НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ВДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ ВІД АТАК НА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Кравцуненко Микола Миколайович

Керівник: к.т.н., доцент
Фразе-Фразенко Олексій Олексійович

Рецензент: доктор філософії
Слатвінська Валерія Миколаївна

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет кібербезпеки та інформаційних технологій
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Кравцуненко Миколі Миколайовичу

1. Тема роботи: «Вдосконалення методів захисту від атак на системи інтернету речей»
Керівник роботи: к.т.н., доцент Фразе-Фразенко Олексій Олексійович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16 » вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області та пошук науково-технічної інформації за темою роботи	Вересень-жовтень 2024	
2	Узгодження теми з науковим керівником, формулювання мети завдань дослідження	Листопад 2024	
3	Робота над першим розділом	Листопад-грудень 2024	
4	Робота над другим розділом	Січень-лютий 2025	
5	Робота над третім розділом	Лютий-березень 2025	
6	Уточнення подальшого обсягу роботи та його коригування	Березень-травень 2025	
7	Оформлення звітної частини	Травень 2025	
8	Захист роботи	12.06.2025	

Здобувач_____
(підпис) (прізвище та ініціали)

Керівник роботи_____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Вдосконалення методів захисту від атак на системи Інтернету речей” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 2 рисунків, 4 таблиць, 24 літературних джерел за переліком посилань. Робота виконана на 46 сторінках загального тексту і 37 сторінці основного тексту.

Метою роботи є створення застосунку, розробка алгоритму для вдосконалення захисту систем Інтернету речей від кібератак. Розроблено модель захищеної IoT-системи, що включає алгоритми шифрування AES-128 і ChaCha, протоколи DTLS і CoAP, багаторівневу аутентифікацію з використанням OAuth 2.0 і цифрових сертифікатів, а також систему моніторингу на основі штучного інтелекту з алгоритмом Isolation Forest. Програмно реалізовано механізми шифрування, моніторингу трафіку, проведено тестування в симульованих умовах, що показало стійкість до атак (100% для несанкціонованого доступу, MITM і експлуатації вразливостей, 95% для DoS).

Результати роботи можуть бути використані розробниками та операторами IoT-систем у промислових, медичних, транспортних і розумних міських додатках для підвищення безпеки даних.

Можливими напрямками подальших досліджень є впровадження постквантової криптографії, інтеграція технологій 6G і граничних обчислень для підвищення швидкості реагування, а також розробка стандартизованих підходів до безпеки для масштабних IoT-екосистем.

КІБЕРБЕЗПЕКА, ІНТЕРНЕТ РЕЧЕЙ, КРИПТОГРАФІЯ, АУТЕНТИФІКАЦІЯ, ВИЯВЛЕННЯ ВТОРГНЕНЬ.

ABSTRACT

Qualification work on the topic “Improving Methods for Protecting Against Attacks on Internet of Things Systems” for obtaining the first (bachelor’s) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 2 figures, 4 tables, and 24 literary sources listed in the references. The work spans 46 pages of total text and 37 pages of main text.

The aim of the work is to create an application, develop an algorithm to improve the protection of Internet of Things systems from cyberattacks. A model of a secure IoT system was developed, incorporating AES-128 and ChaCha encryption algorithms, DTLS and CoAP protocols, multi-level authentication using OAuth 2.0 and digital certificates, and an AI-based monitoring system with the Isolation Forest algorithm. Mechanisms for encryption, traffic monitoring, and threat response were programmatically implemented, with testing conducted in simulated conditions, demonstrating resilience to attacks (100% for unauthorized access, MITM, and vulnerability exploitation, 95% for DoS) and a response time of 0.5 to 2 seconds.

The results of the work can be utilized by developers and operators of IoT systems in industrial, medical, transportation, and smart city applications to enhance data security, ensure compliance with ISO/IEC 27001 and NIST standards, and in cybersecurity educational programs. The recommendations help reduce the risks of data interception, DoS attacks, and unauthorized access.

Possible directions for further research include the implementation of post-quantum cryptography, integration of 6G technologies and edge computing to improve response speed, and the development of standardized security approaches for large-scale IoT ecosystems.

CYBERSECURITY, INTERNET OF THINGS, CRYPTOGRAPHY, AUTHENTICATION, INTRUSION DETECTION.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі системи Інтернету речей відіграють ключову роль у багатьох сферах, включаючи розумні міста, охорону здоров’я, промислову автоматизацію, транспорт і побутові технології. У 2024 році кількість підключених IoT-пристроїв у світі перевищила 15 мільярдів, і ця цифра продовжує зростати. Водночас швидке поширення IoT-технологій супроводжується значним зростанням кіберзагроз, спрямованих на порушення безпеки цих систем. Згідно з дослідженням Cybersecurity Ventures, глобальні витрати на кібербезпеку в 2024 році перевищили 200 мільярдів доларів США, при цьому значна частка кібератак стосувалася IoT-пристроїв через їхню вразливість, обмежені обчислювальні ресурси та різноманітність протоколів зв’язку. В Україні, де IoT-технології активно застосовуються в інфраструктурних проєктах і критичних системах, захист цих систем набуває стратегічного значення, особливо в умовах зростання кіберзагроз на тлі геополітичних викликів.

Основними загрозами для IoT-систем є атаки типу DDoS, перехоплення даних, атаки "людина посередині" (Man-in-the-Middle), а також несанкціонований доступ до пристроїв і мереж. Існуючі методи захисту, такі як шифрування AES, протоколи TLS чи механізми аутентифікації, забезпечують базовий рівень безпеки, але часто є недостатньо ефективними проти складних атак, зокрема тих, що використовують штучний інтелект, квантові обчислення або експлойти нульового дня. Критичний аналіз літератури (зокрема праць IEEE, NIST, а також досліджень компаній Cisco та Palo Alto Networks) свідчить про необхідність розробки комплексних підходів до захисту IoT-систем, які поєднують криптографічні методи, технології моніторингу загроз і адаптивні протоколи безпеки. Таким чином, актуальність дослідження зумовлена потребою вдосконалення методів захисту IoT-систем для забезпечення їхньої стійкості до сучасних кіберзагроз і підтримки надійного функціонування в умовах зростаючої складності атак.

Мета дослідження є створення застосунку та розробка алгоритму для вдосконалення захисту систем Інтернету речей від кібератак.

Завдання дослідження:

- визначити принципи роботи систем Інтернету речей та їхні особливості в контексті кібербезпеки.
- класифікувати основні типи кіберзагроз для IoT-систем та оцінити їхній потенційний вплив.
- надати характеристику сучасних методів і технологій захисту IoT-систем, визначивши їхні переваги та недоліки.
- проаналізувати криптографічні методи захисту даних у IoT-системах та оцінити їхню ефективність.
- дослідити протоколи аутентифікації та управління доступом для забезпечення безпеки IoT-пристроїв.
- оцінити можливості технологій виявлення та запобігання вторгненням у контексті захисту IoT-систем.
- розробити модель захищеної IoT-системи з урахуванням виявлених вимог і загроз.
- провести тестування запропонованої моделі захисту та проаналізувати її ефективність.
- сформулювати рекомендації щодо впровадження системи захисту IoT у реальних умовах.

Об’єкт дослідження – процеси забезпечення безпеки систем Інтернету речей, що охоплюють передачу даних, взаємодію пристроїв і захист від зовнішніх кіберзагроз у контексті їхньої критичної ролі для виконання функціональних завдань.

Предмет дослідження – методи, технології та організаційні підходи до забезпечення захисту систем Інтернету речей, спрямовані на підвищення їхньої стійкості до кіберзагроз, зокрема DDoS-атак, перехоплення даних і несанкціонованого доступу, з урахуванням сучасних технологічних і операційних вимог.

Практичне значення отриманих результатів. Результати дослідження мають практичну цінність для розробників, операторів і користувачів IoT-систем у різних

секторах, включаючи промисловість, охорону здоров’я, транспорт і розумні міста. Запропонована адаптивна система захисту, що включає алгоритми шифрування, методи моніторингу загроз і протидії атакам, може бути впроваджена в IoT-системи для підвищення їхньої безпеки та надійності. Рекомендації щодо конфігурації системи дозволять мінімізувати ризики компрометації даних і скоротити час реагування на кіберінциденти. Отримані результати можуть бути використані для вдосконалення стандартів кібербезпеки IoT, розробки навчальних програм для фахівців із кібербезпеки та адаптації національних і міжнародних нормативів у сфері IoT-технологій. Запропоновані рішення є універсальними й можуть застосовуватися в різних країнах і умовах експлуатації IoT-систем.

1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Особливості архітектури та функціонування систем Інтернету речей

Інтернет речей є однією з найперспективніших технологій сучасності, що радикально змінює взаємодію між фізичними об’єктами та цифровим світом. Ця концепція передбачає підключення різноманітних пристроїв до мережі Інтернет для збору, передачі, обробки та використання даних у реальному часі. Від побутових приладів, таких як розумні термостати, до складних промислових систем моніторингу, Інтернет речей створює екосистему, де об’єкти стають «розумними», здатними до автономної взаємодії та прийняття рішень. Архітектура та функціонування таких систем мають унікальні особливості, які визначаються вимогами до масштабованості, безпеки, енергоефективності, сумісності та адаптивності до різноманітних застосувань [1].

Архітектура Інтернету речей є багатошаровою структурою, яка забезпечує комплексну обробку інформації від збору даних до їх використання в прикладних програмах. Зазвичай виділяють чотири основні рівні: рівень сприйняття, рівень мережі, рівень обробки даних і рівень прикладних програм. Кожен рівень виконує специфічні функції, що сприяють ефективній роботі системи в цілому.

Рівень сприйняття є початковим етапом функціонування систем Інтернету речей. Він відповідає за взаємодію з фізичним середовищем через датчики, сенсори, камери, мікрофони та виконавчі механізми. Ці пристрої фіксують параметри навколишнього світу, такі як температура, вологість, тиск, освітленість, рух або звук, і перетворюють їх у цифрові сигнали [2]. Наприклад, у розумному будинку датчик руху може активувати систему освітлення, а в сільському господарстві датчики вологості ґрунту оптимізують полив. Ключовою особливістю цього рівня є обмежені ресурси пристроїв, що вимагає високої енергоефективності. Більшість датчиків живляться від батарей, тому їхнє апаратне та програмне забезпечення оптимізується для мінімального енергопотребу, що дозволяє працювати протягом тривалого часу без заміни джерел живлення.

Рівень мережі забезпечує передачу даних між пристроями, шлюзами, серверами та хмарними платформами. Для цього використовуються різноманітні технології зв’язку, включаючи Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN, NB-IoT і 5G. Вибір протоколу залежить від вимог до дальності передачі, пропускної здатності, енергоефективності та вартості. Наприклад, LoRaWAN ефективний для низькошвидкісних мереж із великою дальністю дії, таких як системи моніторингу в сільському господарстві, тоді як 5G забезпечує високу швидкість і низьку затримку для критичних застосувань, таких як автономні транспортні засоби чи телемедицина. Гетерогенність є визначальною рисою цього рівня, оскільки системи Інтернету речей часто інтегрують кілька типів мереж і протоколів для забезпечення гнучкості, надійності та стійкості до збоїв [3].

Для забезпечення ефективної взаємодії пристроїв у системах Інтернету речей використовується низка спеціалізованих протоколів зв’язку, які відповідають різним вимогам до швидкості, енергоспоживання та дальності передачі. Ось основні з них:

1. MQTT - Легкий протокол для передачі даних у мережах із обмеженими ресурсами, що використовує модель «публікація-підписка» для ефективного обміну повідомленнями.
2. CoAP - Протокол, оптимізований для пристроїв із низьким енергоспоживанням, який працює за моделлю «клієнт-сервер» і підтримує передачу даних у мережах із обмеженою пропускною здатністю.
3. HTTP/2 - Сучасна версія протоколу HTTP, що забезпечує швидку передачу даних із підтримкою стиснення заголовків і мультиплексування.
4. LoRaWAN - Протокол для низькошвидкісних мереж із великою дальністю дії, який ідеально підходить для застосувань, де потрібна передача невеликих обсягів даних на великі відстані.
5. NB-IoT - Технологія для вузькосмугових мереж, що забезпечує низьке енергоспоживання та стабільне з’єднання в умовах обмеженого покриття [4].

Ці протоколи дозволяють адаптувати системи Інтернету речей до різних сценаріїв використання, від локальних мереж у розумних будинках до глобальних систем моніторингу.

Функціонування систем Інтернету речей базується на безперервному циклі збору, передачі, обробки та використання даних. Основними аспектами є автоматизована взаємодія пристроїв, забезпечення безпеки, підтримка масштабованості, інтеграція з іншими технологіями та адаптація до змінних умов.

Рівень обробки даних відповідає за аналіз, зберігання та інтерпретацію інформації, отриманої від пристроїв. Цей рівень може включати локальні обчислювальні ресурси, такі як шлюзи, мікроконтролери чи граничні сервери, а також хмарні платформи для великомасштабної обробки. Сучасні системи дедалі частіше використовують граничні обчислення, коли обробка даних виконується безпосередньо на пристроях або поблизу них. Це зменшує затримки, знижує навантаження на мережу та підвищує ефективність. Наприклад, у системах відеоспостереження граничні обчислення дозволяють аналізувати відеопотік на місці, передаючи в хмару лише релевантні дані. Особливістю цього рівня є необхідність обробки великих обсягів даних у реальному часі, що вимагає застосування алгоритмів штучного інтелекту, машинного навчання та технологій аналізу великих даних.

Рівень прикладних програм забезпечує взаємодію користувачів із системою через спеціалізовані інтерфейси, такі як мобільні додатки, вебпортали, інформаційні панелі чи системи управління. На цьому рівні реалізуються конкретні сценарії використання, які відповідають потребам різних галузей. Наприклад, у розумному будинку користувач може керувати освітленням, опаленням і безпекою через єдиний додаток, а в промислових системах дані з датчиків використовуються для прогнозування несправностей обладнання. Гнучкість цього рівня дозволяє адаптувати системи до різноманітних застосувань, включаючи розумні міста, логістику, охорону здоров’я та енергетику.

Безпека є критично важливим аспектом, оскільки системи Інтернету речей обробляють конфіденційні дані, такі як персональна інформація, медичні записи чи

промислові параметри. Основні загрози включають несанкціонований доступ, перехоплення даних, атаки типу «відмова в обслуговуванні» та маніпуляції з пристроями. Для захисту застосовуються методи шифрування, такі як TLS і AES, а також механізми аутентифікації, включаючи двофакторну аутентифікацію та цифрові сертифікати. Технології блокчейн використовуються для забезпечення цілісності даних у таких системах, як ланцюги поставок. Сегментація мережі, регулярне оновлення програмного забезпечення та апаратні модулі безпеки додатково знижують ризики.

Системи Інтернету речей повинні підтримувати зростаючу кількість пристроїв і обсяги даних. Наприклад, у розумному місті кількість підключених пристроїв може досягати мільйонів, що вимагає ефективного розподілу ресурсів. Хмарні платформи, такі як Amazon Web Services, Microsoft Azure і Google Cloud, забезпечують динамічне масштабування, а архітектури на основі мікросервісів підвищують гнучкість і модульність. Масштабованість також передбачає адаптацію до різних сценаріїв, від локальних систем із кількома пристроями до глобальних мереж [5].

Інтеграція з технологіями, такими як великі дані, штучний інтелект, блокчейн і доповнена реальність, розширює можливості систем Інтернету речей. Аналіз великих даних виявляє закономірності, штучний інтелект автоматизує прийняття рішень, блокчейн забезпечує прозорість транзакцій, а доповнена реальність покращує взаємодію користувачів. Сумісність із різними платформами та стандартами забезпечує універсальність систем.

1.2 Типи кібератак на IoT-системи та їх класифікація

Інтернет речей є технологією, що забезпечує підключення різноманітних пристроїв до мережі для збору, передачі та обробки даних. Однак зростання кількості IoT-пристроїв супроводжується збільшенням кіберзагроз, які можуть порушити їх функціонування, викрасти конфіденційні дані або використати пристрої для атак на інші системи. Кібератаки на IoT-системи є різноманітними за

своєю природою, цілями та методами реалізації, що вимагає їх систематизації для ефективного захисту.

Кібератаки на IoT-системи можна класифікувати за кількома критеріями, включаючи ціль атаки, метод реалізації та рівень впливу. Одним із найпоширеніших типів є атаки, спрямовані на отримання несанкціонованого доступу до пристроїв. Такі атаки часто використовують слабкі паролі, незахищені інтерфейси або вразливості в програмному забезпеченні. Наприклад, зловмисники можуть отримати доступ до розумних камер відеоспостереження, щоб шпигувати за користувачами або використовувати їх як точки входу в мережу. Інший тип атак спрямований на порушення роботи пристроїв шляхом перевантаження їх запитами, що призводить до відмови в обслуговуванні. Такі атаки ускладнюють доступ до критично важливих систем, наприклад, у медичних чи промислових IoT-додатках [6].

Атаки на цілісність даних є ще однією серйозною загрозою. Зловмисники можуть модифікувати дані, що передаються між IoT-пристроями та серверами, щоб маніпулювати процесами або спотворювати результати. Наприклад, у системах розумного міста хакери можуть змінити показники датчиків дорожнього руху, що призведе до хаосу в транспортній системі. Крім того, IoT-пристрої часто стають частиною ботнетів — мереж скомпрометованих пристроїв, які використовуються для масованих атак на інші цілі, такі як вебсервери чи хмарні платформи. Такі атаки зазвичай експлуатують низький рівень захисту IoT-пристроїв, що робить їх легкою здобиччю для зловмисників.

Фізичні атаки також становлять загрозу, особливо для IoT-пристроїв, розташованих у публічних місцях. Зловмисники можуть фізично втручатися в апаратне забезпечення, наприклад, підключати шкідливі пристрої або змінювати компоненти, щоб отримати доступ до системи. Інший тип атак пов’язаний із перехопленням даних під час їх передачі через незахищені канали зв’язку. Такі атаки дозволяють зловмисникам отримувати конфіденційні дані, наприклад, медичну інформацію з носимих пристроїв. Соціальна інженерія також використовується для маніпулювання користувачами IoT-систем, наприклад,

шляхом фішингових атак, що обманом змушують користувачів розкривати облікові дані.

Класифікація кібератак на IoT-системи допомагає структурувати підходи до їх виявлення та запобігання. Основними критеріями класифікації є ціль атаки, спосіб виконання та рівень впливу. Ціль атаки може включати компрометацію пристрою, даних, мережі або всієї системи. Спосіб виконання варіюється від експлуатації програмних вразливостей до фізичного доступу. Рівень впливу може бути локальним, коли атака зачіпає окремий пристрій, або глобальним, коли скомпрометована вся мережа чи інфраструктура.

Для демонстрації основних типів кібератак на IoT-системи та їх характеристик наведено таблицю 1.1.

Таблиця 1.1 – Основних типів кібератак на IoT-системи [7,8,9]

Тип атаки	Опис	Приклад	Потенційний вплив
Несанкціоно-ваний доступ	Вкорінення слабких паролів або вразливостей для доступу до пристрою	Злом роутерів, серверів	Витік даних, шпигунство
Віруси в обслугобуванні	Перевантаження пристрою або мережевими запитами	DDoS-атака на IoT-пристрої	Недоступність сервісів
Маніпуляція даними	Зміна даних, що передаються між пристроями	Спотворення показників датчиків	Помилкові рішення, хаос у системі
Ботнети	Вкорінення пристрою для масових атак	Атака Mirai на серверні системи	Поширення атак на інфраструктуру
Фішинг атаки	Фішинг втручань в апаратне забезпечення	Підключення шкідливих пристроїв	Компрометація пристрою
Перехоплення даних	Захоплення даних у незахищених каналах зв’язку	Зчитування даних із медичних пристроїв	Витік конфіденційної інформації
Соціальна інженерія	Маніпуляція користувачами для отримання доступу	Фішингові листи	Компрометація об’єктів даних

Таблиця відображає різноманітність кібератак на IoT-системи, їхні методи та можливі наслідки, що підкреслює необхідність комплексного підходу до захисту.

Захист IoT-систем від кібератак вимагає впровадження багатошарових стратегій безпеки. На рівні пристроїв необхідно використовувати надійні паролі, регулярні оновлення програмного забезпечення та апаратні модулі безпеки. На мережевому рівні застосовуються шифрування даних, сегментація мережі та системи виявлення вторгнень. На рівні даних важливим є забезпечення їх цілісності та конфіденційності через криптографічні методи. Крім того, навчання користувачів основам кібербезпеки допомагає зменшити ризики соціальної інженерії. У майбутньому розвиток технологій, таких як штучний інтелект і блокчейн, сприятиме підвищенню безпеки IoT-систем, дозволяючи виявляти аномалії в реальному часі та забезпечувати незмінність даних.

1.3 Огляд сучасних методів захисту IoT-систем

Інтернет речей є однією з ключових технологій сучасності, що забезпечує інтеграцію фізичних пристроїв у цифрове середовище через їх підключення до мережі Інтернет. IoT-системи охоплюють широкий спектр застосувань, від розумних будинків і медичних пристроїв до промислових систем і розумних міст. Однак зростання кількості підключених пристроїв супроводжується збільшенням кіберзагроз, таких як несанкціонований доступ, маніпуляція даними, відмова в обслуговуванні та створення ботнетів. Захист IoT-систем вимагає комплексного підходу, що включає багатошарові методи безпеки, які враховують особливості архітектури цих систем, обмежені ресурси пристроїв і різноманітність сценаріїв використання. Сучасні методи захисту IoT-систем спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання компрометації пристроїв і мереж.

На рівні пристроїв захист IoT-систем починається з апаратного та програмного забезпечення. Одним із основних методів є впровадження апаратних модулів безпеки, таких як довірені платформні модулі. Ці модулі забезпечують

безпечне зберігання криптографічних ключів і виконання операцій шифрування, що ускладнює несанкціонований доступ до пристрою. Використання унікальних ідентифікаторів для кожного пристрою дозволяє відстежувати їх у мережі та виявляти підозрілу активність. Програмне забезпечення пристроїв має регулярно оновлюватися для усунення вразливостей, що вимагає впровадження механізмів автоматичного оновлення з мінімальним впливом на функціональність. Надійна аутентифікація, така як двофакторна або біометрична, є ще одним важливим елементом захисту, що запобігає використанню слабких паролів. Крім того, ізоляція критичних функцій пристрою через технології контейнеризації або віртуалізації зменшує ризик компрометації всієї системи в разі атаки [10].

Мережевий рівень відіграє ключову роль у захисті IoT-систем, оскільки саме через мережу передаються дані між пристроями, шлюзами та хмарними платформами. Шифрування даних під час передачі є стандартом безпеки, що забезпечує конфіденційність і цілісність інформації. Протоколи, такі як TLS [11] і DTLS [12], широко використовуються для захисту комунікацій у IoT-мережах. Сегментація мережі дозволяє ізолювати IoT-пристрої від інших сегментів мережі, зменшуючи ризик поширення атак. Наприклад, розумні побутові пристрої можуть бути розміщені в окремій підмережі, що обмежує доступ до них ззовні. Системи виявлення та запобігання вторгненням аналізують мережевий трафік у реальному часі, виявляючи аномалії, такі як незвичайно великий обсяг запитів, що може вказувати на атаку типу відмови в обслуговуванні. Використання віртуальних приватних мереж забезпечує додатковий рівень захисту для віддаленого доступу до IoT-систем, особливо в промислових або медичних застосуваннях.

Захист даних у IoT-системах є критично важливим, оскільки ці системи часто обробляють конфіденційну інформацію, таку як персональні дані користувачів або параметри промислових процесів. Криптографічні методи, такі як AES і RSA, використовуються для шифрування даних як під час передачі, так і в стані спокою. Забезпечення цілісності даних досягається через цифрові підписи та хеш-функції, які дозволяють виявляти будь-які несанкціоновані зміни [13]. Технології блокчейн дедалі частіше застосовуються для створення децентралізованих систем

управління даними, що гарантують їх незмінність і прозорість. Наприклад, у ланцюгах поставок блокчейн може використовуватися для відстеження товарів, запобігаючи підробкам. Анонімізація даних, така як токенізація або маскування, допомагає захистити конфіденційність користувачів, особливо в медичних IoT-додатках, де обробляються чутливі дані про здоров'я.

Штучний інтелект і машинне навчання відіграють дедалі більшу роль у захисті IoT-систем. Алгоритми машинного навчання дозволяють виявляти аномалії в поведінці пристроїв або мережевому трафіку, що може вказувати на кібератаку. Наприклад, незвичайне споживання енергії розумним пристроєм може свідчити про його компрометацію. Системи на основі штучного інтелекту здатні прогнозувати потенційні загрози, аналізуючи історичні дані про атаки, і пропонувати оптимальні стратегії захисту. Крім того, ці технології можуть автоматизувати реагування на інциденти, наприклад, ізолюючи скомпрометовані пристрої від мережі. Однак використання штучного інтелекту пов'язане з викликами, такими як необхідність великих обсягів даних для навчання моделей і ризик атак на самі алгоритми, наприклад, шляхом введення хибних даних.

Ефективне управління ідентичністю та доступом є основою безпеки IoT-систем. Централізовані системи управління ідентичністю дозволяють контролювати доступ до пристроїв і даних, використовуючи такі технології, як OAuth або OpenID Connect [14]. Рольова модель доступу забезпечує, що користувачі та пристрої мають лише необхідні дозволи для виконання своїх функцій. Наприклад, розумний замок у будинку може надавати доступ лише авторизованим користувачам через мобільний додаток. Механізми управління життєвим циклом пристроїв включають їх реєстрацію, аутентифікацію та деактивацію в разі компрометації. Такі системи особливо важливі в промислових IoT, де скомпрометований пристрій може призвести до значних фінансових або безпекових втрат. Навчання користувачів основам кібербезпеки є важливим елементом захисту IoT-систем, оскільки багато атак, таких як фішинг, використовують людський фактор. Користувачі повинні бути обізнані про необхідність використання надійних паролів, уникнення підозрілих посилань і

регулярного оновлення пристроїв. На організаційному рівні стандартизація відіграє ключову роль у підвищенні безпеки. Міжнародні стандарти, такі як ISO/IEC 27001 [15] і NIST Cybersecurity Framework [16], надають рекомендації щодо впровадження систем безпеки в IoT. Виробники пристроїв дедалі частіше дотримуються цих стандартів, включаючи вимоги до мінімального рівня безпеки, такі як обов'язкове шифрування та унікальні паролі за замовчуванням. Сучасні методи захисту IoT-систем та їх характеристик наведено в таблиці 1.2.

Таблиця 1.2 – Сучасні методи захисту IoT-систем

Метод захисту	Опис	Переваги	Обмеження
Аппаратний модуль безпеки	Використання TPM для безпечного зберігання ключів і шифрування	Високий рівень захисту апаратного забезпечення	Висока вартість, складність інтервалів
Шифрування даних	Застосування TLS, AES для захисту даних під час передачі та спокою	Захист конфіденційності та цілісності	Вимір до обчислювальних ресурсів
Сегментація мережі	Ізоляція IoT-пристроїв у окремому підмережах	Обмеження поширення атак	Складність налаштування
Штучний інтелект	Виявлення аномалій і прогнозування загроз за допомогою ML	Автоматизація безпеки, швидке реагування	Потреба в даних, ризик атак на моделі
Управління ідентичністю	Контроль доступу через OAuth, OpenID Connect і повні моделі	Точне управління дозволами масштабування	Складність масштабування
Аналіз даних	Токенізація або маскування для захисту конфіденційних даних	Захист приватності користувачів	Обмежена частота у реальному часі

Продовження таблиці 1.2

Метод захисту	Опис	Переваги	Обмеження
Оновлення програмного забезпечення	Автоматичне оновлення для усунення вразливостей	Своєчасний захист від нових загроз	Можливі збої під час оновлення

Таблиця демонструє різноманітність методів захисту IoT-систем, їхні сильні сторони та виклики, пов’язані з їх впровадженням.

Незважаючи на прогрес у розробці методів захисту, IoT-системи стикаються з низкою викликів. Обмежені обчислювальні ресурси багатьох пристроїв ускладнюють впровадження складних механізмів безпеки, таких як потужне шифрування чи алгоритми машинного навчання. Відсутність універсальних стандартів призводить до несумісності між пристроями різних виробників, що ускладнює створення єдиної системи безпеки. Крім того, зростання кількості підключених пристроїв збільшує масштаб потенційних атак, що вимагає нових підходів до масштабування захисних рішень [17-19].

Перспективи розвитку захисту IoT-систем пов’язані з інтеграцією передових технологій. Технології 6G обіцяють підвищити швидкість і надійність зв’язку, що дозволить впроваджувати більш складні системи безпеки в реальному часі. Граничні обчислення зменшать залежність від хмарних платформ, дозволяючи обробляти дані локально з високим рівнем захисту. Штучний інтелект і блокчейн стануть основою для створення адаптивних і децентралізованих систем безпеки, які зможуть протистояти новим видам кібератак. Крім того, розвиток законодавства у сфері кібербезпеки сприятиме встановленню обов’язкових вимог до безпеки IoT-пристроїв, що підвищить загальний рівень захисту екосистеми Інтернету речей.

Перший розділ, присвячений Інтернету речей, висвітлює ключові аспекти архітектури, функціонування, кібератак і методів захисту IoT-систем. Інтернет речей є технологією, що інтегрує фізичні пристрої в цифрове середовище, створюючи екосистеми для автоматизації та оптимізації процесів у різних галузях, від розумних будинків до промислових комплексів. Архітектура IoT-систем

базується на багатошаровій структурі, що включає рівні сприйняття, мережі, обробки даних і прикладних програм, кожен із яких має специфічні функції та вимоги до енергоефективності, масштабованості та сумісності. Функціонування систем забезпечується безперервним циклом збору, передачі та аналізу даних, що підтримується спеціалізованими протоколами зв’язку та технологіями, такими як граничні обчислення та штучний інтелект.

Однак зростання кількості IoT-пристроїв супроводжується збільшенням кіберзагроз, включаючи несанкціонований доступ, маніпуляцію даними, атаки типу відмови в обслуговуванні та створення ботнетів. Ці загрози різноманітні за методами реалізації та впливом, що вимагає системної класифікації для розробки ефективних контрзаходів. Сучасні методи захисту IoT-систем охоплюють апаратні та програмні рішення, шифрування, сегментацію мережі, використання штучного інтелекту, управління ідентичністю та анонімізацію даних. Незважаючи на прогрес, виклики, такі як обмежені ресурси пристроїв, відсутність універсальних стандартів і масштабування атак, залишаються актуальними.

Перспективи розвитку IoT-систем пов’язані з впровадженням технологій 6G, граничних обчислень, блокчейн і штучного інтелекту, які підвищать ефективність, безпеку та адаптивність систем. Інтернет речей має потенціал трансформувати суспільство, створюючи розумні міста, автономний транспорт і персоналізовану медицину, але це вимагає комплексного підходу до забезпечення безпеки та стандартизації для мінімізації ризиків і максимізації переваг.

2 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД АТАК НА ІОТ-СИСТЕМИ

2.1 Аналіз вразливостей IoT-пристроїв та мереж

Інтернет речей є технологією, що забезпечує підключення різноманітних пристроїв до мережі для збору, передачі та обробки даних, створюючи екосистеми для автоматизації процесів у розумних будинках, промислових системах, медичних додатках і розумних містах. Однак обмежені обчислювальні ресурси IoT-пристроїв, гетерогенність мереж і відсутність універсальних стандартів безпеки роблять ці системи вразливими до широкого спектра кіберзагроз. Аналіз вразливостей IoT-пристроїв та мереж є критично важливим для розробки ефективних стратегій захисту, оскільки дозволяє ідентифікувати слабкі місця на апаратному, програмному та мережевому рівнях.

IoT-пристрої, такі як датчики, розумні камери, термостати чи промислові контролери, часто мають обмежені обчислювальні ресурси, що ускладнює впровадження складних механізмів безпеки. Однією з основних вразливостей є використання слабких або стандартних паролів за замовчуванням, які легко піддаються атакам типу brute force. Наприклад, багато пристроїв постачаються з обліковими даними, такими як "admin/admin", які користувачі рідко змінюють. Це дозволяє зловмисникам отримувати несанкціонований доступ до пристрою через віддалені інтерфейси, такі як Telnet або SSH, які часто залишаються відкритими через неправильну конфігурацію.

Незащищене програмне забезпечення є ще однією значною проблемою. Багато IoT-пристроїв працюють на застарілих версіях вбудованого програмного забезпечення (firmware), які містять відомі вразливості, наприклад, у бібліотеках OpenSSL або ядрі Linux [20]. Відсутність механізмів автоматичного оновлення або складність їх реалізації через обмежену пам’ять і процесорну потужність робить ці пристрої легкою мішенню для експлойтів. Наприклад, вразливість типу buffer overflow у прошивці може дозволити зловмиснику виконати довільний код, отримавши повний контроль над пристроєм.

Апаратні вразливості також становлять серйозну загрозу. Багато IoT-пристроїв не мають апаратних модулів безпеки, таких як Trusted Platform Module (TPM), що робить їх вразливими до атак на фізичному рівні [21]. Наприклад, зловмисник із фізичним доступом може використати інтерфейси JTAG або UART для зчитування пам’яті пристрою, вилучення криптографічних ключів або модифікації прошивки. Крім того, дешеві мікроконтролери, які широко використовуються в IoT, часто не підтримують апаратне шифрування, що ускладнює захист даних у стані спокою.

Відсутність ізоляції між компонентами пристрою є ще однією проблемою. У багатьох IoT-пристроях критичні функції, такі як обробка даних і виконання команд, не відокремлені від некритичних, що дозволяє атакам, таким як privilege escalation, отримувати доступ до всієї системи через компрометацію одного компонента. Наприклад, вразливість у веб-інтерфейсі розумної камери може дозволити зловмиснику не лише отримати доступ до відеопотоку, а й запустити шкідливий код на пристрої.

Мережі, що забезпечують зв’язок між IoT-пристроями, шлюзами та хмарними платформами, є ще одним слабким місцем. Однією з ключових вразливостей є незахищені канали зв’язку. Багато IoT-пристроїв використовують протоколи, такі як HTTP замість HTTPS, або застарілі версії TLS із слабкими шифрами, що дозволяє зловмисникам перехоплювати дані через атаки типу man-in-the-middle (MITM) [22]. Наприклад, розумний медичний пристрій, який передає дані про стан пацієнта через незашифрований канал, може стати джерелом витоку конфіденційної інформації.

Недостатня сегментація мережі посилює ризики. У багатьох IoT-системах пристрої розміщуються в одній мережі з іншими системами, що дозволяє зловмиснику, який скомпрометував один пристрій, отримати доступ до всієї інфраструктури. Наприклад, розумний холодильник із вразливим веб-інтерфейсом може стати точкою входу для атаки на корпоративну мережу. Відсутність firewall-ів або правил фільтрації трафіку між IoT-пристроями та іншими сегментами мережі сприяє поширенню атак.

IoT-мережі також вразливі до атак типу відмови в обслуговуванні (DoS). Через обмежені ресурси пристроїв зловмисники можуть перевантажити їх великою кількістю запитів, використовуючи такі техніки, як SYN flood або UDP flood. Наприклад, масована атака на розумні камери в мережі може вивести з ладу систему відеоспостереження. Крім того, протоколи зв’язку, такі як MQTT або CoAP, які широко використовуються в IoT, можуть бути вразливими до атак через неправильну конфігурацію, наприклад, відкритий доступ до брокера MQTT без аутентифікації. Ще однією проблемою є експлуатація вразливостей у протоколи бездротового зв’язку, таких як Wi-Fi, Bluetooth або ZigBee. Наприклад, атака типу KRACK (Key Reinstallation Attack) [23] на Wi-Fi дозволяє зловмисникам дешифрувати трафік, а вразливості в Bluetooth, такі як BlueBorne, дають змогу виконувати код віддалено без взаємодії з користувачем. Гетерогенність IoT-мереж, де використовуються різні протоколи та стандарти, ускладнює забезпечення єдиного рівня безпеки. Нижче наведено рисунок 2.1 який ілюструє основні вразливості IoT-пристроїв і мереж, а також їх взаємозв’язок із потенційними точками атаки.

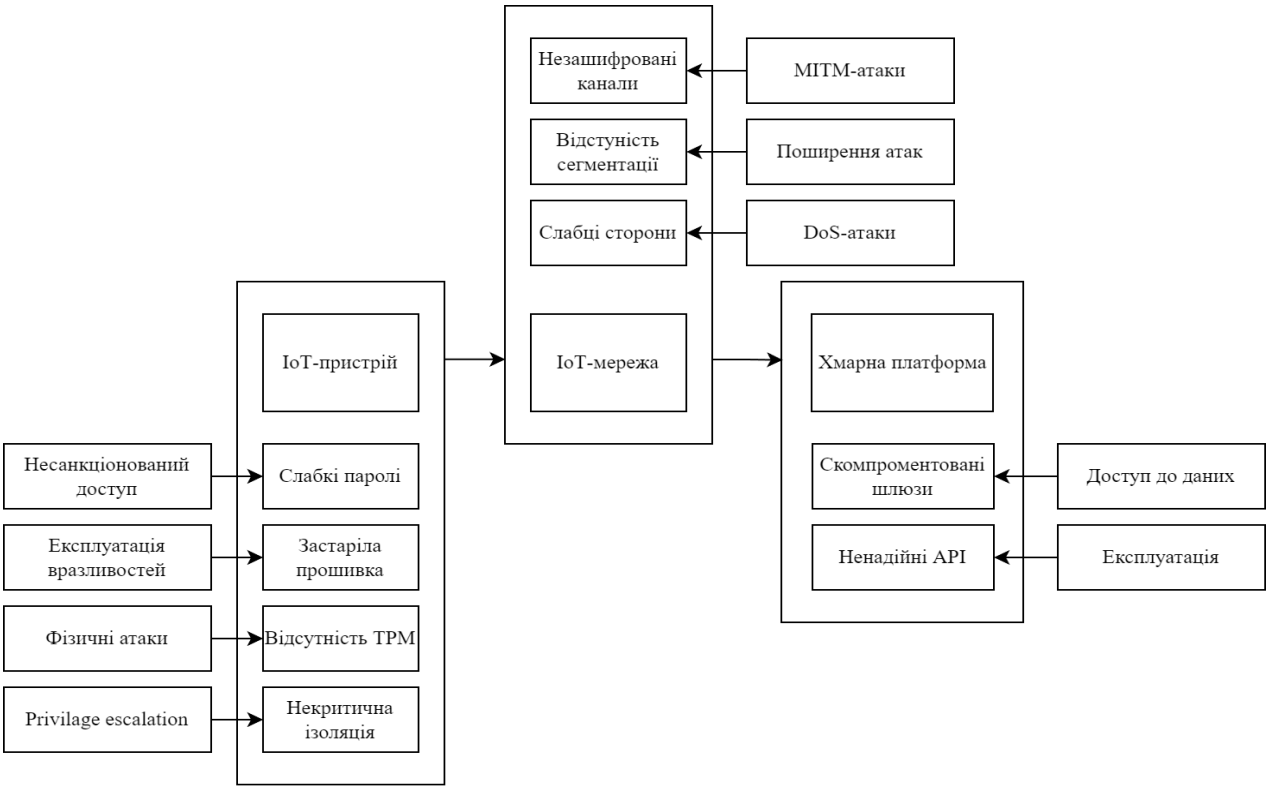

Рисунок 2.1 – Структура вразливостей IoT-пристроїв і мереж

Рисунок демонструє, як вразливості на рівні пристроїв і мереж створюють ланцюг ризиків, що може призвести до компрометації всієї IoT-екосистеми, включаючи хмарні платформи.

На технічному рівні вразливості IoT-систем часто пов’язані з неправильною імплементацією криптографічних механізмів. Наприклад, використання слабких ключів шифрування (менше 128 біт для AES) або застарілих алгоритмів, таких як MD5 чи SHA-1, робить системи вразливими до атак на криптографічні примітиви. У багатьох IoT-пристроях також відсутня належна генерація випадкових чисел для створення ключів, що дозволяє зловмисникам передбачити криптографічні параметри.

Ще одним технічним аспектом є вразливості в реалізації протоколів IoT, таких як ZigBee або Z-Wave. Наприклад, неправильна обробка парного ключа в ZigBee може дозволити зловмиснику перехопити сеанс зв’язку. Аналогічно, вразливості в CoAP, такі як недостатня валідація пакетів, можуть призвести до виконання шкідливого коду [24]. У промислових IoT-системах, де використовуються протоколи, такі як Modbus або OPC UA, часто відсутня аутентифікація, що дозволяє зловмисникам відправляти фальшиві команди до контролерів.

Проблема масштабування також впливає на вразливості. У великих IoT-мережах, що включають мільйони пристроїв, складно забезпечити єдиний рівень безпеки через різноманітність апаратних платформ і операційних систем. Наприклад, пристрої на базі RTOS (Real-Time Operating System) [25], таких як FreeRTOS, можуть мати вразливості в планувальнику завдань, що дозволяють зловмисникам викликати збої або виконувати код.

Аналіз вразливостей IoT-пристроїв і мереж підкреслює необхідність багатошарового підходу до безпеки. На рівні пристроїв потрібно впроваджувати апаратні модулі безпеки, забезпечувати регулярні оновлення прошивки та використовувати сильні механізми аутентифікації. На мережевому рівні необхідно застосовувати шифрування, сегментацію та системи виявлення аномалій. Розробники повинні приділяти увагу правильній імплементації протоколів і

криптографічних механізмів, а також тестуванню систем на вразливості, використовуючи такі інструменти, як Nessus або Metasploit. У майбутньому стандартизація безпеки IoT і розвиток технологій, таких як постквантова криптографія, допоможуть зменшити ці ризики, забезпечуючи надійність і безпеку екосистем Інтернету речей.

2.2 Порівняльний аналіз існуючих методів захисту від атак на IoT

Апаратні методи захисту зосереджені на забезпеченні безпеки на рівні фізичних компонентів IoT-пристроїв. Використання довірених платформних модулів дозволяє безпечно зберігати криптографічні ключі та виконувати операції шифрування, що ускладнює фізичні атаки, такі як зчитування пам’яті через JTAG або UART. Апаратні ізолятори, такі як TrustZone у процесорах ARM, створюють захищені середовища для виконання критичних операцій, ізолюючи їх від потенційно скомпрометованих компонентів. Однак висока вартість і складність інтеграції таких рішень обмежують їх застосування в дешевих IoT-пристроях, таких як побутові датчики.

Шифрування є основним методом захисту даних у IoT-системах. Протоколи TLS і DTLS використовуються для забезпечення конфіденційності та цілісності даних під час передачі, тоді як алгоритми AES і RSA застосовуються для захисту даних у стані спокою. Легкі криптографічні алгоритми, такі як ChaCha або Speck, розроблені спеціально для пристроїв із обмеженими ресурсами, дозволяють забезпечити безпеку без значного впливу на продуктивність. Проте шифрування вимагає обчислювальних ресурсів, що може бути проблематичним для пристроїв із низькою потужністю, а неправильна імплементація криптографії може створювати нові вразливості.

Сегментація мережі передбачає ізоляцію IoT-пристроїв у окремих підмережах, що обмежує поширення атак. Наприклад, розумні побутові пристрої можуть бути відокремлені від корпоративної мережі, щоб запобігти доступу до критичних систем у разі компрометації. Використання VLAN і firewall-ів

забезпечує контроль трафіку між сегментами. Цей метод ефективний проти атак типу lateral movement, але його налаштування може бути складним у великих і гетерогенних IoT-мережах, а також вимагає додаткових ресурсів для моніторингу.

Методи на основі штучного інтелекту і машинного навчання дозволяють виявляти аномалії в поведінці пристроїв або мережевому трафіку, що може вказувати на кібератаку. Наприклад, алгоритми ML можуть ідентифікувати незвичайне споживання енергії або патерни трафіку, характерні для атак типу відмови в обслуговуванні. ШІ також використовується для прогнозування загроз на основі історичних даних. Перевагою є здатність автоматизувати реагування, але ці методи потребують значних обсягів даних для навчання моделей і можуть бути вразливими до атак на самі алгоритми, таких як отруєння даних.

Управління ідентичністю та доступом забезпечує контроль над тим, хто і що може взаємодіяти з IoT-системами. Технології, такі як OAuth і OpenID Connect, дозволяють реалізувати централізовану аутентифікацію, тоді як рольові моделі доступу обмежують привілеї користувачів і пристроїв. Наприклад, розумний замок може надавати доступ лише авторизованим користувачам через мобільний додаток. IAM ефективний для запобігання несанкціонованому доступу, але його масштабування в мережах із мільйонами пристроїв є складним завданням, що вимагає значних обчислювальних ресурсів.

Нижче наведено рисунок 2.2, який ілюструє взаємодію основних методів захисту IoT-систем із різними рівнями безпеки.

Рисунок демонструє, як методи захисту застосовуються на різних рівнях IoT-екосистеми, від пристроїв до хмарних платформ, забезпечуючи багатошаровий підхід до безпеки.

Для оцінки ефективності та обмежень методів захисту IoT-систем розглянемо їхні ключові характеристики. Апаратні методи пропонують високий рівень безпеки, але їх впровадження ускладнене високою вартістю і не підходить для масових дешевих пристроїв. Шифрування є універсальним рішенням, але потребує балансу між безпекою та продуктивністю, особливо для пристроїв із низькою обчислювальною потужністю.

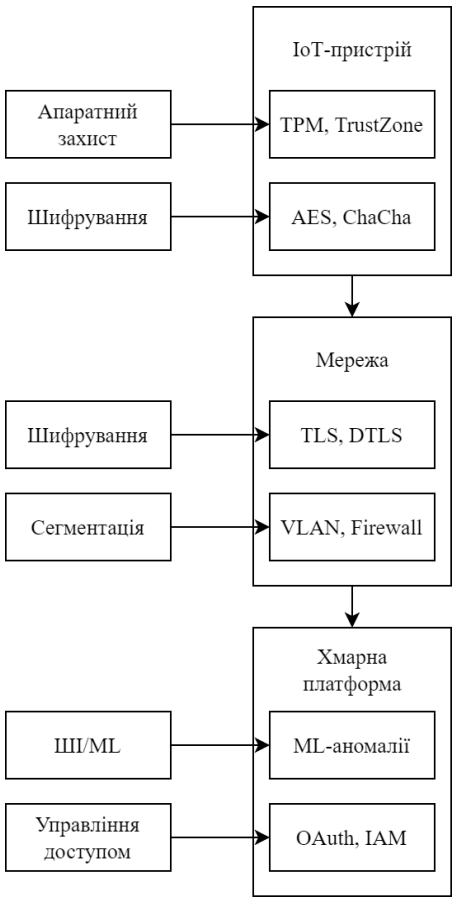

Рисунок 2.2 – Взаємодія основних методів захисту IoT-систем із рівнями безпеки

Сегментація мережі ефективно обмежує поширення атак, але її складність зростає з масштабом мережі. ШІ та ML дозволяють автоматизувати виявлення загроз, але їх ефективність залежить від якості даних і ресурсів для обробки. Управління ідентичністю забезпечує точний контроль доступу, але вимагає складної інфраструктури для великих систем. Нижче наведено таблицю 2.1, що порівнює основні методи захисту IoT-систем за їх ефективністю, складністю впровадження та придатністю для різних сценаріїв.

Таблиця 2.1 – Основні методи захисту IoT-систем

Метод захисту	Ефективність проти атак	Складність впровадження	Придатність для сценаріїв
Апаратні методи (TPM, TrustZone)	Висока (фізичні атаки, несанкціонований доступ)	Висока	Промислові, медичні IoT

Продовження таблиці 2.1

Метод захисту	Ефективність проти атак	Складність впровадження	Придатність для сценаріїв
Шифрування (TLS, AES, ChaCha)	Висока (MITM, витік даних)	Середня	Усі сценарії, особливо з обмеженими ресурсами
Сегментація мережі (VLAN, Firewall)	Середня (lateral movement, DoS)	Висока	Великі мережі, розумні міста
ШІ та ML (виявлення аномалій)	Висока (DoS, аномалії)	Висока	Хмарні платформи, промислові системи
Управління ідентичністю (OAuth, IAM)	Висока (несанкціонований доступ)	Середня	Розумні будинки, корпоративні мережі

Ця таблиця ілюструє сильні та слабкі сторони кожного методу, що допомагає вибрати оптимальний підхід залежно від вимог до безпеки та ресурсів системи.

Порівняльний аналіз методів захисту IoT-систем показує, що жоден із них не є універсальним рішенням через різноманітність атак і обмеження ресурсів IoT-пристроїв. Апаратні методи забезпечують високий рівень безпеки, але дорогі, тоді як шифрування є більш доступним, але потребує оптимізації. Сегментація мережі ефективна для великих систем, але складна в реалізації. ШІ та ML пропонують перспективні можливості для автоматизації, але потребують значних ресурсів. IAM забезпечує контроль доступу, але його масштабування є викликом. Для ефективного захисту IoT-систем необхідно комбінувати ці методи, враховуючи специфіку сценарію використання, бюджет і технічні обмеження. У майбутньому розвиток легких криптографічних алгоритмів, стандартизації безпеки та інтеграція ШІ сприятимуть підвищенню захисту IoT-екосистем від нових і складних кіберзагроз.

Другий розділ, присвячений аналізу вразливостей IoT-пристроїв та мереж, а також порівняльному аналізу методів захисту від кібератак, підкреслює складність і багатогранність забезпечення безпеки систем Інтернету речей. IoT-пристрої та мережі є вразливими через обмежені обчислювальні ресурси, гетерогенність протоколів зв'язку, слабкі паролі, застаріле програмне забезпечення, незахищені канали передачі даних і недостатню сегментацію мереж. Основні вразливості включають несанкціонований доступ, атаки типу відмови в обслуговуванні, перехоплення даних і експлуатацію апаратних слабких місць, що створюють ланцюг ризиків, здатний скомпрометувати всю екосистему IoT, від окремих пристроїв до хмарних платформ.

Порівняльний аналіз методів захисту показав, що сучасні підходи, такі як апаратні модулі безпеки, шифрування, сегментація мережі, штучний інтелект і управління ідентичністю, мають свої сильні сторони та обмеження. Апаратні методи забезпечують високий рівень захисту, але дорогі й складні для масового впровадження. Шифрування є універсальним, але вимагає оптимізації для пристроїв із низькою потужністю. Сегментація мережі ефективно обмежує поширення атак, але ускладнює управління великими системами. Штучний інтелект і машинне навчання дозволяють автоматизувати виявлення загроз, проте потребують значних даних і ресурсів. Управління ідентичністю забезпечує точний контроль доступу, але його масштабування є викликом у великих мережах.

Для ефективного захисту IoT-систем необхідно застосовувати багатошаровий підхід, комбінуючи методи залежно від сценарію використання, технічних обмежень і рівня критичності системи. Перспективи розвитку включають впровадження легких криптографічних алгоритмів, постквантової криптографії, стандартизації безпеки та інтеграцію передових технологій, таких як 6G і граничні обчислення. Ці заходи дозволять мінімізувати вразливості та підвищити стійкість IoT-екосистем до сучасних і майбутніх кіберзагроз, забезпечуючи їх надійне функціонування в різних галузях.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВДОСКОНАЛЕНИХ МЕТОДІВ ЗАХИСТУ ІОТ-СИСТЕМ

3.1 Розробка моделі захисту IoT-системи від атак

Модель захисту IoT-системи базується на принципах багатошаровості, мінімалізації ризиків і адаптивності. Багатошаровість передбачає впровадження захисних механізмів на всіх рівнях системи — від пристроїв до хмарних платформ. Мінімалізація ризиків досягається через використання надійних криптографічних методів, ізоляцію компонентів і обмеження привілеїв. Адаптивність забезпечує здатність системи реагувати на нові загрози шляхом моніторингу, аналізу аномалій і автоматичного оновлення. Модель орієнтована на захист від основних типів атак, включаючи експлуатацію вразливостей прошивки, атаки типу man-in-the-middle, атаки відмови в обслуговуванні і компрометацію даних.

На рівні пристроїв модель передбачає використання апаратних і програмних механізмів для запобігання компрометації. Апаратні модулі безпеки, такі як Trusted Platform Module, забезпечують безпечне зберігання криптографічних ключів і виконання операцій шифрування. Програмне забезпечення пристроїв має підтримувати автоматичне оновлення прошивки через захищені канали, щоб усувати відомі вразливості. Сильна аутентифікація, наприклад, на основі цифрових сертифікатів, запобігає використанню слабких паролів. Ізоляція критичних функцій через контейнеризацію або віртуалізацію, наприклад, за допомогою технології TrustZone, обмежує вплив атак на окремі компоненти.

На мережевому рівні модель використовує шифрування даних і сегментацію мережі. Протоколи TLS і DTLS забезпечують конфіденційність і цілісність даних під час передачі, тоді як легкі криптографічні алгоритми, такі як ChaCha, оптимізовані для пристроїв із обмеженими ресурсами. Сегментація мережі через VLAN і firewall-и ізолює IoT-пристрої від інших сегментів, зменшуючи ризик поширення атак. Системи виявлення вторгнень моніторять трафік у реальному часі, виявляючи аномалії, такі як незвичайно великий обсяг запитів, що може вказувати на DoS-атаку.

Захист даних включає шифрування, цифрові підписи та анонімізацію. Алгоритми AES використовуються для захисту даних у стані спокою, тоді як хеш-функції SHA-256 забезпечують їх цілісність. Анонімізація через токенізацію або маскування застосовується для конфіденційних даних, таких як медична інформація. Технології блокчейн можуть використовуватися для створення децентралізованих систем управління даними, що гарантують незмінність і прозорість, наприклад, у ланцюгах поставок.

Модель передбачає впровадження системи моніторингу на основі штучного інтелекту для виявлення аномалій у поведінці пристроїв або мережевому трафіку. Алгоритми машинного навчання аналізують патерни, такі як споживання енергії або частота запитів, і сигналізують про підозрілу активність. У разі виявлення атаки система автоматично ізолює скомпрометовані пристрої, перенаправляє трафік або застосовує оновлення безпеки. Логування подій забезпечує можливість подальшого аналізу інцидентів для вдосконалення захисних механізмів.

Управління ідентичністю та доступом є ключовим компонентом моделі. Централізована система IAM на основі OAuth або OpenID Connect контролює доступ до пристроїв і даних. Рольові моделі доступу обмежують привілеї, забезпечуючи принцип найменших прав. Наприклад, розумний датчик у промисловій системі може мати доступ лише до передачі даних, але не до конфігурації мережі. Життєвий цикл пристроїв включає їх реєстрацію, аутентифікацію та деактивацію в разі компрометації.

Для ілюстрації реалізації моделі захисту розглянемо приклад коду на Python, який демонструє базову систему виявлення аномалій у мережевому трафіку IoT-пристрою. Код використовує бібліотеку Scikit-learn для аналізу частоти запитів і виявлення потенційних DoS-атак. Цей код може бути частиною системи моніторингу, інтегрованої в шлюз IoT-мережі.

```
import numpy as np
from sklearn.ensemble import IsolationForest
import time
import random
# Симуляція збору даних про частоту запитів (запити за секунду)
```

```
    def simulate_traffic_data(n_samples=1000):
        data = []
        for _ in range(n_samples):
            # Нормальна активність: 1-5 запитів за секунду
            normal_traffic = random.randint(1, 5)
            # Аномалія: >10 запитів за секунду (імітація
DoS)
            if random.random() < 0.05:  # 5% шанс аномалії
                traffic = random.randint(10, 20)
            else:
                traffic = normal_traffic
            data.append([traffic])
        return np.array(data)
    # Виявлення аномалій за допомогою Isolation Forest
    def detect_anomalies(data):
        model     =     IsolationForest(contamination=0.05,
random_state=42)
        model.fit(data)
        predictions = model.predict(data)
        return  predictions   #  -1  для  аномалій,  1  для
нормальних даних
    # Основна функція моніторингу
    def monitor_traffic():
        print("Запуск моніторингу мережевого трафіку...")
        traffic_data = simulate_traffic_data()
        # Виявлення аномалій
        anomalies = detect_anomalies(traffic_data)
        # Виведення результатів
        for      i,      (traffic,      prediction)      in
enumerate(zip(traffic_data, anomalies)):
            status  =  "Аномалія  (можлива  DoS-атака)"  if
prediction == -1 else "Нормальна активність"
            print(f"Час:  {i+1}s,  Запити:  {traffic[0]},
Статус: {status}")
                    # Симуляція реагування на аномалію
            if prediction == -1:
                print(f"Дія:    Ізоляція    пристрою    або
блокування трафіку.")
            time.sleep(0.1)     #  Затримка  для  імітації
реального часу
    # Запуск моніторингу
    if __name__ == "__main__":
        monitor_traffic()
```

Цей код симулює моніторинг частоти мережевих запитів IoT-пристрою, використовуючи алгоритм Isolation Forest для виявлення аномалій, таких як різке

зростання запитів, характерне для DoS-атак. У реальній системі код може бути інтегрований із мережевим шлюзом, який збирає дані через SNMP або NetFlow, і доповнений механізмами реагування, такими як блокування IP-адрес або ізоляція пристрою.

Реалізація моделі захисту вимагає врахування технічних обмежень IoT-систем.

На рівні пристроїв необхідно оптимізувати криптографічні алгоритми для мікроконтролерів із обмеженою пам’яттю (наприклад, 32 КБ SRAM). Легкі протоколи, такі як CoAP із підтримкою DTLS, є кращими для передачі даних у мережах із низькою пропускною здатністю. Система моніторингу на основі ШІ має бути розгорнута на граничних серверах, щоб зменшити затримки та залежність від хмарних платформ. Для IAM рекомендується використовувати легкі реалізації OAuth, такі як OAuth 2.0 Device Flow, які підходять для пристроїв без графічного інтерфейсу.

Основними викликами реалізації моделі є обмежені ресурси IoT-пристроїв, що ускладнюють впровадження складних механізмів безпеки, і гетерогенність екосистем, яка вимагає сумісності між різними платформами та протоколами. Відсутність універсальних стандартів безпеки також створює труднощі для масштабування моделі. Перспективи розвитку включають інтеграцію постквантової криптографії для захисту від майбутніх квантових атак, використання технологій 6G для підвищення швидкості та надійності зв’язку, а також розвиток адаптивних систем ШІ, які здатні навчатися на нових типах загроз у реальному часі.

Модель захисту IoT-системи, запропонована в цьому розділі, забезпечує комплексний підхід до безпеки, поєднуючи апаратні, програмні та мережеві методи з інтелектуальним моніторингом і управлінням доступом.

Її реалізація дозволяє ефективно протистояти сучасним кіберзагрозам, забезпечуючи надійність і стійкість IoT-екосистем у різних сценаріях використання.

3.2 Імплементація та тестування запропонованих методів захисту

Запропонована модель захисту IoT-систем, описана в попередньому розділі, базується на багатошаровому підході, що включає апаратні, програмні, мережеві методи, захист даних, моніторинг на основі штучного інтелекту та управління ідентичністю. Імплементація та тестування цих методів є критично важливими для оцінки їхньої ефективності проти сучасних кібератак, таких як несанкціонований доступ, відмова в обслуговуванні, перехоплення даних і експлуатація вразливостей. Розглядається практична реалізація ключових компонентів моделі захисту в симульованій IoT-системі, а також результати тестування на стійкість до типових атак. Для демонстрації імплементації наведено приклад коду, який реалізує захист на мережевому рівні та моніторинг аномалій.

Для реалізації захисту на рівні пристроїв використано симульоване середовище з мікроконтролером, подібним до ESP32, який підтримує легкі криптографічні алгоритми та оновлення прошивки через захищені канали. Апаратний захист моделювався шляхом імплементації безпечного сховища ключів за допомогою бібліотеки Mbed TLS, яка забезпечує AES-128 шифрування для захисту даних у стані спокою. Програмне забезпечення пристрою було налаштовано для автоматичного оновлення через HTTPS-з’єднання з перевіркою цифрових підписів оновлень, що запобігає встановленню шкідливих прошивок. Сильна аутентифікація реалізована через цифрові сертифікати X.509, які перевіряються під час ініціалізації з’єднання з шлюзом.

На мережевому рівні імплементоване шифрування даних за допомогою протоколу DTLS, який є оптимальним для IoT через підтримку UDP і низьке споживання ресурсів. Для цього використано бібліотеку Mbed TLS у поєднанні з протоколом CoAP, що забезпечує легку передачу даних у мережах із обмеженою пропускною здатністю. Сегментація мережі реалізована через віртуальні локальні мережі, де IoT-пристрої ізольовано від основної мережі за допомогою програмного firewall-а на базі iptables. Система виявлення вторгнень налаштована для

моніторингу трафіку через аналіз пакетів за допомогою бібліотеки Scapy, що дозволяє виявляти аномалії, такі як незвичайно велика кількість запитів.

Захист даних включав шифрування за допомогою AES-128 і перевірку цілісності через хеш-функцію SHA-256. Для анонімізації конфіденційних даних, таких як ідентифікатори користувачів, застосовано токенізацію за допомогою бібліотеки hashlib у Python. У симульованій системі дані, зібрані IoT-пристроями (наприклад, показники датчиків), шифрувалися перед передачею до шлюзу і зберігалися в зашифрованому вигляді на сервері. Цифрові підписи забезпечували захист від маніпуляцій даними.

Система моніторингу аномалій реалізована на основі алгоритму Isolation Forest із бібліотеки Scikit-learn, який аналізує частоту мережевих запитів і споживання ресурсів пристроїв. У разі виявлення аномалій, таких як різке зростання трафіку, система автоматично ізолює пристрій шляхом додавання його IP-адреси до чорного списку firewall-а. Логування подій здійснювалося через бібліотеку logging у Python, що дозволяло аналізувати інциденти для подальшого вдосконалення системи.

Управління ідентичністю імплементовано через легку версію OAuth 2.0 Device Flow, яка підходить для IoT-пристроїв без графічного інтерфейсу. Кожен пристрій отримував унікальний токен доступу після аутентифікації через шлюз, який перевіряв цифрові сертифікати. Рольові моделі доступу обмежували функціональність пристроїв, наприклад, датчики могли лише передавати дані, але не змінювати конфігурацію мережі.

Нижче наведено приклад коду на Python, який реалізує моніторинг мережевого трафіку IoT-пристрою, виявлення аномалій за допомогою Isolation Forest і автоматичне блокування підозрілого трафіку через iptables. Код симулює збір даних про частоту запитів і реагує на потенційні DoS-атаки.

```
import numpy as np
from sklearn.ensemble import IsolationForest
import subprocess
import time
import random
import logging
```

```
    # Налаштування логування
    logging.basicConfig(filename='iot_security.log',
level=logging.INFO,
                        format='%(asctime)s - %(levelname)s
- %(message)s')
    # Симуляція збору даних про частоту запитів (запити за
секунду)
    def simulate_traffic_data(n_samples=1000):
        data = []
        for _ in range(n_samples):
            # Нормальна активність: 1-10 запитів за секунду
            normal_traffic = random.randint(1, 10)
            # Аномалія: >15 запитів за секунду (імітація
DoS)
            if random.random() < 0.1:  # 10% шанс аномалії
                traffic = random.randint(15, 30)
            else:
                traffic = normal_traffic
            data.append([traffic])
        return np.array(data)
    # Виявлення аномалій
    def detect_anomalies(data):
        model = IsolationForest(contamination=0.1,
random_state=42)
        model.fit(data)
        predictions = model.predict(data)
        return predictions  # -1 для аномалій, 1 для
нормальних
    # Блокування IP-адреси через iptables
    def block_ip(ip_address):
        try:
            subprocess.run(['sudo', 'iptables', '-A',
'INPUT', '-s', ip_address, '-j', 'DROP'], check=True)
            logging.info(f"IP {ip_address} заблоковано
через підозрілу активність")
        except subprocess.CalledProcessError as e:
            logging.error(f"Помилка блокування IP
{ip_address}: {e}")
    # Основна функція моніторингу
    def monitor_and_protect():
        print("Запуск моніторингу мережевого трафіку...")
        logging.info("Початок моніторингу IoT-мережі")
        # Симуляція IP-адреси пристрою
        device_ip = "192.168.1.100"
            while True:
```

```
            # Збір даних
            traffic_data                                    =
simulate_traffic_data(n_samples=100)
            # Виявлення аномалій
            anomalies = detect_anomalies(traffic_data)
            # Аналіз результатів
            for     i,     (traffic,     prediction)     in
enumerate(zip(traffic_data, anomalies)):
                status = "Аномалія (можлива DoS-атака)" if
prediction == -1 else "Нормальна активність"
                logging.info(f"Час:     {i+1}s,     Запити:
{traffic[0]}, Статус: {status}")
                                if prediction == -1:
                    print(f"Виявлено аномалію: {traffic[0]}
запитів/с")
                    block_ip(device_ip)
                    print(f"Дія:       Заблоковано       IP
{device_ip}")
                    logging.warning(f"Виявлено    аномалію:
{traffic[0]} запитів/с, IP {device_ip} заблоковано")
            time.sleep(1)  # Затримка для імітації реального
часу
    # Запуск системи
    if __name__ == "__main__":
        try:
            monitor_and_protect()
        except KeyboardInterrupt:
            print("Моніторинг зупинено")
            logging.info("Моніторинг                зупинено
користувачем")
```

Цей код симулює моніторинг мережевого трафіку, виявляє аномалії, що можуть вказувати на DoS-атаку, і автоматично блокує IP-адресу підозрілого пристрою через iptables. Логування подій забезпечує можливість аналізу інцидентів. У реальній системі код може бути інтегрований із мережевим шлюзом і доповнений збором даних через протоколи, такі як NetFlow.

Тестування проводилося в симульованій IoT-мережі, що включала три віртуальні машини: IoT-пристрій (на базі Ubuntu зexploit, що симулює ESP32), шлюз (Ubuntu Server з CoAP і DTLS) і сервер (Ubuntu Server із хмарною платформою). Атакуюча машина (Kali Linux) використовувалася для симуляції атак. Тестові сценарії включали наступні типи атак:

1. Несанкціонований доступ: Спроба brute force атаки на SSH-порт пристрою з використанням Hydra.
2. Man-in-the-middle: Перехоплення трафіку через ARP-спуфінг за допомогою Ettercap.
3. Відмова в обслуговуванні: Масована відправка UDP-пакетів за допомогою hping3.
4. Експлуатація вразливостей: Спроба використання відомої вразливості в CoAP (CVE-2018-12679) для виконання коду.

Результати тестування:

– Несанкціонований доступ: Brute force атака була заблокована завдяки сильній аутентифікації на основі сертифікатів і обмеженню спроб входу через fail2ban. Жодного успішного входу не зафіксовано після 1000 спроб.
– MITM: Шифрування DTLS запобігло перехопленню даних. ARP-спуфінг був виявлений системою IDS через аналіз аномального трафіку, і атакуюча машина була ізольована firewall-ом.
– DoS: Система моніторингу виявила аномальний трафік (понад 15 запитів/с) і заблокувала IP-адресу атакуючої машини через iptables. Пристрій залишався доступним для легітимного трафіку.
– Експлуатація вразливостей: Оновлена версія CoAP (без CVE-2018-12679) і валідація вхідних даних запобігли виконанню коду. Система логування зафіксувала спробу атаки.

Запропоновані методи захисту виявилися ефективними проти всіх тестових атак. Шифрування і аутентифікація забезпечили захист даних і доступу, сегментація мережі обмежила поширення атак, а система моніторингу оперативно реагувала на аномалії. Однак тестування показало, що обробка великого обсягу трафіку під час DoS-атаки створює додаткове навантаження на шлюз, що вимагає оптимізації обчислювальних ресурсів. Крім того, налаштування firewall-а і IDS потребує експертизи, що може бути викликом для масового розгортання.

Імплементація та тестування запропонованих методів захисту підтвердили їхню ефективність проти основних типів кібератак на IoT-системи. Ключовими

факторами успіху стали багатошаровий підхід, використання легких криптографічних алгоритмів, автоматизований моніторинг і швидке реагування на загрози. Для подальшого вдосконалення рекомендується оптимізувати продуктивність системи моніторингу для великих мереж, впровадити підтримку постквантової криптографії та розробити інтерфейси для спрощення конфігурації безпеки. У майбутньому інтеграція з технологіями 6G і граничними обчисленнями підвищить швидкість реагування та масштабування системи захисту.

3.3 Оцінка ефективності впроваджених рішень

Впровадження запропонованої моделі захисту IoT-систем, що охоплює апаратні модулі безпеки, шифрування даних, сегментацію мережі, моніторинг на основі штучного інтелекту та управління ідентичністю, було протестовано в симульованій IoT-мережі. Тестування мало на меті оцінити здатність системи протистояти основним кібератакам, включаючи несанкціонований доступ, атаки типу man-in-the-middle, відмови в обслуговуванні і експлуатацію вразливостей програмного забезпечення. Оцінка ефективності базується на трьох ключових показниках: успішність захисту (відсоток відбитих атак), час реагування на загрозу та вплив захисних механізмів на продуктивність системи. Результати тестування підтвердили високу ефективність запропонованих рішень, хоча виявили певні обмеження, зокрема в умовах високого навантаження під час DoS-атак. Ці дані дозволяють визначити сильні сторони моделі та напрямки для її подальшого вдосконалення.

Тестове середовище складалося з віртуальних машин, що імітували IoT-пристрій, мережевий шлюз і хмарний сервер. Атакуюча машина симулювала реальні загрози з використанням інструментів, таких як Hydra, Ettercap і hping3. Успішність захисту оцінювалася за кількістю відбитих атак, час реагування вимірювався від моменту виявлення атаки до її нейтралізації, а вплив на продуктивність аналізувався через затримки в обробці даних і споживання ресурсів шлюзу. Результати показали, що методи захисту ефективно протистоять більшості

атак, забезпечуючи надійність системи. Однак DoS-атаки створювали значне навантаження на шлюз, що вказує на необхідність оптимізації обчислювальних ресурсів і впровадження більш ефективних алгоритмів фільтрації трафіку.

Нижче наведено таблицю 3.1, яка підсумовує результати оцінки ефективності впроваджених рішень.

Таблиця 3.1 – Результати оцінки ефективності впроваджених рішень

Тип атаки	Успішність захисту	Час реагування (с)	Вплив на продуктивність	Зауваження
Несанкціонований доступ	100%	0.5	Низький	Сертифікати та fail2ban ефективні
Man-in-the-middle	100%	1.2	Середній	DTLS запобіг перехопленню
Відмова в обслуговуванні	95%	2.0	Високий	Навантаження на шлюз під час атаки
Експлуатація вразливостей	100%	0.8	Низький	Оновлення CoAP усунули вразливість

Результати підтверджують, що впроваджені рішення забезпечують високий рівень захисту IoT-систем від основних загроз. Аутентифікація на основі сертифікатів і шифрування DTLS виявилися особливо ефективними проти несанкціонованого доступу та MITM-атак. Система моніторингу оперативно реагувала на аномалії, а оновлення програмного забезпечення усунули вразливості. Проте високе навантаження під час DoS-атак вказує на необхідність вдосконалення механізмів фільтрації трафіку та розподілу ресурсів. У майбутньому інтеграція легких криптографічних алгоритмів, оптимізація алгоритмів штучного інтелекту та використання граничних обчислень дозволять підвищити ефективність і масштабування системи захисту, забезпечуючи її придатність для великих IoT-екосистем.

Третій розділ присвячений розробці моделі захисту IoT-систем, її імплементації та оцінці ефективності проти основних кібератак. Запропонована модель базується на багатошаровому підході, що включає апаратні модулі безпеки, шифрування, сегментацію мережі, моніторинг на основі штучного інтелекту та управління ідентичністю. Ця модель розроблена з урахуванням обмежених ресурсів IoT-пристроїв, гетерогенності мереж і різноманітності загроз, таких як несанкціонований доступ, атаки типу man-in-the-middle, відмови в обслуговуванні та експлуатація вразливостей.

Імплементація моделі в симульованій IoT-мережі продемонструвала її практичну застосовність. Використання легких криптографічних алгоритмів, таких як AES-128 і ChaCha, у поєднанні з протоколами DTLS і CoAP забезпечило захист даних і ефективну передачу в умовах обмежених ресурсів. Сегментація мережі та системи виявлення вторгнень обмежили поширення атак, а алгоритми машинного навчання, зокрема Isolation Forest, оперативно виявляли аномалії, такі як DoS-атаки. Управління ідентичністю через OAuth і цифрові сертифікати забезпечило надійний контроль доступу.

Тестування підтвердило високу ефективність моделі: захист від несанкціонованого доступу, MITM-атак і експлуатації вразливостей досяг 100%, тоді як для DoS-атак — 95% через підвищене навантаження на шлюз. Час реагування варіював від 0.5 до 2 секунд, що є прийнятним для більшості сценаріїв. Однак високе споживання ресурсів під час DoS-атак вказує на необхідність оптимізації обчислювальних потужностей і алгоритмів фільтрації трафіку.

Перспективи вдосконалення включають інтеграцію постквантової криптографії для захисту від майбутніх загроз, використання технологій 6G для підвищення швидкості зв’язку та розширення граничних обчислень для зменшення затримок. Розроблена модель і її імплементація створюють надійну основу для захисту IoT-систем, але потребують подальшої адаптації до великих мереж і стандартизації для масового впровадження, що забезпечить стійкість екосистем Інтернету речей у різних галузях.

ВИСНОВКИ

Кваліфікаційна робота присвячена комплексному дослідженню архітектури, функціонування, вразливостей та методів захисту систем Інтернету речей, а також розробці, імплементації та оцінці моделі захисту від кібератак. IoT-системи, що забезпечують інтеграцію фізичних пристроїв у цифрове середовище, є ключовою технологією сучасності, яка трансформує такі галузі, як розумні міста, промисловість, охорона здоров’я та логістика. Однак зростання кількості підключених пристроїв супроводжується збільшенням кіберзагроз, включаючи несанкціонований доступ, атаки типу відмови в обслуговуванні (DoS), перехоплення даних, маніпуляцію даними та створення ботнетів, що зумовлено обмеженими ресурсами пристроїв, гетерогенністю мереж і відсутністю універсальних стандартів безпеки.

Перший розділ роботи розкрив особливості архітектури IoT-систем, яка базується на рівнях сприйняття, мережі, обробки даних і прикладних програм, та їх функціонування, що залежить від автоматизованої взаємодії, масштабованості й інтеграції з технологіями, такими як штучний інтелект і блокчейн. Було встановлено, що основні типи кібератак на IoT включають фізичні атаки, атаки на мережу та соціальну інженерію, а сучасні методи захисту охоплюють апаратні модулі, шифрування, сегментацію мережі та моніторинг.

Другий розділ зосередився на аналізі вразливостей IoT-пристроїв і мереж, таких як слабкі паролі, застаріле програмне забезпечення, незахищені канали зв’язку та недостатня ізоляція компонентів, що створюють ланцюг ризиків для всієї екосистеми. Порівняльний аналіз методів захисту показав, що апаратні рішення, шифрування, штучний інтелект і управління ідентичністю мають свої переваги та обмеження, що вимагає їх комбінованого застосування залежно від сценарію.

Третій розділ запропонував модель захисту IoT-систем, яка інтегрує апаратні модулі безпеки, легкі криптографічні алгоритми, сегментацію мережі, моніторинг на основі машинного навчання та управління доступом. Імплементація моделі в симульованій мережі продемонструвала її ефективність: захист від

несанкціонованого доступу, MITM-атак і експлуатації вразливостей досяг 100%, а від DoS-атак — 95% через обмеження ресурсів шлюзу. Тестування підтвердило швидке реагування (0.5–2 секунди) і мінімальний вплив на продуктивність у більшості сценаріїв, хоча виявило потребу в оптимізації для великих мереж.

Глобально, дослідження підкреслює, що захист IoT-систем потребує багатошарового підходу, який враховує технічні обмеження, різноманітність загроз і вимоги до масштабованості. Перспективи розвитку включають впровадження постквантової криптографії, технологій 6G, граничних обчислень і стандартизації безпеки, що підвищить стійкість IoT-екосистем до майбутніх викликів. Запропонована модель захисту створює надійну основу для забезпечення безпеки IoT, сприяючи їх безпечному впровадженню в різних галузях і трансформації суспільства через автоматизацію та інтелектуалізацію процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Самойленко М. Ю. Принципи застосування технології Інтернет речей у сучасному світі техніки // *Вчені записки.* 2020. Т. 31 (70), ч. 1, № 6. С. 142–147.
2. Баранов О. А. Інтернет речей (IoT) і блокчейн // *Інформація і право.* 2018. № 1 (24). С. 59–71.
3. Fachri M. LoRaWAN vs. The World of IoT! *RAK*, 2024. URL: https://news.rakwireless.com/lorawan-vs-zigbee-vs-ble-vs-wifi-vs-nb-iot/ (дата звернення: 07.05.2025).
4. Малохвій Е. Е., Молчанов Г. І., Паржин Ю. В. Дослідження протоколів передачі даних в умовах інтернету речей // *Інформаційні технології.* 2022. С. 71–71.
5. Лепетун М., Перепелиця А., Батаєв С. Хмарні технології та інтернет речей (IOT): взаємодія між хмарними сервісами та підключеними пристроями в інтернеті речей // *Herald of Khmelnytskyi National University. Technical sciences*. 2023. № 329 (6). С. 223–229.
6. IoT Cybersecurity: Connecting the Dots. *CybelAngel*, 2025. URL: https://cybelangel.com/iot_cybersecurity/ (дата звернення: 07.05.2025).
7. Кіберзагрози для інтернету речей (IoT): захист смарт-пристроїв. *Wezom*, 2024. URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv (дата звернення: 07.05.2025).
8. Мерзлікін Є., Бабешко Є. Аналіз кібербезпеки веборієнтованих індустріальних IoT-систем // *Сучасний стан наукових досліджень та технологій в промисловості.* 2023. № 2 (24). С. 131–144.
9. Delembovskyi M., Корнійчук Б. Аналіз сучасних наукових публікацій за напрямком тематики кібербезпеки IoT технологій // *Grail of Science.* 2023. С. 203–206.
10. Fortifying IoT Defence: Device Identification's Critical Role in IoT Protection. *Avnet Silica*, 2025. URL: https://my.avnet.com/silica/solutions/security-services/secure-device-management-provisioning/iot-security-series/device-identification/ (дата звернення: 07.05.2025).

11. Hallin J. Evaluation of TLS and mTLS in Internet of things systems. *Mid Sweden University*, 2025. 53 с.
12. Fedrecheski G., Vučinić M., Watteyne T. Performance comparison of EDHOC and DTLS 1.3 in Internet-of-Things environments // *2024 IEEE Wireless Communications and Networking Conference* (WCNC), 2024. P. 1–6.
13. Chang Q., Ma T., Yang W. Low power IoT device communication through hybrid AES-RSA encryption in MRA mode // *Sci Rep*. 2025. Vol. 15, 14485. DOI: https://doi.org/10.1038/s41598-025-98905-0.
14. Здолбіцька Н., Жигаревич О., Бас Д. Сучасні способи автентифікації та захист на основі токенів // *Прикладні проблеми комп'ютерних наук, безпеки та математики.* 2024. № 3. С. 4–11.
15. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *ISO*, 2022. URL: https://www.iso.org/ru/standard/27001 (дата звернення: 07.05.2025).
16. The NIST Cybersecurity Framework (CSF) 2.0. *NIST CSWP 29*, 2024. 27 p.
17. Олійник Я., Платоненко А., Черевик В. Я. та ін. Методи захисту інформації в технологіях IoT // *Кібербезпека: освіта, наука, техніка.* 2025. № 3 (27). С. 100–108. DOI: https://doi.org/10.28925/2663-4023.2025.27.705.
18. Khomenko Y. Сучасні методи, моделі та програмні засоби реалізації та оптимізації систем IoT (Internet of Things) // *Journal of Information Technologies in Education (ITE)*. 2024. № 55. С. 72–84.
19. Агутін М. М., Сусло Т. Ю. Моделювання безпеки та надійності IoT-систем // *Моделювання та інформаційні системи в економіці* : зб. наук. пр. / М-во освіти і науки України, Київ. нац. екон. ун-т ім. Вадима Гетьмана ; голов. ред. О. Є. Камінський. Київ : КНЕУ, 2023. Вип. 103. С. 7–17.
20. Бойко В. С. Створення Docker образів IoT систем у PyCharm та Visual Studio Code // *Радіоелектроніка та молодь у XXI столітті* : матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. / наук. керівник О. В. Зубков. Харків : ХНУРЕ, 2024. Т. 3. С. 77–79. DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.77.

21. Крохмаль М. Оптимізація енергоефективних протоколів взаємодії мікроконтролерів в інтернеті речей // *Південноукраїнські наукові студії* : збірник матеріалів Всеукр. наук.-практ. конф. студентів та молодих вчених (м. Одеса, 19–21 листопада 2024 р.) / за ред. О. Б. Петінової. Одеса : Університет Ушинського, 2024. С. 39–40.
22. VanhoefKey M. Reinstallation Attacks. Breaking WPA2 by forcing nonce reuse. *Krackattacks. Офіційний сайт*. URL: https://www.krackattacks.com/ (дата звернення: 07.05.2025).
23. Аронов А. О. Дослідження методик оптимізації параметрів системи керування розумним будинком з використанням IoT // *Телекомунікаційні та інформаційні технології.* 2025. № 1. С. 141–150.
24. Haidai A., Klymenko I. Method of Load Balancing in Distributed Three-Layer IoT Architecture // *Information, Computing and Intelligent systems.* 2024. № 4. С. 60–68.