Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Модель безпеки інформаційної системи на базі технологій IoT

(тема)

Виконав:

студент II курсу, групи СПм-20-1

Литвиненко Д.С.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: проф. Кучук Г.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Литвиненку Денису Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Модель безпеки інформаційної системи на базі технологій IoT

затверджена наказом по університету від “ 05 ” листопада 2021 р. № 1657 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2021 р.

3. Вхідні дані до роботи 1) узагальнена модель середовища Інтернету речей;
2) підтримувані стандартні методи і засоби інфораційної безпеки;
3) розробити оцінку рівня безпеки.

4. Перелік питань, що потрібно опрацювати у роботі
1) огляд Інтернету речей у ретроспективі та аналіз його сучасного стану;
2) аналіз аспектів безпеки в системі Інтернету речей;
3) побудова загальної моделі системи безпеки;
4) оцінка рівня безпеки;
5) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд – презентація – 12 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд Інтернету речей у ретроспективі та	09.11.21-12.11.21	
	аналіз його сучасного стану		
2	Аналіз аспектів безпеки в системі IoT	13.11.21-22.11.21	
3	Побудова загальної моделі системи безпеки	23.11.21-29.11.21	
4	Оцінка рівня безпеки	30.11.21-03.12.21	
5	Оформлення матеріалів кваліфікаційної роботи	04.12.21-07.12.21	
6	Подання кваліфікаційної роботи керівникові та	08.12.21-09.12.21	
	її попередній захист		
7	Подання кваліфікаційної роботи на	10.12.21-11.12.21	
	рецензування		

Дата видачі завдання 08 листопада 2021 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Кучук Г.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 81 с., 7 рис., 1 табл., 2 дод., 36 джерел.

БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ, ВИКОНАВЧІ ПРИСТРОЇ, ІНТЕРНЕТ РЕЧЕЙ, ІНТЕРОПЕРАБЕЛЬНІСТЬ, КОНЦЕПЦІЇ БЕЗПЕКИ, МІЖМАШИННА ВЗАЄМОДІЯ, МОДЕЛЬ БЕЗПЕКИ, РІВЕНЬ БЕЗПЕКИ ІОТ.

Метою кваліфікаційної роботи є побудова моделі безпеки для середовища Інтернету речей, яка має бути невибагливою до обчислювальних ресурсів та виконуватися у найменший час.

У ході виконання кваліфікаційної роботи представлено вступ до IoT, його компоненти, підключення та додатки. Обговорюються проблеми безпеки IoT для запобігання внутрішнім і зовнішнім загрозам. Дослідження було зосереджено на рівнях і функціях Інтернету речей для вирішення проблем безпеки IoT. Визначено заходи безпеки, які підвищують швидкість роботи мережі IoT та сприяють зниженню енергоспоживання.

ABSTRACT

Master’s thesis: 81 pages, 7 figures, 1 table, 2 appendices, 36 sources.

EXECUTIVE DEVICES, INTERNET OF THINGS, INTEROPERABILITY, IOT SECURITY LEVEL, MACHINE INTERACTION, SECURITY CONCEPTS, SECURITY MODEL, WIRELESS SENSOR NETWORKS

The purpose of the qualification work is to determine security model for IoT, which should be unpretentious to computing resources and be performed in the shortest time.

Introduction to IoT, its components, connections and applications are presented during the qualification work. IoT security issues to prevent internal and external threats are discussed. The research focused on the levels and functions of the Internet of Things to address IoT security issues. Security measures have been identified that increase the speed of the IoT network and help reduce energy consumption.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACL – список контролю доступу (англ., Access Control List).

AMQP – розширений протокол черги повідомлень (англ., Advanced Message Queuing Protocol)

ARP – протокол визначення адрес (англ., Address Resolution Protocol)

CA – посвідчення сертифікатів (англ., Certification Authority)

CoAP – обмежений прикладний протокол (англ., Constrained Application Protocol)

DoS – атака на відмову в обслуговуванні (англ., Denial-of-Service)

H2H – взаємодія за типом «людина –людина» (англ., Human to Human)

IoT – Інтернет речей (англ., Internet of Things)

IPsec – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP (англ., IP Security)

M2H – взаємодія за типом «машина–людина» (англ., Machine to Human)

M2M – взаємодія за типом «машина–машина» (англ., Machine to Machine)

MQTT – телеметричний протокол транспортування черги повідомлень (англ., Message Queuing Telemetry Transport)

PKI – інфраструктура відкритих ключів (англ., Public Key Infrastructure)

RFID – радіочастотна ідентифікація (англ., Radio Frequency Identification)

SOA – сервісно-орієнтована архітектура (англ., Service-Oriented Architecture)

WSN – бездротова сенсорна мережа (англ., Wireless Sensor Network)

XMPP – розширюваний протокол обміну повідомленнями та присутності (англ., Extensible Messaging and Presence Protocol)

ВСТУП

Нині відбувається новий виток технічного розвитку цивілізації, який полягає у переході до автоматизації як процесів на виробничих підприємствах, а й процесів, які у повсякденному житті кожної людини. Ідея полягає у використанні великої кількості невеликих малопотужних з обчислювальної та енергетичної точки зору пристроїв для виконання однотипних простих завдань. Така технологія закладена в основі «розумного дому» та «розумного міста» і узагальнено називається «Інтернет речей» (англ., IoT – Internet of Things) [1]. Подібні технології використовують у розподілених геоінформаційних системах. При цьому керування цими пристроями здійснюється за допомогою комп’ютера або смарт-пристрою, а у разі міжмашинної взаємодії (M2M) – взагалі без участі людини [2].

Інтернет речей – порівняно нова інтелектуальна комунікація у світі, яка має багато застосувань, таких як промисловість, комунікації, сільське господарство, бізнес тощо. Дослідники та організації зосереджуються на розвитку Інтернету речей для того з багатьох причини. Нова технологія стикається з великим колом проблем, таких як архітектура, стандарт і безпека. Вважається, що кількість пристроїв, інтегрованих у середовище Інтернету речей, перевищила один мільярд.

З виходом на ринок великої кількості виробників кінцевого, комунікаційного та керуючого обладнання постало питання про інтероперабельність компонентів складної структури, а також про можливість їх роботи без загрози виникнення несанкціонованого доступу, витоку або розкриття інформації, що циркулює в системі. Отже, поряд з інтенсивним розповсюдженням по всьому світу і широким застосуванням цієї технології в багатьох галузях виробництва та життєзабезпечення гостро постає питання про безпеку не тільки пересічних користувачів цієї технології, а й критично важливої інформації, що циркулює при

міжмашинній взаємодії. Тому однією із задач є визначення найбільш зручної форми структурування аспектів безпеки стосовно цього середовища.

На даний момент немає єдиної системи критеріїв, що визначають стан безпеки середовища Інтернету речей. На основі розглянутих моделей пропонується власна трирівнева структура безпеки, що включає також властивості шару «fog»: виконавчі та сенсорні пристрої, шлюзи та мережа Інтернет, додатки та хмарні сервіси. Описано основні методи підвищення безпеки для всіх трьох шарів, а також наведено математичну модель, за допомогою якої можна зробити якісну та кількісну оцінку безпеки.

1 РОЗВИТОК, СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ IOT

1.1 Історія та тенденції IoT

Останні кілька років IoT є роками розквіту цієї нової технології. Очікується, що майбутнє світу зміниться завдяки використанню технології IoT протягом найближчих років. Її стрибок нової технології запровадить новий світ послуг, які підвищать якість життя. Інфраструктура Інтернету речей має за мету змінити форму зв’язку між пристроями та людиною для реалізації обміну величезною кількістю інформації. Таким чином, IoT створює новий гнучкий світ спілкування між людьми та мільярдами пристроїв.

IoT став критерієм для багатьох додатків, особливо, промисловості та комунікацій. Крім того, IoT сприяє розвитку багатьох галузей, таких як сільське господарство, навколишнє середовище, медичний сектор, освіта, транспорт, економіка тощо. Ці програми представляють багато великих проектів IoT, таких як розумні будинки, розумні транспортні засоби, розумні фабрики, розумні ферми, розумні лікарні, розумні школи, розумне місто тощо. Ця нова технологія покращує повсякденне життя.

IoT має важливий вплив у бізнес-секторі, де ринок IoT досяг прибутку в 290 мільярдів доларів у 2017 році. Цей прибуток має тенденцію збільшуватися на 30% на рік. Крім того, Інтернет речей відіграє важливу роль для людей з обмеженими можливостями та людей похилого віку з багатьма рівнями незалежності за розумну ціну.

Очевидно, що метою IoT є створення з’єднань обчислювальних пристроїв, механічних і цифрових машин, об’єктів і людей через програми за допомогою веб-інтерфейсу та мобільних додатків. Середовище IoT має можливість передавати дані по мережі без необхідності комунікації від людини до людини або від людини до комп’ютера. Система IoT складається з

чотирьох основних компонентів, які поділяються на речі, комунікації, програми та аналіз даних.

Технологія IoT використовує переваги кожного об’єкта і створює нову систему з новими можливостями.

IoT має велику кількість розумних об’єктів, і очікувана кількість до 2020 року становила 50 мільярдів об’єктів [3]. Багато компаній і науково-дослідницьких організацій впроваджують практичний план впливу IoT на економіку та більшість сфер життя протягом десяти років. Cisco є першою компанією, яка представила багато проектів, що охоплюють понад 24 мільярди смарт-об’єктів до 2019 року. Крім того, компанія Morgan Stanley охоплює багато проектів з мільярдами розумних об’єктів, і до 2020 року ця кількість була збільшена до 75 мільярдів підключених пристроїв. До 2025 року компанія Huawei надасть 100 мільярдів підключень IoT [4]. Очевидно, що серед більшості компаній існує жорстка конкуренція за представлення мережі IoT з численними мільярдами підключених смарт-об’єктів.

У 1982 році ідея Інтернету виникла з використанням протоколу Інтернету (TCP/IP). Ідея взаємозв’язку багатьох пристроїв була викристалізована для створення терміна Інтернет. У 1990 році Джон Ромкі та Саймон Хакетт створили тостер, який був підключений до Інтернету за допомогою протоколу TCP/IP і контролювався за допомогою SNMP MIB (англ., Simple Networking Management Protocol Management Information Base) [5]. Термін IoT почав існувати, коли Кевін Ештон ввів концепцію Інтернету речей IoT і створив Центр Auto-ID MIT у 1999 році. Його ідея була зосереджена на зв’язуванні інформації RFID з Інтернетом. Ця ідея була простою та надійною, що забезпечувала зв’язки між усіма пристроями один з одним [6]. У 1999 році Енді Стенфорд-Кларк з IBM і Арлен Ніппер з Arcom (тепер Eurotech) створили протокол між машинами, який був першим протоколом для підключення пристроїв під назвою MQ Telemetry Transport (MQTT) [7]. У 2000 році компанія LG анонсувала перший підключений холодильник. Ідея підключеного холодильника була побудована за

допомогою сканування штрих-коду та RFID [8]. У 2008 році IPSO Alliance пропагував з’єднання Інтернет-протоколу за допомогою смарт-об’єктів. IPSO Smart Objects був проектом, який забезпечував зв’язок між розумними об’єктами та програмними додатками інших пристроїв і сервісів [9]. У 2010 році компанія Google представила проект під назвою самокерований автомобіль. Цей проект перетворив традиційне керування на інтелектуальне керування шляхом розробки підключеного та автономного автомобіля. Цей автомобіль містив датчик і камеру, які підвішені на Toyota Prius. Проект вважався новим винаходом у промисловості та комунікаційній техніці [10]. У 2010 році багато видів досліджень почали вирішувати проблеми IoT, пов’язані з Bluetooth і високим енергоспоживанням. Ці дослідження представили нову техніку впровадження розумного Bluetooth під назвою Bluetooth Low Energy (BLE). BLE надає багато застосувань у індустрії фітнесу, охорони здоров’я, безпеки та домашніх розваг [11]. У 2013 році IoT використовує багато технологій, таких як бездротовий зв’язок,

З попередніх розділів зрозуміло, що природа IoT – це гетерогенна мережа, яка містить мільярд різних розумних об’єктів або речей (пристроїв). Розумні об’єкти або речі можуть бути фізичними та віртуальними. Фізичні речі – це датчики та електричні об’єкти, а віртуальні – це інформація чи дані, які збираються, обробляються, зберігаються та доступні для використання. Існує три підключення для передачі даних, які поділяються на з’єднання «машина-машина» (M2M), «машина-людина» (M2H) і «людина-людина» (H2H) [12].

Слід зауважити, що є відмінності між IoT та Інтернетом. Щоб краще зрозуміти характеристики Інтернету речей, слід прояснити деякі основні характеристики Інтернету речей, такі як неоднорідність, динамічні зміни, величезні масштаби та взаємозв’язок. Що стосується неоднорідності, то в IoT існує велика кількість різних пристроїв з різними апаратними та програмними платформами. Ці пристрої можуть взаємодіяти один з одним через різні мережі [12]. Тому операції між різними пристроями дуже складні.

З цієї причини системи безпеки IoT є слабкими механізмами протидії багатьом загрозам і атакам. Що стосується динамічних змін, Інтернет речей повинен забезпечувати динамічне середовище для виявлення будь-яких змін у стані пристроїв, не потребуючи мати справу з людиною або пристроями. Зміни пристроїв можна побачити в багатьох формах, наприклад, у режимі сну, прокиданні, підключеному або відключеному стані. Крім того, розташування та швидкість пристроїв змінюються автоматично [12]. В результаті цього виникають проблеми з аутентифікацією, авторизацією та контролем доступу. У цей момент зловмисники можуть легко використовувати ці проблеми для отримання доступу, моніторингу та знищення даних і пристроїв.

У разі величезних масштабів кожен пристрій IoT генерує дані, тому пристрої IoT виробляють величезну кількість даних. Цю величезну кількість даних необхідно проаналізувати та обробити. Таким чином, багато послуг вимагають управління аналізом великих даних. Крім того, всіма пристроями слід керувати та спілкуватися між собою. З точки зору взаємозв’язку, будь-який пристрій може підключатися та спілкуватися з Інтернетом. Функції з’єднання забезпечують доступ до мережі та сумісність.

Новий пристрій або людина може інтегруватися з пристроями IoT за допомогою механізму аутентифікації. Система IoT може забезпечити автоматичний процес ідентифікації нового пристрою або людини. Усі функції IoT забезпечують інтеграцію, контроль, індексацію, відстеження, підключення та автономні операції.

IoT перетворює традиційне керування в інтелектуальне. Тому IoT здатен покращити інтелектуальний взаємозв’язок між фізичними та віртуальними об’єктами для створення нової системи віддаленого керування. Інтелектуальне керування означає, що всі розумні об’єкти автоматично контролюють велику кількість даних, що сприяє економії часу.

IoT надає точні дані за допомогою автономного та онлайнового аналізу. Цей процес сприяє прийняттю рішень і покладає край усім проблемам збору

даних. Інтернет речей може забезпечити ефективність і низькі експлуатаційні витрати, використовуючи багато засобів, таких як покращення використання, ефективність процесів і продуктивність, наприклад розумні лічильники.

Проте система IoT має ряд серйозних недоліків. Складність є найважливішою проблемою, оскільки операції IoT дуже складні, і немає гнучкої інтеграції між пристроями. Існують різні пристрої з різним дизайном, розгортанням та обслуговуванням, тому будь-яка слабкість програмного або апаратного забезпечення буде мати серйозні проблеми [13]. Мережа IoT страждає від проблем автентифікації та контролю доступу, оскільки смарт-об’єкти – це гетерогенні пристрої, які базуються на різних платформах (апаратних засобах та мережах). Більше того, всі пристрої повинні взаємодіяти з іншими пристроями через різні мережі. Таким чином, проблеми безпеки є найбільшими, оскільки всі пристрої та дані піддаються різним загрозам і атакам. Існують різні загрози та атаки, які можуть спричинити серйозні проблеми в мережі. Крім того, всі персональні дані всіх користувачів піддаються найнебезпечнішим атакам. Крім того, IoT не має правил, які б пояснювали, як захистити пристрої та дані.

1.2 Основні проблеми безпеки IoT

IoT представляє багато послуг і додатків, але вимагає важливого загального протоколу, методів, архітектури, стандартів і механізмів безпеки для досягнення інтеграції між віртуальним світом і реальним світом на одній платформі. Як правило, існують три групи проблем IoT, які можна розділити на: архітектуру; стандартизацію; безпеку та конфіденційність.

Що стосується архітектурної проблеми, то, як згадувалося вище, кількість різноманітних смарт-об’єктів з кожним днем збільшується. Кожен розумний пристрій генерує дані для надання багатьох послуг у будь-який час і в будь-якому місці. Ці послуги вимагають певної інфраструктури для підтримки, інтеграції та аналізу згенерованих даних для того, щоб

передбачити майбутнє рішення. Тому Інтернету речей потрібна динамічна архітектура, щоб представити цілісний план, який використовується для підтримки різних об’єктів і додатків [14].

Що стосується проблеми стандартизації, то це означає відсутність належної можливості для об’єктів однаково використовувати та отримувати доступ до мережевих ресурсів. Нажаль, традиційних мережевих стандартів недостатньо для підтримки нових смарт-об’єктів і програм. Отже, мережа IoT повинна мати певний стандарт для підтримки нових об’єктів і додатків [14].

Як згадувалося вище, IoT містить багато датчиків, які мають обмежену потужність. Таким чином, використання традиційних методів безпеки не підтримуватиме підключення IoT між машинами. З цієї причини Інтернету речей потрібні механізми безпеки для досягнення низької обчислювальної потужності та зручних систем безпеки. Зловмисники можуть використовувати різні методи на різних рівнях, щоб зруйнувати мережу IoT. Таким чином, безпека даних є пріоритетом у проектуванні мережі IoT. З цього моменту проблеми безпеки та конфіденційності IoT відіграють істотну роль у системі IoT.

Проблеми безпеки та конфіденційності Інтернету речей розглянуті у наступних пунктах.

1.2.1 Конфіденційність користувачів і захист даних

Система IoT заснована на передачі та обміні інформацією/даними за допомогою середовищ між різними розумними об’єктами. Обмінювані дані можуть включати особисту інформацію про користувачів, яка відображає особистість і поведінку користувачів. Як згадувалося вище, система IoT забезпечує автоматичну ідентифікацію будь-якого пристрою та людини. Вся інформація про користувачів може бути зібрана з пов’язаних з ними об’єктів, які зберігаються в системі або передаються через носії між різноманітними розумними об’єктами [15]. Вся приватна інформація користувачів без будь-

яких механізмів аутентифікації піддається найнебезпечнішим атакам і загрозам. Таким чином, конфіденційність і захист даних відіграють життєво важливу роль у мережі IoT.

Конфіденційність базується на трьох основних складових. По-перше, секретність – захист усіх повідомлень, які можуть бути зрозумілі лише призначеним одержувачам. По-друге, анонімність – можливість надсилати й отримувати повідомлення без розкриття особи відправника та одержувача. По-третє, автономність – це уникнення зіткнення з нападниками.

1.2.2 Управління довірою та інтеграція політик

Через обмеженість протоколів, ресурсів і потужності різних розумних об’єктів існує надзвичайно велика проблема управління довірою IoT. Управління довірою є важливою частиною безпеки Інтернету речей, інформаційної безпеки, послуг, програм і конфіденційності користувачів. Управління довірою є важливим елементом взаємодії між розумними об’єктами для обміну даними та керування ними. Рівні Інтернету речей мають різні та неоднорідні пристрої. Наприклад, кожен пристрій генерує величезну кількість даних, які піддаються різним атакам, загрозам і помилкам. Ці помилки та атаки можуть поширюватися на всіх рівнях Інтернету речей. Як наслідок, точність даних і якість послуг буде знижена, і користувачі не приймуть це. Довірче управління в IoT має досягати таких цілей [16]:

- забезпечувати довірчі відносини об’єктів IoT і приймати рішення відносно довіри щодо спілкування та співпраці один з одним;
- зберігати конфіденційність користувачів, передачу даних і довірче спілкування відповідно до політики інтеграції IoT;
- підвищити якість послуг IoT, безпеку та надійність системи.

1.2.3 Наскрізна безпека

IoT містить мільярди розумних об’єктів, і кожен розумний об’єкт надсилає величезну кількість даних іншим об’єктам. Розумний об’єкт має бути автентифікованим і мати механізми безпеки для захисту користувачів, пристроїв і служб. У той же час механізми безпеки використовуються для запобігання загрозам і атакам на доступ до даних або послуг. Ця операція називається наскрізною безпекою. Домен наскрізної безпеки включає пристрої IoT, шлюз IoT, доступ і мережеве підключення, додаток IoT, платформу та користувачів. Основними вимогами наскрізної безпеки є аутентифікація, контроль доступу та процеси шифрування. Сценарій наскрізної безпеки полягає в наступному. Коли будь-який розумний об’єкт хоче підключитися до іншого, обидва вони мають бути аутентифікованими об’єктами. Після автентифікації розумного об’єкта він може надсилати та отримувати дані чи команди. Тоді смарт-об’єкт може безпосередньо під’єднатися до хмари. Відповідальний за хмару забезпечує процес аутентифікації та контролює повідомлення між смарт-об’єктами. Після впровадження процесів аутентифікації та контролю смарт-об’єкт підключається до Інтернету через шлюз. Потім процес шифрування використовується для шифрування повідомлень, якими обмінюються розумні об’єкти [17].

1.2.4 Аутентифікація та управління ідентифікацією

Механізм аутентифікації відіграє важливу роль в безпеці IoT і може бути реалізований багатьма методами, такими як ідентифікатор, пароль та інфраструктура відкритих ключів (PKI). Але традиційні механізми аутентифікації непридатні для IoT через неоднорідність і складність об’єктів [18]. Що стосується управління ідентифікацією, то воно використовується для управління ідентифікаторами, послугами та функціями смарт-об’єктів.

Він надає послуги ідентифікації, аутентифікації та контролю доступу. Керування ідентифікацією використовується для визначення з’єднань смарт-об’єктів. Цей механізм включає підключення, мережеві домени та програми на платформі IoT. Тому управління ідентифікацією залежить від міцності механізмів аутентифікації.

1.2.5 Авторизація та контроль доступу

Механізми авторизації та контролю доступу надають користувачам доступ до мережевих ресурсів і послуг. Аутентифікація та контроль доступу запобігають доступу неавторизованих користувачів до ресурсів мережі. Як згадувалося вище, пристрої Інтернету речей мають обмежену ємність і потужність, тому впровадження методологій авторизації та контролю доступу не є легкою місією. На додаток до гетерогенності та складності пристроїв, методології авторизації та контролю доступу можуть бути непридатними для системи IoT [18].

1.2.6 Рішення безпеки та стійкість до загроз

Система управління безпекою використовується для визначення методологій безпеки рівнів IoT. Використовується для запобігання багатьох атак і загроз. Стратегія системи безпеки залежить від захисту пристроїв, середовищ передачі, обміну даними, послуг і бізнес-моделей. Рішення безпеки формують зручне середовище для того, щоб система IoT відповідала характеру різних пристроїв і додатків. Існує багато механізмів безпеки, таких як безпека протоколу Інтернету (IPsec), асиметрична та симетрична криптографія, аутентифікація тощо [19].

У більш широкому плані також необхідно визначити принципи безпеки IoT, які коротко описані нижче. Основна проблема IoT полягає в тому, що немає правил, законів та умов надання послуг, які б забезпечували різні рівні

захисту даних. Таким чином, основним принципом є встановлення правил та законів, і компанії та організації мають можливість безпечно використовувати мережу IoT.

Наступним принципом є надання надійного веб-інтерфейсу та мобільних додатків для полегшення зв’язку між людьми та розумними об’єктами через ці програми. Крім того, математичні алгоритми є важливими питаннями для впровадження методологій безпеки IoT, таких як процеси аутентифікації та шифрування. Ці механізми мають відповідати різним пристроям і додаткам.

1.3 Вимоги безпеки

Вимоги безпеки стають важливою частиною впровадження ефективного IoT. Розробка рішень безпеки та системи управління спирається на принципи безпеки. Існують основні вимоги для створення системи безпеки IoT, які пояснюються далі [20].

Доступність. Метою доступності є надання можливості користувачам отримати доступ до послуг у будь-який час і в будь-якому місці. Важливо постійно зберігати зв’язок між користувачами та мережевими ресурсами. Таким чином, усі користувачі повинні пройти аутентифікацію для протидії атакам та загрозам мережевим ресурсам. Доступність може запобігти таким вузьким місцям, як конфлікти в системі та перевантаження мережі, які впливають на потік даних.

Підзвітність – не може запобігти атакам і загрозам в Інтернеті речей, але є важливою для збереження та підтримки інших вимог безпеки, таких як цілісність і конфіденційність. Вона використовується для відстеження будь-якого пристрою, який надсилає та отримує дані для спостереження та виявлення будь-яких невідомих операцій, забезпечуючи правила пристроїв, користувачів та їх дії чи поведінку.

Аудит – життєво важливий принцип вимог безпеки для виявлення

слабкості безпеки IoT. Він заснований на системі оцінки та послугах і використовується для вимірювання того, наскільки система IoT відповідає певному стандарту додатків.

Аутентифікація та авторизація. Аутентифікація є найважливішою вимогою безпеки, яка ідентифікує користувача як аутентифікований об’єкт з використанням таких механізмів безпеки, як відкритий і закритий ключ (криптографічні алгоритми). З точки зору авторизації, він використовується для надання користувачам дозволу на використання мережевих служб або ресурсів.

Контроль доступу – реалізується адміністратором мережі, щоб надати користувачам конкретні завдання або автентифікований доступ для використання мережевих ресурсів, таких як читання, запис, редагування або модифікація даних. Таким чином контроль доступу надає автентифікованим користувачам реалізацію конкретних завдань.

Приватність. Приватність використовується для забезпечення приватної інформації користувачів. Це може запобігти незаконним користувачам. Існує багато рівнів і форм приватності, наприклад:

- приватність у пристроях, це залежить від фізичної та комутаційної приватності (пристрої можуть бути піддані крадіжці інформації);
- приватність під час спілкування залежить від комунікацій пристроїв IoT (використовується для запобігання розголошенню даних під час спілкування);
- приватність на етапах обробки та зберігання (використовується для захисту оброблених даних).
- приватність ідентифікації та місцезнаходження (використовується для надання дозволу авторизованим користувачам на доступ до інформації про географічне положення пристроїв IoT).

Конфіденційність – є важливою концепцією вимог безпеки для запобігання доступу неавторизованих користувачів до даних. Конфіденційність забезпечує ідентифікацію, аутентифікацію та авторизацію

для будь-якого розумного об’єкта в мережі IoT. Існує багато механізмів безпеки, які гарантують конфіденційність даних, наприклад механізми аутентифікації.

Цілісність – є однією з концепцій безпеки, яка дозволяє авторизованим користувачам отримувати доступ, читати, видаляти або змінювати дані, але в обмежених умовах. Таким чином, цілісність може запобігти внутрішнім атакам, які є найнебезпечнішою проблемою в мережі, оскільки вони є авторизованими користувачами з автентифікацією. Крім того, кіберзлочинці можуть змінювати дані під час передачі, тому цілісність може запобігти зовнішнім атакам для доступу або зміни даних.

Безвідмовність. Значення безвідмовності можна легко пояснити. Вона використовується, щоб довести, що відправник і одержувач не можуть заперечувати, що їхні повідомлення належать їм. Таким чином, безвідмовність може запобігти внутрішнім атакам.

2 АНАЛІЗ АСПЕКТІВ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В IOT

2.1 Загальні відомості

У спеціальній літературі представлено безліч варіантів класифікації загроз середовища Інтернету речей. Зазвичай, такі роботи засновані на архітектурі безпеки середовища IoT загалом із підкресленням загроз, притаманних тим чи іншим ланкам. Тому автори пропонують власні моделі, що враховують усі аспекти безпеки для цієї технології. Так, наприклад, елементи безпеки розподіляють на чотири великі групи [21], а саме: ідентифікація, агрегація даних, прийняття рішень, об’єднання елементів у єдину систему.

До ідентифікації відноситься, як правило, застосування RFID-датчиків та зчитувачів з метою однозначно ідентифікувати пристрій у мережі, а також визначити його розташування [22]. Варто зазначити, що Інтернет речей працює в режимі обмеженого використання електроенергії, і застосування RFID-технології задовольняє всім вимогам цієї парадигми.

Під агрегацією даних розуміється здатність збирати величезні обсяги інформації від сенсорів та виконавчих пристроїв, у тому числі RFID-датчиків, і передавати їх у необхідному форматі, наприклад, у форматі JSON або XML, на веб-сервер або інший пристрій, що володіє необхідними обчислювальними потужностями.

До фази прийняття рішень відноситься виділення з усього обсягу даних, зібраних від датчиків, тільки тих, що мають найбільш інформативний характер. На основі відібраних відомостей у разі міжмашинної взаємодії приймається те чи інше рішення та виконується дія. У разі взаємодії «людина–машина» користувачеві пропонується вибрати одну із запропонованих дій. Даний етап повинен бути обчислювально швидким і забезпечувати негайний вплив на виконавчі пристрої та сенсори.

Об’єднання елементів у єдину систему визначає наступний рівень етапу прийняття рішень, де належна увага приділяється інтероперабельності, взаємодії пристроїв різних виробників, протоколів передачі, обробки та зберігання даних, тощо.

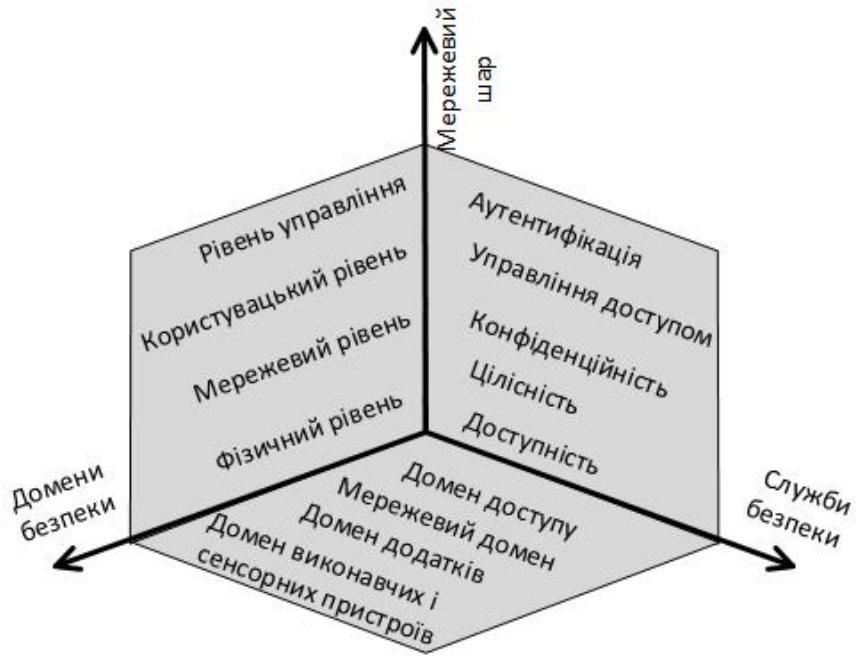

Рисунок 2.1 – Складові безпеки середовища IoT [23]

У роботі [23] було запропоновано розгорнуту систему класифікації процесів середовища Інтернету речей. Так, архітектура безпеки середовища розглядається як три виміри: служби безпеки, мережевий рівень та домен безпеки. Причому перший вимір включає: аутентифікацію, управління доступом, конфіденційність, цілісність, доступність та ін. Третій вимір включає чотири підрозділи, які характеризують принцип роботи середовища. Перший підрозділ – це домен виконавчих та сенсорних пристроїв. Він відповідає за вимоги до надійності, специфіки експлуатації, тощо. Другий підрозділ – домен доступу, до завдання якого входить визначення правомірності доступу до системи як користувача, так і пристроїв між собою. Третій – мережевий домен, який визначає умови доступу до вузлів мережі,

маршрутизацію інформаційного трафіку тощо. Останній домен програм відповідає за безпеку інформації, що циркулює всередині програмного забезпечення. Тут більша увага приділяється помилкам у проектуванні та програмуванні, а також особливостям роботи з критично важливою або персональною інформацією, наприклад, з інформацією про стан здоров'я пацієнта. Класифікація, що обговорюється, представлена на рисунку 2.1.

У роботі [24] запропоновано розбиття на вісім складових:

- комунікаційне обладнання, яке відповідає за передачу інформації між пристроями;
- датчики, що збирають та представляють фізичні величини у цифровій формі;
- виконавчі пристрої, що виконують дії з керуючого сигналу;
- зберігання, ідентифікація та локалізація даних;
- інтерфейси для взаємодії «людина–машина»;
- обчислювальні пристрої;
- визначення розташування пристроїв як фізичних об'єктів;
- ідентифікація фізичних приладів як унікальних об'єктів.

За цією методикою кожному з перерахованих компонентів ставиться у відповідність експертна оцінка за такими параметрами: цілісність, справжність, конфіденційність, секретність, доступність та регульованість. За цією методикою оцінюється стан захищеності, виходячи з вжитих заходів для конкретних компонентів середовища Інтернету речей [24].

Альтернативна модель безпеки у роботі [25] містить рівень виконавчих пристроїв, транспортний рівень та прикладний рівень. У роботі проаналізовано особливості та питання безпеки кожного рівня та запроваджено відповідні типові рішення характерних для них проблем. У ній дано порівняння характеристик різних дозволів шляхом аналізу особливостей технологій, обговорено питання безпеки середовища Інтернету речей як неподільної сутності та представлено деякі потенційні напрямки розвитку загальної архітектури безпеки для всієї системи IoT, а також прості та

ефективні рішення для забезпечення безпеки даних великого обсягу. Структура моделі представлена у таблиці 2.1.

Таблиця 2.1 – Складові безпеки середовища Інтернету речей за [25]

Рівень виконавчих пристроїв	Безпека пристроїв	RFID-пристрої, бездротові сенсорні пристрої, GPS-пристрої
	Безпека мережі пристроїв	
Транспортний рівень	Доступ до мережі	WiFi-мережі, Ad hoc- мережі
	Мережа Інтернет	Мобільний Інтернет, Інтернет
	Локальна мережа	Безпека локальної мережі
Прикладний рівень	Додатки Інтернету речей	Інформаційна логістика, інтелектуальна мережева безпека, моніторинг середовища
	Підтримка додатків	Безпека середовища розробки, платформи хмарних обчислень, проміжні технології безпеки

Таким чином, можна зробити висновок про те, що на даний момент не існує єдино вірного підходу до формалізації безпеки середовища Інтернет речей. Той чи інший спосіб або відбиває загальні аспекти, або заглиблюється в окремі випадки. Слід зазначити, що зі швидким темпом розвитку технології видозмінюються також характерні загрози, що призводить до неактуальності моделей.

2.2 Тип загроз, атак, розголошень, уразливостей

Визначення загроз, вразливостей, впливів та атак спрямоване на забезпечення захисту системи IoT, що є найважливішою темою на даний

момент. Це є істотною частиною безпеки IoT. Якщо визначення нападу зрозуміле, його можна запобігти. Наприклад, деякі загрози можуть пошкодити фізичні пристрої, середовища передачі, мережу мобільного зв’язку, протоколи, сервери додатків, програмне забезпечення, сховища даних або різні послуги.

2.2.1 Загрози

Загрози використовують слабке місце безпеки системи IoT і пошкоджують або крадуть інформацію. Загрози можуть завдати шкоди апаратному та програмному забезпеченню. Існує два види загроз, які поділяються на внутрішні та зовнішні.

Внутрішні загрози можуть бути створені з внутрішньої мережі. Внутрішня атака – це аутентифіковані авторизовані користувачі, і це є найнебезпечніші загрози. Цілей внутрішніх загроз багато. По-перше, загрози можуть вкрасти дані та всю інформацію про біометричну систему ідентифікації. По-друге, внутрішні загрози можуть використовувати слабкість контролю доступу та пошкодити автентифікацію, авторизацію та підзвітність для контролю доступу користувачів. Такого роду загрози можна запобігти за допомогою пароля або біометричних даних. По-третє, причиною коливань потужності є стрибок напруги, який викликає вихід з ладу електронного обладнання.

Зовнішні загрози можуть генеруватися від неавтентифікованого користувача, який використовує коди та сценарії для проникнення, контролю або пошкодження розумних об’єктів та крадіжки даних [26]. Зовнішні загрози включають віруси, хробаки, трояни та шпигунські програми. Такого роду загроз можна запобігти за допомогою антивірусного та антишпигунського програмного забезпечення.

2.2.2 Уразливі місця

Уразливості виникають у мережі через слабкість системи, яка дозволяє зловмисникам отримувати доступ до даних, редагувати деякі команди або пошкоджувати мережу за допомогою атаки Denial of Services (англ., DoS). Його можна знайти в пристроях, операційній системі та програмах, протоколах зв’язку та мережевих політиках [27]. Існує багато типів уразливостей, таких як руткіт на основі віртуальної машини, перехоплення сеансів, вразливості протоколу Інтернету, збій візантійського режиму та вичерпання ресурсів.

Що стосується руткіту на основі віртуальної машини, то це тип шкідливого програмного забезпечення, яке працює у віртуальному середовищі (віртуальна операційна система або програма). Його можна виявити за допомогою потужної системи безпеки для обладнання та віртуальної машини. Щодо захоплення сесії, це стосується того, що зловмисник краде сеанс між двома користувачами, щоб отримати доступ до даних для здійснення шкідливих дій. Атака типу «людина посередині» (MIM) – відома атака серед кіберзлочинців. Вона використовує слабкість Інтернет-протоколів. Ця атака ставить себе між користувачами та мережею, щоб підслуховувати та захоплювати дані, щоб змінити, прочитати або пошкодити дані. Візантійська помилка – це помилка, яка виникає в хмарному сховищі через помилки програмного забезпечення або апаратну несправність. Цьому можна запобігти за допомогою криптографічних алгоритмів. Вичерпання ресурсів відбувається через споживання або витоку ресурсів і слабку конструкцію. Нарешті, виснаження ресурсів викликає DoS-атаки [28].

2.2.3 Розголошення

Розголошення – це проблема або помилка, яка виникає в конфігурації системи. Це дозволяє зловмисникам отримати доступ до даних. У цьому

випадку зловмисники можуть захопити смарт-об’єкти або отримати криптографічні ключі. При цьому дані або пристрій можуть бути замінені шкідливими [29].

2.2.4 Атаки

Мотивацією атак є крадіжка або перехоплення даних і послуг. Таким чином, цілями атак є прослуховування, контроль доступу та керування даними та пристроями. Вплив атак можна розділити на пасивну та активну атаку. Завдання пасивної атаки – лише підслуховування або збір інформації про мережу. Це може бути реалізовано за допомогою сканування портів і аналізу трафіку. Це не може зашкодити доступності та цілісності, але зашкодить конфіденційності. Функцією активних атак є модифікація, знищення та блокування інформації чи ресурсів. Це шкодить конфіденційності, доступності та цілісності.

Є дві основні сутності атак: внутрішні та зовнішні. Джерелом внутрішніх атак є автентифіковані користувачі в мережі. Вони є найнебезпечнішим типом атаки, оскільки руйнують більшість вимог безпеки. Зовнішні зловмисники – це неавтентифіковані користувачі, які намагаються отримати доступ до мережі різними способами.

Поширені типи атак можна проілюструвати наступним чином.

Атаки на фізичній основі. Цей тип атаки також називається фальсифікацією пристрою. Сценарій цієї атаки можна пояснити в наступному розділі. Усі пристрої IoT інтегровані один з одним. Через деякий час певні пристрої залишаються без нагляду, тому при атаці їх можно легко викрасти і вставити в атакуючу мережу. Метою цієї атаки є крадіжка даних, маніпулювання додатками або підробка пристроїв [20].

Атаки на основі імітації. Сценарій цієї атаки ілюструється наступним чином. Коли користувач хоче поговорити з іншим, цей користувач надсилає повідомлення із запитом на вхід. Запитуване повідомлення містить ім’я та IP-

адресу цього користувача. Зловмисник може підслухати або перехопити запитане повідомлення по каналу зв’язку. У цей момент зловмисник може видати себе за аутентифікованого користувача, щоб змінити всю інформацію [29].

Атаки на основі даних. Це називається розкриттям і означає, що база даних стає доступною для неавтентифікованих користувачів через підслуховування даних, викрадення сеансів або незаконний доступ до пристрою [20].

Атаки на основі спуфінгу. Метою атаки на основі спуфінгу є обман мережі або користувачів шляхом порушення механізму аутентифікації. Зловмисник може обдурити користувача, зробивши себе автентифікованим користувачем, щоб вкрасти дані або зв’язок. Існують різні типи спуфінгу, які поділяються на спуфінг IP і підробку за протоколом розділення адрес (ARP). Що стосується підробки IP-адреси, зловмисник може захопити будь-яке повідомлення користувача (наприклад, електронну пошту). Це повідомлення містить IP-заголовок. Зловмисник може змінити IP-заголовок, щоб відображалося, що це повідомлення надходить від автентифікованого користувача. Що стосується підробки ARP, зловмисник може надіслати підроблений протокол призначення адрес, щоб зв’язати MAC зловмисника із законним користувачем. Після того, як IP-адреса зловмисника підключена до справжньої IP-адреси, зловмисник може надсилати та отримувати дані в мережу або з неї.

Атаки на основі доступу. Вони відбуваються, коли неавторизований користувач намагається отримати доступ до мережі. Зловмисник намагається підключитися до IP-адреси і видає себе за автентифікованого користувача [20].

Атаки на основі ідентифікації. Зловмисник намагається вкрасти особу пристрою або користувача, виконавши три кроки. По-перше, зловмисник використовує техніку підслуховування для прослуховування даних. По-друге, зловмисник використовує відстеження для відстеження

ідентифікаційного номера будь-якого користувача. По-третє, зловмисник краде або дублює пароль користувачів [20].

Атаки на основі приватності. Хакери можуть легко зібрати величезну кількість приватної інформації про користувачів. Існує багато методів атак на основі приватності. По-перше, зловмисники можуть використовувати шкідливе програмне забезпечення для отримання секретної інформації про користувачів. По-друге, зловмисники можуть стежити за місцезнаходженням користувачів. По-третє, зловмисники можуть захопити паролі користувачів шляхом злому [20].

Сигнальні атаки. Сенс атак із введенням сигналу полягає в тому, що зловмисник вводить підроблені дані в мережу, щоб отримати доступ, змінити та пошкодити передані дані [30].

Атаки на основі бічних каналів. Зловмисник може знайти ключ шифрування та отримати доступ до даних. Існує багато прикладів атак на основі побічних каналів, таких як аналіз часу, споживання енергії, аналіз трафіку та приватні дані [30].

Сніфінг або розвідувальні атаки. Цей тип атаки перехоплює будь-який мережевий пакет. Потім він аналізує всю інформацію за допомогою сканування портів, аналізу трафіку та аналізу пакетів.

Атаки відмови в обслуговуванні (DoS). Це найбільш небезпечні напади. Метою DoS є наповнення мережі незаконними запитами на перевантаження мережі та запобігання всім законним запитам на доступ до мережі. Це призводить до споживання пропускної здатності та втрати ресурсів мережі. Це робить мережеві послуги недоступними [27].

2.3 Багаторівнева архітектура IoT та властивості безпеки

2.3.1 Багаторівнева архітектура Інтернету речей

Система IoT складається з шести рівнів, як показано на рисунку 2.2, а саме: рівень кодування; рівень сприйняття; мережевий рівень; рівень проміжного програмного забезпечення; прикладний рівень; бізнес-рівень.

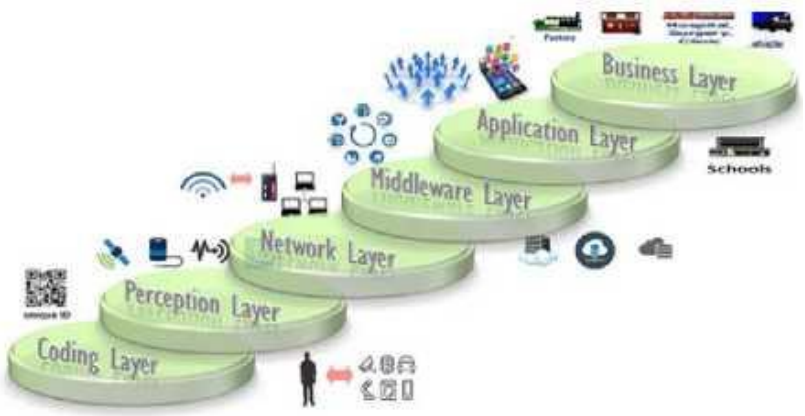

Рисунок 2.2 – Рівнева архітектура IoT

Рівень кодування. Рівень кодування є першим рівнем IoT і забезпечує процес ідентифікації для кожного розумного пристрою системи Інтернету речей. Кожному пристрою присвоюється унікальний ідентифікатор, який його відрізняє [3].

Рівень сприйняття. Основним обладнанням на рівні сприйняття є пристрій радіочастотної ідентифікації (RFID), бездротова сенсорна мережа (WSN), всі види датчиків, GPS, Bluetooth тощо. Основне призначення рівня сприйняття – зв’язувати різні пристрої в мережі IoT. Основними функціями рівня сприйняття є збір даних з різних фізичних пристроїв і перетворення даних у цифровий сигнал. Потім рівень сприйняття передає дані на мережевий рівень [3, 31].

Мережевий рівень. Основним обладнанням мережевого рівня є мережа

мобільного зв’язку, Інтернет та будь-який інший вид надійної мережі. Цей рівень отримує всю інформацію від рівня сприйняття та передає дані на рівень проміжного програмного забезпечення через такі середовища передачі, як Wi-Fi, Bluetooth, WiMAX, ZigBee, GSM, 3G та 4G, використовуючи протоколи зв’язку, такі як IPv4, IPv6, MQTT та DDS. Мережевий рівень відповідає за обробку, управління та обслуговування даних [31].

Рівень проміжного програмного забезпечення. Рівень проміжного програмного забезпечення отримує величезну кількість інформації від мережевого рівня та обробляє дані за допомогою деяких інтелектуальних систем обробки, таких як хмарні обчислення, щоб забезпечити прямий доступ до бази даних для зберігання всієї інформації в хмарі [23]. Функція рівня проміжного програмного забезпечення заснована на сервісно-орієнтованій архітектурі (англ., SOA), яка складається з кількох процесів, згрупованих у додатки, склад служби, керування послугами, абстракцію об’єктів, довіру, управління конфіденційністю та безпекою. Функція процесу заявок полягає в передачі всіх функцій системи кінцевим користувачам. Процес складання сервісу надає функції кожному смарт-об’єкту та керує ними. Процес абстракції об’єктів відповідає за гармонійний доступ між різними об’єктами спільною мовою. Захист даних, що ними обмінюються, забезпечується процесом управління довірою, приватністю та безпекою.

Прикладний рівень. Цей рівень використовує оброблені дані для виконання різних програм. Додатки IoT відображають вимоги користувачів (у сфері промисловості, освіти, медичному секторі, комунікацій), тому вони є корисними для розвитку IoT [32]. Прикладний рівень використовує різну кількість протоколів, таких як обмежений протокол програми (CoAP), протокол телеметрії транспортування черги повідомлень (MQTT), розширений протокол черги повідомлень (AMQP) і розширюваний протокол обміну повідомленнями та присутності (XMPP).

Бізнес-рівень. Це останній рівень багаторівневої архітектури Інтернету

речей. Він відповідає за управління додатками та послугами системи IoT. Бізнес-рівень використовується для створення різних моделей, кожна з яких має певні переваги [31].

2.3.2 Особливості безпеки Інтернету речей

Функції безпеки IoT відображають характеристики безпеки IoT, які допомагають розробити тактичний план для вирішення проблем безпеки IoT. Є три «традиційні» функції безпеки IoT, а решта – «сучасні» функції.

Проблеми рівня сприйняття. Як згадувалося вище, основна функція рівня сприйняття – збір даних і передача даних за допомогою сенсорних вузлів, які мають обмежену потужність. Традиційні механізми безпеки не є зручними для системи IoT, тому місія проектування системи захисту дуже складна.

Проблеми мережевого рівня. Мережевий рівень включає в себе дані передачі, середовища та протоколи, тому на цьому рівні існує різноманітність різних атак. Механізми безпеки IoT повинні бути сильними для захисту даних, носіїв і протоколів.

Проблеми прикладного рівня. Існують різні програми в IoT. Тоді мережа IoT піддається різним атакам. Це призводить до витоку даних і проблем контролю доступу.

Ідентифікація та визначення місця розташування об’єктів. Методологія ідентифікації вказує розташування пристроїв у системі IoT за допомогою системи доменних імен (DNS). DNS забезпечує відображення адрес для кожного пристрою, і кожен пристрій має назву та IP-адресу. Ця методологія є незахищеною системою імен, оскільки існує багато атак, таких як атаки «отруєння» кешу MIM та DNS [18].

Аутентифікація та авторизація. Внаслідок неоднорідності та складності природи IoT звичайні методи аутентифікації та авторизації можуть не підходити для системи безпеки IoT. Для вирішення цієї проблеми існує

багато досліджень.

Протиріччя між безпекою і вартістю. Існує звуження між безпекою та вартістю. Коли рівень безпеки IoT підвищується, збільшується продуктивність вузлів. Таким чином, буде збільшена вартість обслуговування мережі.

Легкі алгоритми безпеки (симетрична та асиметрична криптографія ключа). Як згадувалося раніше, усі сенсори мають обмежену обчислювальну потужність та енергію, тому алгоритми шифрування та механізми безпеки мають бути алгоритмічно-легкими для зменшення обчислювальної потужності, енергії та часу. Але для реалізації більшості алгоритмів шифрування потрібні потужність і час. На проблемі зменшення обчислювальної потужності і часу фокусуються багато досліджень.

Приватність IoT (політика збору даних та очищення даних). Вся інформація про поведінку користувачів і обмін даними піддається кільком атакам. Проблеми конфіденційності IoT класифікуються на політику збору даних та очищення даних. Політика збору даних залежить від типу методології збирання даних. Очищення даних використовує криптографічну методологію для захисту даних [18].

Асиметричність і складність. Через неоднорідність пристроїв важко керувати всіма пристроями мережі IoT одночасно. Це призводить до того, що система безпеки стає слабкою. Крім того, складність середовища IoT є результатом використання різних пристроїв і додатків, які потребують різних механізмів безпеки.

3 МОДЕЛЬ СИСТЕМИ БЕЗПЕКИ IOT

3.1 Рівні безпеки IoT

Базова архітектура безпеки IoT складається з трьох основних рівнів, які можна розділити на рівень сприйняття, мережевий рівень та прикладний рівень. Кожен рівень має власні компоненти, стандарти зв’язку та протоколи. З метою підвищення загальної захищеності системи IoT рівні безпеки забезпечують різні протоколи безпеки, послуги та механізми безпеки. Таким чином, кожен рівень намагається досягти своїх основних цілей: інформаційна безпека, фізична безпека та система управління безпекою. На рисунку 3.1 показано архітектуру рівнів безпеки IoT. У наступних розділах відображаються компоненти, функції, проблеми та заходи безпеки кожного рівня безпеки.

У таблиці Б.1 наведені компоненти та функції кожного рівня безпеки IoT із відображенням атак, проблем та вимоги безпек, які необхідні для кожного рівня. Крім того, таблиця Б.1 ілюструє перелік методів безпеки для вирішення проблем безпеки в системі IoT. Що стосується вимог безпеки, вони забезпечують високий рівень системи безпеки для мережі IoT і покращують її продуктивність.

3.1.1 Рівень сприйняття

Як згадувалося вище, дані збираються з різних пристроїв і передаються через бездротову мережу. Дані перетворюються в сигнали, які піддаються багатьом загрозам. Зловмисники можуть легко отримувати доступ, контролювати та знищувати дані та обладнання.

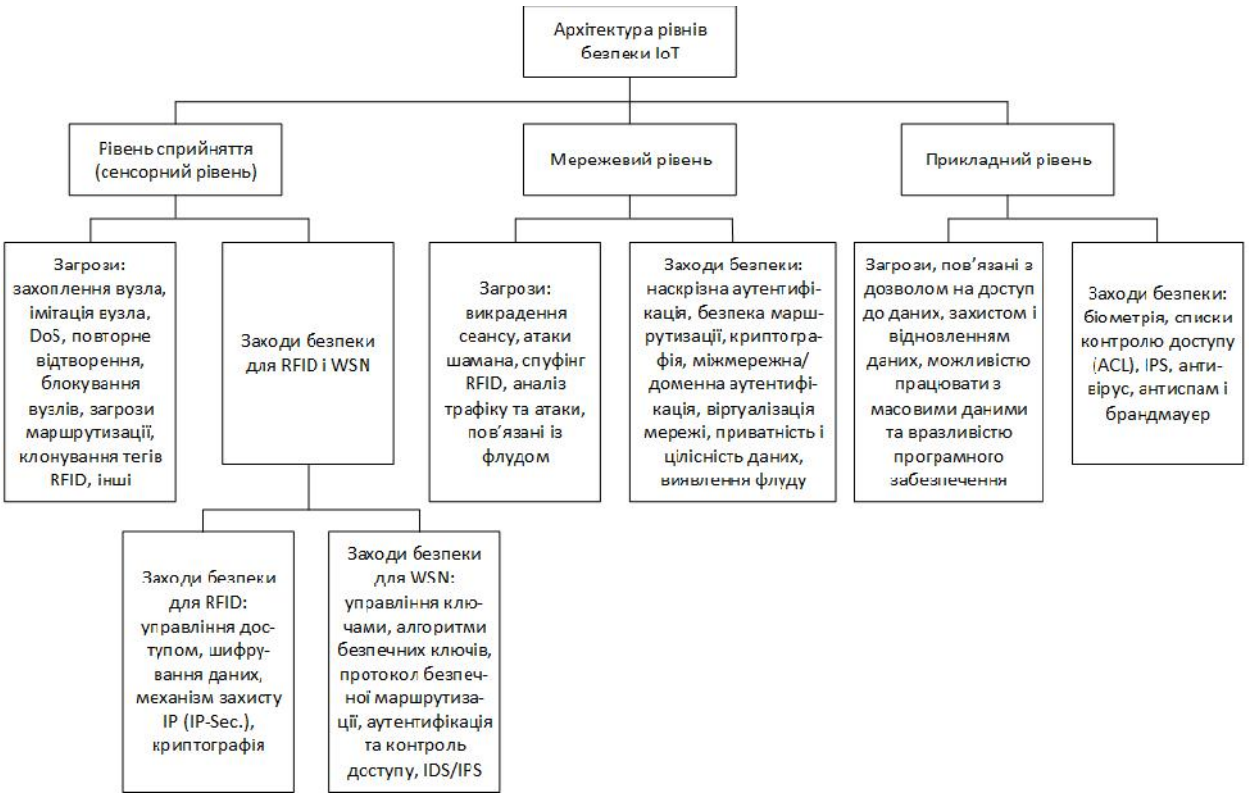

Рисунок 3.1 – Загрози та заходи безпеки на кожному рівні безпеки IoT

3.1.1.1 Категорії атак на рівень сприйняття

Як згадувалося вище, основними компонентами рівня сприйняття є RFID і WSN, тому слід зосередитися на поширених атаках у WSN, RFID та деяких ефективних атаках на рівні сприйняття, як показано на рисунку 3.2.

Атаки та загрози рівня сприйняття можна поділити на атаки WSN, атаки RFID та найпоширеніші атаки на рівні сприйняття.

3.1.1.2 Загрози WSN

Атака захоплення вузла. Цей тип атаки може знищити WSN або сенсорний вузол шляхом надсилання або отримання даних для доступу та зміни конфіденційної інформації. Атаки можуть контролювати ключові вузли або вузли шлюзу. Ця атака може призвести до витоку інформації та

загрожувати всій мережі.

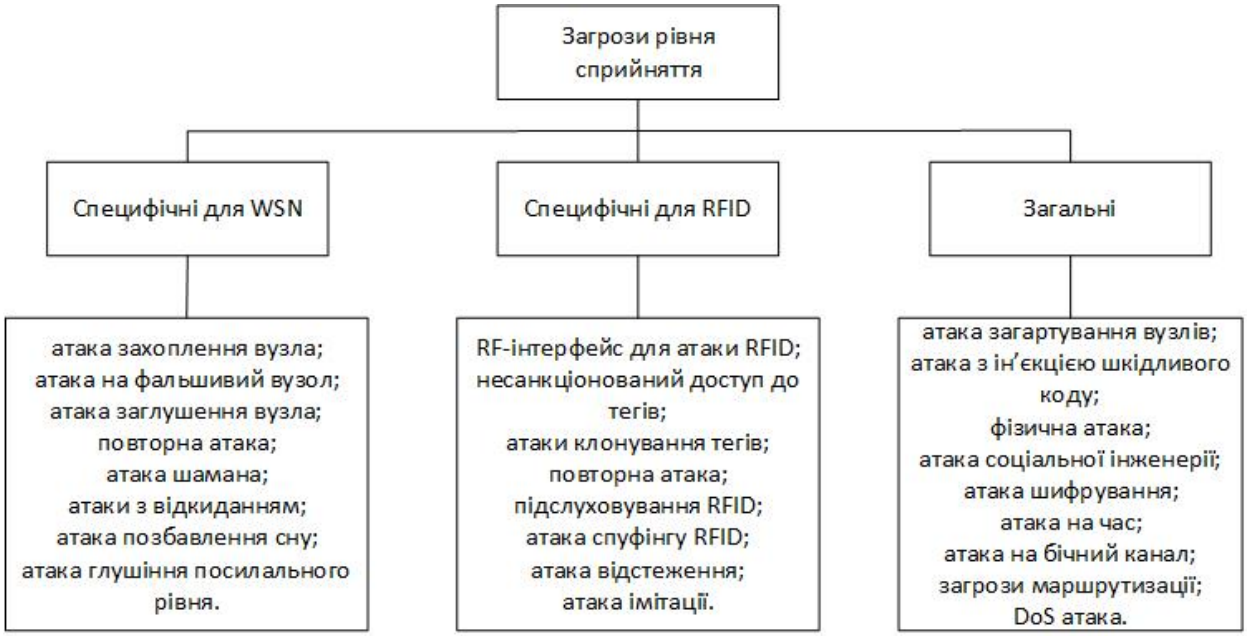

Рисунок 3.2 – Можливі загрози рівня сприйняття

Атака на фальшивий вузол. Зловмисник додає або впроваджує підроблений вузол в систему IoT, після чого поміщає підроблений код або дані в мережу IoT. Цей тип атаки може зупинити передачу даних, спожити потужність вузлів і зруйнувати мережу.

Атака заглушення вузла. Це відома атака в WSN. Зловмисники намагаються залучити доступ до радіочастот вузлів. Після цього блокуються сигнали, що призводить до припинення зв'язку вузлів і служб Інтернету речей.

Повторна атака. Метою цієї атаки є зламати процес аутентифікації, щоб стати автентифікованим користувачем. Сценарій цієї атаки полягає в тому, що зловмисник надсилає велику кількість повідомлень, які були отримані хостом призначення. Таким чином, зловмисник може змінити або відтворити вузол, підробивши інформацію користувачів.

Атака шамана. Зловмисник має намір контролювати вузли в WSN, щоб змусити їх прийняти неправдиву інформацію для боротьби з неправильним

вузлом в атакованій мережі. Цей тип атаки призводить до зменшення розподіленого сховища і впливає на багатошляхову маршрутизацію та підтримку топології.

Атаки з відкиданням. Це найнебезпечніша атака в WSN, яка використовує два способи; атаки вибіркової переадресації та синхронізації. Що стосується атаки вибіркової переадресації, зловмисник вибирає деякі пакети і пересилає їх до мережі зловмисників, а решту пакетів скидає для досягнення своєї/її шкідливої мети. Таким чином, деякі вузли не можуть пересилати пакети. Що стосується атак синхронізації, то «атаки синхронізації мають на меті розширити свої слоти протоколів MAC і поширити їх на інші вузли» [33].

Атака позбавлення сну. Під час цієї атаки зловмисник споживає заряд акумулятора сенсорного вузла, постійно роблячи його зайнятим. Ця атака впливає на продуктивність системи та сервісу IoT.

Атака глушіння посилального рівня. Метою цієї атаки є передбачити отримувані пакети за допомогою протоколу MAC у WSN. Ця атака зосереджена на передачі сигналу вузлів WSN.

3.1.1.3 Загрози RFID

RF-інтерфейс для атаки RFID. Ця атака залежить від атаки DoS, яка використовує шумовий сигнал і посилає його через радіочастотний сигнал. Це призводить до припинення спілкування.

Несанкціонований доступ до атаки тегів. Метою атаки несанкціонованого доступу до мітки є порушення процесу аутентифікації для отримання доступу до мітки RFID. Зловмисник може читати, змінювати або видаляти дані.

Атаки клонування тегів. Зловмисник може створити дублікат тегу, щоб користувач не міг відрізнити оригінальний тег від підробленого. Згодом користувач може надсилати або отримувати підроблену інформацію, а

зловмисник може захопити оригінальний тег, щоб бути автентифікованим користувачем.

Повторна атака. Метою цієї атаки є те, що зловмисник може отримати дані та записати дані на карту атаки за допомогою мікропроцесорів. У цьому випадку зловмисник отримує доступ до дозволу системи. Тоді зловмисник стає аутентифікованим користувачем і отримує доступ до даних або змінює дані.

Атака підслуховування RFID. Зловмисник може легко підслуховувати дані від тега до користувача або від користувача до тега, щоб порушити конфіденційність і отримати всю інформацію. Характеристики атаки підслуховування RFID такі ж, як і атаки підслуховування WSN, оскільки RFID має ті ж характеристики, що й WSN.

Атака спуфінгу RFID. Ідея цієї атаки полягає в тому, що зловмисник може поширювати неправильні дані про систему RFID і змусити RFID вважати, що це оригінальні дані. Відправник і одержувач мають справу з неправильними даними, що дозволяє зловмиснику отримати доступ до даних і контролювати мережу.

Атака відстеження. Це небезпечна атака, оскільки зловмисник може прочитати мітку RFID або особисту інформацію. Метою атаки відстеження є збір інформації про мережу IoT за допомогою інструментів сканування портів.

Атака імітації. Зловмисник може виявити пристрій у мережі та видати себе за користувача. Потім зловмисник генерує пакети, які містять конфіденційну інформацію або характеристики пристрою. Метою цієї атаки є зміна інформації RFID. Цей процес відомий як перехоплення або підробка законної особи. Атака видавання себе за іншу особу призводить до розкриття інформації.

3.1.1.4 Загальні атаки на рівні сприйняття

Атака загартування вузлів. Цей тип атаки може пошкодити сенсорний вузол, надсилаючи та одержуючи дані в систему IoT або з неї, щоб отримати доступ та контролювати всю важливу інформацію.

Атака з ін’єкцією шкідливого коду. Зловмисник може виконувати свої завдання за допомогою атаки MIM і поміщати себе між двома вузлами. Тоді він може ввести шкідливий код у вузол, щоб отримати доступ до системи та контролювати або пошкодити дані.

Фізична атака. Метою цієї атаки є пошкодження та знищення мережі IoT. Зловмисник може маніпулювати та експлуатувати мережеві пристрої Інтернету речей з метою пошкодження системи безпеки мережі та служб.

Атака соціальної інженерії. Зловмисник використовує користувачів мережі IoT для отримання приватної інформації за допомогою інструментів підслуховування та сніфінга.

Атака шифрування. Існують три типи атак шифрування, які можна класифікувати на атаки на час і атаки на бічний канал.

Атака на час. Її можна реалізувати шляхом аналізу часу алгоритму шифрування, який необхідний для реалізації механізму шифрування. Мета цієї атаки – отримати ключ шифрування.

Атака на бічний канал. Зловмисник намагається знайти ключ шифрування, який використовується для шифрування та дешифрування даних, щоб отримати доступ до даних. Серйозними наслідками цієї атаки є витрати часу та енергії та витік інформації.

Загрози маршрутизації. Це реалізується шляхом повторної відправки маршрутної інформації та створення циклів маршрутизації. Ця атака спричиняє такі пошкодження:

- контроль і блокування мережевої передачі;
- збільшення помилки повідомлень (таким чином, мережевий шлях розшириться);

- збільшення наскрізної затримки.

DoS атака. Широко відома у мережі IoT і викликає втрату мережевих ресурсів або послуг і споживає пропускну здатність.

3.1.1.5 Заходи безпеки рівня сприйняття

Вище обговорювалося багато різних типів загроз і атак у WSN, RFID та найпоширеніших атак на рівні сприйняття. Для підвищення рівня безпеки системи IoT необхідні заходи безпеки, оскільки розумні об’єкти IoT мають бути захищені з високою ефективністю. Заходи безпеки повинні забезпечувати низьке споживання енергії та часу. Заходи безпеки для рівня сприйняття поділяються на два пункти; заходи безпеки для WSN та заходи безпеки для RFID. Слід використовувати такі заходи безпеки, що задовольняють вимогам конфіденційності, цілісності, доступності, приватності та аутентичності. Також ці заходи безпеки впливатимуть на зменшення часу та споживання енергії. У таблицях Б.2 і Б.3 показано порівняння заходів безпеки для WSN та RFID, що дозволяє зробити логічний висновок щодо вибору найбільш придатного механізму безпеки для WSN та RFID з низьким споживанням енергії та часу. У таблицях Б.2 і Б.3 показано, що кожен механізм безпеки відповідає вимогам безпеки та запобігає найнебезпечнішим атакам. Крім того, наведено переваги та недоліки заходів безпеки.

Також існують інші методи безпеки для рівня сприйняття, які розглядатимуться далі.

Безпечне завантаження. Криптографічні хеш-алгоритми використовуються для перевірки пристроїв і програмного забезпечення Інтернету речей за допомогою цифрового підпису. Цей механізм безпеки не підходить для системи IoT, оскільки потребує енергії та часу.

Анонімність – найкраще рішення для мережі IoT для захисту приватної інформації користувачів. Недоліком анонімності є те, що вона потребує

більшої обчислювальної потужності.

Оцінка ризику – важливий метод захисту мережі IoT і запобігання багатьом загрозам і атакам, оскільки вона здатна виявити будь-яку помилку в системі безпеки, виявляти будь-які загрози та атаки на пристроях IoT за допомогою багатьох методів, таких як IPS. Оцінка ризику забезпечує багато механізмів безпеки, які є відповідними методами для природи середовища IoT.

Механізми безпеки повинні забезпечувати низьке споживання енергії та часу для досягнення високої продуктивності мережі IoT. Тому алгоритми безпеки необхідно модифікувати та покращувати, адаптуючи їх до смарт-об’єктів системи IoT.

3.1.2 Мережевий рівень

Як зазначалося вище, основним обладнанням мережевого рівня є мережа мобільного зв’язку та Інтернет. Мережевий рівень має справу з даними, засобами передачі та протоколами зв’язку, тому вважається родючою землею для багатьох загроз, нападів і проблем.

3.1.2.1 Атаки та проблеми мережевого рівня

На мережевому рівні зловмисник намагається отримати доступ до переданої інформації, засобів передачі та протоколів зв’язку. Метою зловмисника є знищення конфіденційності та цілісності. Рисунок 3.3 ілюструє класифікацію атак і проблем мережевого рівня.

На мережевому рівні можливо багато атак, які завдають шкоди переданим даним, середовищам передачі та протоколам. Далі показано різні типи атак [27, 33].

Атака аналізу трафіку. Сценарій цієї атаки полягає в тому, що зловмисник намагається отримати більше інформації про користувачів і

мережу за допомогою деяких інструментів, таких як сканування портів і атаки перехоплення.

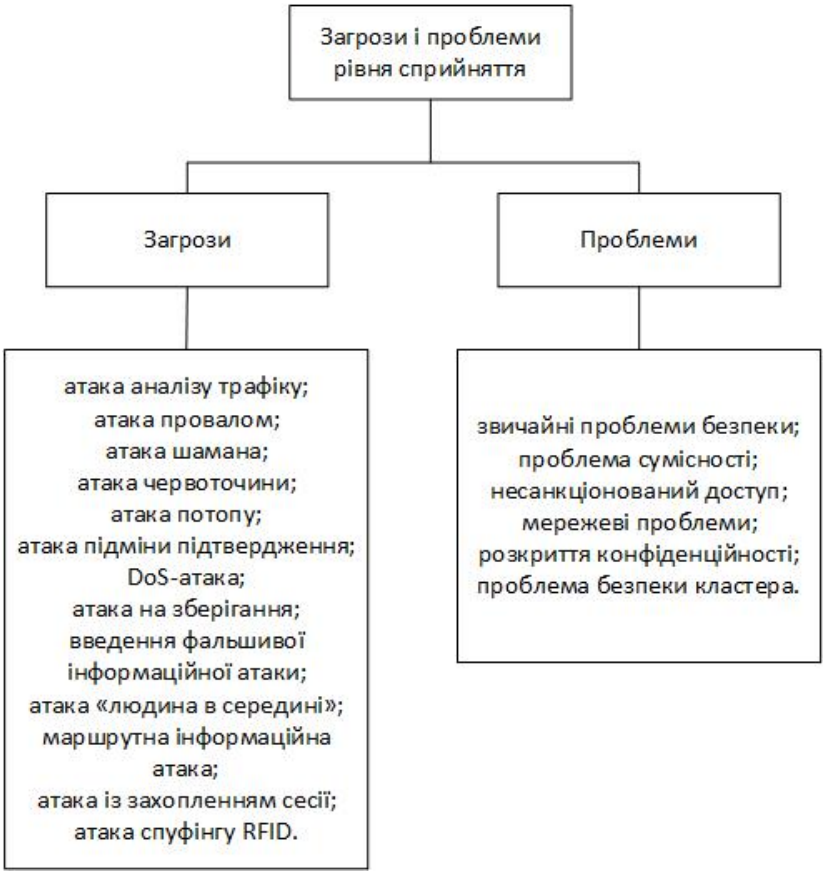

Рисунок 3.3 – Класифікація загроз і проблем мережевого рівня

Атака провалом. Зловмисник використовує будь-який слабкий вузол і контролює його. У той саме час зловмисник робить цей вузол більш надійним і привабливим для інших сусідніх вузлів. Він може скинути всі пакети та зупинити передачу даних. Таким чином, аварійна атака може заблокувати мережеві послуги та споживати електроенергію та час. Цей вид атаки призводить до DoS-атаки, яка є найнебезпечнішою атакою.

Атака шамана. Цей тип атаки дуже небезпечний, особливо у WSN. Зловмисник може загрожувати будь-якому вузлу в WSN і представляє його з великою кількістю ідентифікацій. У той саме час цей вузол може приймати неправдиву інформацію і негативно впливати на мережу IoT.

Атака червоточини. Ця атака не залежить від канального рівня і не потребує дешифрування зашифрованих пакетів. Ця атака може маніпулювати оригінальним бітом каналу, який має зв’язок з низькою затримкою. Зловмисник може перемістити початкове місце бітів у каналі зв’язку за допомогою помилкових бітів і отримати доступ до системи IoT.

Атака потопу. Є дуже ризикованою атакою в мережі IoT. Реалізується за допомогою підробних циклів маршрутизації. Зловмисник може відправити велику кількість повідомлень від шкідливого вузла до багатьох вузлів мережі IoT. Ця атака викликає затор і блокує канал зв’язку.

Атака підміни підтвердження. Використовується для вибіркової переадресація атаки для контролю будь-якого вузла в мережі IoT для досягнення цілі зловмисників. Таким чином втрачається багато пакетів.

DoS-атака. Зловмисник надсилає велику кількість повідомлень або пакетів до мережі, щоб зробити мережеві ресурси та послуги недоступними. Це також призводить до споживання пропускної здатності, перевантаження системи та запобігання більшості законних запитів від автентифікованих та авторизованих користувачів.

Атака на зберігання. Усі користувачі системи IoT повинні зберігати свою особисту інформацію на різноманітних пристроях або в хмарах. Тому багато атак використовують ці пристрої для отримання доступу та контролю даних.

Введення фальшивої інформаційної атаки. Під час цієї атаки зловмисник може маніпулювати одним вузлом у WSN і вводити шкідливу інформацію в мережу IoT. Таким чином, зловмисник може отримати доступ до мережі та отримати повний контроль над мережею IoT.

Атака «людина в середині». Як згадувалося вище, зловмисник опиняється між двома сенсорними вузлами і підслуховує всю інформацію, щоб отримати доступ до інформації про два сенсорні вузли. Метою цього зловмисника є використання каналу зв’язку або протоколу для порушення конфіденційності та приватності.

Маршрутна інформаційна атака. Метою інформаційної атаки маршрутизації є підробка та зміна інформації про маршрутизацію. Ця атака викликає багато проблем, таких як надсилання помилкових повідомлень і різних помилок, відключення мережевого трафіку та створення фальшивого циклу маршрутизації для пошкодження мережі IoT.

Атака із захопленням сесії. Зловмисник намагається вкрасти сеанс між двома вузлами, щоб отримати доступ і контролювати всю інформацію користувачів і мережі.

Атака спуфінгу RFID. Ця атака завдає шкоди сигналам RFID. Зловмисник захоплює передані дані за допомогою підробних сигналів RFID і робить їх аутентифікованими. Зловмисник використовує ці сигнали для передачі шкідливих даних, які вважаються довіреними.

Мережевий рівень страждає від багатьох проблем, які спричиняють затор, перевантаження мережі та розкриття конфіденційності [14].

Звичайні проблеми безпеки. Мережа IoT страждає від поширених проблем безпеки, таких як підслуховування, DoS, MIM, захоплення сеансів, вторгнення вірусів і незаконного доступу до мережі, які завдають шкоди конфіденційності та цілісності.

Проблема сумісності. Як згадувалося вище, IoT включає в себе гетерогенні пристрої, тому є багатошляхові та багатодоступні методи. Через цю гетерогенну природу система безпеки та координація мережі слабкі. Ця проблема призводить до того, що мережа IoT піддається безлічі різних атак і вразливостей.

Розкриття конфіденційності. Розкриття конфіденційності є найбільшою проблемою в системі IoT. Зловмисник може захопити або викрасти особисті дані користувачів (наприклад, IP-адресу, місцезнаходження тощо) за допомогою соціальної інженерії, атак підслуховування та перехоплення.

Проблема безпеки кластера. Проблема безпеки кластера є основною проблемою на мережевому рівні, оскільки мережа IoT має велику кількість пристроїв. Кожен пристрій генерує дані. Таким чином, всі пристрої

передають величезну кількість даних. Це призводить до використання великого обсягу трафіку даних, що спричиняє перевантаження мережі та блокує мережевий трафік.

3.1.2.2 Заходи безпеки мережевого рівня

Заходи безпеки мережевого рівня зосереджені на досягненні двох основних вимог безпеки, а саме: конфіденційність і цілісність даних. Заходи безпеки мережевого рівня вказують на відповідні механізми безпеки для досягнення вимог безпеки та запобігання атакам. У таблиці Б.4 наведено різні заходи безпеки мережевого рівня [3, 14].

3.1.3 Прикладний рівень

Як згадувалося вище, основним обладнанням прикладного рівня є інтелектуальне співтовариство. Цілями зловмисників є такі дані та послуги, як контроль над додатками, пошкодження сервісів, вимкнення/ввімкнення серверів (наприклад, додаток Smart Grid) та крадіжка інформації користувача.

3.1.3.1 Загальні проблеми та атаки прикладного рівня

Дозволи на доступ до даних. Існує велика кількість користувачів, які використовують різні програми. Таким чином, існує багато дір для вразливостей програмного забезпечення, таких як атаки шифрування, спам і шкідливі програми.

Захист і відновлення даних. Механізми захисту та обробки даних не є достатніми для запобігання втрати та пошкодження даних. Тому для мережі IoT потрібна система керування вузлами.

Здатність працювати з масовими даними та вразливими місцями

прикладного програмного забезпечення. Відбуваються переривання мережі і втрата даних через велику кількість вузлів, величезну кількість передачі даних і складне середовище.

Уразливості програмного забезпечення. Існує багато вразливостей програмного забезпечення, таких як фішинг, троян, вірус, хробак, руткіт, переповнення буфера, шкідливі скрипти.

3.1.3.2 Заходи безпеки прикладного рівня

Існують два основні заходи безпеки прикладного рівня: біометричні дані та списки контролю доступу (англ., ACL – Access Control List). Біометрія забезпечує захист інформації та запобігає внутрішнім і зовнішнім атакам. ACL можуть налаштовувати ролі, щоб дозволити автентифікованим і авторизованим користувачам запити на доступ до мережі. ACL можуть відстежувати та контролювати мережевий трафік. Інструментами безпеки є IPS, антивірус, антиспам і брандмауер. З наведених вище рішень для рівнів безпеки IoT слід визначити такі:

- безпека мережі IoT за допомогою брандмауера, IPS тощо;
- аутентифікація за допомогою цифрового підпису та біометричних даних;
- захист зв’язку за допомогою аутентифікації та шифрування PKI;
- безпека виконання коду за допомогою криптографічних алгоритмів та програмних засобів;
- захист зберігання даних за допомогою шифрування та авторизації;
- зміцнення заходів безпеки.

4 ОПИС МОДЕЛІ УПРАВЛІННЯ БЕЗПЕКОЮ

Метою запропонованої моделі є побудова системи управління безпекою для мережі IoT, що забезпечує зменшення часу та споживання енергії та надає відповідні механізми безпеки для рівнів безпеки IoT. Запропонована модель допомагає дослідникам та дизайнерам вибрати зручні протоколи та механізми безпеки на кожному рівні з метою захисту даних та розумних об’єктів. Запропонована модель використовується для запобігання або зменшення атак, загроз і проблем, наскільки це можливо. Цілі запропонованої моделі можна представити таким чином:

- детальний вибір відповідних механізмів безпеки для рівнів безпеки IoT з поясненням переваг та недоліків механізмів безпеки;
- забезпечення захищеності додатків;
- забезпечення вимог безпеки, таких як контроль доступу, контроль маршрутизації, аутентифікація, конфіденційність і цілісність для кожного рівня безпеки;
- забезпечення надійних функціональних можливостей для кожного розумного об’єкта в IoT, IDS/IPS та відновлення безпеки;
- виявлення та запобігання більшості загроз і атак;
- захищеність конфіденційної інформації користувачів;
- виявлення будь-яких помилок в передачі даних.

У запропонованій моделі використано платформу Things Board, яка надає безліч механізмів безпеки. Є можливість керувати стратегією вибору алгоритмів безпеки для досягнення високого рівня вимог безпеки та зменшення споживання енергії та часу.

Запропонована модель реалізується у трьох етапах. Перший етап – це рівні безпеки Інтернету речей, які включають рівні сприйняття, мережевий та додатків. На другому етапі використовуються протоколи безпеки та механізми рівня безпеки IoT. Третій етап пов’язаний з роботою серверів баз

даних, які використовуються для кожного рівня безпеки IoT для зберігання всієї інформації про механізми безпеки. Сервери баз даних призначені для збереження файлів журналів методів безпеки та користувачів і є корисними для адміністратора та користувачів.

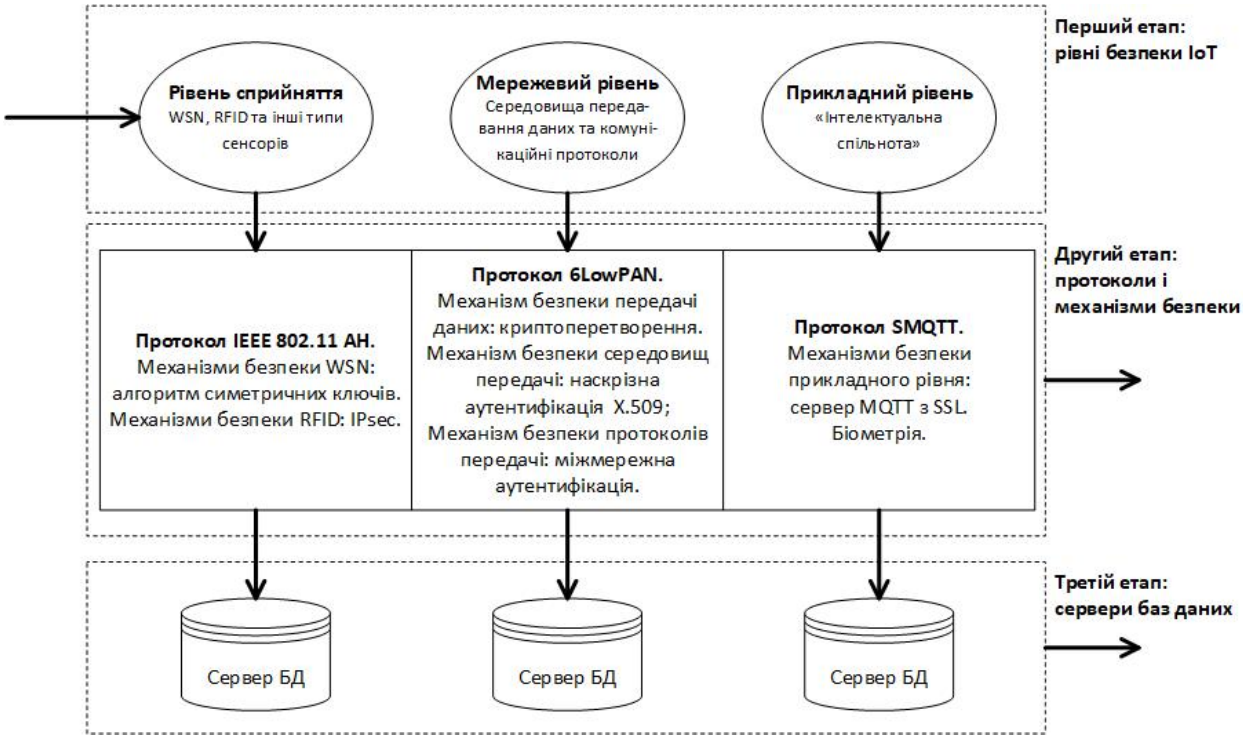

Рисунок 4.1 – Запропонована модель управління безпекою

4.1 Три етапи реалізації запропонованої моделі

Перший етап запропонованої моделі обговорювався в попередніх розділах, тому тут слід зосередитися на другому і третьому етапах.

Другий етап розділений на три основні фази. Перша фаза другого етапу описує використовуваний протокол і механізми безпеки рівня сприйняття. Найбільш придатним протоколом для рівня сприйняття є IEEE 802.11 AH, тому що він підходить для бездротового зв’язку. Це легкий протокол, і його реалізація споживає мало енергії та часу, зменшуючи проблему накладних витрат. Він забезпечує ефективний двонаправлений обмін пакетами, щоб

дозволити датчику заощадити більше енергії, використовуючи зв’язок висхідного та низхідного напрямків між датчиками. Датчик надсилає дані та переходить у режим сну, закінчуючи свою місію. Він має короткий фрейм MAC, що дозволяє збільшити час сну для економії енергії. IEEE 802.11 AH забезпечує приватність та конфіденційність завдяки алгоритму шифрування.

Зручні механізми безпеки рівня сприйняття можна визначити згідно з попереднім оглядом механізмів безпеки, що було пояснено у таблицях Б.2 і Б.3. Відповідними механізмами безпеки WSN є керування ключами (PKI) та захищені алгоритми ключа з використанням алгоритмів симетричного ключа, які забезпечують низьке енергоспоживання. Для RFID використовується механізм IPSec, оскільки він забезпечує алгоритми аутентифікації та шифрування.

Для забезпечення односторонньої хеш-функції в алгоритмах аутентифікації використовується маркер доступу. Одностороння хеш-функція дозволяє користувачам отримати маркер доступу, який дозволить отримувати доступ до певного ресурсу, не використовуючи своє ім’я користувача та пароль. Отримавши маркер доступу, користувач може його відобразити, з метою отримання доступу на певний період часу до певного ресурсу на віддаленому сайті. Клієнт повинен вказати маркер доступу як частину URL-адреси запиту або як ім’я користувача. Маркер доступу на основі алгоритму аутентифікації забезпечує авторизацію, контроль доступу, доступність та конфіденційність.

Використання симетричного алгоритму шифрування надає легкість в реалізації, що пов’язано з низькою потужністю та економією часу. Для захисту приватної інформації користувачів і виявлення помилок мережі використовуються анонімність і оцінка ризиків для всіх типів датчиків.

Друга фаза другого етапу пов’язана з використовуваним протоколом і механізмами безпеки мережевого рівня. Найбільш відповідним протоколом мережевого рівня є 6LowPAN, який використовується для інкапсуляції IPV6. IPV6 надає довгий заголовок у невеликому пакеті. 6LowPAN вимагає низької

пропускної здатності, низького енергоспоживання, має низьку вартість, є мобільним, надійним, забезпечує тривалий час сну, є придатним для побудови масштабованих мереж. Це може зменшити проблему накладних витрат на передачу.

Відповідні механізми безпеки мережевого рівня можна класифікувати на заходи безпеки передачі даних, середовищ передачі та протоколи передачі, які пояснюється в таблиці Б.4.

Криптографічний захист передачі даних реалізується за допомогою алгоритму симетричного ключа. Споживає мало енергії та часу.

Для середовищ передачі використовується алгоритм наскрізної аутентифікації на основі сертифікатів X.509. Він підтримує двостороннє з’єднання Socket Secure Layer (SSL) для створення клієнтського сертифіката та підключення до сервера. Також він використовує механізм PKI, оскільки немає необхідності розповсюджувати відкриті ключі або перевіряти відбитки пальців під час створення або оновлення пар ключів. Це високомасштабована реалізація, оскільки їй не потрібно довіряти окремим об’єктам, але їй потрібна єдина аутентифікація сертифікатів (CA) або обмежена кількість CA. Перевірка особи забезпечується за допомогою секретних закритих ключів.

Для захисту протоколу передачі використовується механізм міжмережної аутентифікації. Це проявляється у зменшенні складності управління мережею.

Третя фаза другого етапу пов’язана з реалізацією протокола і механізмів безпеки прикладного рівня. Використовується протокол Secure MQTT (SMQTT), який використовує шифрування на основі полегшених алгоритмів шифрування, що також дає низьку потужність та економить час. Сервер MQTT через SSL є основою системи безпеки мережі IoT, захищаючи конфіденційну інформацію. SSL захищає програми IoT (програмні інтерфейси та особисту інформацію про користувачів) за допомогою алгоритмів шифрування, надаючи захищеність конфіденційної інформації, аутентифікацію, захищеність критичних елементів та цілісність даних.

Відповідним заходом безпеки для прикладного рівня є біометрія, оскільки вона може запобігти внутрішнім і зовнішнім атакам і захистити всі дані між прикладним рівнем і користувачами. Біометрія – відносно нова тема в області досліджень, і всі дослідження намагаються знайти відповідні алгоритми безпеки для мережі IoT, щоб зменшити споживання енергії та час.

Важливими елементами в мережі IoT для моніторингу, управління та контролю мережевого трафіку виступають списки контролю доступу.

Третій етап запропонованої моделі – сервери баз даних, які зберігають всю інформацію та параметри механізмів безпеки для кожного рівня безпеки, профілі користувачів, помилки механізмів безпеки, лог-файли системи IoT та списки контролю доступу. Третій етап може допомогти (адміністратору та користувачам) керувати всією інформацією про мережу IoT та користувачів

4.2 Введення додаткового рівня

Основною відмінністю запропонованої моделі є наявність проміжного шару шлюзів, або «туманного» (англ., fog) шару, який виконує кілька завдань безпеки: розширює хмарні обчислення до краю мережі, надаючи нові програми та послуги середовища Інтернету речей, які можуть включати обробку критично важливих даних, що потребують конфіденційності та безпеки без передачі їх хмарним сервісам.

У fog-шарі виділяють три елементи:

- шлюзи, які збирають дані від виконавчих та сенсорних пристроїв;
- fog-шлюзи, які обмінюються інформацією між собою;
- шлюзи середовища IoT, які обмінюються повідомленнями з хмарою.

Застосування додаткового рівня дозволяє уникнути передачі конфіденційної інформації загальнодоступними мережами, якщо це не суперечить функціонуванню системи.

Можна організувати також систему перевірки достовірності даних, одержуваних від виконавчих та сенсорних пристроїв, і вирішити завдання

«вузького» місця, коли один шлюз не справляється з обчислювальним та пропускним навантаженням.

Згідно рисунку 4.2, під уніфікацією кодування розуміється розробка єдиного для всіх пристроїв протоколу кодування інформації. Це насамперед стосується RFID-технології, де використовується європейський та японський стандарти. Коди корекції допомагають уникнути колізій, що виникають при одночасному зчитуванні інформації з багатьох бездротових пристроїв [34].

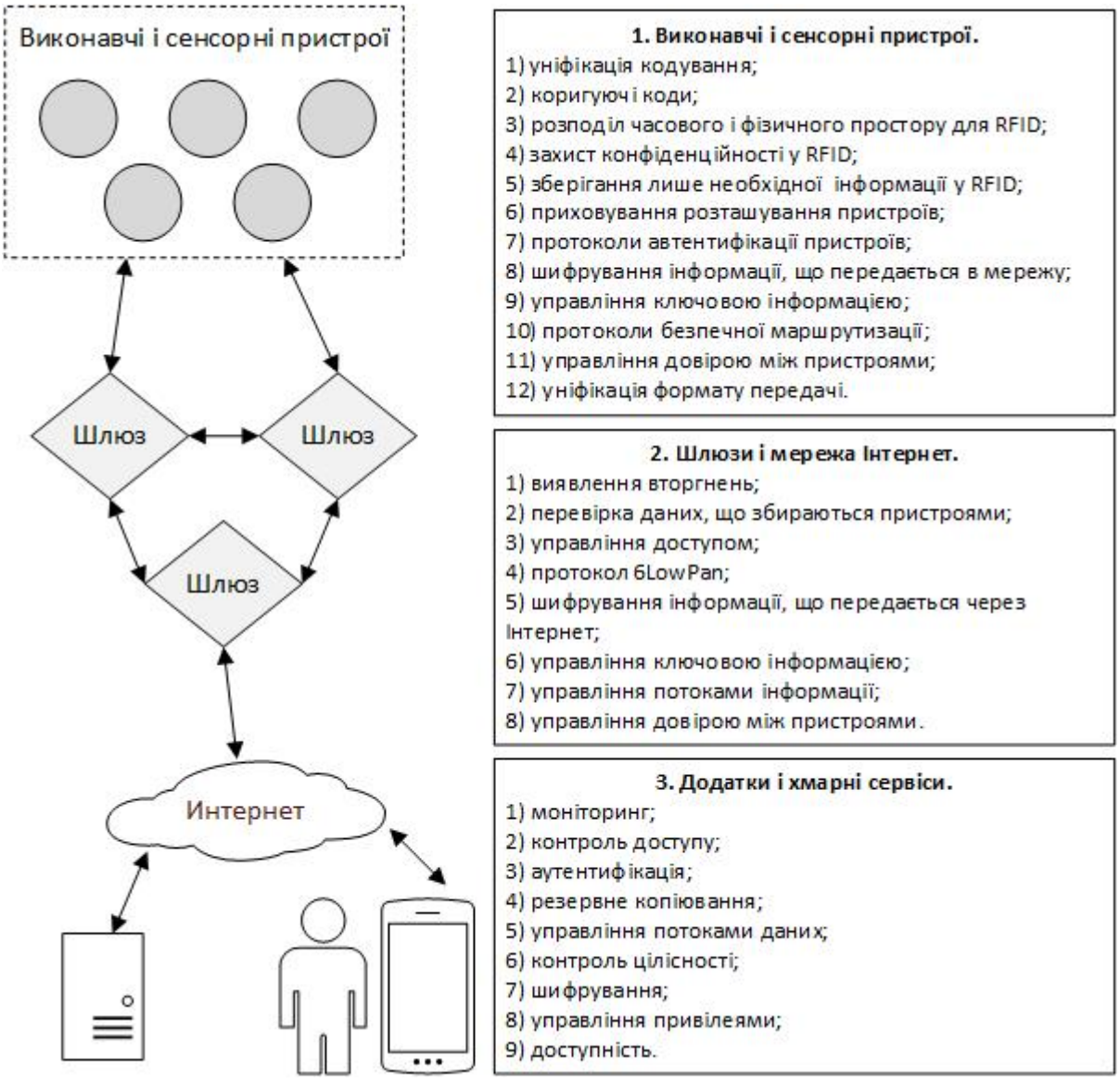

Рисунок 4.2 – Архітектура безпеки середовища Інтернету речей з додатковим шаром

Поділ часового та фізичного простору може також допомогти уникнути появи колізій, пов’язаних із накладанням радіосигналів один на одного. Захист конфіденційності RFID та зберігання в мітках мінімальної кількості компрометуючої інформації припускають той факт, що дані можуть бути зчитані та скопійовані зловмисником. Це можна зробити кількома шляхами [22]. Відкрите розташування пристроїв може сприяти отриманню відомостей зловмисником про розгорнуту систему. Тому не варто забувати про приховування ознак, що демаскують. Протоколи автентифікації пристроїв, як правило, реалізовані за парольною схемою. Більшість виробників використовують стандартні паролі для доступу до пристроїв, і користувачі часто їх не змінюють, що призводить до втрати управління пристроєм [35].

Зважаючи на те, що більшість пристроїв середовища Інтернету речей обмежені в обчислювальних можливостях, а всі дані, передані за бездротовими протоколами, повинні шифруватися, тут передбачається використання легковагих симетричних алгоритмів. Оскільки шифрування симетричне, гостро постає питання зміни, передачі, оновлення ключів шифрування. Протоколи безпечної маршрутизації, а також управління довірою між пристроями зараз будуються на використанні сертифікатів автентичності, наприклад X.509. Уніфікація протоколу даних складається з визначення формату представлення даних: XML, JSON, тощо.

На наступному рівні можна виділити засоби виявлення вторгнень, що використовуються для визначення зловмисних дій. Також окремо виділено пункт про перевірку інформації від виконавчих та сенсорних пристроїв та скорочення її обсягу. Управління доступом на даному рівні включає можливість міжмашинної взаємодії, щоб виключити можливість перехоплення пристроєм інформації, яка йому не призначалася. Застосування нової технології 6LowPAN дозволить впроваджувати пристрої середовища Інтернет речей в рамках існуючої інфраструктури. Для шифрування інформації, що передається мережею Інтернет, тут використовуються протоколи з алгоритмами асиметричного шифрування, що застосовуються в

мережі Інтернет. Управління ключовою інформацією, потоками інформації, довірою між пристроями здійснюється на основі принципів безпеки в Інтернеті.

На останньому рівні розглянуті аспекти безпеки, пов’язані з веб-сервісами та хмарними обчисленнями. Оскільки ці елементи не мають явної специфіки середовища Інтернету речей, на них не слід акцентуватися. Проте останнім часом виникла потреба розробки безпечного протоколу аутентифікації користувачів за допомогою веб-сервісу. Як правило, автори пропонують використовувати двофакторну автентифікацію за допомогою смарт-карток або біометричних ознак людини.

Структуру безпеки середовища Інтернету речей можна представити у вигляді наступної математичної моделі. Нехай існує m виконавчих пристроїв X_m і n шлюзів G_n. Тоді можна описати зв’язки виконавчих та сенсорних пристроїв між собою у вигляді матриці 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 (рисунок 4.2). Тоді добуток матриць характеризуватиме безпеку взаємодії пристроїв у вигляді матриці розміром $m \times p_x$:

$$S_x = C_x \times p_x. \qquad (4.1)$$

Далі опишемо зв’язки між пристроями та шлюзами у вигляді матриці 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 (рисунок 4.2). Тоді добуток матриць характеризуватиме безпеку на межі шлюзів у вигляді матриці розміром $n \times p_b$:

$$D_b = C_b \times P_b. \tag{4.2}$$

Далі розраховується відносна оцінка безпеки за формулою

$$V_1 = \frac{\sum_{r=1}^{m}\sum_{k=1}^{p_x} s_{rk} + \sum_{r=1}^{n}\sum_{k=1}^{p_b} d_{rk}}{T_x + T_b}, \tag{4.3}$$

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:

$$V_1(t) = \frac{\sum_{r=1}^{m}\sum_{k=1}^{p_x} s_{rk}(t) + \sum_{r=1}^{n}\sum_{k=1}^{p_b} d_{rk}(t)}{T_x + T_b}. \tag{4.4}$$

Це зручно під час проектування середовища Інтернету речей та визначення поточного стану безпеки.

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 за (4.1-4.4), отримуємо матриці S_g, D_v та оцінку V_2 (4.5). Аналогічно для третього рівня розраховується оцінка V_3 (4.6) для

хмарних сервісів, абонентських пристроїв та виходу до мережі Інтернет:

$$V_2 = \frac{\sum_{r=1}^{m}\sum_{k=1}^{p_x} s_{rk} + \sum_{r=1}^{n}\sum_{k=1}^{p_b} d_{rk}}{T_g + T_v}; \quad (4.5)$$

$$V_3 = \frac{\sum_{r=1}^{m}\sum_{k=1}^{p_x} s_{rk} + \sum_{r=1}^{n}\sum_{k=1}^{p_b} d_{rk}}{T_f + T_z}; \quad (4.6)$$

Маючи всі три матриці та відносні оцінки, можна зробити кількісну та якісну оцінку стану безпеки всієї системи. Причому додавання, зміна або видалення пристроїв та зв’язків, а також параметрів безпеки проводиться додаванням, зміною, видаленням рядків та стовпчиків відповідних матриць.

ВИСНОВКИ

Найбільшими проблемами Інтернету речей (IoT) є проблеми безпеки та приватності. Тому розуміння значення та видів загроз, атак і вразливостей середовища IoT є важливим. Усі ці небезпеки є основним фактором при створенні будь-якої системи безпеки, щоб виявляти та запобігати їх за допомогою відповідних методів безпеки. В роботі представлено порівняння між механізмами безпеки для кожного рівня безпеки IoT, які були розроблені для визначення впливу заходів безпеки на споживану потужність і час. За підсумками порівнянь була запропонована модель управління безпекою для системи IoT, яка дозволяє вибирати найбільш придатні протоколи та алгоритми безпеки. Отже, метою запропонованої моделі є захист даних, середовищ передачі, протоколів та програм для запобігання більшості загроз та атак. Також запропонована модель використовується для виявлення помилок мережі та захисту приватної інформації користувачів.

Запропонована модель може допомогти розробникам керувати методами безпеки на кожному рівні безпеки IoT. Основним внеском запропонованої моделі був вибір і керування відповідними механізмами безпеки для досягнення низького споживання енергії та часу.

У цій роботі запропоновано метод оцінки безпеки середовища Інтернету речей. Завдяки декомпозиції середовища на три архітектурні компоненти стало можливим провести аналіз та чисельну оцінку комплексних параметрів безпеки кожного рівня. На другому рівні пропонується використовувати не єдиний шлюз, а кілька шлюзів. Тим самим формується fog-шар, що забезпечує міжкомпонентну стійкість інформаційного обміну, дозволяє обробляти невеликі обсяги інформації всередині компонентного рівня без передачі критично важливої інформації на хмарні послуги.

Завдяки відносно невеликій обчислювальній складності запропонованої

моделі оцінки 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.

За темою кваліфікаційної роботи опубліковано тези доповіді в рамках дев’ятої міжнародної науково-технічної конференції «Проблеми інформатизації» [36].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Wu Q., Ding G., Xu Y., Feng S., Du Z., Wang J., Long, K. Cognitive internet of things: A new paradigm beyond connection. IEEE Internet of Things Journal, 2014, no. 1(2), pp. 129-143.

2. Nikolov A., Pencheva E., Atanasov I., Nikolova K. A case of service interaction in M2M device management. In: Paper presented at the 2016 8th IFIP Int. Conf. on New Technologies, Mobility and Security, NTMS, 2016.

3. M.U. Farooq, Waseem M., Khairi A., Mazhar S., "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications, vol. 111, no. 7, pp. 1-6, 2015.

4. Huawei, "Tap Into New Growth with Intelligent Connectivity", White paper global connectivity index, 2018, at available at https: www.huawei.com/ minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180716

5. Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. Proc.Living in the Internet of Things: Cybersecurity of the IoT, London, UK, pp. 1-7, 28-29 March 2018.

6. Jayavardhana G., Rajkumar B., Slaven M., Marimuthu P., "Internet of Things (IoT): A vision, Architectural Elements, and Future Directions", Elsevier, Future Generation Computer Systems, vol. 29, pp. 1645-1660, 2013.

7. Amri Y., Setiawan M.A., "Improving Smart Home Concept with the Internet of Things Concept Using RaspberryPi and NodeMCU", Proc. the IOP Conf. Series: Materials Science and Engineering, vol. 325, no. 2018, pp. 1-10, 2018.

8. Osisanwo F., Kuyoro S., Awodele O., "Internet Re- frigerator-A Typical Internet of Things (IoT)", Proc. the 3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM'2015), London (UK), pp. 59-63, 23-24 March 2015.

9. Jimenez J., Koster M., Tschofenig H., "IoT Semantic Interoperability",

Proc. of the Workshop 2016', San Jose, Us, 17-18 March 2016, available at http://www.ipso-alliance.org/wp-content/uploads/2016/01/ipso-paper.pdf

10. Sharon L. Poczter, Luka M. Jankovic, "The Google Car: Driving Toward A Better Future?", Journal of Business Case Studies, vol. 10, no. 1, pp. 7-14, 2014.

11. Mario Collotta, Giovanni Pau, "A Solution Based on Bluetooth Low Energy for Smart Home Energy Management", Journal of Energy Research, Engineering and Policy, vol. 8, no. 10, pp.11916-11938, 2015.

12. Keyur K Patel, Sunil M Patel, "Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", International Journal of Engineering Science and Computing, vol. 6, no. 5, pp. 6122- 6131, 2016.

13. Soumyalatha, Shruti G Hegde, "Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges", International Journal of Advanced Networking & Applications (IJANA)", Proc. the 1st Int. Conf. on "Innovations in Computing & Networking" (ICICN-2016), Raja Rajeswari College of Engineering, Bangalore, India, pp. 477- 482, 12-13 May 2016.

14. Bhoopathy V., R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 466-474, 2012.

15. Jing Deng, Richard Han, Shivakant Mishra, "Countermeasures against Traffic Analysis Attacks in Wireless Sensor Networks", Proc. the First Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 5-9 September 2005.

16. Zheng Yan, Peng Zhang, Athanasios V. Vasilakos, "A Survey on Trust Management for Internet of Things", Journal of Network and Computer Applications, vol. 42, pp. 120-134, 2014.

17. Zhen Ling, Kaizheng Liu, Yiling Xu, YierJin, XinwenFu, "An End-to-End View of IoT Security and Privacy", Proc. the GLOBECOM 20172017 IEEE Global Communications Conference. Singapore, Malay, pp. 1-7, 4-8 December

2017.

18. Krishna Kanth Gupta, Sapna Shukla, "Internet of Things: Security Challenges for Next Generation Networks", Proc. the 1st Int. Conf. on Innovation and Challenges in Cyber Security (ICICCS 2016), Noida, India, pp. 315-318, 3-5 February 2016.

19. Sathish Alampalayam Kumar, Tyler Vealey, Harshit Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions", Proc. the System Sciences (HICSS), 49th Hawaii International Conference on System Sciences, Koloa, HI, USA, pp. 5771- 5780, 5-8 Jan. 2016.

20. Mohamed Abomhara and Geir M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security, vol. 4, pp. 65-88, 2015.

21. Gigli M., Koo S. Internet of things: services and applications categorization. Adv Internet Things, 2011, no. 1(02), pp. 27-41.

22. Seol S., Lee E., KimW. Indoor mobile object tracking using RFID. Future Generation Computer Systems, 2017, no. 76, pp. 443-451.

23. Li H., ZhouX. Study on security architecture for Internet of Things. In: Applied informatics and communication. Springer Berlin Heidelberg, 2011, pp. 404-411.

24. Mayer C.P. Security and privacy challenges in the internet of things. Electron Commun EASST, 2009, no. 17, pp. 1-12.

25. Jing Q., Vasilakos A. V., Wan J., Lu J., Qiu D. Security of the internet of things: Perspectives and challenges. Wireless Networks, 2014, no. 20(8), pp. 2481-2501.

26. Maryam Daud, Quratulain Khan, Yasir Saleem, "A Study of Key Technologies for IoT and associated Security Challenges", Proc. the Int. Symp. on Wireless Systems and Networks (ISWSN), Lahore, Pakistan, pp. 1-6, 19-22 November 2017.

27. Alma Oracevic, Selma Dilek, Suat Ozdemir, "Security in internet of things: A survey", Proc. the 2017 Int. Symp. on Networks, Computers and

Communications (ISNCC), Marrakech, Morocco, pp. 1-6, 16-18 May 2017.

28. W.Sharon Inbarani, C.Kumar Charlie Paul, W.Andrew Jerome Jeevakumar, "A Survey on Security Threats and Vulnerabilities in Cloud Computing", Int. Journal of Scientific & Engineering Research, vol. 4, pp. 1-4, 2013.

29. Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey", Wiley Hindawi Security and Communication Networks, vol. 2017, pp.1-41, 2017.

30. Ahmad W. Atamli, Andrew Martin, "Threat-based Security Analysis for the Internet of Things", Proc. the 2014 International Workshop on Secure Internet of Things, wroclaw, Poland, pp. 35-43, 10-10 September 2014.

31. Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017, pp. 1-25, 2017.

32. Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey", Elsevier, Computer Networks, vol. 54, pp. 27872805, 2010.

33. Otmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi, "Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures, Electronic Journal of Information Technology, Issue 9, pp. 24-37, 2016.

34. Finkenzeller K. RFID handbook fundamentals and applications in contactless smart cards and identification West Sussex. Wiley, 2003.

35. Проблема «admin:password»: стандартные пароли помогли создать ботнет из почти 400 000 IoT-устройств. URL: https://habrahabr.ru/ company/pt/blog/311754/ (дата доступу: 30.10.2017).

36. 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.