ладу критичних сервісів.

Рівень периферійних обчислень та хмари (Edge/Cloud Layer) концентрує загрози централізованого управління та зберігання даних.

- Single Point of Failure: Компрометація периферійного шлюзу надає зловмиснику повний контроль над локальним сегментом мережі та можливість горизонтального переміщення (Lateral Movement) до ізольованих підмереж.
- Cloud Misconfiguration: Некоректне налаштування прав доступу до об'єктних сховищ (наприклад, відкриті S3 buckets) або баз даних є основною причиною масових витоків даних (Data Leakage).
- Insecure API: Відсутність обмежень частоти запитів (Rate Limiting) та слабка автентифікація API-інтерфейсів створюють умови для несанкціонованого доступу до бекенд-систем.

Прикладний рівень (Application Layer) є найбільш вразливим до атак, спрямованих на логіку роботи додатків та людський фактор.

- Broken Authentication & Session Management: Недоліки реалізації механізмів сесій (передбачувані ID сесій, відсутність таймаутів) дозволяють перехоплювати контроль над акаунтами користувачів (Account Takeover).
- Injection Attacks: Вразливості типу SQL Injection та Command Injection у веб-інтерфейсах дозволяють виконувати довільний код на сервері.
- Social Engineering: Фішингові кампанії, спрямовані на викрадення облікових даних користувачів, залишаються високоефективним методом первинного проникнення в систему, оскільки до 80% інцидентів ініціюються через компрометацію легітимних акаунтів.

Проект OWASP (Open Web Application Security Project) розробив спеціалізований перелік найбільш критичних вразливостей екосистеми Інтернету речей, який слугує де-факто стандартом для аудиту безпеки та моделювання загроз. Дана класифікація базується на аналізі реальних інцидентів та систематизує вектори атак за ступенем їх поширеності та критичності наслідків[9].

I1: Слабкі, вгадувані або жорстко закодовані паролі (Weak, Guessable, or Hardcoded Passwords). Домінування даної вразливості зумовлене практикою використання виробниками ідентичних облікових записів (admin/admin) для цілих серій пристроїв. Як продемонстрував ботнет Mirai, автоматизований брутфорс по словнику дозволяє скомпрометувати мільйони хостів за лічені години, перетворюючи їх на вузли DDoS-атак.

I2: Незахищені мережеві сервіси (Insecure Network Services). Наявність на пристроях активних служб, що не є необхідними для штатного функціонування (Telnet, FTP, UPnP), створює додаткові вектори для експлуатації переповнення буфера або виконання довільного коду. Відкриті порти без належного контролю доступу дозволяють зловмисникам ідентифікувати тип пристрою та версію ПЗ.

I3: Незахищені інтерфейси екосистеми (Insecure Ecosystem Interfaces). Вразливості у зовнішніх точках входу — веб-панелях, хмарних API та мобільних додатках. Відсутність валідації вхідних даних призводить до атак типу SQL

Injection та XSS, а слабка автентифікація API дозволяє отримати доступ до бекенд-систем.

I4: Відсутність механізму безпечного оновлення (Lack of Secure Update Mechanism). Критична архітектурна вада, що унеможливлює виправлення знайдених багів. Відсутність перевірки цифрового підпису прошивки дозволяє зловмисникам впровадити модифікований образ ПЗ із бекдором під виглядом легітимного оновлення (Firmware Downgrade Attack).

I5: Використання застарілих компонентів (Use of Insecure or Outdated Components). Інтеграція у прошивку сторонніх бібліотек (Third-party libraries) з відомими CVE-вразливостями, підтримка яких припинена розробниками, створює ризики Supply Chain атак.

I6: Недостатній захист конфіденційності (Insufficient Privacy Protection). Збір надлишкової телеметрії без належної анонімізації та механізмів отримання згоди користувача порушує вимоги GDPR та створює загрози деанонімізації суб'єктів даних.

I7: Незахищена передача та зберігання даних (Insecure Data Transfer and Storage). Зберігання ключів шифрування та персональних даних у відкритому вигляді у флеш-пам'яті пристрою, а також передача трафіку без використання протоколів TLS, робить дані вразливими до перехоплення та крадіжки.

I8: Відсутність управління пристроями (Lack of Device Management). Неможливість моніторингу стану парку пристроїв, відсутність інструментів інвентаризації та дистанційного відкликання скомпрометованих сертифікатів ускладнює реагування на інциденти.

I9: Небезпечні налаштування за замовчуванням (Insecure Default Settings). Постачання пристроїв із максимально пермісивними правами доступу (running as root) та вимкненими функціями безпеки змушує користувача самостійно "закручувати гайки", що часто ігнорується.

I10: Відсутність фізичного захисту (Lack of Physical Hardening). Наявність відкритих інтерфейсів налагодження (JTAG, UART) дозволяє зловмисникам

отримати прямий доступ до ядра системи при фізичному контакті з пристроєм, що є типовим сценарієм для вуличних камер та сенсорів.

Систематизація описаних вразливостей наведена у (Таблиці 1.4)

Таблиця 1.4

Класифікація вразливостей згідно з OWASP IoT Top 10

Ранг	**Вразливість**	**Технічний опис**	**Вплив на систему**
I1	Weak Passwords	Default credentials, hardcoded keys	RCE, Botnet recruitment
I2	Insecure Network Services	Open ports (Telnet/SSH), UPnP	Buffer Overflow, DoS
I3	Insecure Interfaces	Insecure Web/Cloud/Mobile API	Data Breach, Unauthorized Access
I4	No Secure Updates	Lack of firmware signing, anti-rollback	Persistent compromise
I5	Outdated Components	EOL libraries, known CVEs	Supply Chain Attacks
I6	Insufficient Privacy	Excessive PII collection	GDPR violation, Identity Theft
I7	Insecure Data Transfer	Cleartext storage, lack of encryption	Eavesdropping, Credential Theft
I8	No Device Management	No asset tracking, audit logs	Delayed Incident Response
I9	Insecure Defaults	Permissions as root, verbose logging	Privilege Escalation
I10	Physical Hardening	Exposed JTAG/UART ports	Firmware Extraction, Cloning

Розуміння векторів атак — специфічних шляхів та методів, які зловмисники використовують для експлуатації вразливостей, є необхідною умовою для побудови ешелонованого захисту. Сучасні сценарії атак на IoT

варіюються від автоматизованого сканування портів до таргетованих операцій класу APT (Advanced Persistent Threat)[13,14].

Brute-Force атаки та формування ботнетів. Вектор базується на автоматизованому переборі автентифікаційних даних (Dictionary Attack) за протоколами SSH та Telnet. Парадигматичним прикладом реалізації даного вектору є ботнет Mirai (2016), шкідливе ПЗ якого сканувало публічний діапазон IPv4-адрес, виявляючи пристрої з дефолтними обліковими записами BusyBox. Інфіковані хости об'єднувалися у децентралізовану мережу (C&C), сумарна потужність якої перевищувала 600 000 вузлів. Це дозволило реалізувати безпрецедентні за масштабом атаки на інфраструктуру DynDNS, демонструючи критичність проблеми Hardcoded Credentials.

Man-in-the-Middle (MITM) атаки. Технічна реалізація включає перехоплення сесії зв'язку (Session Hijacking) шляхом розгортання підроблених точок доступу (Rogue Access Point / Evil Twin) або використання технік ARP/DNS Spoofing у локальній мережі. У контексті розумного будинку це створює ризики ін'єкції нелегітимних команд (Replay Attack), наприклад, для відключення сигналізації, оскільки багато застарілих протоколів IoT не підтримують взаємну автентифікацію та перевірку цілісності повідомлень (Message Integrity Check)[5,15].

Distributed Denial-of-Service (DDoS). Використання ресурсів скомпрометованих IoT-пристроїв для генерації волюметричних атак (Volumetric Attacks) є домінуючою загрозою доступності сервісів. Інцидент з атакою на хостинг-провайдера OVH (2016) з піковим навантаженням понад 1 Tbps підтвердив здатність IoT-ботнетів генерувати трафік, що перевищує пропускну здатність магістральних каналів. Для систем розумного міста (Smart Grid, Traffic Control) такі атаки становлять загрозу національного масштабу, здатну паралізувати функціонування критичної інфраструктури[7,26].

Ін'єкції коду (SQL/Command Injection). Вектор спрямований на експлуатацію вразливостей валідації вхідних даних у веб-інтерфейсах та API хмарних платформ. Успішна SQL-ін'єкція надає зловмиснику несанкціонований

доступ до централізованих баз даних (Data Exfiltration), що містять персональні профілі громадян та конфігураційні параметри інфраструктури.

Атаки на критичну інфраструктуру (Cyber-Physical Attacks). Хрестоматійний приклад хробака Stuxnet (2010) продемонстрував вразливість промислових контролерів (PLC/SCADA) до складних атак із використанням експлойтів нульового дня (Zero-Day). Шкідливе ПЗ модифікувало логіку роботи частотних перетворювачів, залишаючись невидимим для систем моніторингу, що призвело до фізичного руйнування обладнання. Цей прецедент довів можливість кінетичного впливу через кіберпростір.

Supply Chain Attacks. Компрометація ланцюга постачання (впровадження бекдорів на етапі виробництва або модифікація оновлень ПЗ) дозволяє обійти периметрові засоби захисту, оскільки шкідливий код має легітимний цифровий підпис довіреного вендора.

Висновок до першого розділу

В першому розділі було досліджено, як традиційна житлово-комунальна інфраструктура та міські системи управління трансформуються у відкриті екосистеми, інтегровані інформаційні технології та керовані потоки даних у реальному часі. Аналіз архітектурних принципів, запропонованих міжнародними організаціями та стандартами, показав, що масштабованість, модульність та взаємозв'язок між усіма компонентами виступають ключовими факторами успішного впровадження смарт-рішень. Однак кожен із цими принципами забезпечує певні компроміси: прагнення до гнучкості та розширюваності системи часто зменшує її захищеність від зовнішніх впливів, а відкритість до інноваційних рішень забезпечує поверхню негативних наслідків.

Детальне дослідження структури IoT-системи на п'яти рівнях архітектури виявило, що кожен із цих шарів має відповідні різні характеристики та свої слабкі місця. Периферійні датчики та пристрої, обмежені енергією та обчислювальною потужністю, не можуть задіяти складні методи шифрування, що робить їх вразливими до використання простих помилок у налаштуваннях та фізичного

несанкціонованого доступу. Мережевий рівень, через який передаються дані між компонентами, постійно піддається ризикам перехоплення та модифікації інформації, особливо коли канали передачі даних не захищені належним чином. Проміжні обчислювальні вузли, хоча й призначені для прискорення обробки інформації на місцевому рівні, парадоксально залишаються критичними точками вразливості, оскільки саме там накопичується велика кількість чутливих даних. Центральні хмарні платформи агрегують найбільш важливу інформацію та керуючі функції, тому їх порушення може паралізувати роботу всієї системи та призвести до масових витоків персональних даних. В кінці, прикладні інтерфейси, хоча й видаються найвіддаленішими від апаратної частини, часто залишаються найпростішою мішенню для нападу, порушуючи саме тут людський фактор та помилки в програмній логіці створюють найбільші можливості для проникнення.

Комплексний аналіз загроз та вразливостей, заснований на дослідженні реальних кібератак, продемонстрував, що сучасні атаки на IoT-системи спрямовані на всі рівні архітектури одночасно. Історичні приклади, від масового зараження мільйонів пристроїв ботнетами до цілеспрямованих атак на критичну інфраструктуру, показують, що зловмисники активно використовують як технічні недоліки у коді так і організаційні помилки у тому, як керуються пристроями та даними. Особливо серйозною проблемою є те, що IoT-обладнання часто працює дуже довго, а витрати на виправлення та оновлення багатьох пристроїв дуже високі, тому невразливості, про які люди давно знають, залишаються актуальною загрозою.

Підсумовуючи результати першого розділу, можна констатувати, що проблема безпеки в системах «розумний дім» та «розумне місто» не є суто технічною проблемою, а охоплює складне переплетення технічних рішень, процесів управління, нормативного регулювання та людських факторів. Знання про архітектуру IoT-системи та розуміння характеру загроз, які виявляються на кожному рівні, дають необхідну основу для розробки ефективних методів

захисту та практичних стратегій управління ризиками, які будуть більш детально відзначені в наступних розділах цієї роботи.

Розділ 2. АНАЛІЗ ПРАКТИЧНИХ РИЗИКІВ І РЕАЛЬНИХ АТАК НА СИСТЕМИ «РОЗУМНИЙ ДІМ/МІСТО»

2.1 Методологія оцінки та аналізу ризиків

Формалізація процесу управління інформаційною безпекою в гетерогенних IoT-середовищах вимагає застосування системного підходу до ідентифікації, класифікації та квантифікації ризиків. Методологічний базис дослідження спирається на стандарти NIST SP 800-30 (Guide for Conducting Risk Assessments)[7] та настановчі документи ENISA, що визначають ризик-менеджмент як ітеративний процес, спрямований на мінімізацію ймовірності настання негативних подій та їхніх наслідків.

Базова модель оцінки ризику R може бути представлена як функція від трьох змінних: активів A, вразливостей V та загроз T:

$$R=f(A,V,T)$$

На практичному рівні величина ризику (Risk Magnitude) визначається як добуток ймовірності реалізації загрози (Likelihood) на ступінь потенційного впливу (Impact)[23]:

$$Risk=Likelihood\times Impact$$

Процес оцінки включає етап ідентифікації активів (Asset Identification), що передбачає категоризацію компонентів системи за ступенем їх критичності[3]. Для екосистеми розумного житла до критичних активів віднесено підсистеми фізичного доступу, відеоспостереження та масиви персональних даних (PII). У масштабах розумного міста пріоритетними об'єктами захисту є системи SCADA/ICS управління енерго- та водопостачанням, інтелектуальні транспортні системи (ITS) та муніципальні бази даних[26].

Для візуалізації та пріоритизації загроз застосовується метод Матриці ризиків (Risk Matrix)[7]. Даний інструмент дозволяє ранжувати ідентифіковані загрози шляхом зіставлення рівнів ймовірності (Low, Medium, High) та впливу

(Low, Medium, High, Critical). Ризики, що потрапляють у "червону зону" матриці (висока ймовірність / критичний вплив), класифікуються як неприйнятні та вимагають негайної імплементації контрзаходів (Risk Mitigation)[25]. Ризики середнього рівня підлягають плановому усуненню, тоді як низькі ризики можуть бути прийняті (Risk Acceptance) за умови постійного моніторингу.

2.2 Реальні приклади кібератак на IoT-системи розумних міст та домів

Аналіз емпіричних даних інцидентів інформаційної безпеки підтверджує статус IoT-екосистем як пріоритетного вектору атак для кіберзлочинних угруповань. Дослідження ретроспективних кейсів дозволяє ідентифікувати патерні компрометації та оцінити кінетичний вплив на критичну інфраструктуру.

Інцидент з ботнетом Mirai (2016) став поворотним моментом у розумінні загроз, пов'язаних з масовим розгортанням незахищених IoT-пристроїв. Вектор розповсюдження шкідливого програмного забезпечення базувався на скануванні портів 23 (Telnet) та 2323 з наступним застосуванням словникової атаки (Dictionary Attack) по списку з 62 пар дефолтних облікових даних (наприклад, admin/admin, root/12345), характерних для пристроїв на базі BusyBox (IP-камери, DVR, маршрутизатори). Успішна автентифікація дозволяла завантажити бінарний файл коригування, який перетворював пристрій на вузол розподіленої мережі (Botnet) під управлінням командно-контрольного сервера (C2)[9,14].

Масштаб інциденту характеризується безпрецедентними показниками об'ємних атак (Volumetric DDoS). У вересні 2016 року атака на ресурс "Krebs on Security" досягла пікового значення 623 Гбіт/с, а згодом атака на провайдера OVH зафіксувала рекордні 1.1 Тбіт/с. Кульмінацією стала атака на інфраструктуру DNS-провайдера Dyn, яка спричинила відмову в обслуговуванні для значної частини інтернет-сервісів на східному узбережжі США.

Оприлюднення вихідного коду Mirai призвело до проліферації модифікованих версій (variants), адаптованих для експлуатації нових вразливостей. Згідно зі звітом ENISA, цей прецедент підтвердив, що сукупна

обчислювальна потужність мільйонів скомпрометованих IoT-пристроїв становить стратегічну загрозу для стабільності глобальної мережі Інтернет.

Сектор енергетичної інфраструктури є пріоритетною ціллю для APT-угруповань, орієнтованих на дестабілізацію критичних сервісів. Хрестоматійним прикладом кінетичного впливу на системи Smart Grid є серія атак на енергетичний комплекс України[14,26].

У грудні 2015 року було реалізовано першу у світі підтверджену кібератаку на енергосистему (BlackEnergy). Вектор первинного проникнення базувався на фішинговій розсилці (Spear Phishing) з шкідливим вкладенням, що дозволило скомпрометувати корпоративний сегмент мережі. Після етапу горизонтального переміщення (Lateral Movement) та ескалації привілеїв, зловмисники отримали доступ до SCADA-систем. Операція завершилася дистанційним відключенням підстанцій через інтерфейси HMI, що призвело до знеструмлення близько 230 000 абонентів.

У 2016 році атака повторилася із застосуванням спеціалізованого шкідливого ПЗ Industroyer (CrashOverride), розробленого безпосередньо для взаємодії з промисловими протоколами (IEC 60870-5-101/104, IEC 61850). Цей інцидент продемонстрував еволюцію інструментарію зловмисників від використання стандартних адміністративних утиліт до розробки модульного кіберзброї, здатної автоматизовано керувати комутаційним обладнанням.

Основною причиною успішності даних атак є наявність застарілих (legacy) компонентів у системах АСУ ТП, відсутність суворої ізоляції технологічних мереж (Air Gap) та складнощі з регулярним оновленням ПЗ (Patch Management) на критично важливому обладнанні, зупинка якого для обслуговування є неприпустимою.

Цифровізація транспортної інфраструктури створює нові вектори загроз, пов'язані з маніпуляцією даними у реальному часі. Системи розумного паркування та керування трафіком, що базуються на розподілених сенсорних мережах, є вразливими до атак на цілісність даних (Integrity Attacks)[7,9].

Дослідження безпеки інфраструктури Smart Parking (2019) виявили критичні вразливості у протоколах обміну даними між паркувальними сенсорами та шлюзами агрегації. Відсутність наскрізного шифрування та слабка автентифікація дозволили реалізувати сценарії Sensor Spoofing, коли зловмисник емулює сигнали зайнятості паркомісць. Це призводить до дезінформації водіїв, штучного створення заторів та фінансових збитків операторів паркувального простору.

Більш критичними є загрози для автоматизованих систем керування дорожнім рухом (Traffic Signal Control Systems). Компрометація контролерів світлофорних об'єктів через незахищені бездротові інтерфейси (часто використовуються незашифровані радіоканали 5.8 GHz або 900 MHz) може призвести до одночасного включення дозвільного сигналу на перехрестях, що створює безпосередню загрозу життю та здоров'ю громадян (Public Safety Risk)[26]. Такі сценарії класифікуються як кіберфізичні атаки з високим ступенем кінетичного впливу.

У сегменті Smart Home зростає кількість інцидентів, пов'язаних з несанкціонованим доступом до систем відеоспостереження та контролю доступу (Smart Locks)[14]. Вразливості у протоколах автентифікації хмарних платформ (наприклад, Ring, Nest) та масова практика перевикористання паролів (Password Reuse) створюють передумови для атак типу Credential Stuffing.

Успішна компрометація дозволяє зловмисникам здійснювати несанкціонований відеомоніторинг (Unauthorized Surveillance) та аудіоперехоплення. Критичним наслідком є можливість проведення аналізу життєвих патернів мешканців (Pattern of Life Analysis) — визначення графіків присутності вдома, періодів відпусток та розпорядку дня. Ця інформація використовується кримінальними елементами для планування квартирних крадіжок (Burglary), мінімізуючи ризики зустрічі з господарями.

У 2020 році правоохоронні органи США зафіксували серію інцидентів ("Smart Home Hijacking"), де зловмисники дистанційно деактивували системи сигналізації та розблоковували смарт-замки перед фізичним проникненням. Крім

майнових збитків, такі атаки завдають значної психологічної шкоди жертвам, підриваючи відчуття безпеки у власному житлі (Digital Harassment).

Україна стала полігоном для відпрацювання методів кібернетичного впливу на критичну інфраструктуру в умовах повномасштабного військового конфлікту. Атаки на енергетичний сектор (2015–2016) створили прецедент конвергенції кібернетичних та фізичних загроз (Cyber-Physical Convergence), де компрометація промислових систем управління (ICS/SCADA) використовувалася як інструмент державного тиску (State-Sponsored Attacks).

В умовах воєнного стану суттєво трансформувався ландшафт загроз для цивільних IoT-систем. Зафіксовано численні випадки використання вразливих IP-камер зовнішнього відеоспостереження (CCTV) ворожими спецслужбами для ведення тактичної розвідки (Intelligence Gathering) та коригування ракетних ударів. Це демонструє, що технології подвійного призначення (Dual-Use Technologies) у цивільному секторі можуть становити загрозу національній безпеці при недостатньому рівні захисту[21,26].

Згідно зі звітом CERIDAP (2025), прискорена цифровізація муніципального управління в Україні часто відбувалася з пріоритетом швидкості впровадження сервісів (Time-to-Market), що призвело до накопичення "технічного боргу" у сфері безпеки. Системи Smart City, розгорнуті без врахування вимог воєнного часу, демонструють підвищену вразливість до деструктивних впливів, що вимагає перегляду архітектурних підходів до побудови муніципальних цифрових екосистем з урахуванням факторів кіберстійкості (Cyber Resilience).

2.3 Аналіз наслідків та оцінка впливу атак (Impact Assessment)

Квантифікація наслідків реалізації кіберзагроз є інтегральною складовою процесу управління ризиками. Вплив (Impact) інцидентів інформаційної безпеки на екосистеми IoT класифікується за масштабом ураження та характером заподіяної шкоди.

На рівні домогосподарства (Smart Home Impact Analysis):

- Privacy Violation: Несанкціонований збір аудіовізуальної інформації та метаданих про спосіб життя мешканців призводить до порушення конституційних прав на недоторканність приватного життя.
- Physical Safety Risks: Дистанційна деактивація систем охоронної сигналізації або маніпуляція кліматичним обладнанням (наприклад, відключення опалення взимку) створює пряму загрозу здоров'ю та майну власників.
- Financial Loss: Прямі фінансові збитки внаслідок крадіжок, шахрайства з платіжними даними або збільшення рахунків за комунальні послуги через роботу пристроїв у складі ботнетів (Cryptojacking).

На муніципальному рівні (Smart City Impact Analysis):

- Critical Infrastructure Disruption: Атаки на системи життєзабезпечення (енерго-, водопостачання, транспорт) характеризуються каскадним ефектом (Cascading Effect), коли відмова одного елемента провокує ланцюгову реакцію в суміжних секторах, що може призвести до гуманітарної катастрофи.
- Economic Damage: Згідно з оцінками ENISA, середньозважена вартість ліквідації наслідків успішної атаки на об'єкт критичної інфраструктури становить 2.7 млн USD. Ця сума включає витрати на Incident Response, відновлення цілісності даних, юридичний супровід та компенсаційні виплати.
- Reputational & Social Impact: Втрата довіри громадян до цифрових сервісів муніципалітету та дестабілізація суспільно-політичної ситуації внаслідок перебоїв у наданні базових послуг.

Для українських муніципалітетів, що функціонують в умовах дефіциту бюджетних ресурсів, реалізація ризиків високого рівня (High Impact) може призвести до тривалого паралічу адміністративних функцій, що підкреслює необхідність превентивного інвестування в системи кіберстійкості.

2.4 Матриця ризиків та пріоритизація загроз для IoT-систем

На основі емпіричного аналізу векторів атак та оцінки потенційного деструктивного впливу розроблено адаптовану матрицю ризиків для екосистем «розумний дім» та «розумне місто». Даний інструмент забезпечує візуалізацію ландшафту загроз у системі координат «Ймовірність реалізації» (Likelihood) — «Ступінь впливу» (Impact), що дозволяє формалізувати процес прийняття рішень щодо розподілу ресурсів на імплементацію контрзаходів.

Класифікація ризиків здійснюється за чотирма квадрантами пріоритетності:

1. Критичні ризики (Critical Severity): Характеризуються високою частотою реалізації та катастрофічними наслідками. До цієї категорії віднесено автоматизовані атаки на автентифікацію (Brute-force/Dictionary Attacks), волюметричні DDoS-атаки з використанням ботнет-мереж, компрометацію централізованих хмарних платформ та масовий витік персональних даних (PII). Стратегія обробки даних ризиків передбачає негайну імплементацію коригувальних заходів (Immediate Mitigation)[25,7].

2. Високі ризики (High Severity): Включають вектори атак із середньою ймовірністю, але значним впливом на операційну діяльність. Сюди належать фізичне втручання у роботу периферійного обладнання (Physical Tampering), соціоінженерні атаки (Phishing) та експлуатація вразливостей у застарілих програмних компонентах (Legacy Software). Дана категорія вимагає розробки планів мінімізації у короткостроковій перспективі[8,9].

3. Ризики «Чорний лебідь» (High Impact / Low Probability): Загрози з низькою ймовірністю реалізації, але катастрофічним потенціалом впливу. До них належать цільові атаки з використанням вразливостей нульового дня (Zero-day exploits), атаки на ланцюг постачання (Supply Chain Attacks) та державно-спонсоровані операції проти критичної інфраструктури. Стратегія захисту базується на впровадженні систем виявлення аномалій та розробці планів аварійного відновлення (Disaster Recovery Plans)[22,25].

4. Операційні ризики (Low Severity): Включають незначні конфігураційні помилки та локальні технічні збої, що не мають системного впливу. Для даної категорії застосовується стратегія прийняття ризику (Risk Acceptance) за умови постійного моніторингу.

Систематизація ризиків у вигляді матриці дозволяє перейти від реактивної моделі безпеки до ризик-орієнтованого підходу, забезпечуючи адекватність захисних заходів реальним загрозам[6,25].

Висновок до другого розділа

В другому розділі був проведений комплексний аналіз практичних ризиків та реальних інцидентів, який демонструє глибоку розбіжність між теоретичними моделями безпеки та тим, як фактично розгортаються атаки на IoT-екосистеми в умовах реального світу. Методологічна основа дослідження, виконана за стандартами NIST та ENISA, дозволила формалізувати процеси оцінки ризиків через математичний аналіз між активами, вразливостями та загрозами, однак емпіричні дані показують, що найнебезпечніші атаки часто обирають шляхи найменшого опору, експлуатуючи архітектурні компроміси та організаційні дефекти замість звернення до складних технічних експлойтів. Аналіз ретроспективних кейсів від ботнету Mirai до атаки на енергетичну інфраструктуру України засвідчив, що сукупна обчислювальна потужність навіть слабко захищених IoT-пристроїв стає стратегічною загрозою для критичних систем на національному та глобальному рівнях.

Історичні приклади, як інструменти в розділі, розкрили закономірність, за якою еволюцію зловмисників нерідко випереджає розвиток механізмів захисту. Ботнет Mirai припинив експлуатацію дефолтних паролів у масовому феномені, який досі залишається основним вектором компрометації; атаки BlackEnergy та Industroyer на енергосистему України показали, що розробники зловмисників готові інвестувати у створення спеціалізованої кіберзброї для досягнення політичних цілей; а інциденти в сегменті Smart Home показали, що приватна сфера громадян не є забезпеченою від цифрового втручання та що технічна

безпека часто приймається у жертву зручності користувача. Особливо тривожним є закономірність: системи, розгорнуті у спіш та з оптимальною функціональністю, накопичують такий обсяг технічного боргу у сфері безпеки, що їх наступне коригування стає дорогим та технічно складним.

Оцінка наслідків атак на різних рівнях архітектури показала, що вплив компрометації масштабується залежно від критичності ураженої системи. Для домогосподарств несанкціонований доступ до відеокамер та смарт-замків не лише порушує приватність, а й трансформує житлове середовище в простір для аналізу життєвих патернів із плануванням призначення крадіжок; для муніципалітетів атаки на енергосистеми, водопостачання чи транспортну логістику створюють каскадні ефекти, коли відмова одного компонента запускає ланцюгову реакцію відмов у суміжних секторах, викликану гуманітарними катастрофами. Дослідження показало, що середньозважена вартість ліквідації наслідків успішної атаки на критичну інфраструктуру переважає мільйони доларів США, не враховуючи невимірних соціальних та репутаційних збитків.

Розроблена матриця ризиків, яка систематизує загрози за ступенями вірогідності та впливу, надала структурований інструмент для переходу від реактивного реагування на інциденти до проактивного управління ризиками. Критичні загрози, що характеризуються як високою частотою такої атаки і деструктивними наслідками, вимагають поточного впровадження контрзаходів, тоді як категорія «чорних лебедів» — загроза низької ймовірності, але катастрофічного впливу — вимагає розвитку системи раннього виявлення та планів аварійного відновлення. Контекст України як територія, де теоретичні моделі кіберзагрози перетворилися на практичні дії, особливо в умовах військового конфлікту, висвітлює гостру необхідність переосмислення архітектурних підходів до побудови муніципальних цифрових екосистем з орієнтацією на кіберстійкість та резильентність. Знання, накопичене в цьому розділі про реальні вектори атаки та реальні дослідження їх реалізації, створюють основу для розробки адаптованих стратегій захисту, які будуть представлені в наступних частинах дисертації.

Розділ 3. МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IoT-СИСТЕМ

3.0 Міжнародні стандарти та фреймворки безпеки IoT

Побудова комплексної стратегії захисту гетерогенних систем «розумний дім» та «розумне місто» неможлива без спирання на верифіковані міжнародні практики та стандартизовані методології. Сучасний ландшафт нормативного регулювання у сфері Інтернету речей (IoT) пропонує розробникам та операторам систем набір фреймворків, які систематизують підходи до проектування захищених архітектур, управління ризиками та забезпечення відповідності (Compliance) законодавчим вимогам. Імплементація цих стандартів дозволяє перейти від хаотичного застосування засобів захисту до побудови цілісної системи інформаційної безпеки.

Національний інститут стандартів і технологій США (NIST) розробив адаптивну структуру Cybersecurity Framework (CSF) 2.0, яка стала де-факто глобальним стандартом управління кіберризиками. У контексті IoT-екосистем даний фреймворк базується на п'яти фундаментальних функціях ядра (Framework Core)[25]:

1. Identify (Ідентифікація): Повна інвентаризація активів (Asset Management), визначення бізнес-середовища та оцінка ризиків ланцюга постачання.

2. Protect (Захист): Впровадження механізмів контролю доступу (Identity Management), захист даних у стані спокою та транзиті, а також забезпечення регулярного обслуговування систем.

3. Detect (Виявлення): Реалізація систем безперервного моніторингу аномалій та подій безпеки (Continuous Monitoring).

4. Respond (Реагування): Розробка планів реагування на інциденти, аналіз причин та мітігація наслідків.

5. Recover (Відновлення): Планування відновлення функціональності та комунікація зі стейкхолдерами.

Спеціалізована серія публікацій NIST IR 8259 та NIST IR 8259A конкретизує вимоги для виробників IoT-пристроїв, визначаючи набір базових технічних можливостей (Core Baseline Capabilities)[8]. До них віднесено: вимогу унікальної фізичної або логічної ідентифікації кожного пристрою в мережі; можливість зміни конфігурації програмного забезпечення; захист даних криптографічними методами; логічне розмежування інтерфейсів доступу до локальних та мережевих ресурсів; механізми безпечного оновлення прошивки (Secure OTA Update) з перевіркою цифрового підпису; а також документування стану кібербезпеки пристрою. NIST також пропонує модель зрілості (Maturity Model) процесів безпеки, що дозволяє організаціям еволюціонувати від реактивного рівня (Partial) до адаптивного (Adaptive), де захист базується на предиктивній аналітиці загроз.

Європейське агентство з кібербезпеки (ENISA) розробило комплекс настанов, які лягли в основу європейського підходу до регулювання безпеки IoT[6]. Ключовим документом у цій сфері став стандарт ETSI EN 303 645 «Cyber Security for Consumer Internet of Things: Baseline Requirements», який вважається першим глобально застосовним стандартом для споживчого сегменту IoT.

Стандарт ETSI EN 303 645 постулює 13 високорівневих положень, які декомпозуються на 68 конкретних вимог[5]. Серед найкритичніших імперативів:

- Заборона універсальних паролів за замовчуванням: Виробники зобов'язані відмовитися від практики hardcoded credentials (типу admin/admin) на користь унікальних паролів для кожного пристрою або механізмів примусової зміни пароля при першому запуску.
- Впровадження політики розкриття вразливостей: Обов'язкова наявність публічного каналу для повідомлення про знайдені вразливості (Vulnerability Disclosure Policy).
- Управління життєвим циклом ПЗ: Забезпечення своєчасного випуску патчів безпеки та прозорість термінів підтримки продукту.
- Захист комунікацій: Використання протоколів TLS/DTLS для шифрування трафіку та забезпечення цілісності даних.

Ці вимоги охоплюють весь життєвий цикл пристрою — від проектування (Security by Design) до виведення з експлуатації (End-of-Life), включаючи процедури безпечного видалення користувацьких даних (Sanitization).

Інститут інженерів електротехніки та електроніки (IEEE) та Міжнародна організація зі стандартизації (ISO) фокусуються на архітектурній інтероперабельності та системному менеджменті безпеки. Стандарт IEEE P2413 визначає референсну архітектуру (Standard for an Architectural Framework for the IoT), яка уніфікує підходи до побудови систем у різних доменах (Smart City, Industrial IoT, Healthcare), сприяючи створенню крос-платформних рішень та зменшенню фрагментації ринку[2]. Серія стандартів ISO/IEC 27400 та ISO/IEC 27402 інтегрує специфіку IoT у загальну систему управління інформаційною безпекою (ISMS) згідно з ISO/IEC 27001[20]. Ці документи визначають вимоги до ідентифікації ризиків (Risk Identification), контролю відповідності та захисту персональних даних (PII Protection) у контексті IoT-систем, забезпечуючи гармонізацію технічних заходів з організаційними процедурами.

Загальний регламент про захист даних (GDPR) є критично важливим нормативним актом для систем Smart City та Smart Home, оскільки вони оперують масивами чутливої інформації (геолокація, біометрія, поведінкові

патерни). Регламент вводить поняття «персональні дані» в широкому сенсі, включаючи технічні ідентифікатори (MAC-адреси, RFID-теги), які дозволяють прямо чи опосередковано ідентифікувати особу.

Ключовим принципом GDPR є стаття 25 «Data Protection by Design and by Default» (Захист даних на етапі проектування та за замовчуванням)[19]. Це зобов'язує розробників інтегрувати механізми приватності безпосередньо в архітектуру системи, а не додавати їх постфактум. До таких механізмів належать:

- Мінімізація даних (Data Minimization): Збір лише того обсягу даних, який необхідний для виконання конкретної функції.
- Псевдонімізація та шифрування: Обробка даних таким чином, щоб їх неможливо було співвіднести з конкретною особою без додаткової інформації.
- Прозорість та контроль: Надання користувачам інструментів для реалізації їхніх прав (право на доступ, право на забуття, право на обмеження обробки).

Недотримання вимог GDPR тягне за собою значні фінансові санкції (до 4% від глобального річного обігу), що робить відповідність регламенту (Compliance) економічним імперативом для операторів IoT-систем[19].

3.1 Організаційні заходи безпеки

Формування резильєнтної (resilient) архітектури IoT неможливе без інтеграції технічних засобів захисту з комплексом організаційно-адміністративних заходів. На відміну від інструментальних методів, спрямованих на нейтралізацію векторів атак на логічному та фізичному рівнях, організаційні заходи фокусуються на створенні регламентованого середовища управління ризиками (Security Governance), формуванні культури кібербезпеки та забезпеченні безперервності бізнес-процесів.

Фундаментом організаційної безпеки є розробка та затвердження Політики інформаційної безпеки (Information Security Policy) — документа вищого рівня, що детермінує стратегічні цілі, зону відповідальності та допустимий рівень ризику (Risk Appetite)[25]. Для екосистем «розумне місто», де відбувається

конвергенція IT (Information Technology) та OT (Operational Technology), критично важливою є гармонізація політик між муніципальними департаментами (транспорт, енергетика, комунальні служби). Ефективна імплементація політики вимагає інституціоналізації функції CISO (Chief Information Security Officer), на якого покладається відповідальність за координацію процесів захисту. У контексті організаційної структури має бути впроваджено матрицю розподілу відповідальності (RACI Matrix), яка чітко визначає власників інформаційних активів (Asset Owners) та осіб, відповідальних за операційну безпеку.

Враховуючи високу залежність IoT-інфраструктури від зовнішніх контрагентів (хмарних провайдерів, виробників обладнання, розробників ПЗ), управління ризиками ланцюга постачання (SCRM) стає пріоритетним завданням. Організаційні заходи повинні включати:

- Включення до контрактів жорстких вимог щодо безпеки (Security Clauses) та угод про рівень обслуговування (SLA), що гарантують своєчасний випуск оновлень (Security Patches).
- Обов'язковий аудит безпеки постачальників (Vendor Security Assessment) на етапі тендерних процедур.
- Юридичне закріплення відповідальності за витік даних та порушення вимог GDPR.

Людський фактор залишається домінуючим вектором первинної компрометації систем (через фішинг або соціальну інженерію). Комплексна програма Security Awareness Training повинна бути диференційованою[6]:

- Для персоналу: Регулярні тренінги з кібергігієни, розпізнавання соціоінженерних атак та безпечної роботи з адміністративними інтерфейсами.
- Для мешканців (End-users): Розробка інтуїтивно зрозумілих інструкцій (Best Practice Guides) щодо налаштування домашніх пристроїв, зміни дефолтних паролів та управління приватності.

Ключовим елементом організаційної готовності є наявність формалізованого Плану реагування на інциденти (Incident Response Plan, IRP),

розробленого згідно з рекомендаціями NIST SP 800-61[27]. План має регламентувати процедури детекції, стримування (Containment), ерадиікації (Eradication) загрози та відновлення сервісів.

Для забезпечення стійкості критичної міської інфраструктури обов'язковим є розробка Плану забезпечення безперервності бізнесу (Business Continuity Plan, BCP) та Плану аварійного відновлення (Disaster Recovery Plan, DRP). Ці документи визначають параметри RTO (Recovery Time Objective) та RPO (Recovery Point Objective), а також регламентують процедури переходу на резервні центри обробки даних у разі катастрофічних збоїв.

Забезпечення відповідності політикам безпеки досягається через механізми регулярного внутрішнього та зовнішнього аудиту. Результати аудитів є підставою для перегляду матриці ризиків та актуалізації захисних заходів в рамках циклу PDCA (Plan-Do-Check-Act). Для систем класу Smart City прозорість результатів безпекових аудитів є фактором формування суспільної довіри до цифрових ініціатив влади.

3.2 Технічні засоби забезпечення безпеки

Технічні засоби інформаційної безпеки формують операційне ядро захисту IoT-екосистем, забезпечуючи безпосереднє втілення політик та процедур, визначених на організаційному рівні. Якщо організаційні заходи встановлюють стратегічний вектор управління ризиками, то технічні інструменти реалізують конкретні захисні механізми на фізичному, канальному, мережевому та прикладному рівнях архітектури[3]. Для гетерогенних систем класу «розумний дім» та «розумне місто», що об'єднують пристрої з критично різними обчислювальними можливостями, застосування уніфікованих технічних засобів є неможливим, тому інженерний підхід базується на диференційованому виборі інструментарію відповідно до критичності активу та потенційних векторів загроз.

Фундаментальним елементом технічного захисту є криптографічний захист даних, що забезпечує конфіденційність та цілісність інформаційних

потоків. Для захисту даних у транзиті, які курсують між сенсорами, шлюзами та хмарними платформами, критично необхідним є використання протоколів Transport Layer Security (TLS) версій 1.2 або 1.3. Ці протоколи гарантують встановлення захищеного каналу зв'язку, унеможливлюючи пасивний перехоплення трафіку та атаки типу Man-in-the-Middle завдяки перевірці цифрових сертифікатів сторін. Стосовно даних у стані спокою, що зберігаються у локальній пам'яті пристроїв або в базах даних хмарних платформ, стандартом де-факто є симетричне шифрування за алгоритмом AES з довжиною ключа 256 біт. Однак для класу ресурсно обмежених IoT-пристроїв, де апаратна реалізація AES є енерговитратною, доцільним є застосування оптимізованих потокових шифрів, таких як ChaCha20-Poly1305, які забезпечують високу криптостійкість при значно меншому навантаженні на процесор. Ключовим аспектом криптографічної безпеки залишається управління життєвим циклом ключів шифрування, що вимагає використання спеціалізованих систем управління ключами (KMS) та категоричної заборони на зберігання секретів у вихідному коді прошивок.

Не менш важливою складовою технічного захисту є механізми ідентифікації та автентифікації суб'єктів доступу[24]. Традиційна парольна автентифікація в умовах IoT демонструє свою неспроможність протистояти сучасним загрозам, тому імперативом стає впровадження багатофакторної автентифікації (MFA)[9]. Цей підхід вимагає підтвердження особи щонайменше за двома незалежними факторами, якими можуть виступати знання пароля, володіння апаратним токеном (стандарт FIDO2) або біометричні характеристики. Для систем розумного міста, де адміністратори мають привілейований доступ до критичної інфраструктури, MFA є безальтернативною вимогою, що нівелює ризики компрометації облікових записів через фішинг або перебір паролів. Управління ідентичністю в масштабах міста доцільно реалізовувати через федеративні протоколи (Federated Identity Management), такі як OpenID Connect, що дозволяє створити єдиний простір довіри для доступу до

різних муніципальних сервісів без необхідності множинного адміністрування облікових записів[25].

Логічне розмежування прав доступу в IoT-системах базується на принципі найменших привілеїв (Principle of Least Privilege), згідно з яким кожен суб'єкт отримує лише той набір повноважень, який є мінімально необхідним для виконання його функціональних обов'язків[24]. Реалізація цього принципу здійснюється через моделі управління доступом. Якщо модель Role-Based Access Control (RBAC) є ефективною для статичних структур, то для динамічних середовищ розумного міста перевагу віддають атрибутивному контролю доступу (Attribute-Based Access Control, ABAC). ABAC дозволяє формувати гранулярні політики доступу, враховуючи контекстні атрибути, такі як час доби, геолокація користувача, стан мережі та тип пристрою, що забезпечує гнучку адаптацію системи безпеки до поточних умов експлуатації.

Захист програмного забезпечення IoT-пристроїв від модифікації зловмисниками забезпечується механізмами безпечного оновлення (Secure OTA Update) та контролю цілісності прошивки[8]. Процедура оновлення повинна включати обов'язкову перевірку цифрового підпису образу прошивки перед його інсталяцією, що гарантує автентичність джерела оновлення та відсутність несанкціонованих змін у коді. Апаратна підтримка безпеки реалізується через використання модулів Trusted Platform Module (TPM) або Secure Element (SE), які виступають коренем довіри (Root of Trust) для системи. Ці компоненти забезпечують безпечне зберігання криптографічних ключів у ізольованому середовищі, недоступному для програмного вилучення навіть у випадку компрометації операційної системи пристрою, а також підтримують технологію Secure Boot, яка запобігає завантаженню неавторизованого коду на етапі старту системи.

Архітектурним методом обмеження поверхні атаки є сегментація мережі, яка передбачає поділ єдиної мережевої інфраструктури на ізольовані логічні зони за допомогою технологій VLAN та міжмережевих екранів[6]. Такий підхід дозволяє локалізувати інциденти безпеки: компрометація вразливої смарт-

лампочки в гостьовій мережі не надасть зловмиснику доступу до критично важливих систем керування опаленням або безпекою, що знаходяться в захищеному сегменті. Додатковий рівень ізоляції забезпечується використанням архітектури периферійних обчислень (Edge Computing), де обробка чутливих даних відбувається локально на шлюзі без їх передачі у публічну хмару, що знижує ризики перехоплення та залежність від доступності зовнішніх каналів зв'язку.

Захист програмних інтерфейсів (API Security) завершує комплекс технічних засобів, оскільки саме API є основними точками взаємодії компонентів розподіленої системи[25]. Безпека API забезпечується використанням сучасних стандартів авторизації, таких як OAuth 2.0, та застосуванням токенів доступу (JSON Web Tokens) з обмеженим часом життя. Обов'язковим є впровадження механізмів обмеження частоти запитів (Rate Limiting) для захисту від DoS-атак та вичерпання ресурсів, а також сувора валідація всіх вхідних даних для запобігання ін'єкціям коду. Комплексне застосування описаних технічних засобів дозволяє сформувати ешелоновану систему захисту, стійку до широкого спектру сучасних кіберзагроз.

3.3 Системи моніторингу та виявлення атак (IDS/IPS, SIEM)

Забезпечення кіберстійкості IoT-екосистем неможливе без розгортання комплексних систем активного моніторингу, здатних ідентифікувати аномальну активність та нейтралізувати загрози в режимі реального часу. Оскільки периметр захисту в розподілених мережах розумного міста є розмитим, фокус зміщується з превентивного блокування доступу на виявлення компрометації на ранніх стадіях Kill Chain. Технічну основу цього підходу складають системи виявлення та запобігання вторгненням (IDS/IPS), платформи управління подіями інформаційної безпеки (SIEM) та рішення для оркестрації реагування (SOAR)[25,27].

Першим ешелоном детекції виступають системи IDS (Intrusion Detection Systems) та IPS (Intrusion Prevention Systems). Мережеві сенсори NIDS

здійснюють глибокий аналіз трафіку (Deep Packet Inspection), порівнюючи пакети з базою сигнатур відомих атак. Однак для IoT-середовища, де домінують пропрієтарні протоколи та специфічні вектори загроз, класичний сигнатурний аналіз є недостатнім. Тому сучасні рішення інтегрують евристичні алгоритми та методи поведінкового аналізу (Behavioral Analysis), які формують динамічний профіль «нормальної» поведінки пристрою. Будь-яке відхилення від базової лінії (Baseline) — наприклад, спроба смарт-камери встановити з'єднання з сервером у нетиповій географічній зоні або різке зростання обсягу вихідного трафіку — класифікується як інцидент. Системи IPS, на відміну від пасивних IDS, мають мандат на автоматичне блокування шкідливої активності шляхом розриву TCP-сесій або модифікації правил брандмауера, що дозволяє зупинити розповсюдження хробака або DDoS-атаку без втручання оператора[25,27].

Централізація та кореляція даних про події безпеки покладається на системи класу SIEM (Security Information and Event Management)[27]. Функціональне ядро SIEM забезпечує агрегацію журналів аудиту (Logs) з гетерогенних джерел: кінцевих IoT-пристроїв, мережевого обладнання, серверів додатків та систем контролю доступу. Процес нормалізації даних дозволяє привести різнорідні формати логів до єдиної таксономії, що уможливлює застосування правил крос-кореляції. Це дозволяє виявляти складні, розподілені у часі атаки, які неможливо помітити, аналізуючи кожен компонент ізольовано. Наприклад, SIEM здатна пов'язати серію невдалих спроб автентифікації на VPN-шлюзі з подальшим скануванням портів у внутрішній мережі SCADA, ідентифікувавши це як цілеспрямовану атаку APT. Для систем розумного міста SIEM є критично важливим інструментом ситуаційної обізнаності (Situational Awareness), що надає операторам цілісну картину стану безпеки муніципальної інфраструктури.

Еволюційним розвитком аналітичних спроможностей є впровадження технологій UEBA (User and Entity Behavior Analytics). Ці системи застосовують алгоритми машинного навчання для виявлення інсайдерських загроз та компрометації облікових записів (Account Takeover). Аналізуючи патерни

доступу користувачів та сутностей (пристроїв), UEBA виявляє аномалії, які не порушують формальних правил доступу, але є підозрілими у контексті. Прикладом може слугувати нетипова активність адміністратора енергомережі у неробочий час або масове вивантаження конфіденційних даних, що може свідчити про зловживання повноваженнями або викрадення сесії.

Для мінімізації часу реагування (Mean Time to Respond, MTTR) застосовуються платформи SOAR (Security Orchestration, Automation, and Response)[27]. SOAR дозволяє формалізувати процедури реагування у вигляді автоматизованих сценаріїв (Playbooks). У випадку підтвердження інциденту, система здатна виконати заздалегідь визначений алгоритм дій: ізолювати скомпрометований сегмент мережі через SDN-контролер, відкликати скомпрометовані сертифікати доступу та створити тікет для групи розслідування (SOC Analyst). Автоматизація рутинних операцій дозволяє розвантажити аналітиків та забезпечити миттєву реакцію на швидплинні загрози, що є критичним для захисту динамічних IoT-середовищ.

Ефективність функціонування систем моніторингу безпосередньо залежить від якості вхідних даних[25]. Тому обов'язковою вимогою до проектування IoT-систем є реалізація розширеного логування подій (Audit Trails), що включає фіксацію спроб доступу, змін конфігурації та помилок виконання. Логи повинні передаватися до захищеного централізованого сховища в режимі реального часу через захищені канали (Syslog-ng over TLS), щоб унеможливити їх модифікацію зловмисником у разі захоплення контролю над кінцевим пристроєм. Тільки побудова замкненого циклу «моніторинг – аналіз – реагування» гарантує здатність системи протистояти сучасним кіберзагрозам.

3.4 Перспективні методи забезпечення безпеки IoT-систем

Еволюція ландшафту кіберзагроз, що характеризується зростанням автоматизації атак та появою нових векторів компрометації, диктує необхідність переходу від статичних захисних механізмів до адаптивних та інтелектуальних систем безпеки. Традиційні методи, такі як сигнатурний аналіз або

периметральний захист, демонструють зниження ефективності в умовах децентралізованих мереж Інтернету речей, що вимагає імплементації проривних технологій. До найбільш перспективних напрямків, здатних фундаментально змінити архітектуру безпеки розумних міст та будинків, належать технології розподілених реєстрів, штучний інтелект, постквантова криптографія та парадигма нульової довіри.

Технологія блокчейн та розподілених реєстрів (Distributed Ledger Technology, DLT) пропонує архітектурне вирішення проблеми довіри та цілісності даних у гетерогенних середовищах без єдиного центру управління. Завдяки використанню криптографічного зв'язування блоків та механізмів консенсусу, DLT забезпечує властивість незмінності (immutability) записаної інформації. У контексті розумного міста це створює надійний фундамент для аудиту критичних операцій: будь-яка команда на зміну режиму роботи світлофорів або енергорозподільчих вузлів фіксується у розподіленому реєстрі, що унеможливлює приховування слідів несанкціонованого втручання[26]. Для сегменту розумного будинку блокчейн відкриває шлях до децентралізованого управління ідентичністю (Self-Sovereign Identity), де користувачі контролюють доступ до своїх даних через криптографічні ключі, не покладаючись на централізованих хмарних провайдерів, які часто стають точками відмови[19]. Разом з тим, впровадження блокчейну в IoT вимагає вирішення проблеми масштабованості та енергоефективності, що стимулює перехід від енерговитратних алгоритмів Proof-of-Work до більш легких моделей консенсусу, таких як Proof-of-Authority або спрямовані ациклічні графи (DAG), адаптовані для обробки високочастотних транзакцій сенсорних мереж.

Інтеграція методів штучного інтелекту (AI) та машинного навчання (ML) трансформує системи виявлення вторгнень з реактивних інструментів у проактивні аналітичні платформи. На відміну від детермінованих алгоритмів, здатних виявляти лише відомі загрози, ML-моделі здатні ідентифікувати аномалії та атаки нульового дня (Zero-day attacks) шляхом аналізу відхилень від базового профілю нормальної поведінки. Використання методів глибокого

навчання (Deep Learning) дозволяє аналізувати високорозмірні дані мережевого трафіку, виявляючи приховані кореляції, характерні для складних цільових атак (APT). У системах розумного будинку такі алгоритми можуть автоматично блокувати нетипові сценарії, наприклад, спробу дистанційного відкриття замків у час, коли геолокація власника вказує на його перебування в іншій країні. Водночас, широке застосування AI створює нові ризики, пов'язані з так званими змагальними атаками (Adversarial Attacks), коли зловмисники навмисно спотворюють вхідні дані для обману класифікаторів системи безпеки, що вимагає розробки стійких до маніпуляцій моделей.

Найвищу ефективність демонструють гібридні системи, які поєднують швидкість сигнатурних методів з аналітичною глибиною машинного навчання[27]. Така архітектура дозволяє фільтрувати відомі загрози з мінімальною затримкою, передаючи складні та нестандартні патерни на обробку нейронним мережам. Для інфраструктури розумних міст це означає можливість кореляції подій із сотень тисяч сенсорів у реальному часі, що дозволяє оперативно виявляти розподілені атаки, такі як DDoS, ще на етапі формування ботнету. Важливим аспектом залишається забезпечення інтерпретованості рішень AI (Explainable AI), оскільки оператори критичної інфраструктури повинні розуміти логіку автоматичних блокувань для уникнення помилкових спрацювань, що можуть призвести до перебоїв у наданні сервісів.

Довгостроковою стратегічною загрозою для IoT-систем є розвиток квантових обчислень, здатних у майбутньому зламати сучасні асиметричні алгоритми шифрування (RSA, ECC), на яких базується вся інфраструктура відкритих ключів (PKI)[24]. Це актуалізує проблему «збережи зараз, розшифруй пізніше» (Harvest Now, Decrypt Later), коли зловмисники накопичують зашифрований трафік з розрахунком на майбутній декриптинг. Відповіддю на цей виклик є перехід до постквантової криптографії (PQC) — нових математичних алгоритмів, стійких до квантового криптоаналізу. Організаціям, що розгортають довговічну інфраструктуру розумних міст, необхідно вже зараз імплементувати криптографічну гнучкість (crypto-agility), щоб забезпечити

безболісну міграцію на стандарти PQC, затверджені NIST, такі як кристалічні решітки (Lattice-based cryptography).

Парадигма архітектури нульової довіри (Zero Trust Architecture) стає фінальним елементом перспективної стратегії безпеки, відкидаючи застарілу концепцію довіреного периметра[22]. У середовищі Zero Trust жоден пристрій або користувач, незалежно від його фізичного розташування в мережі, не вважається довіреним за замовчуванням. Кожна транзакція або запит на доступ підлягає суворій автентифікації, авторизації та перевірці контексту безпеки. Для IoT-систем це реалізується через мікросегментацію мережі, де кожен розумний пристрій функціонує у власному ізольованому мікроперіметрі, маючи доступ лише до тих ресурсів, які критично необхідні для його роботи. Такий підхід мінімізує радіус ураження у випадку компрометації окремого вузла та унеможливлює горизонтальне переміщення зловмисника всередині мережі, забезпечуючи стійкість системи навіть в умовах часткового злому.

Висновок до третього розділу

В третьому розділі було систематизовано комплексний арсенал методів та засобів забезпечення безпеки IoT-систем, що охоплює спектр від міжнародних нормативних стандартів до авангардних технологій штучного інтелекту та постквантової криптографії. Дослідження демонструвало, що успішна реалізація захисту гетерогенних екосистем розумного дому та міста вимагає ув’язування трьох взаємодоповнюючих шарів: нормативно-методологічного (стандарти NIST, ETSI, ISO, GDPR), організаційно-управлінського (політики, процедури, управління ризиками) та технічно-інструментального (криптографія, моніторинг, система виявлення вторгнень). Жоден із цих компонентів не є достатнім в ізоляції, проте їх синергетична інтеграція формує стійку архітектуру, здатну протистояти широкому спектру сучасних та прогнозованих загроз.

Аналіз міжнародних стандартів, що глобальне співтовариство розробило узгоджену системну вимогу, яка прогресивно еволюціонує з попередніх рекомендацій NIST до обов’язкових правових норм GDPR та ETSI EN 303 645.

Ці документи встановили прозорі очікування щодо виробників та операторів IoT-пристроїв, забороняючи практики типу жорстко закодованих паролів та вимагаючи впровадження механізмів безпечного оновлення. прошивки, управління ризиками ланцюга постачання та документування стану безпеки. Однак виявлене розташування стандартів часто випадає в ролі фільтра, який відраховує саме хабітус, на якому базується індустріалізація IoT — тобто яскрава різниця між декларативними вимогами та реальною практичною виробництвом пристроїв під тиском商業конкуренції та прискорення часу виходу на ринок.

Організаційні заходи безпеки дозволили розпізнати той факт, що технічні засоби є безсильними в умовах чіткої розподіленої відповідальності, формалізованих процесів управління ризиками та культурою кібербезпеки у лавах персоналу та кінцевих користувачів. Найбільш критичним виявляється людський фактор як домінуючий вектор первинної компрометації: фішингові атаки та соціальна інженерія залишаються найефективнішими методами проникнення навіть у хороші захищені системи, що актуалізує необхідне навчання та формування свідомості щодо регулярної кібергігієни. На рівні критичної інфраструктури обов’язковість розробки формалізованих планів реагування на інциденти та аварійне відновлення виходить не лише рекомендацією, а економічним імперативом, після чого вартість ліквідації наслідків успішної атаки на об’єкт розумного міста має значення стійкості превентивних інвестицій на порядок.

Технічні засоби, що містять систему в розділі, створили ешелонований захист, декриптографічне захист даних, механізми сильної автентифікації та сегментації мережі формують першу лінійну оборону, тоді як системи моніторингу талення вторгнення (IDS/IPS, SIEM, UEBA) забезпечують ранню детекцію компрометації та швидкість реагування в режимі реального часу. Виявлено, що традиційні підходи до бази сигнатурного аналізу та периметрального захисту демонструють зниження ефективності в децентралізованих IoT-середовищах, що вимагають переходу до більш гнучких

та адаптивних структур, здатних розпізнавати нові та невідомі угрози через аналіз відхилень від базової лінії нормальної поведінки.

Визначено, що майбутня безпека IoT-екосистеми не потребує інтеграції технологій, особливо штучного інтелекту та машинного навчання для проактивного виявлення аномалій та атак нульового дня, блокчейну для забезпечення цілісності та непростовності критичних операцій, а також постквантової криптографії для захисту від довгострокових загроз квантових обчислень. Парадигма архітектури нульової довіри (Zero Trust) утверджується як стратегічна основа подальшого розвитку, відкидаючи застарілу концепцію фіксованого периметра захисту при завантаженні мікросегментації та безперервної верифікації кожної операції незалежно від місця в мережі. Сукупність знань, методів та технологій, систематизована в цьому розділі, дає практичну основу для розробки комплексних стратегій захисту конкретних IoT-систем та виступає фундаментом для переходу до прикладної реалізації захисту в наступних частинах дисертаційної роботи.

Розділ 4. ПОРІВНЯЛЬНИЙ АНАЛІЗ РІВНЯ ЗАХИЩЕНОСТІ ТИПОВИХ ТА МОДЕРНІЗОВАНИХ IoT-АРХІТЕКТУР

4.1 Аналіз вразливостей типової архітектури та ефективність модернізації

Дослідження рівня захищеності кіберфізичних систем класу «розумний дім» та «розумне місто» базується на методології порівняльного аналізу двох полярних архітектурних моделей: типової конфігурації (Baseline), що відображає поточний стан більшості розгорнутих систем, та запропонованої еталонної захищеної архітектури (Secure Reference Architecture)[7]. Типова модель характеризується наявністю «плоскої» мережевої топології, де всі компоненти — від критично важливих серверів управління та шлюзів безпеки до побутових смарт-лампочок із сумнівним рівнем захисту — функціонують у єдиному широкомовному домені без логічної ізоляції. У такій архітектурі управління пристроями здійснюється переважно через незахищені протоколи прикладного рівня (HTTP, CoAP або MQTT без шифрування), а механізми автентифікації спираються на заводські налаштування або слабкі парольні політики, що створює ідеальні умови для реалізації атак[8,9]. Натомість, розроблена еталонна модель імплементує парадигми Zero Trust та Defense-in-Depth, передбачаючи сувору мікросегментацію мережі на ізольовані VLAN, обов'язкове використання криптографічних протоколів TLS версії 1.3 для захисту каналів управління та впровадження суворої багатофакторної автентифікації для всіх адміністративних інтерфейсів.

Для об'єктивізації оцінки ефективності запропонованих контрзаходів було проведено моделювання ключових векторів атак та розраховано метрики ризику згідно з методикою Common Vulnerability Scoring System (CVSS) версії 3.1[23]. Аналіз результатів демонструє суттєве зниження поверхні атаки. Наприклад, у

типовій архітектурі загроза Brute-Force атак на служби SSH/Telnet класифікується як критична (CVSS 9.8) через поширеність жорстко закодованих облікових даних (hardcoded credentials)[9]. Впровадження багатофакторної автентифікації (MFA) у поєднанні з автоматизованими системами блокування IP-адрес (наприклад, Fail2Ban) трансформує цей вектор у категорію низького ризику (CVSS 2.1), оскільки успішна атака вимагає не лише підбору пароля, але й компрометації другого фактора, що є технічно складним завданням для автоматизованих ботнетів.

Аналогічна позитивна динаміка спостерігається у протидії атакам на перехоплення трафіку (Sniffing) та Man-in-the-Middle. У базовому сценарії передача телеметрії відкритим текстом створює високий ризик (CVSS 8.6) витоку конфіденційних даних або підміни команд керування. Перехід на архітектуру з примусовим шифруванням TLS 1.3 та взаємною автентифікацією клієнта і сервера (mTLS) фактично нейтралізує цей вектор, знижуючи ризик до рівня низького (CVSS 1.9), оскільки зловмисник без валідного клієнтського сертифіката не зможе навіть встановити з'єднання з шлюзом. Проблема горизонтального переміщення зловмисника (Lateral Movement), яка є критичною для плоских мереж (CVSS 8.8), вирішується шляхом мікросегментації мережі та налаштуванням правил міжмережевого екранування, що локалізує потенційний інцидент у межах одного сегмента і знижує загальний ризик до прийнятного рівня (CVSS 2.9)[6,22].

Зведені результати кількісного оцінювання ефективності модернізації системи захисту представлені у (Таблиці 1.5):

Таблиця 4.1

Зведена матриця порівняльного аналізу ефективності засобів захисту та динаміки показників ризику (CVSS v3.1)

Вектор атаки	**Вразливість типової архітектури (Baseline)**	**Запропонований контрзахід (Secure Architecture)**	**Динаміка ризику (CVSS Score)**

Brute-Force (SSH/Telnet)	Використання слабких та дефолтних паролів (admin/admin), відсутність блокування	Впровадження MFA, відключення root-доступу, Fail2Ban (блокування після 3 спроб)	9.8(Critical)\downarrow2.1 (Low)
Sniffing / MITM	Передача чутливих даних та команд відкритим текстом (HTTP, MQTT)	Примусове шифрування TLS 1.3, взаємна автентифікація (mTLS), Pinning сертифікатів	8.6(High)\downarrow1.9 (Low)
Denial of Service (DoS)	Відсутність обмежень на кількість з'єднань та частоту запитів	Rate Limiting на рівні API Gateway, налаштування таймаутів, IPS Suricata	7.5(High)\downarrow3.7 (Low)
Network Lateral Movement	Плоска мережева топологія, відсутність внутрішніх бар'єрів	Мікросегментація (VLAN/Subnets), суворі правила Firewall між сегментами (ACL)	8.8(High)\downarrow2.9 (Low)

4.1.1 Результати сканування вразливостей

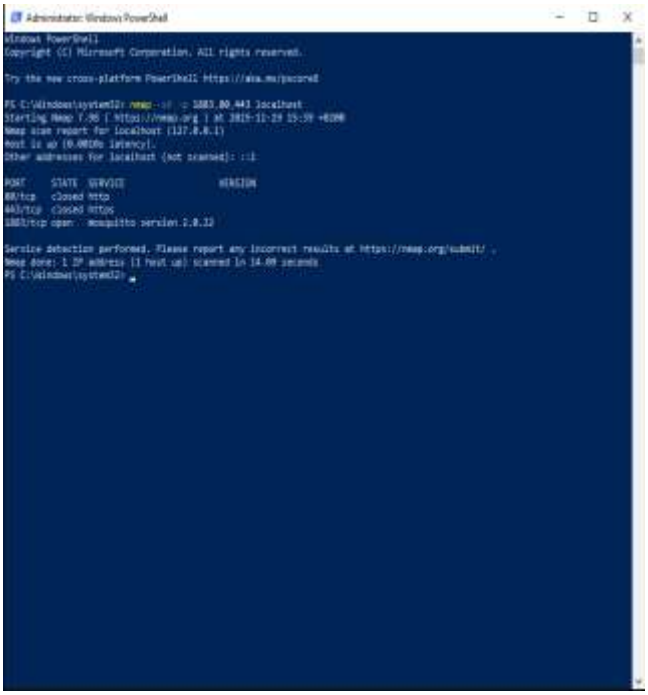
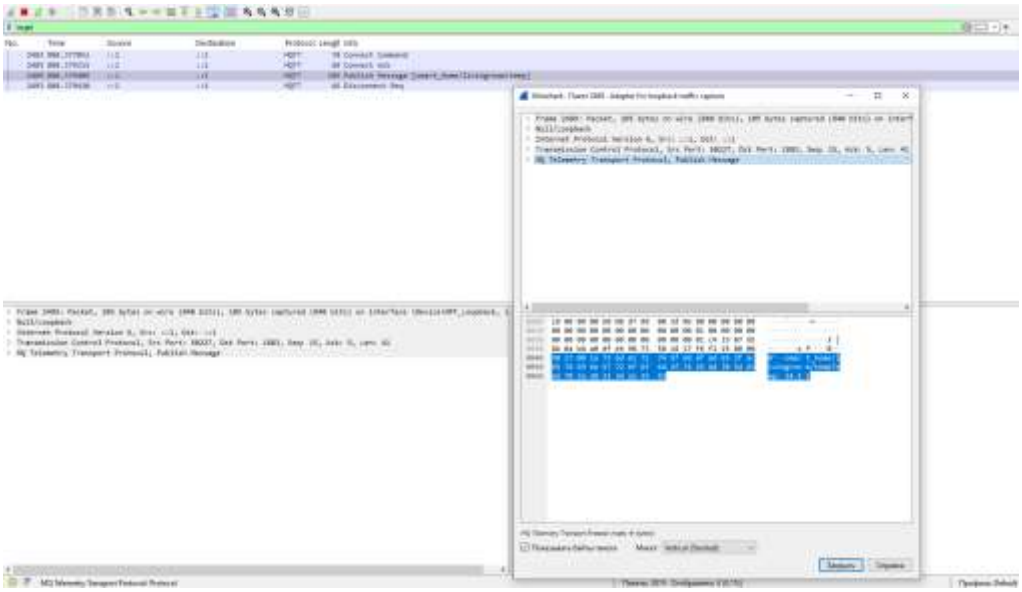


Рис. 4.1. Результат сканування портів локального вузла утилітою Nmap.

Результати сканування підтвердили наявність відкритих сервісів (MQTT на порту 1883), які у базовій конфігурації не вимагають автентифікації, що створює передумови для несанкціонованого доступу.

Наступним етапом стала перевірка можливості перехоплення даних. За допомогою аналізатора трафіку Wireshark було досліджено обмін даними між емульованим сенсором та брокером (Рис. 4.2).



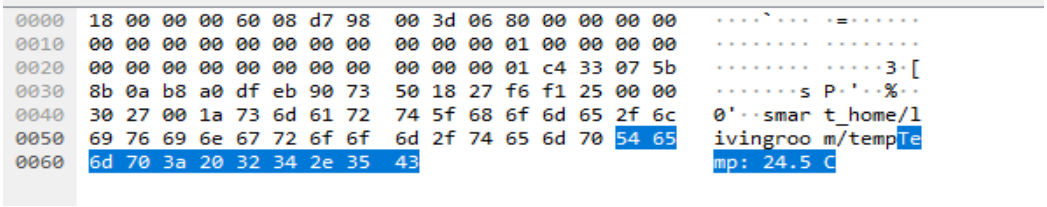


Рис. 4.2. Результат перехоплення незашифрованого MQTT-трафіку в локальному середовищі.

Аналіз дампу пакетів демонструє, що корисне навантаження (Payload) передається у відкритому текстовому вигляді (Cleartext), що підтверджує критичну вразливість до атак типу Sniffing та MITM. Як свідчать дані таблиці, комплексна модернізація архітектури дозволяє досягти кардинального зниження інтегрального показника ризику за всіма ключовими векторами загроз. Переведення критичних вразливостей у категорію низького залишкового ризику підтверджує ефективність запропонованої моделі та обґрунтовує доцільність інвестицій у впровадження ешелонованої системи захисту для критичних інфраструктур розумного міста та приватних систем розумного будинку.

4.2 Кількісна оцінка рівня захищеності модернізованої архітектури

Перед проведенням математичного розрахунку ризиків було виконано практичну верифікацію інструментарію тестування та засобів захисту.

Для оцінки стійкості системи до атак перебору паролів (Brute-Force) було розроблено спеціалізований скрипт на мові Python (Рис. 4.3).

Рис. 4.3. Фрагмент розробленого програмного засобу для тестування стійкості механізмів автентифікації.

Даний інструмент реалізує алгоритм словникової атаки, що дозволяє автоматизовано перевіряти надійність парольної політики IoT-пристроїв.

На основі виявлених вразливостей було розроблено та імплементовано комплексну конфігурацію безпеки (Рис. 4.4), що включає налаштування брокера Mosquitto та правила мережевого екрану.

Рис. 4.4. Комплексна конфігурація захисту: налаштування TLS та правила iptables.

Застосування даних налаштувань забезпечує примусове шифрування трафіку (порт 8883) та блокування нелегітимних з'єднань на мережевому рівні. Для верифікації ефективності запропонованих архітектурних рішень та отримання об'єктивних метрик захищеності застосовано методику кількісного оцінювання інформаційних ризиків. У рамках математичної моделі[7], інтегральний ризик компрометації системи ***R*** формалізується як функціональна залежність від ймовірності реалізації загрози ***P*** та магнітуди потенційного збитку ***I***:

$$R = P \times I$$

У контексті порівняльного аналізу, де величина потенційного збитку ***I*** (втрата конфіденційності, цілісності або доступності) розглядається як константа для обох архітектур, цільовою функцією модернізації є мінімізація ймовірності успішної реалізації атаки (***P*** \to min). Для типової архітектури ("Baseline"), що

характеризується відсутністю ешелонованого захисту, кумулятивна ймовірність компрометації (***P***_{baseline}) визначається як ймовірність об'єднання незалежних подій успішної експлуатації окремих вразливостей. Оскільки компрометація системи можлива через будь-який незахищений вектор (слабкий пароль АБО відкритий порт АБО відсутність шифрування)[7], формула набуває вигляду:

$$P_{baseline} = 1 - \Pi^{n}_{i=1}(1 - P_i)$$

де ***P_i*** — ймовірність успішної експлуатації ***i***-го вектору атаки. Враховуючи високу вразливість типових конфігурацій (наприклад, ймовірність успішного Brute-force підбору дефолтного пароля ***P***_{bf} \to 1), інтегральна ймовірність злому наближається до критичного значення: ***P***_{baseline} \to 1. Для модернізованої архітектури ("Secure"), що реалізує принцип глибокого захисту (Defense-in-Depth), ймовірність успішної атаки суттєво знижується за рахунок введення компенсуючих заходів контролю. Ефективність зниження інтегрального ризику (***E***) визначається як відносне зменшення метрики ризику[23]:

$$E = (1 - \frac{\mathrm{R}secure}{\mathrm{R}baseline}) \times 100\%$$

Використовуючи скорингові оцінки CVSS v3.1 з Таблиці 4.1 як чисельний еквівалент рівня ризику (***R*** \approx CVSS\ Score), проведемо розрахунок усередненої ефективності для ключових векторів атак:

$$E_{avg} = (1 - \frac{\Sigma\, CVSSsecure}{\Sigma CVSSbaseline}) \times 100\%$$

Підставляючи емпіричні дані:

$$\Sigma CVSS_{baseline} = 9.8 + 8.6 + 7.5 + 8.8 = 34.7$$

$$\Sigma CVSS_{secure} = 2.1 + 1.9 + 3.7 + 2.9 = 10.6$$

$$E_{avg} = (1 = \frac{10.6}{34.7}) \times 100\% \approx 69.45\%$$

Отриманий результат свідчить, що імплементація комплексу запропонованих технічних та організаційних заходів дозволяє знизити інтегральний рівень кіберризику системи майже на 70%. Це підтверджує математичну обґрунтованість переходу до захищеної архітектури та переводить

систему зі стану критичної вразливості у стан контрольованого залишкового ризику (Residual Risk), що є достатнім для безпечної експлуатації в реальних умовах.

4.3 Оцінка економічної доцільності модернізації архітектури безпеки

Інтегральним критерієм прийняття рішення щодо імплементації системи захисту є не лише технічна досконаліть, але й економічна ефективність інвестицій. Для обґрунтування доцільності переходу на модернізовану архітектуру застосовано методику розрахунку коефіцієнта повернення інвестицій у інформаційну безпеку (Return on Security Investment, ROSI)[7]. Базова формула розрахунку ROSI визначається як відношення чистої вигоди від уникнення збитків до вартості захисних заходів:

$$ROSI = \frac{(ALE \times M) - Cost}{Cost} \times 100\%$$

де:

- ALE (Annualized Loss Expectancy) — очікувана грошова оцінка щорічних збитків від інцидентів безпеки за відсутності засобів захисту. Розраховується як добуток вартості одного інциденту (SLE) на частоту виникнення (ARO): ALE = SLE \times ARO[27].
- M (Mitigation Ratio) — коефіцієнт ефективності системи захисту, що відображає ступінь зниження ризику. На основі розрахунків у п. 4.2, приймаємо M = 0.6945 (або 69.45%).
- Cost — сукупна вартість володіння системою захисту (TCO), що включає капітальні витрати (CAPEX) на впровадження та операційні витрати (OPEX) на підтримку[20].

Для модельного сценарію (об'єкт критичної інфраструктури малого масштабу або елітне приватне домоволодіння) емпірична оцінка ALE становить 5000 USD (включаючи прямі фінансові втрати, вартість відновлення даних та репутаційні збитки). Вартість модернізації (Cost) оцінюється у 300 USD, оскільки запропонована архітектура базується переважно на реконфігурації

існуючого обладнання (Open-Source рішення, налаштування VLAN, політики безпеки) і не вимагає закупівлі дороговартісних апаратних засобів.

Проведемо розрахунок економічної ефективності:

$$ROSI = \frac{(5000 \times 0.6945) - 300}{300} \times 100\%$$

$$ROSI = \frac{3472.5 - 300}{300} \times 100\%$$

$$ROSI = \frac{3172.5}{300} \times 100\% \approx 1057\%$$

Отриманий показник ROSI \gg 100% демонструє екстремально високу рентабельність запропонованих заходів. Це пояснюється тим, що основний внесок у зниження ризиків вносить впровадження організаційних та архітектурних змін (мікросегментація, MFA, криптографічний захист), які мають низьку собівартість реалізації при високому коефіцієнті мітігації загроз. Такий результат підтверджує гіпотезу про те, що інвестування в грамотну архітектуру безпеки є економічно вигіднішим, ніж ліквідація наслідків потенційних кіберінцидентів[7,27].

Висновок до четвертого розділу

В четвертому розділі було проведено порівняльний аналіз типів архітектури IoT-системи та запропонованої модернізованої моделі, що дозволяє кілька оцінити ефективність механізмів захисту. Типова конфігурація з плоскою мережевою топологією та відсутністю ешелонованого захисту демонструє критичну вразливість до атаки, дефолтні паролі та незашифровані комунікаційні канали залишаються основними векторами компрометації. Контрастом служить розроблена модель, побудована на принципах Zero Trust та Defense-in-Depth, яка через мікросегментацію мережі, криптографічне захист та багатофакторну автентифікацію трансформує ризики з критичної категорії до контрольованого рівня залишкового.

Практична верифікація вразливостей через емуляцію реальних атак підтвердила теоретичні передбачення та дозволила отримати об'єктивні метрики. Експеримент з перехопленням незашифрованого MQTT-трафіку

продемонстрував, що базова конфігурація передає критичні дані відкритому тексту, що за шкалою CVSS класифікується як критичне (8.6 балів). Впровадження TLS 1.3 та зовнішньої автентифікації знижує цей ризик до 1.9 балів, свідчучи про кардинальну трансформацію профілю безпеки. Математичні розрахунки показали, що комплексна модернізація забезпечує зниження інтегрального кіберризику на 69,45%, переводячи систему у стан контрольованого залишкового ризику.

Найбільш значущим результатом стала демонстрація економічної доцільності інвестування безпеку через розрахунок коефіцієнта повернення інвестицій (ROSI = 1057%). Цей результат показує екстремально високу рентабельність запропонованих заходів за рахунок синергії низької собівартості реалізації з високою ефективністю пом’якшення загроз, трансформуючи IoT через розряд витратних обтяжень у категорію стратегічних інвестицій. Практичні експерименти, математичні моделі та економічні розрахунки дають об'єктивне обґрунтування необхідності переходу на модернізовані архітектури та створюють основу для розробки конкретних рекомендацій щодо впровадження систем захисту.

Розділ 5. РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ «РОЗУМНИЙ ДІМ/МІСТО»

5.1 Рекомендації для користувачів розумних будинків

Результати математичного моделювання загроз, проведені у четвертому розділі, емпірично підтвердили гіпотезу, що найслабшою ланкою в ланцюгу захисту IoT-екосистем є людський фактор[14]. Навіть передові технічні засоби нівелюються ігноруванням базових правил кібергігієни (Cyber Hygiene), оскільки експлуатація дефолтних налаштувань дозволяє зловмиснику отримати повний контроль над системою за тривіальний час. Відтак, кінцевий користувач виступає де-факто адміністратором безпеки власного цифрового простору, і його дії безпосередньо детермінують рівень резистентності системи до зовнішніх впливів.

Фундаментальним рівнем захисту є впровадження суворої політики управління автентифікацією (Credential Management). Користувачам необхідно відмовитися від практики використання заводських паролів на користь унікальних криптографічно стійких комбінацій для кожного пристрою, що включають повний набір символьних класів. Для нівелювання ризиків, пов'язаних з когнітивним навантаженням при запам'ятовуванні складних паролів, рекомендовано застосування менеджерів паролів. Критично важливою умовою є активація багатофакторної автентифікації (MFA) для всіх адміністративних інтерфейсів та хмарних акаунтів, що, згідно з розрахунками ефективності захисту, знижує ймовірність успішної атаки перебору паролів до статистично незначущих величин[24,28].

Другим ешелоном захисту виступає управління життєвим циклом програмного забезпечення. Оскільки значна частка векторів атак базується на експлуатації відомих вразливостей (CVE), користувачам слід налаштувати автоматичне оновлення прошивок (OTA Updates) для всіх компонентів інфраструктури[9]. Пристрої, що досягли статусу End-of-Life і більше не отримують патчів безпеки, підлягають виведенню з експлуатації, оскільки вони перетворюються на персистентні точки входу для зловмисників.

На архітектурному рівні домашньої мережі ключовою рекомендацією є впровадження логічної сегментації. Виділення IoT-пристроїв у ізольовану гостьову мережу (Guest Network) або окремий VLAN створює бар'єр для горизонтального переміщення (Lateral Movement) загрози, захищаючи персональні комп'ютери та сховища даних від компрометації через вразливу побутову техніку. Додатково необхідно провести гартування (Hardening) мережевого периметра: змінити дефолтні облікові дані маршрутизатора, деактивувати протокол UPnP та заблокувати віддалений доступ до панелі керування з глобальної мережі[1,5].

Завершальним елементом стратегії персональної безпеки є підвищення ситуаційної обізнаності. Регулярний аудит журналів подій (Logs) та налаштування автоматичних сповіщень про критичні дії (наприклад, відключення системи охорони або вхід з нового пристрою) дозволяють виявити інцидент на ранній стадії[25]. Поєднання технічних заходів з критичним мисленням щодо методів соціальної інженерії формує надійний захист приватного цифрового простору.

5.2 Рекомендації для органів місцевого самоврядування та операторів розумних міст

Органи місцевого самоврядування та оператори муніципальної інфраструктури, виступаючи гарантами стабільності функціонування розумного міста, несуть стратегічну відповідальність за захист критичних сервісів та масивів чутливих даних громадян. Масштабність та гетерогенність міської IoT-екосистеми вимагає переходу від фрагментарних тактичних рішень до системного стратегічного планування, де кібербезпека інтегрована у модель сталого розвитку як базовий компонент (Security as an Enabler)[11]. Рекомендації для даної категорії стейкхолдерів базуються на імперативах забезпечення високої доступності сервісів (High Availability) та суворого дотримання регуляторних вимог.

Першочерговим стратегічним пріоритетом є розробка та затвердження комплексної Політики безпеки критичної інфраструктури, гармонізованої з

міжнародними стандартами NIST CSF та рекомендаціями ENISA. Фундаментом цієї політики має стати тотальна інвентаризація та класифікація активів (Asset Management), що дозволить виявити приховані залежності між різними доменами (енергетика, водопостачання, транспорт) та змоделювати сценарії каскадних відмов. Регулярні незалежні аудити безпеки та стрес-тестування (Penetration Testing) інфраструктури повинні трансформуватися з реактивної процедури у плановий процес безперервного моніторингу відповідності[20,27].

Архітектурна стійкість розумного міста забезпечується впровадженням принципів відмовостійкості (Resilience) та надлишковості (Redundancy). Враховуючи високі ризики DDoS-атак на централізовані платформи, критично важливою є географічна диверсифікація центрів обробки даних та дублювання магістральних каналів зв'язку. Це гарантує безперервність надання життєво важливих послуг навіть в умовах фізичного знищення окремих вузлів внаслідок техногенних катастроф або цілеспрямованих атак. Обов'язковою умовою є наявність автоматизованих механізмів аварійного перемикання (Failover) та регулярна верифікація планів відновлення після катастроф (Disaster Recovery Plan), що мінімізує показники RTO (Recovery Time Objective)[25,27].

Соціальний аспект безпеки полягає у формуванні довіри громадян до цифрових ініціатив влади. Забезпечення прозорості процесів обробки даних досягається через публікацію відкритих звітів про цілі збору телеметрії та терміни її зберігання. Інституціоналізація муніципальних центрів реагування на інциденти (CERT) та створення каналів зворотного зв'язку (Vulnerability Disclosure Program) дозволяє залучити спільноту до процесу виявлення загроз, формуючи культуру колективної відповідальності.

У правовому полі домінуючим вектором є забезпечення комплаєнсу з вимогами GDPR та національного законодавства[19]. Це вимагає імплементації парадигми Privacy by Design на етапі архітектурного проектування будь-якого нового муніципального сервісу. Призначення посадових осіб з захисту даних (Data Protection Officer, DPO) та проведення обов'язкової оцінки впливу на

приватність (DPIA) перед запуском систем дозволяє мінімізувати юридичні ризики та захистити цифрові права громадян[20].

Завершальним елементом стратегії є управління ризиками ланцюга поставок (Supply Chain Risk Management). При проведенні тендерних закупівель IoT-рішень муніципалітети зобов'язані інтегрувати в договори жорсткі вимоги щодо рівня обслуговування (SLA), які гарантують своєчасний випуск патчів безпеки та надання довгострокової технічної підтримки. Юридичне закріплення фінансової відповідальності вендорів за інциденти, спричинені вразливістю їхніх продуктів, є дієвим інструментом підвищення якості програмного забезпечення в державному секторі.

5.3 Пропозиції для розробників і виробників IoT-пристроїв

Виробники апаратного та програмного забезпечення для Інтернету речей виступають архітекторами довіри у цифровому просторі, і саме на етапі проектування закладається фундамент резильєнтності системи до майбутніх векторів атак. В умовах ескалації кіберзагроз стратегічним імперативом для індустрії стає зміна виробничої парадигми з пріоритету швидкості виходу на ринок (Time-to-Market) на пріоритет безпеки продукту (Security-First).

Фундаментальною вимогою є імплементація методології безпечного життєвого циклу розробки (Secure Software Development Life Cycle, SSDLC)[24]. Реалізація принципу Security by Design вимагає інтеграції процедур безпеки на кожному етапі створення продукту: від архітектурного моделювання загроз (Threat Modeling) до написання коду. Критично важливим є впровадження практик DevSecOps, що передбачає автоматизоване використання інструментів статичного (SAST) та динамічного (DAST) аналізу коду в пайплайнах безперервної інтеграції (CI/CD). Це дозволяє виявляти та усувати вразливості, такі як переповнення буфера чи ін'єкції коду, ще на етапі компіляції, мінімізуючи "технічний борг" у сфері безпеки.

Технічна реалізація пристроїв повинна суворо відповідати базовим вимогам міжнародних стандартів ETSI EN 303 645 та NIST IR 8259. Абсолютним

стандартом індустрії має стати категорична відмова від використання жорстко закодованих облікових даних (Hardcoded Credentials) та універсальних паролів адміністратора. Архітектура пристрою повинна передбачати генерацію унікальних криптографічних ідентифікаторів при першому запуску або примушувати користувача до зміни заводських налаштувань. Захист комунікаційних інтерфейсів вимагає обов'язкової імплементації протоколів шифрування транспортного рівня (TLS 1.2/1.3) з валідацією сертифікатів (Certificate Pinning), що унеможливлює атаки типу Man-in-the-Middle[3,5].

Сучасний ландшафт загроз диктує необхідність апаратного посилення безпеки (Hardware Hardening). Виробникам рекомендується використовувати мікроконтролери з підтримкою технології безпечного завантаження (Secure Boot), яка гарантує запуск виключно авторизованого та підписаного цифровим підписом коду. Інтеграція апаратних модулів довіри (Hardware Root of Trust), таких як TPM або HSM, забезпечує захищене середовище для генерації та зберігання криптографічних ключів, унеможливлюючи їх екстракцію навіть при фізичному доступі зловмисника до пристрою. Додатковим заходом є фізичне відключення або програмне блокування інтерфейсів налагодження (JTAG/UART) на серійних зразках продукції[5,8].

Критичним елементом прозорості екосистеми є формування специфікації програмних компонентів (Software Bill of Materials, SBOM). Надання повного переліку використовуваних сторонніх бібліотек та Open Source компонентів дозволяє оперативно ідентифікувати та нейтралізувати ризики, пов'язані з атаками на ланцюги постачання (Supply Chain Attacks). Процес супроводу продукту повинен регламентуватися політикою координованого розкриття вразливостей (Coordinated Vulnerability Disclosure, CVD) із чітким визначенням каналів комунікації з дослідниками безпеки.

Забезпечення довгострокової надійності вимагає реалізації механізму безпечного оновлення прошивки "по повітрю" (Secure OTA Updates). Процедура оновлення має бути атомарною, стійкою до збоїв живлення та включати обов'язкову перевірку цифрового підпису пакету оновлення перед його

інсталяцією. Завершальним етапом є незалежна верифікація безпеки продукту шляхом сертифікації згідно з міжнародними стандартами (наприклад, UL 2900 або Eurosmart IoT Security Certification) та публічне декларування гарантованого терміну підтримки оновлень безпеки, що надає споживачам об'єктивний критерій для вибору захищеного рішення[5,6].

5.4 Адаптація рекомендацій для українського контексту

Імплементація концепцій розумного міста та житла в Україні відбувається в унікальних умовах перманентної гібридної агресії, що вимагає фундаментальної адаптації загальносвітових практик кібербезпеки до реалій національної оборони. У вітчизняному контексті захист IoT-екосистем трансформується з суто технічної дисципліни у складову національної безпеки, оскільки цифрова інфраструктура життєзабезпечення розглядається супротивником як легітимна ціль для кінетичних та кібернетичних атак, спрямованих на дестабілізацію тилу та створення гуманітарних криз.

Стратегічним архітектурним пріоритетом для українських Smart City має стати забезпечення автономності та живучості (Survivability)[22] критичних сервісів. Архітектура систем управління енерго-водопостачанням та транспортом повинна проектуватися з урахуванням можливості функціонування в умовах повної ізоляції від глобальної мережі та центральних дата-центрів. Це актуалізує застосування технологій периферійних обчислень (Edge Computing), які дозволяють локальним контролерам насосних станцій або теплопунктів підтримувати технологічні процеси в автономному режимі («острівний режим») навіть при фізичному пошкодженні магістральних каналів зв'язку. Муніципалітети зобов'язані розробити та відпрацювати жорсткі протоколи фізичної ізоляції сегментів мережі для локалізації наслідків кібератак та недопущення каскадного поширення відмов на суміжні об'єкти критичної інфраструктури.

Нормативно-правове регулювання сфери IoT вимагає негайної уніфікації та гармонізації з європейським законодавством, зокрема з положеннями EU

Cyber Resilience Act, з урахуванням специфіки воєнних загроз. Нагальною потребою є розробка національного галузевого стандарту, який встановить імперативні вимоги до кіберзахисту IoT-систем, що закуповуються за бюджетні кошти. Цей стандарт має детермінувати «червоні лінії» безпеки, порушення яких є неприпустимим, нівелюючи практику закупівлі найдешевших рішень із нульовим рівнем захисту[5]. Впровадження обов'язкової сертифікації обладнання для об'єктів критичної інфраструктури дозволить створити бар'єр для проникнення вразливих технологій у державний сектор.

Питання технологічного суверенітету та безпеки ланцюгів постачання набуває критичного значення в умовах війни. Залежність національної інфраструктури від апаратних платформ іноземного виробництва, особливо з юрисдикцій з високим рівнем геополітичного ризику, створює загрози наявності недекларованих можливостей (Backdoors) та несанкціонованого збору розвідувальної інформації[14]. Державна політика повинна фокусуватися на стимулюванні вітчизняного сегменту DefenseTech та Smart City через грантові механізми та державні замовлення, що сприятиме імпортозаміщенню критичних компонентів та розвитку довіреної мікроелектроніки. Диверсифікація постачальників є ключовим інструментом мінімізації ризиків, пов'язаних із глобальними логістичними кризами та політичним тиском.

Реалізація зазначених заходів неможлива без системного розвитку людського капіталу. Дефіцит кваліфікованих фахівців із безпеки промислових систем управління (ICS/SCADA) є стратегічним викликом, що вимагає інтеграції спеціалізованих освітніх модулів у програми технічних університетів та створення центрів компетенцій на базі профільних відомств[26]. Ефективна протидія гібридним загрозам можлива лише у форматі державно-приватного партнерства, де експертиза приватного сектору кібербезпеки поєднується з адміністративними ресурсами Держспецзв'язку та Служби безпеки України для побудови ешелонованої оборони українських міст.

5.5 Перспективи розвитку та удосконалення систем

Експоненційне зростання складності IoT-інфраструктури та перманентна еволюція векторів атак детермінують необхідність технологічної трансформації парадигми кібербезпеки. Аналіз перспективних трендів свідчить, що архітектура захисту розумних екосистем наступного покоління буде базуватися на адаптивності, інтелектуалізації та криптографічній стійкості до загроз постквантової ери.

Стратегічним технологічним викликом найближчого десятиліття є поява квантових обчислювальних потужностей, здатних скомпрометувати сучасні стандарти асиметричного шифрування (RSA, ECC), що складають основу PKI-інфраструктури Інтернету речей[30]. Відповіддю на цю загрозу є активна імплементація алгоритмів постквантової криптографії (Post-Quantum Cryptography, PQC). Для забезпечення довгострокової життєздатності інфраструктури розумних міст критично важливим є закладання принципу криптографічної гнучкості (Crypto-agility) на етапі проектування, що дозволить здійснювати безшовну міграцію на нові криптографічні примітиви через механізми оновлення прошивки без необхідності апаратної модернізації парку пристроїв.

Якісний стрибок у ефективності детекції загроз пов'язаний з інтеграцією технологій штучного інтелекту (AI) та машинного навчання (ML) у контур безпеки[27]. Традиційні сигнатурні методи поступаються місцем системам поведінкової аналітики (User and Entity Behavior Analytics, UEBA), здатним виявляти аномалії та атаки нульового дня в режимі реального часу. Перспективним напрямком є розвиток концепції самовідновлюваних мереж (Self-Healing Networks), де AI-агенти не лише ідентифікують інцидент, але й автономно реалізують сценарії реагування: ізолюють скомпрометовані сегменти, перерозподіляють навантаження та ініціюють відновлення конфігурацій, забезпечуючи живучість системи без втручання людини.

Архітектурним стандартом де-факто стає модель нульової довіри (Zero Trust Architecture), що постулює відмову від концепції захищеного

периметра[22]. У середовищі ZTA кожен запит на доступ до ресурсу підлягає суворій верифікації контексту, незалежно від місця його ініціації. Впровадження технологій динамічної мікросегментації дозволить реалізувати гранулярний контроль доступу на рівні окремих IoT-датчиків, гарантуючи локалізацію інцидентів та мінімізацію радіусу ураження.

Додатковий рівень довіри та прозорості забезпечує інтеграція технологій розподілених реєстрів (Distributed Ledger Technology). Блокчейн-рішення відкривають шлях до створення децентралізованих систем управління ідентичністю (Decentralized Identity, DID), що усуває ризики єдиної точки відмови, притаманні централізованим центрам сертифікації[20]. Використання смарт-контрактів дозволяє автоматизувати процеси безпечної взаємодії гетерогенних пристроїв та забезпечити незмінність журналів аудиту, що є критичним для розслідування інцидентів.

Успішна реалізація зазначених перспективних напрямків вимагає консолідації зусиль держави, індустрії та наукової спільноти. Створення відкритих платформ для обміну даними про загрози (Threat Intelligence Sharing) та розробка інтероперабельних стандартів безпеки є необхідною умовою для побудови стійкої цифрової екосистеми, здатної забезпечити безпеку та комфорт громадян у світі майбутнього.

Висновок до п’ятого розділу

В п’ятому розділі було розроблено комплекс практичних рекомендацій для різних категорій стейкхолдерів. Для користувачів розумних домів основною засадою зберігається збереження кібергігієни: відмова від дефолтних паролів на унікальній комбінації, активація багатофакторної автентифікації та автоматичне оновлення прошивки. На рівнях мережі критично важливо ввести сегмент IoT-пристроїв в ізольовану VLAN для запобігання горизонтальній переміщенню загрози.

Органи місцевого самоврядування мають дієвий системний перехід до стратегічного планування, де кібербезпека інтегрована як базова складова

розвитку. Першочергові заходи включають розробку Політики безпеки критичної інфраструктури, тотальну інвентаризацію активів та регулярні системи аудиту. Архітектурна стійкість досягається через географічну диверсифікацію центрів обробки даних та забезпечення автономного функціонування сервісів у режимі розриву з глобальною мережею.

Розробники IoT-пристроїв мають переорієнтацію з оптимальної швидкості на оптимальну безпеку через запровадження методології SSDLC та Security by Design. Абсолютним стандартом є статистична відмова від жорстко закодованих паролів, обов'язкова реалізація шифрування TLS, апаратне посилення безпеки та публікація Software Bill of Materials.

Для контексту гібридної агресії критичне українське місце є адаптація глобальних практик до реальної національної оборони. Архітектура критичної інфраструктури повинна проектуватися з урахуванням можливостей автономного функціонування в ізоляції, що актуалізує Edge Computing. Нагальною є розробка національного стандарту безпеки IoT та стимулювання вітчизняного DefenseTech-сегменту.

Перспективи розвитку пов'язані з інтеграцією постквантової криптографії, широким застосуванням AI для проактивного виявлення аномалій та впровадженням архітектури нульової довіри як стандарту де-факто. Успішна реалізація вимагає консолідації зусиль держави, індустрії та наукової спільноти в напрямку створення стійкої цифрової екосистеми.

Висновок

У дипломній роботі проведено комплексне дослідження проблематики забезпечення інформаційної безпеки в гетерогенних системах Інтернету речей класів «розумний дім» та «розумне місто». На основі системного аналізу архітектурних особливостей, моделювання векторів загроз та оцінки ефективності захисних механізмів отримано низку наукових та практичних результатів, що підтверджують актуальність та досягнення мети дослідження.

У ході аналізу архітектури та ландшафту загроз встановлено, що домінуюча сьогодні типова конфігурація IoT-систем характеризується високим рівнем фрагментації, використанням застарілих комунікаційних протоколів без вбудованого шифрування та наявністю «плоскої» мережевої топології. Визначено, що найбільшу небезпеку становлять вразливості прикладного рівня та рівня пристроїв, зокрема повсюдне використання жорстко закодованих автентифікаційних даних та відсутність механізмів безпечного оновлення програмного забезпечення. Систематизація векторів атак згідно з класифікацією OWASP IoT Top 10 дозволила виділити критичні загрози, серед яких компрометація облікових записів, DDoS-атаки ботнетів та атаки на ланцюги постачання займають провідні позиції.

Розробка та застосування адаптованої матриці ризиків для IoT-середовищ дозволили класифікувати загрози за ступенем їх впливу на конфіденційність, цілісність та доступність даних. Доведено, що в умовах гібридної війни кіберзагрози для систем Smart City трансформуються у загрози національній безпеці, оскільки атаки на критичну інфраструктуру, таку як енерго- та водопостачання, мають кінетичний ефект та здатні спричинити масштабні гуманітарні кризи. Це підкреслює необхідність зміни парадигми захисту від суто технічної до стратегічної, орієнтованої на забезпечення живучості та автономності систем.

Ключовим етапом роботи став порівняльний аналіз захищеності типової та запропонованої модернізованої архітектури. Математичне моделювання підтвердило, що впровадження комплексу заходів, який включає

мікросегментацію мережі, перехід на захищені протоколи TLS 1.3, застосування багатофакторної автентифікації та реалізацію політик нульової довіри, дозволяє знизити інтегральний показник кіберризику системи майже на 70%. Таке зниження фактично переводить стан системи з категорії критичної вразливості у стан контрольованого залишкового ризику, що є необхідною умовою для безпечної експлуатації.

Розрахунок коефіцієнта повернення інвестицій у безпеку (ROSI) продемонстрував високу економічну ефективність запропонованих рішень, показник якої перевищує 1000%. Це свідчить про те, що превентивні витрати на архітектурну оптимізацію та організаційні заходи є на порядок нижчими за потенційні збитки від ліквідації наслідків успішних кібератак, що обґрунтовує економічну доцільність інвестицій у підхід Security by Design.

За результатами дослідження розроблено диференційовані рекомендації для ключових стейкхолдерів: користувачам запропоновано зосередитися на кібергігієні та сегментації домашніх мереж; муніципалітетам — впровадити стратегії забезпечення автономності критичних вузлів та диверсифікації постачальників; а розробникам — перейти до методології безпечного життєвого циклу розробки та впровадження апаратних коренів довіри. Визначено, що подальша еволюція систем захисту буде спрямована на впровадження адаптивних механізмів на базі штучного інтелекту для виявлення аномалій у реальному часі, перехід до постквантової криптографії для нівелювання перспективних загроз та широке застосування архітектури нульової довіри як де-факто стандарту індустрії. Таким чином, запропонована комплексна стратегія захисту дозволяє суттєво підвищити рівень кіберстійкості IoT-систем, забезпечуючи безпечне функціонування інфраструктури та захист приватності в умовах сучасних викликів.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [43].

Список використаних джерел

1. NIST SP 1800-15. Guide to Iot Security. National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.1800-15
2. NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. National Institute of Standards and Technology, 2011. https://doi.org/10.6028/NIST.SP.800-39
3. NIST SP 800-213. Cybersecurity and Privacy Guidance for IoT Devices. National Institute of Standards and Technology, 2023. https://doi.org/10.6028/NIST.SP.800-213-draft
4. ACEEE Research. Energy Efficiency of Wireless Technologies. American Council for an Energy-Efficient Economy, 2022. https://www.aceee.org/
5. ETSI EN 303 645. Cybersecurity for Consumer Internet of Things. European Telecommunications Standards Institute, 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
6. ENISA Good Practices for IoT Security. European Union Agency for Cybersecurity, 2020. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
7. NIST IR 8228. Considerations for Managing Internet of Things Cybersecurity and Privacy Risks. National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.IR.8228
8. NIST IR 8259A. IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.IR.8259A
9. OWASP IoT Top 10. Open Web Application Security Project, 2021. https://owasp.org/Top10/2021/A00_2021_Introduction/
10. NIST SP 800-53 (Security and Privacy Controls

https://doi.org/10.6028/NIST.SP.800-53r5

11. Roman, R., Zhou, J., & Lopez, J. On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2340-2365, 2013.
https://www.nics.uma.es/pub/papers/roman2013iot.pdf
12. Atzori, L., Iera, A., & Morabito, G. The Internet of Things: A survey. Computer networks, 54(15), 2787-2805, 2010.
DOI: 10.1016/j.comnet.2010.05.010
13. Modeling and reasoning of IoT architecture in semantic ontology dimension
https://doi.org/10.1016/j.comcom.2020.02.006
14. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
15. RFC 6234. US Secure Hash Algorithms. Internet Engineering Task Force, 2011.
https://datatracker.ietf.org/doc/html/rfc6234
16. RFC 3394. AES Key Wrap Algorithm. Internet Engineering Task Force, 2002.
https://datatracker.ietf.org/doc/html/rfc3394
17. RFC 7539. ChaCha20 and Poly1305 AEAD Ciphers. Internet Engineering Task Force, 2015.
https://datatracker.ietf.org/doc/html/rfc7539
18. "National Institute of Standards and Technology. Technical Security Testing and Penetration Testing Procedures. NIST Special Publication 800-115, 2008.
https://doi.org/10.6028/NIST.SP.800-115
19. GDPR (EU) 2016/679. General Data Protection Regulation. European Parliament and Council of the European Union, 2016.
https://eur-lex.europa.eu/eli/reg/2016/679/oj
20. The NIST Cybersecurity Framework (CSF) 2.0
https://doi.org/10.6028/NIST.CSWP.29
21. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile

https://doi.org/10.6028/NIST.SP.800-61r3

22. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-207
23. CVSS 3.1. Common Vulnerability Scoring System. FIRST (Forum of Incident Response and Security Teams), 2019. https://www.first.org/cvss/v3-1/specification-document
24. NIST SP 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://doi.org/10.6028/NIST.SP.800-171r3
25. NIST SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations https://doi.org/10.6028/NIST.SP.800-161r1-upd1
26. NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security https://doi.org/10.6028/NIST.SP.800-82r3
27. NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile https://doi.org/10.6028/NIST.SP.800-61r3
28. FIDO2/WebAuthn. Web Authentication: An API for accessing Public Key Credentials. World Wide Web Consortium (W3C), 2021. https://www.w3.org/TR/webauthn-2/
29. RFC 6749. The OAuth 2.0 Authorization Framework. Internet Engineering Task Force, 2012. https://datatracker.ietf.org/doc/html/rfc6749
30. NIST Post-Quantum Cryptography Standardization. National Institute of Standards and Technology, 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/
31. Довженко, Н., Мазур, Н., Костюк, Ю., & Рзаєва, С. (2024). Інтеграція IoT та штучного інтелекту в інтелектуальні транспортні системи.

Кібербезпека: освіта, наука, техніка, 2(26), 430–444. https://doi.org/10.28925/2663-4023.2024.26.708

32. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Кібербезпека: освіта, наука, техніка, 1(25), 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
33. Довженко, Н., Іваніченко, Є., Костюк, Ю., & Петришин, Л. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938
34. I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi:10.1007/978-3-030-30859-9_2
35. V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518
36. O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.
37. V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.
38. B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76

39. M. Moshenchenko, et al., Optimization algorithms of smart city wireless sensor network control, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, 2021, 32–42.
40. O. Bahatskyi, V. Bahatskyi, V. Sokolov, Smart Home Subsystem for Calculating the Quality of Public Utilities, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 168–173.
41. V. Zhebka, et al., Methods for predicting failures in a smart home, in: Digital Economy Concepts and Technologies Workshop, vol. 3665, 2024, 70–78.
42. Viktoriia Onyshchenko, Svitlana Shevchenko and Olena Negodenko. Models of Information Processing in IoT Networks on the Basis of Fundamental Trigonometric Splines. - 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications. Science and Technology PIC S&T`2019. C. 613-616. ISSN ISBN 978-1-7281-4184-8.
43. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf

Додаток А

Тестування стійкості механізмів автентифікації.

```
import paho.mqtt.client as mqtt
import time
import sys
 # ПАРАМЕТРИ АТАКИ
TARGET_IP = "192.168.1.100"      # IP адреса IoT-мережі
TARGET_PORT = 1883               # Стандартний MQTT порт
TIMEOUT = 2                      # Timeout з'єднання (сек)
USERNAMES = ["admin", "root", "user", "service", "mqtt_user"]
PASSWORDS = ["123456", "password", "admin123", "12345", "root"]
def try_connect(username, password):
"""
Спроба підключення до MQTT брокера
 """
try:
print(f"[*] Trying credentials: ({username}:{password}) ...", end="")
client = mqtt.Client()
client.username_pw_set(username, password)
 client.connect(TARGET_IP, TARGET_PORT, TIMEOUT)
 client.loop_start()
time.sleep(0.5)
 if client.is_connected():
print(f" [SUCCESS!]")
print(f"[+] VALID CREDENTIALS FOUND: {username}:{password}")
client.disconnect()
return True
else:
```

```
print(f" [FAILED]")
return False
 except Exception as e:
print(f" [ERROR] {e}")
return False
# ОСНОВНИЙ ЦИКЛ BRUTE-FORCE АТАКИ
 print("--- Starting IoT Brute-Force Simulation Tool ---")
print(f"Target: {TARGET_IP}:{TARGET_PORT}")
found = False
for username in USERNAMES:
for pwd in PASSWORDS:
if try_connect(username, pwd):
found = True
break
if found:
break
if not found:
print("[!] No credentials found in dictionary.")
```

Комплексна конфігурація захисту: налаштування TLS та правила iptables

```
bash
# ========================================
# 1. КОНФІГУРАЦІЯ MQTT БРОКЕРА (mosquitto.conf)
# ========================================
# Заборона анонімного доступу
allow_anonymous false
# Шлях до файлу паролів
password_file /etc/mosquitto/passwd
# Використання TLS/SSL для шифрування
listener 8883
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key
cafile /etc/mosquitto/certs/ca.crt
# Відключення незахищеного порту 1883
# listener 1883 (коментуємо для безпеки)
# ========================================
# 2. ПРАВИЛА МЕРЕЖЕВОГО ЕКРАНУ (IPTABLES)
# ========================================
# Очищення старих правил
```

```
iptables -F
# Політика за замовчуванням: БЛОКУВАТИ все вхідне
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
# Дозвіл вже встановлених з'єднань
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Дозвіл локального трафіку (Loopback)
iptables -A INPUT -i lo -j ACCEPT
# Дозвіл захищеного MQTT (Port 8883)
iptables -A INPUT -p tcp --dport 8883 -j ACCEPT
# Блокування спроб DoS-атак (обмеження частоти запитів)
iptables -A INPUT -p tcp --dport 8883 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
# Логування відхилених пакетів
iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: "
```