УДК 004.056:004.7

ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Андрій ІВАНУСА, Мар'ян ТКАЧ, Андрій ПЕТРОВИЧ, Юрій ТКАЧ
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі спроектовано архітектуру захищеної IoT-системи та розроблено комплексний підхід до її захисту. Запропоноване рішення поєднує шифрування TLS/SSL, апаратний модуль TPM, рольовий контроль доступу та поведінкову аналітику UBA для забезпечення надійності та протидії загрозам у мережах Інтернету речей.*

Ключові слова: *інтернет речей, кібербезпека, протоколи IoT, TPM, MQTT, шифрування, контроль доступу.*

Abstract. *he paper designs the architecture of a secure IoT system and develops a comprehensive approach to its protection. The proposed solution combines TLS/SSL encryption, a TPM hardware module, role-based access control, and User Behavior Analytics (UBA) to ensure reliability and counter threats in Internet of Things networks.*

Keywords: *Internet of Things, cybersecurity, IoT protocols, TPM, MQTT, encryption, access control.*

Стрімкий розвиток технологій Інтернету речей вимагає нових підходів до проектування мережевої інфраструктури, де питання безпеки стають критично важливими. При проектуванні мережі Інтернету речей необхідно включати дві складові: фізичне проектування мережі, яке охоплює пристрої та протоколи, та логічне проектування, що представляє абстрактне розуміння сутностей і процесів . Відсутність єдиних стандартів безпеки робить вразливими більшість сучасних IoT-систем, що зумовлює необхідність розробки комплексних рішень захисту на всіх рівнях архітектури.

В основі розробленої системи лежить чотирирівнева модель протоколів, що забезпечує надійну взаємодію між пристроями та сервером. На канальному рівні використовуються технології IEEE 802.11 (WiFi) для всіх сенсорів, хоча також можуть застосовуватися Ethernet, WiMax та LR-WPAN. Мережевий рівень базується на протоколі IPv4, що забезпечує ідентифікацію хостів та адресацію, з підтримкою 6LoWPAN для малопотужних мереж. Транспортний рівень реалізує підтримку TCP для надійного зв'язку та UDP для швидкої передачі даних. На рівні додатків використовуються протоколи MQTT для міжмашинної взаємодії, WebSocket для двостороннього зв'язку, а також HTTP та CoAP.

Для практичної реалізації системи було обрано топологію, що включає розумний дверний замок, датчик відкриття вікна, розумну лампу, дат-

чик включення світла та шлюз, який виконує роль базової станції . Шлюз відповідає за маршрутизацію даних, при цьому мережа Інтернету речей ізольована в адресному просторі 192.168.25.0/24, що ускладнює несанкціонований доступ зловмисників. Взаємодія компонентів системи базується на моделі "запит-відповідь" та Push-Pull із використанням REST та WebSocket API.

Оскільки дослідження показують, що більшість IoT систем не шифрують трафік, у розробленій системі впроваджено багаторівневу модель захисту, графічне зображення якої наведено на рисунку нижче. Запропонована концепція безпеки охоплює забезпечення безпеки зв'язку, контроль доступу, апаратний захист та операційні заходи безпеки.

Для захисту каналів передачі даних обрано метод Еліптичної криптографії, який є ефективним для пристроїв з обмеженими обчислювальними ресурсами. Шифрування та аутентифікація реалізуються через протокол TLS/SSL поверх MQTT на платформі IBM Watson IoT Platform. Замість прямого підключення датчиків використовується смартфон з додатком, що проходить етап аутентифікації через токени. Додатково в систему впроваджено сертифікат безпеки X.509 для унікальної ідентифікації пристроїв, що дозволяє визначити довірені вузли та обмежити доступ для непідтверджених девайсів.

Важливим елементом захисту є впровадження контролю доступу та безпеки управління через рольову модель. Створено спеціальні ролі, які обмежують права пристроїв та шлюзу, дозволяючи їм виконувати лише необхідні операції. Для виявлення загроз використовується аналітична система безпеки UBA, яка будує модель поведінки користувача та виявляє аномальну активність. Також проводиться регулярний місячний аудит інфраструктури за допомогою сервісу AWS IoT Device Defender.

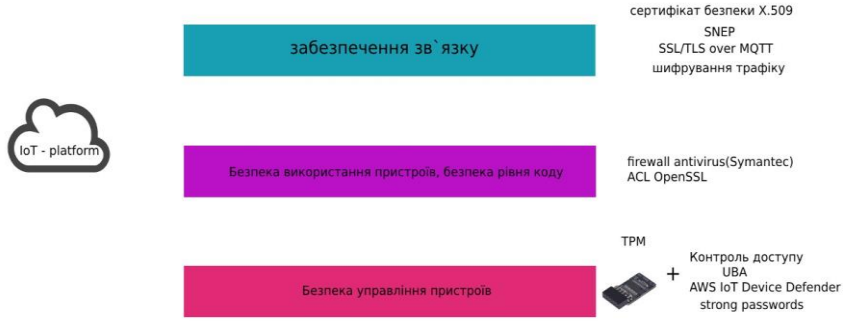

Рисунок 1 – Система методів безпеки для спроектованої системи

Для підвищення захищеності від фізичного злому та підробки ключів впроваджено апаратний модуль TPM. Він забезпечує цілісність пристрою, створює корінь довіри та генерує ключі шифрування, працюючи в безпечному режимі для мінімізації шкоди від шкідливого програмного забезпечення . На рівні коду безпека забезпечується використанням бібліотеки OpenSSL для перевірки автентичності, а також обмеженням функціоналу програмного коду пристроїв лише виконанням специфічних завдань, що запобігає їх використанню у ботнетах.

Додаткові операційні заходи безпеки включають використання брандмауера для контролю вхідного і вихідного трафіку, встановлення антивірусного програмного забезпечення Symantec, регулярне оновлення прошивок із перевіркою безпечного завантаження та використання надійних унікальних паролів .

У підсумку, в роботі спроектовано захищену IoT систему, що базується на комплексному підході до інформаційної безпеки. Реалізована архітектура поєднує ізольовану мережеву топологію з використанням надійних протоколів. Основна наукова та практична цінність полягає у впровадженні комбінованої системи захисту, яка включає криптографічний захист трафіку, сувору аутентифікацію, апаратний захист та інтелектуальний аналіз загроз. Такий підхід дозволяє нівелювати ризики компрометації пристроїв та забезпечити цілісність і конфіденційність даних у мережі Інтернету речей.

Література

1. Cirani S., Ferrari G., Picone M., Veltri L. Internet of Things: Architectures, Protocols and Standards. Hoboken : Wiley, 2018. 376 p.

2. Suthar S., Das R. Demystifying Internet of Things Security : Successful IoT Device/Edge and Cloud Security Design. Berkeley : Apress, 2019. 339 p.

3. MQTT Version 3.1.1 : OASIS Standard / ed. by A. Banks, R. Gupta. OASIS, 2014. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html (дата звернення: 27.10.2025).

4. Arthur W., Challener D. A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security. New York : Apress, 2015. 343 p.

5. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP) : RFC 7252. IETF, 2014. 112 p. URL: https://tools.ietf.org/html/rfc7252 (дата звернення: 27.10.2025).