ДОДАТОК А
ГРАФІЧНИЙ МАТЕРІАЛ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

Модель безпеки інформаційної системи на базі технологій IoT

Кваліфікаційна робота
Другий (магістерський) рівень

Автор:
Литвиненко Д.С.,
студ. гр. СПм-20-1

Керівник:
Кучук Г.А.,
проф. каф. ЕОМ

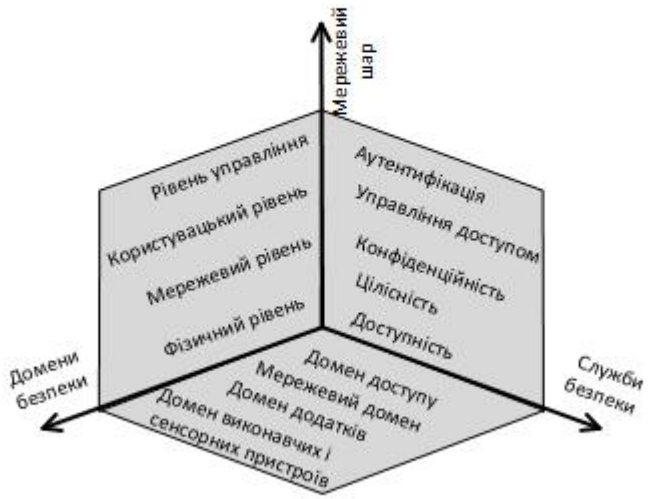
Мета і задачі роботи

Метою кваліфікаційної роботи є розробка моделі безпеки, придатної для типових інформаційних систем на базі технологій IoT. Модель має бути невибагливою до обчислювальних ресурсів та виконуватися у найменший час.

Задачі:

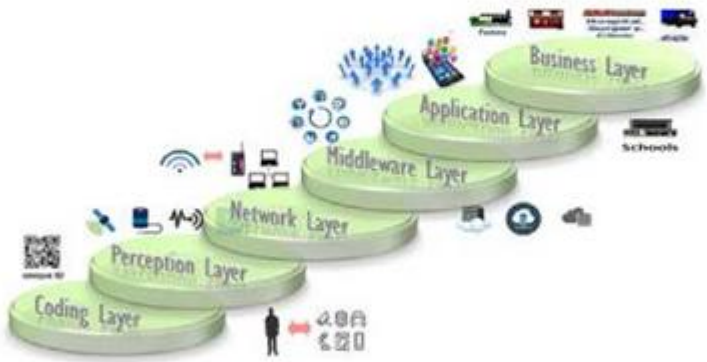
- проаналізувати особливості багаторівневої архітектури IoT;
- дослідити основні проблеми безпеки середовища IoT;
- побудувати модель системи безпеки;
- розробити оцінку рівня безпеки середовища IoT.

Складові безпеки середовища IoT



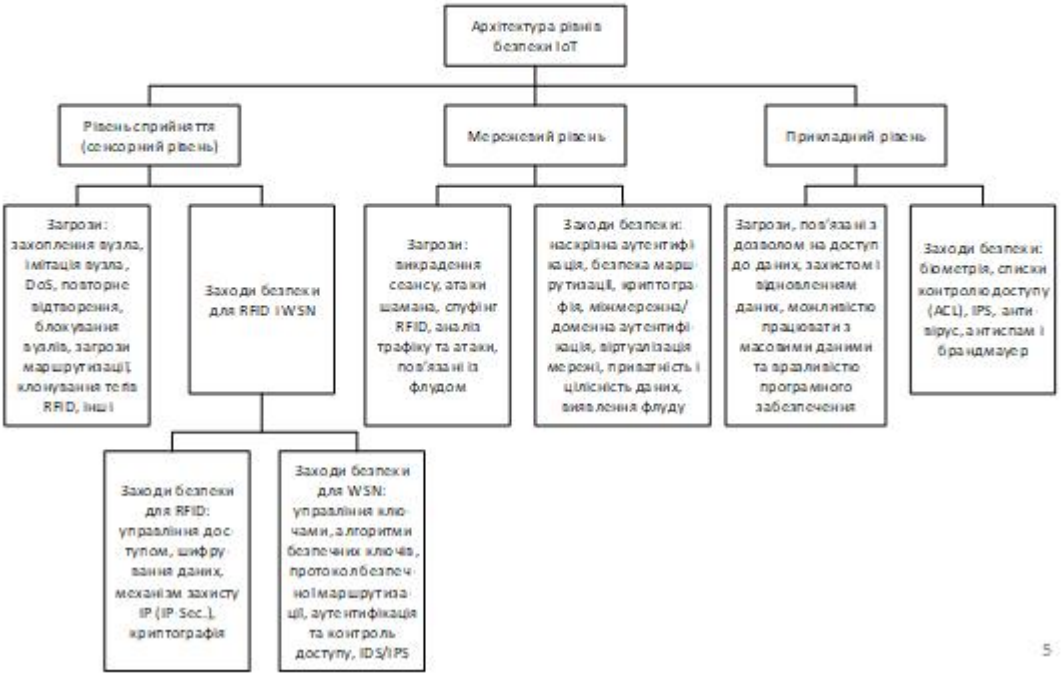
3

Рівнева архітектура IoT



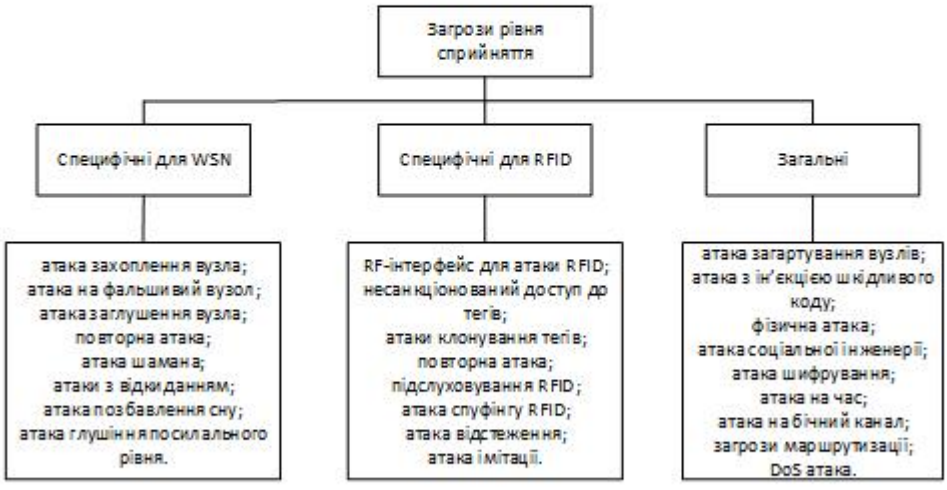
4

Загрози та заходи безпеки на кожному рівні безпеки IoT



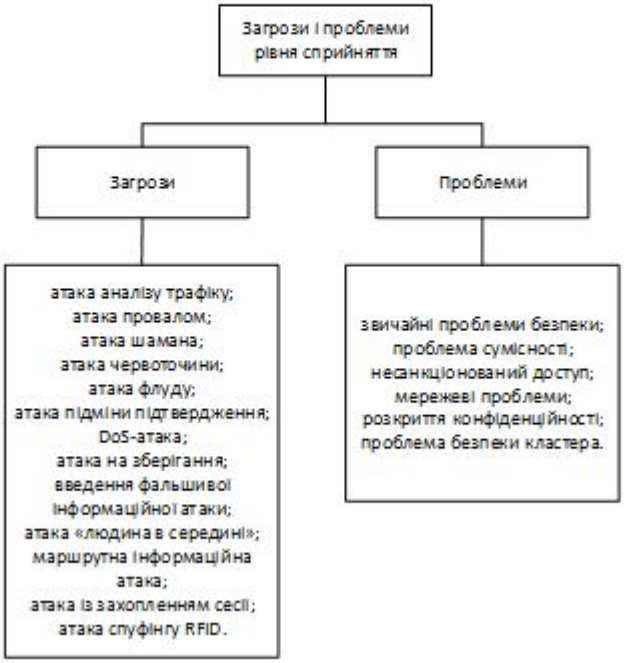
5

Можливі загрози рівня сприйняття



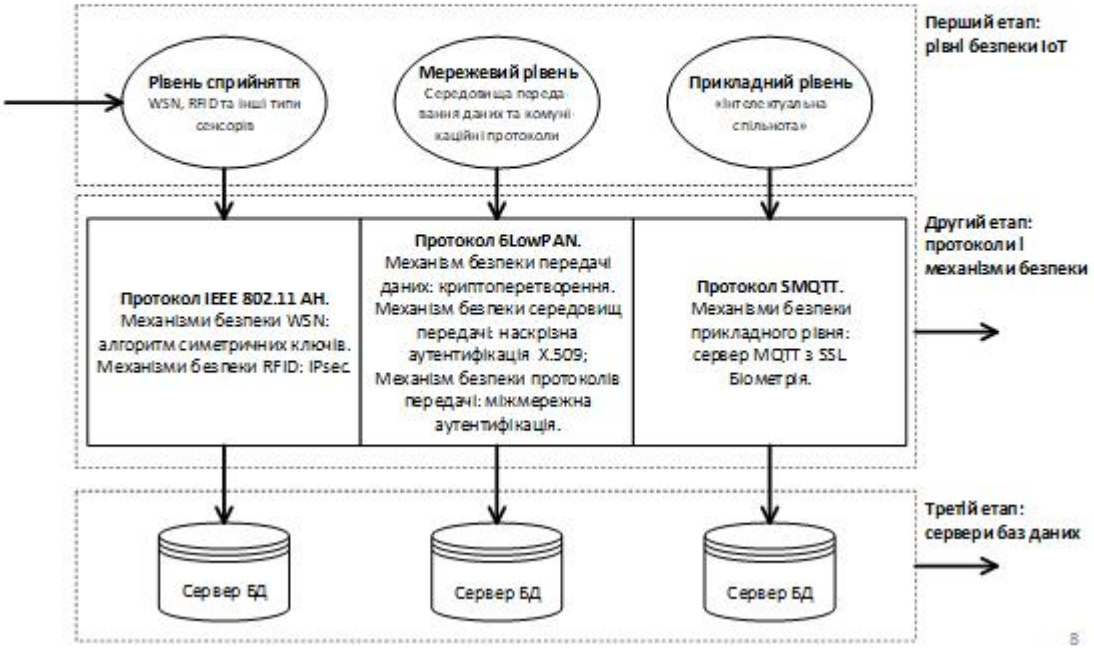
6

Загрози і проблеми мережевого рівня



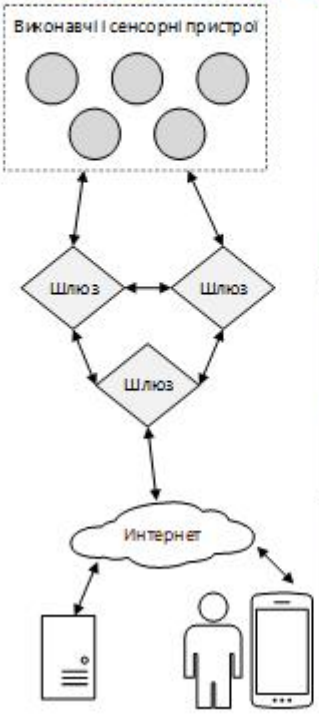
7

Запропонована модель управління безпекою



8

Архітектура безпеки середовища Інтернету речей з додатковим шаром



1. Виконавчі і сенсорні пристрої.
1) уніфікація кодування;
2) коригуючі коди;
3) розподіл часового і фізичного простору для RFID;
4) захист конфіденційності у RFID;
5) зберігання лише необхідної інформації у RFID;
6) приховування розташування пристроїв;
7) протоколи автентифікації пристроїв;
8) шифрування інформації, що передається в мережу;
9) управління ключовою інформацією;
10) протоколи безпечної маршрутизації;
11) управління довірою між пристроями;
12) уніфікація формату передачі.

2. Шлюзи і мережа Інтернет.
1) виявлення вторгнень;
2) перевірка даних, що збираються пристроями;
3) управління доступом;
4) протокол 6LowPan;
5) шифрування інформації, що передається через Інтернет;
6) управління ключовою інформацією;
7) управління потоками інформації;
8) управління довірою між пристроями.

3. Додатки і хмарні сервіси.
1) моніторинг;
2) контроль доступу;
3) аутентифікація;
4) резервне копіювання;
5) управління потоками даних;
6) контроль цілісності;
7) шифрування;
8) управління привілеями;
9) доступність.

9

Метод оцінки рівня безпеки (1/3)

- Нехай існує m виконавчих пристроїв X_m і n шлюзів G_n.
- Зв'язки виконавчих та сенсорних пристроїв між собою можна описати матрицею C_x розміром $m \times m$. Визначимо матрицю P_x розміром $m \times p_x$, елементами якої є кількісні параметри безпеки взаємодії кожного пристрою з іншим, що приведені до єдиної шкали відповідно до першого рівня. Тоді добуток матриць характеризуватиме безпеку взаємодії пристроїв у вигляді матриці розміром $m \times p_x$:

$$S_x = C_x \times p_x.$$

- Зв'язки між пристроями та шлюзами можна описати матрицею C_b розміром $n \times m$. Визначимо матрицю P_b розміром $m \times p_b$, елементами якої є кількісні параметри безпеки кожного пристрою при взаємодії зі шлюзом, що приведені до єдиної шкали згідно з першим рівнем. Тоді добуток матриць характеризуватиме безпеку на межі шлюзів у вигляді матриці розміром $n \times p_b$:

$$D_b = C_b \times P_b.$$

10

Метод оцінки рівня безпеки (2/3)

- Далі розраховується відносна оцінка безпеки за формулою

$$V_1 = \frac{\Sigma_{r=1}^{m}\Sigma_{k=1}^{p_x} s_{rk} + \Sigma_{r=1}^{n}\Sigma_{k=1}^{p_b} d_{rk}}{T_x + T_b},$$

- де V_1 – підсумкова оцінка безпеки першого рівня; T_x і T_b – максимально можливі оцінки безпеки у матрицях S_x і D_b, відповідно; s_{rk} – елементи матриці S_x; d_{rk} – елементи матриці D_b.
- Зважаючи на те, що деякі параметри безпеки змінюються із часом, то розраховується оцінка, яка залежить від часу:

$$V_1(t) = \frac{\Sigma_{r=1}^{m}\Sigma_{k=1}^{p_x} s_{rk}(t) + \Sigma_{r=1}^{n}\Sigma_{k=1}^{p_b} d_{rk}(t)}{T_x + T_b}.$$

11

Метод оцінки рівня безпеки (3/3)

- Для другого рівня оцінити рівень безпеки можна шляхом урахування взаємозв'язків шлюзів G_n у вигляді матриці C_g розміром $n \times n$ та характеристик безпеки у вигляді матриці P_g розміром $n \times p_g$. Потім обчислюється їх добуток у вигляді матриці S_g, що кількісно описує стан безпеки взаємодії шлюзів між собою.
- Для оцінки захищеності з виходом інформації до мережі Інтернет складається матриця C_v, що описує зв'язок шлюзів з мережею Інтернет, та матриця P_v, елементами якої є параметри безпеки другого рівня. Застосовуючи операції, як показано вище, отримуємо матриці S_g, D_v та оцінку V_2. Аналогічно для третього рівня розраховується оцінка V_3 для хмарних сервісів, абонентських пристроїв та виходу до мережі Інтернет:

$$V_2 = \frac{\Sigma_{r=1}^{m}\Sigma_{k=1}^{p_x} s_{rk} + \Sigma_{r=1}^{n}\Sigma_{k=1}^{p_b} d_{rk}}{T_g + T_v};$$

$$V_3 = \frac{\Sigma_{r=1}^{m}\Sigma_{k=1}^{p_x} s_{rk} + \Sigma_{r=1}^{n}\Sigma_{k=1}^{p_b} d_{rk}}{T_f + T_z}.$$

12

Апробація результатів

- Кучук Г. А., Литвиненко Д. С., Росінський Д. М. Ключові аспекти безпеки екосистеми Інтернету речей // Проблеми інформатизації. Тези доповідей дев'ятої міжнародної науково-технічної конференції, 18-19 листопада 2021 р., Черкаси: ЧДТУ, 2021. – С. 64.

Проблеми інформатизації: дев'ята міжнародна науково-технічна конференція

КЛЮЧОВІ АСПЕКТИ БЕЗПЕКИ ЕКОСИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

Кучук Г. А., Литвиненко Д.С., Росінський Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтернет речей (IoT) виводить концепцію безпеки на абсолютно новий рівень. Мережевим безпеки вирай необхідно враховувати у світі, де все можна «підключити», а фізичний контакт стає необов'язковим, та для роботи кінцевого пристрою використовуються словесні інструкції з навіть розпізнаванням обличчя. Можна виділити дві категорії небезпек, пов'язані з IoT [1]. Небезпеки першого типу безпосередньо пов'язані з традиційним використанням пристрою і включають такі речі, як перегрів, удари, звукові небезпеки тощо. Впровадження Інтернету речей у продукти може збільшити частоту виникнення цих небезпек. Удосконалення дистанційних операцій означає, що небезпеки такого роду більше не зв'язані фізичними обмеженнями. Небезпеки другого типу опосередковано пов'язані з пристроєм та його роботою, але можуть спричинити проблеми з безпекою через впровадження IoT. Ефектом каскаду може бути порушення властивостей або витік приватної інформації.

Розробники на цей час правила та стандарти належним чином вирішують виключно небезпеки, виникнення першопричину цих небезпек та небезпек застосування для існуючих продуктів. Одним з провідних секторів є побутова техніка. Необхідно також розглядати дрони та подібні пристрої, які можуть поранити людей або нанести фінансові активи. Широко виробляються автономні транспортні засоби, а також з'являються пристрої з підтримкою IoT для автомобільної промисловості, що створює ще одну рамку пробок безпеки. Міжнародні та регіональні стандарти включають [1]: IEC61508, ISO26262, ISO21160, ISO13849, IEC60730-1, UL 5500, CSA Z434, ANSI B11.

Метою даної статті є формулювання ключових аспектів, пов'язаних з підтримкою функціональної безпеки.

До них входить: елементи планування та дизайну; ризики та небезпеки; плани управління; рівні продуктивності (PL); рівні цілісності безпеки (SIL); режими, наслідки та діагностичний аналіз відмов (FMEDA); причинна відповідальність перспективу; сувора документація.

Оскільки IoT продовжує розвиватися, важливо залишатися в курсі стандартів ризиків і безпеки, щоб переконатися, що продукти відповідають нормативним вимогам і вимогам споживачів. Очікується, що оцінка безпеки IoT буде тісно пов'язана з функціонального безпекою, яка була встановлена щонайменше 20-ти століття для промислових середовищ.

Список літератури

1. O. Omolara, A. Abdulahi, O. Alsaaby, M. Alawida, W. Aldhoura, H. Arshad (2021) The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*. 112. 102494. 10.1016/j.cose.2021.102494.

64

Висновки

- В роботі представлено порівняння між механізмами безпеки для кожного рівня безпеки IoT, які були розроблені для визначення ролі заходів безпеки і їхнього впливу на споживану потужність і час.
- За підсумками порівнянь запропонована модель управління безпекою для системи IoT, яка дозволяє вибирати найбільш придатні протоколи та алгоритми безпеки.
- Запропонована модель охоплює захист даних, середовищ передачі, протоколів та програм для запобігання більшості загроз. Може використовуватися для виявлення помилок мережі та захисту приватної інформації користувачів.
- Запропоновано метод оцінки безпеки середовища Інтернету речей.
- Запропонована модель може допомогти розробникам керувати методами безпеки на кожному рівні безпеки IoT. Основним внеском моделі є вибір відповідних механізмів безпеки і керування ними для досягнення низького споживання енергії та часу.

Висновки

- Завдяки відносно невеликій обчислювальній складності запропонованої моделі безпеки, вона може бути реалізована в масштабі реального часу, що може бути актуальним, наприклад, під час аутентифікації або підключення нових пристроїв до середовища Інтернету речей та залучення протоколів інформаційного обміну різного рівня захищеності, а значить, при необхідності вибору найбільш безпечних маршрутів передачі даних.
- В рамках подальшої роботи можна розглядати основні реалізації запропонованої моделі та її варіації, придатні для різних мережевих платформ IoT. Також можна отримати оцінку впливу реалізації запропонованої моделі на енергоспоживання та час виконання.
- Отримана декомпозиційна модель безпеки середовища Інтернету речей є досить універсальною і може бути масштабована на різні об’єкти відповідного кластера інформаційних технологій.

15

ДОДАТОК Б
СПЕЦИФІКАЦІЇ РІВНІВ ЗАХИСТУ

Таблиця Б.1 – Специфікації рівнів безпеки та їх методи безпеки

Рівень	Компоненти	Функції	Атаки/проблеми	Вимоги безпеки	Методи/механізми безпеки
Рівень сприйняття	Всі види датчиків, RFID, GPS, Bluetooth	Зв’язування різних розумних пристроїв в Інтернеті речей, збор інформації, передача даних на мережевий рівень	Захоплення вузла, імітація вузла, відмова в обслуговуванні (DoS), атака повторного відтворення, блокування вузлів, загрози маршрутизації, клонування тегів RFID, інші	Конфіденційність, цілісність, доступність, аутентичність, приватність	Алгоритми хешування, алгоритми криптографії, контроль доступу, IPSec., керування ключами (PKI), система запобігання вторгнень (IPS), протокол шифрування, оцінка ризику
Мережевий рівень	Мобільний зв’язок та Інтернет	Передача інформації	Атаки: викрадення сеансу, атаки шамана, спуфінг RFID, аналіз трафіку та атаки, пов’язані із повінью. Проблеми: сумісність, безпека кластера, мережа незаконного доступу та розкриття конфіденційності	Цілісність, доступність, конфіденційність	Аутентифікація між кінцевими пунктами, безпека та маршрутизація, алгоритми криптографії, міжмережна/доменна автентифікація, технологія віртуалізації мережі, приватність і цілісність даних для виправлення та контролю помилок, виявлення повені.

Продовження таблиці Б.1

Рівень	Компоненти	Функції	Атаки/проблеми	Вимоги безпеки	Методи/механізми безпеки
Прикладний рівень	Інтелектуальна спільнота	Надання багатьох послуг та аналіз інформації	Дозвіл на доступ до даних, захист і відновлення даних, можливість працювати з масовими даними та вразливістю програмного забезпечення	Конфіденційність, аутентичність, авторизація, доступність	Біометрія, списки контролю доступу (ACL), IPS, антивірус, антиспам і брандмауер

Таблиця Б.2 – Заходи безпеки для WSN

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Управління ключами	Генерування та оновлення алгоритмів безпеки за допомогою розподілу ключів, наприклад інфраструктури відкритих ключів (PKI), яка створює відкриті ключі цифрової сертифікації	Конфіденційність, аутентичність та доступність	Проблема фальсифікації, шамана, атаки підслуховування та спуфінгу	Легкі захисні механізми	Потребують час
Алгоритми безпечних ключів	Симетричні та асиметричні алгоритми. Існує багато симетричних алгоритмів (наприклад, RC5) і асиметричних (наприклад, AES)	Конфіденційність, аутентичність, цілісність і приватність	Відтворення, аналіз трафіку, атаки підслуховування та спуфінгу	Сим. алгоритми: менше споживання енергії, вартість, час роботи вузлів	Асим. алгоритми: споживають більше енергії та часу

Продовження таблиці Б.2

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Протокол безпечної маршрутизації	Існує багато алгоритмів безпечної маршрутизації (злиття даних, маршрутизація з кількома переходами, ключові механізми). Протокол безпечного шифрування мережі (SNEP) широко використовується для WSN, забезпечує автентифікацію широкомовної передачі від точки до кількох точок.	Конфіденційність, аутентифікація та цілісність	Маршрутизація загроз	SNEP забезпечує менше часу	Більшість алгоритмів протоколу маршрутизації безпеки споживають енергію та час
Аутентифікація та контроль доступу	Аутентифікації на основі легкої технології з відкритим ключем (наприклад, перед загальним ключем і хеш-функцією). Контроль доступу на асиметричній і симетричній криптосистемі. Потрібна висока швидкість процесора і пам’ять	Автентифікація забезпечує аутентичність та цілісність. Контроль доступу забезпечує конфіденційність, доступність і приватність	Підслуховування, захоплення вузла та атаки шамана	Легка технологія аутентифікації відкритим ключем споживає менше енергії	Традиційні механізми аутентифікації та контролю доступу не застосовуються для системи IoT

Продовження таблиці Б.2

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Система виявлення та запобігання вторгнень IDS/IPS	Наставництво щодо поведінки мережі та користувачів. Використовувалася для виявлення та запобігання більшості підозрілих користувачів і атак	IDS і IPS забезпечують більшість вимог безпеки	Більшість нападів і загроз	IPS використовується для виявлення та запобігання атак і загроз, для автоматичної зупинки атак	IDS вимагає визначення політики безпеки, щоб гарантувати, що загрози та атаки обробляються відповідно до принципів корпоративної політики безпеки

Таблиця Б.3 – Заходи безпеки для RFID

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Управління доступом	Захист чутливих даних користувачів всієї інформації RFID-міток. Прогнозування несанкціонованого доступу до тегів.	Конфіденційність, аутентичність, цілісність	Атаки підслуховування, спуфінгу, імітації та несанкціонований доступ до тегів	Корисно для захисту мікросхем та аналізу антени	Контроль доступу може зайняти більше часу

Продовження таблиці Б.3

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Шифрування даних	Найважливіший метод шифрування RFID-сигналу та даних RFID	Конфіденційність, цілісність, приватність	RF-інтерфейс для RFID, повторного відтворення, підслуховування RFID та атак підробки	Вимагає менше обчислювальної потужності та забезпечує високий рівень безпеки	Потребує більше часу
Механізм захисту IP (IP-Sec.)	Два рівні техніки безпеки: механізми аутентифікації та шифрування. Механізм аутентифікації: для ідентифікації особистості користувача. Механізм шифрування: для шифрування даних і сигналів RFID.	Автентифікація забезпечує цілісність, конфіденційність та автентичність. Шифрування забезпечує конфіденційність	Атаки підслуховування, спуфінгу, зміни даних і клонування тегів	Забезпечує більш безпечні дані та сигнал RFID	Споживає електроенергію і час
Технологія криптографії	Заснована на хеш-функції та алгоритмах шифрування. Використовується для захисту сигналу RFID	Конфіденційність, аутентичність, приватність	Підслуховування RFID, підробка RFID, клону-вання тегів, інтерфейс RF для RFID та відстеження атак	Захищає протоколи зв’язку	Споживає більше енергії та часу

Таблиця Б.4 – Заходи безпеки для мережевого рівня

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Наскрізна аутентифікація та керування ключами	Усі вузли в мережі IoT повинні бути аутентифіковані за допомогою механізму аутентифікації, інфраструктури відкритих ключів і наскрізного шифрування	Конфіденційність і цілісність даних	Незаконний доступ до вузлів, атак DoS та Sinkhole	Забезпечує наскрізну аутентифікацію та шифрування	Важкий механізм безпеки
Безпека та маршрутизація	Наступний кроком заходів безпеки мережевого рівня. Відбувається після процесу аутентифікації. Механізми захищеної маршрутизації важливі для захисту даних і збереження конфіденційності даних	Конфіденційність і цілісність даних	Більшість погроз і атак	Забезпечує багатопрохідність для маршрутизації даних і покращує можливості для виявлення будь-якої помилки в системі	Забирає час
Технологія віртуалізації мережі	Об’єднання апаратних і програмних ресурсів і мережевих функцій в єдину або мережу. Зовнішня віртуалізація об’єднує багато частин мережі у віртуальний блок, (наприклад, локальні мережі), щоб підвищити точність мережі та ефективність даних. Внутрішня забезпечує функціональність мережі програмному забезпеченню на одному мережевому сервері	Конфіденційність і цілісність	Більшість мережевих атак	Використовується для зменшення складності управління мережею	Забирає час

Продовження таблиці Б.4

Заходи безпеки	Використання	Вимоги безпеки	Запобігання нападу	Переваги	Недоліки
Система криптографії	Використовувався для перевірки передачі даних через інші вузли та виявлення будь-яких помилок у мережі	Цілісність даних	Запобігає загартовування даних на вузлі-отримувачі	Виявляє помилку мережі та перевіряє дані. Симетрична ключова криптографія споживає мало енергії та часу	Асиметрична криптографія споживає енергію та час
Аутентифікація між мережами та доменом	Захист протоколів (міжмережева аутентифікація). Захист DNS (міждоменна автентифікація)	Конфіденційність і цілісність	Маршрутизація загроз	Захист мережевих протоколів	Споживає більше енергії
Приватність і цілісність даних	Виявлення та контроль будь-якої помилки, що виникає в мережі. Цілісність даних використовує алгоритми шифрування для перевірки даних, які надсилаються	Цілісність	Незаконний доступ і підробка	Використовується для перевірки вихідних даних	Забирає час
Виявлення повені	Відправник надсилає одержувачу привітальне повідомлення, яке використовується для перевірки сили сигналу. Якщо цей сигнал подібний до одиночних в діапазоні радіоприймача, приймач приймає повідомлення	Конфіденційність	Напад повені	Використовується для перевірки вихідних сигналів	Забирає час