МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056:004.738.5(079.2)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Методи безпеки даних та пристроїв інтернету речей

Виконавець: В.Є. Бобовніков
Керівник: к.т.н., доцент М.Б. Гумен
Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«___» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Бобовнікова Владислава Євгеновича

1. Тема: *Методи безпеки даних та пристроїв інтернету речей*
затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.

2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.

3. Вихідні дані: огляд і аналіз проблем та загроз інтернету речей; визначення особливостей та аналіз загроз безпеки на кожному рівні; розробка рекомендацій та практичних кроків щодо застосування методів безпеки даних та пристроїв у системі IoT; проектування системи інтернету речей та реалізація в ній запропонованих методів безпеки.

4. Зміст пояснювальної записки: огляд особливостей інтернету речей; аналіз загроз безпеки та особливості рівнів архітектури; проектування захищеної IoT системи.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	10.05.2021	*Виконано*
2.	Аналіз літературних джерел	11.05.2021-14.05.2021	*Виконано*
3.	Обґрунтування рішення	15.05.2021-17.05.2021	*Виконано*
4.	Збір інформації	18.05.2021-22.05.2021	*Виконано*
5.	Дослідження сучасних технологій інтернету речей та їх особливостей	23.05.2021-24.05.2021	*Виконано*
6.	Аналіз загроз безпеки системи IoT та методів безпеки	25.05.2021-28.05.2021	*Виконано*
7.	Проектування захищеної системи інтернету речей	29.05.2021-02.06.2021	*Виконано*
8.	Перевірка на антиплагіат	03.06.2021	*Виконано*
9.	Оформлення і друк пояснювальної записки	04.06.2021-06.06.2021	*Виконано*
10.	Оформлення презентації	07.06.2021-08.06.2021	*Виконано*
11.	Отримання рецензій від рецензентів	09.06.2021	*Виконано*

Здобувач вищої освіти В.Є. Бобовніков

(підпис, дата)

Керівник дипломної роботи М.Б. Гумен

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом робота складає 53 сторінки, має 30 рисунків та 2 діаграми. Список використаних джерел містить 26 найменувань і займає 2 сторінки.

Метою дипломної роботи є розробка системи забезпечення безпеки даних і пристроїв у системі інтернету речей.

В роботі на основі аналізу особливостей інтернету речей, аналізу загроз та методів забезпечення безпеки на кожному рівні вирішено задачу побудови системи безпеки даних та пристроїв IoT з реалізацією в ній запропонованих рекомендацій та методів безпеки.

Ключові слова: загроза безпеки, питання безпеки, методи захисту інформації, інтернет речей, рівні інтернету речей.

ЗМІСТ

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНТЕРНЕТУ РЕЧЕЙ 8
1.1 Історія інтернету речей 8
1.2 Інтернет речей в сучасному світі 9
1.3 Особливості роботи інтернету речей 11
1.4 Висновки до першого розділу 16
РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ТА ОСОБЛИВОСТІ РІВНІВ АРХІТЕКТУРИ 17
2.1 Сучасні проблеми інформаційної безпеки 17
2.1.1 Питання безпеки інтернету речей 20
2.1.2 Забезпечення безпеки на сенсорному рівні 22
2.1.3 Безпека мережевого рівня 24
2.1.4 Постановка задачі безпеки на рівні служб 24
2.1.5 Безпеки рівня інтерфейсів 25
2.2 Моніторинг проблем безпеки даних та пристроїв інтернету речей 25
2.3.1 Сенсорний рівень 33
2.3.2 Мережевий рівень 36
2.3.3 Рівень інтерфейсів 38
2.3.4 Особливості рівня служб 40
2.3.5 Міжрівневі загрози 42
2.4 Висновки до другого розділу 45
РОЗДІЛ 3. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ IoT СИСТЕМИ 46
3.1 Постановка задачі до проектування IoT системи 46
3.2 Побудова IoT системи 49
3.3 Вибір методів безпеки та їх реалізація 50
3.4 Висновок до третього розділу 55
ВИСНОВКИ 57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 58

ВСТУП

Актуальність. Інтернет речей безсумнівно можна вважати новим витком розвитку Інтернету, в якому відбувається обмін даними між підключеними до мережі фізичними об'єктами, де кожен пристрій може самостійно взаємодіяти і мати взаємозв'язки з мільярдами інших речей. IoT дає можливість людям дистанційно виконувати різні завдання, які надалі сильно полегшують життя.

Інтернет речей швидкими темпами поширився в багатьох сферах діяльності. Цю концепцію застосовують в розумних будинках, транспортних системах, розумних містах. Завдяки цій системі різні промислові структури, системи охорони здоров'я зробили крок вперед, адже тепер є можливість більшого контролю над безліччю структур та процесів. Збір та обробка даних, які весь час аналізуються із застосуванням штучного інтелекту.

Безсумнівно, такі можливості привертають так само і зловмисників. IoT системи все більше розвивають свої переваги по взаємодії з інтелектуальними системами за допомогою розвитку різних розумних датчиків, різних технологій бездротового зв'язку, хмар і аналізу. Виходячи з інформації, яку надав сайт по створенню різних статистичних даних (statista.com), кількість IoT підключених пристроїв у всьому світі, за станом на 2021 рік перевищило населення планети і склало 10.07 мільярдів підключень. Більш того, за прогнозами на 2030 рік, кількість унікальних підключень складе 25.44 мільярда. Такі значення свідчать про те, що в подальшому тенденція IoT систем стане ще більш ключовим аспектом по впровадженню рішень в різні інфраструктурні комплекси. Однак інтернет речей має безліч труднощів і невирішених проблем.

Однією з таких ключових проблем є безпека. Великому шуму піддалася атака ботнету Mirai, яка змусила всіх звернути увагу на себе. Жертвами проведення такої атаки стало безліч недорогих пристроїв, де стояли стандартні паролі. Завершенням стала розподілена відмова в обслуговуванні (DDoS) проти постачальника системи доменних імен (DNS) Dyn, який є частиною інтернет-

інфраструктури багатьох американських гігантів, в слідстві чого були виведені з ладу доходи та клієнти.

Безпека мереж, додатків, інфраструктури повинна буде розглядатися постійно, адже в іншому випадку втрати будуть дуже високими, але на даному етапі виробники не сильно прагнуть захистити свої пристрої. Не варто забувати про те, що при впровадженні практик з інформаційної безпеки в свої рішення, підвищиться і ціна відповідно. Іншою причиною відмови служать великі витрати на забезпечення великих обсягів обчислень, що відповідно збільшує витрату енергії для різних автономних пристроїв.

Все середовище інтернету речей, яке стосується розробників і користувачів, вимагає безлічі поліпшень у сфері безпеки IoT. При такому ж відношенні, в наступні роки зростання індустрії може припинитися. Використання інтернету речей дійсно допомагає покращувати різні сфери життя, проте без повної безпеки IoT складно говорити про довіру.

Метою дипломної роботи є розробка системи забезпечення безпеки даних і пристроїв у системі інтернету речей.

Досягнення мети досліджень потребує розв’язання таких задач:

- огляд і аналіз проблем та загроз інтернету речей;
- визначення особливостей та аналіз загроз безпеки на кожному рівні;
- проведення порівняльного аналізу методів безпеки IoT.
- розробка рекомендацій та практичних кроків щодо застосування методів безпеки даних та пристроїв у системі IoT.
- проектування системи інтернету речей та запропонування методів безпеки для цієї системи.

Об'єкт дослідження: інформаційна безпека інтернету речей

Предмет дослідження: методи та способи захисту системи інтернету речей

Практична цінність полягає у тому, що на основі проведеного аналізу загроз та методів безпеки спроектовано систему IoT, що забезпечує зменшення впливу кіберзагроз.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Історія інтернету речей

У 1990-і роки можна було спостерігати використання словосполучення "інтернет речей". Одним з першовідкривачів цієї фрази став Кевін Ештон - дослідник технологій RFID, який трохи пізніше став засновником Auto-ID Labs. З часом з'явилися і інші назви для IoT, проте всі вони акцентували увагу на вимогах до підключення і сенсорних вимогах необхідних для фізичних об'єктів. У 1990-ті роки всі дослідження, розробки, обговорення пов'язані з IoT були лише теоретичного характеру і тільки 2000-і роки послужили інтернету речей в досить сильному розвитку цього напрямку.

Різні проекти, ідеї, доопрацювання IoT стали з'являтися на світло, як підсумок - поява великої кількості пристроїв в призначеному для користувача сегменті та в промисловій області. У кінцевому результаті утворилося дві великі сфери застосування і використання IoT (рис. 1.1):

- Consumer Internet of Things (CIoT) основною ідеєю якого стає кінцевий користувач;
- Industrial Internet of Things (IIoT) основні напрямки якого різні галузі виробництва, корпоративне використання, життєдіяльність людини.

Якщо вважати, що визначення задовольняють вимогам IoT, то нові словосполучення пов'язані з IoT створюють велику цінність для об'єктів в повсюдних і автономних мережах, в якій важливу роль відіграє впровадження ідентифікації та обслуговування. Сюди можна віднести Інтернет всього (IoE), який компанія Cisco використовувала для пояснення сукупності IoT і таких пристроїв як смартфони, комп'ютери і інші підключені пристрої.

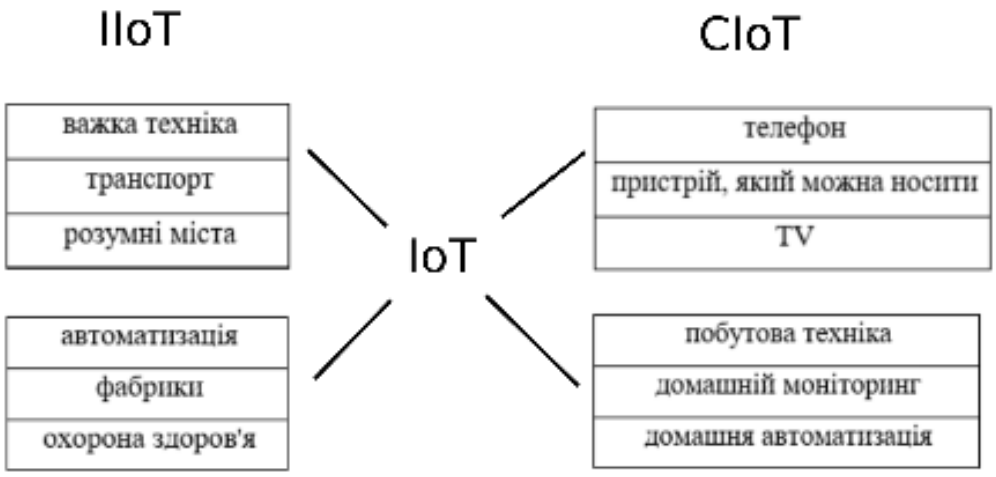

Рис. 1.1 Приклад застосування IIoT та CIoT

1.2 Інтернет речей в сучасному світі

Фізичні об'єкти, які взаємодіють між собою або з зовнішнім середовищем через передачу даних по мережі можна назвати інтернетом речей. У сучасному світі, інтернет речей може служити для машинної взаємодії (M2M), людино-машинної взаємодії та людини з оточенням.

Поповнення кількості нових протоколів і збільшення кількості розумних пристроїв змусить IoT вибрати напрямок, в якому буде об'єднання між розумними і автономними мережами. Впровадження людини в IoT систему дає переваги в охороні здоров'я та готовності до надзвичайних ситуацій. Таким чином інтенет речей сформує систему, яка за допомогою датчиків зможе реагувати на різні події шляхом передачі інформації. Ця система буде мати вплив на підприємства, медичні системи, якість життя і бізнес, використовуючи і впроваджуючи такі можливості як:

- надання інтегрованого середовища для взаємодії між фізичними об'єктами розширюючи канал зв'язку, в якій датчики володіють такими даними як пульс, місце розташування, серцебиття та інше;

- легка взаємодія між адміністраторами та фізичними об'єктами через віддалений доступ завдяки спрощенню процесів автоматизації і управління;
- надання різних вимірів і інших корисних даних через віддалений доступ до пристроїв, що дає перевагу в скороченні витрат на впровадження, розгортання і обслуговування різних систем.

Приклади сучасного використання і впровадження IoT систем:

- Підключені дороги.

Важлива область, куди IoT системи почали впроваджувати - підключені дороги (connected roadways). Проекти, як безпілотний автомобіль Google, Uber, Яндекс потребують впровадження інтенета речей. Така інтеграція дозволить їм краще взаємодіяти з транспортною системою, за допомогою обміну даними і поліпшенням зв'язка з водіями чи іншими безпілотними засобами пересування.

- Підключені фабрики.

Безліч класичних фабрик починає своє перетворення в підключені заводи (connected factory), де різні датчики IoT систем допоможуть вирішити:

- проблеми простою на заводі;
- проблеми якості роботи;
- проблеми пошуку джерел різної виробничої неефективності.

- Розумні підключені будівлі.

Розумні підключені будівлі (smart connected buildings) є доказом успішного впровадження інтернету речей. Будівлі такого типу використовують різні системи датчиків, для підвищення продуктивності і обміну інформацією, яка дозволяє отримувати відомості про те, що відбувається між різними системами. Після таких дій інформація може бути використана для автоматизації різних процесів.

1.3 Особливості роботи інтернету речей

Основоположними елементами інтернету речей, які існують багато років, можна вважати віддалений виклик служб, різні сенсорні пристрої, комунікаційні мережі та обробка подій з урахуванням контекста. IoT намагається представити себе, як єдину мережу розумних об'єктів і людей, які можуть взаємодіяти і спілкуватися один з одним. Умовами для розподіленої середовища є повний взаємозв'язок між об'єктами, гарним прикладом якої є IoT. Архітектура, яка являє собою цілісну систему повинна гарантувати бездоганну роботу власних компонентів (де головним фактором проектування вважається надійність) та пов'язувати фізичну і віртуальні сфери. Головною вимогою для досягнення цілісної системи є ретельний розгляд в момент проектування відновлення після збоїв і масштабованість.

Слід додати, що з тих пір, як динамічна зміна місця розташування і мобільність стали одним з головних аспектів інтернету речей, де всюди використовується смартфон, сучасна архітектура повинна прагнути включати в себе точний рівень адаптованості для правильної обробки різних динамічних взаємодій у всій екосистемі. Надання рівня абстракції на більш високому рівні, який може приховувати деякі деталі реалізації і обмеження, безсумнівно можна вважати перевагою еталонних архітектур і моделей.

Еталонна модель IoT-ARM (IoT Architectural Reference Model) концентрується на розробці і перевірці інтегрованої мережевої архітектури інтернету речей (рис. 1.2).

IoT-ARM відображає різні рівні обслуговування і представлення. Рівень обслуговування включає в себе події обробки і аналітики, систему виявлення служб та управління ресурсами, служби об'єднання повідомлень і сервісної шини підприємства (ESB) за рахунок фізичного і комунікаційних рівнів. В архітектуру також включено управління API, яке необхідно для визначення і спільного використання системних служб і веб-панелей для управління цими API і доступу до них.

Рис. 1.2. Еталонна архітектура IoT

Через важливості управління пристроями, забезпечення безпеки і конфіденційності на різних рівнях, а також здатності однозначно ідентифікувати об'єкти і контролювати їх рівень доступу, ці компоненти сконцентровані в цій архітектурі незалежно.

Аналіз сервіс-орієнтованої архітектури(SOA).

Для безлічі постачальників послуг і користувачів, SOA архітектура буде обов'язковою при використанні інтернету речей. Така архітектура забезпечує взаємодії між множиною різних пристроїв. Загальний вид сервіс-орієнтованої архітектури складається з чотирьох рівнів, кожен з яких має наступні функції:

- сенсорний рівень тісно взаємодіє з доступними апаратними об'єктами для визначення стану речей;
- мережевий рівень являє повноцінну інфраструктуру, яка необхідна для підтримки провідних і бездротових підключень;

- службовий рівень дозволяє створювати і управляти сервісами, які необхідні користувачам або додаткам;
- рівень інтерфейсів надає різні методи користувачем і додатків для можливості взаємодії.

При використанні такої архітектури, система ділиться на підсистеми, які між собою слабо пов'язані і при необхідності їх можна повторно використовувати для забезпечення підтримки всієї системи, де головна увага приділяється до складових компонентів. При такому підході , Можливості архітектури дозволяють зберігати частину системи, яка буде працювати в разі збою конкретного компонента. Для архітектур, де надійність стає головним пріоритетом такі можливості мають вагоме значення.

Ця система має повсюдне використання в бездротових сенсорних мережах (WSN), оскільки має досить високий рівень абстракції та володіє різними перевагами, які пов'язані з WSN. Таким чином IoT може використовувати SOA, адже архітектура надає підвищення взаємодії і масштабованості між об'єктами. Для користувача, при такій архітектурі, стає більш простіше взаємодіяти з протоколами та рівнями цієї системи.

В SOA, інтернет речей розкриває всі свої сильні сторони, адже об'єднання функцій системи, дає можливість створення різноманітних і складних сервісів, розділяючи їх на завдання, де виконання різних сервісів вимагає використання різних об'єктів у всій цій системі (рис. 1.3).

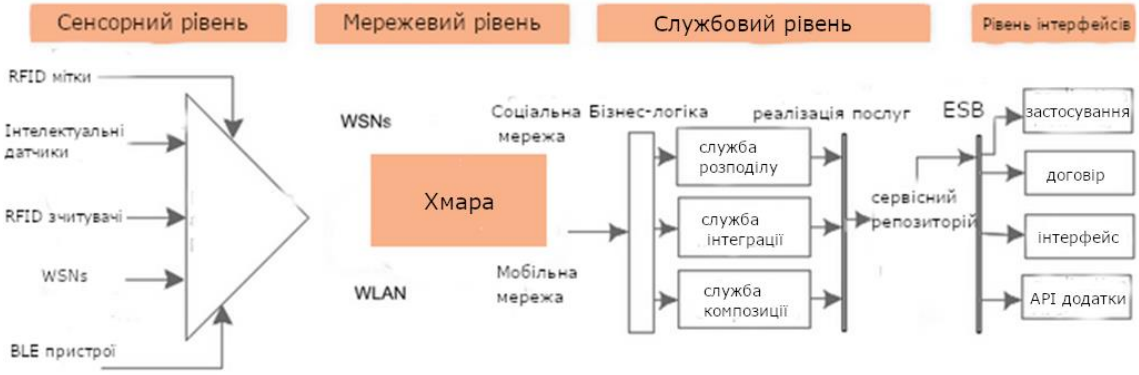

Рис 1.3. Сервіс-орієнтована архітектура для IoT

Компоненти інтернету речей.

- Одним з головних компонентів системи інтернету речей є датчики, які включають ОС з мінімальним відгуком в критично важливих місцях, різні джерела збору, аналізу і обробки інформації, МЕМ і вбудовані системи;
- сенсорні системи зв'язку, які включають в себе персональні мережі бездротового доступу і мережі, які мають слабкі канали зв'язку.
- LAN мережі, які взаємодіють на основі IP. Найчастіше зустрічається використання стандартів 802.11 WiFi
- шлюзи і маршрутизатори, які забезпечують взаємодію всієї мережі;
- глобальні обчислювальні мережі, до яких відносяться оператори стільникового зв'язку, провайдери LPWAN і супутникових мереж;
- хмара, яка виступає в якості постачальника послуг, виробників баз даних, обробки та аналітики даних.
- безпека теж є компонентом системи IoT і включає в себе повне об'єднання архітектури інтернету речей, яка повинна гарантувати справжність, цілісність та інфомаційну безпеку.

Еталонна модель Інтернету речей

На сьогоднішній день ще не було підтверджених і стандартизованих варіантів моделей інтернету речей, проте компанія Cisco запропонувала свою еталонну модель, яка складається з семи рівнів (рис. 1.4). Такий підхід до моделі дозволяє розбити процеси на прості і складні, які відбуваються на кожному рівні.

В цій моделі присутній опис того, як досягнути простоти через вирішення завдань на кожному рівні, що надалі допомагає з такими важливими етапами в інтернеті речей, як масштабованість і забезпечення підтримки. Вона описує і визначає функції, які потрібні для роботи інтернету речей. Ця модель відображає рівень абстракції, після чого зіставляє її функціональні інтерфейси для то-

го, щоб описати систему IoT. Архітектура IoT дозволяє обробляти дані грунтуючись на контексті, створювати і управляти інформацією, що дозволяє отримувати гарні рішення для інтернету речей.

Рівні	Характеристики
Фізичні пристрої та контролери	Пристрої кінцевої точки, експоненціальне зростання, різноманітні
Зв'язок	Надійність, своєчасна передача, комутація та маршрутизація
Туманні обчислення	Перетворення даних в інформацію, яка може бути ефективною
Накопичення даних	Зберігання даних, постійні та перехідні дані
Абстракція даних	Семантика даних, цілісність даних до програми, стандартизація даних
Додатки	Значущі інтерпретації та дії даних
Співробітництво і процеси	Люди, процеси, розширення можливостей та співпраця

Рис 1.4. Еталонна модель IoT

Інтернету речей для проектування необхідно використовувати протоколи зв'язку і інфраструктуру. Рівень 3 називається туманними обчислення, головними функціями якого є перетворення даних і виконання аналітики на рівні даних. Для отримання цих даних, від яких відбуваються наші подальші дії, виконується обробка інформації.

Перші три рівні моделі пов'язані з даними в русі, в той час як більш високі пов'язані з інформацією, яку отримують. Постійна обробка даних в туманних

обчисленнях може виконуватися в реальному часі. При такому підході підвищується рівень цінностей, де процеси і люди виконують дії над системою IoT.

1.4 Висновки до першого розділу

IoT у наш час досить сильно трансформувався і тепер це вважається не тільки мережею об'єднання різних речей, але і перетворенням в цілу парадигму, де необхідно постійне надання різних рішень для інтеграцій та зв'язку, потрібен постійний розрахунок споживання даних та проведення аналізу пристроїв.

В цій концепції в першу чергу починає виділятися сумісність, інтеграція і підключення для безлічі гібридних мереж інтернету речей.

В першому розділі було акцентовано увагу на таких завданнях:

- визначення основних компонентів IoT;
- огляд еталонної архітектури інтернету речей;
- огляд SOA архітектури;
- огляд еталонної моделі системи IoT.

РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ТА ОСОБЛИВОСТІ РІВНІВ АРХІТЕКТУРИ

2.1 Сучасні проблеми інформаційної безпеки

Вхід до інфраструктури інтернету речей та персональних даних можна отримати завдяки майже кожному підключеному пристрою IoT. Ризики, що пов`язані з інтернетом речей виходять на новий рівень через сумісність, програми та автономне прийняття рішень, тому що з`являються різні лазівки в безпеці та потенційні вразливості, завдяки чому питання безпеки та конфіденційності даних мають дуже важливу роль (рис. 2.1).

Рис. 2.1. Проблеми безпеки IoT

Об'єднання мобільних мереж, соціальних мереж, Інтернету, різних розумних об'єктів, вважається інтернетом речей, де надають користувачам різні послуги або додатки (рис.2.2).

Безпека на різних рівнях безпосередньо впливає на успіх IoT систем, так як це підвищує безпеку взаємодії об'єктів, надійність і сумісність. Інтенет речей дійшов до того рівня, коли може з'єднати різні простори (цифровий та фізичний простір, наприклад), де різні датчики взаємодіють з фізичним простором. Ці датчики вже повністю використовуються практично у всьому, від якихось іграшок до систем охорони здоров'я, промислового сегмента, що створює приклад того як різного роду уразливості цифрового світу починають діяти на наш реальний світ.

Система буде вважатися успішною тільки якщо вона може надати гарантії безпеки від вразливостей. Успіх додатків Інтернету речей та інфраструктури Інтернету речей багато в чому залежить від гарантії безпеки і уразливості.

- Вимоги до безпеки в IoT

Інтернет - це велика кількість нових інструментів, які вбудовані в організацію або навіть у системі. Всі підключені пристрої можуть бути потенційним входом до Інтернет-інфраструктури або особистих даних. Дані з таких пристроїв можуть бути проаналізовані, після чого будуть використані. Аналіз цих даних дозволяє створювати невидимі посилання, які можуть бути спрямовані на конфіденційність окремих осіб або організацій.

Проблеми безпеки та конфіденційності є дуже важливими, але потенційні ризики об'єктів прийдуть на новий рівень, оскільки сумісність, гібридні програми та незалежне прийняття рішень створює складність, прогалини безпеки та потенційні вразливості.

Ризики захисту даних виникають у IT, тому що складність може створити високу вразливість у зв'язку з службами. В інтернеті речей, більша частина інформації, пов'язана з нашими особистими даними, такими як дата народження, місце розташування, бюджет тощо. Ризики, які використовують всі набори даних складають один із аспектів проблем великих даних. Інтернет речей повинен

бути реалізований законним, етичним, соціально та політично прийнятним шляхом, з урахуванням юридичних проблем, систематичних підходів, технічних та ділових проблем.

Безпека була великою проблемою, але те, що є найважливішими питаннями безпеки даних та конфіденційності ще не чітко визначені. Безпека даних та конфіденційні проблеми не є новими для інтернету речей, бо подібні проблеми були вирішені з перших днів RFID.

Державний департамент повинен був змінити RFID-мітки, хоча нове покоління є більш безпечним, тому що ризики, пов'язані з інтернетом речей зростуть на новий рівень, оскільки сумісність гібридних додатків та вразливості автономної безпеки починає здійснювати комплексне прийняття рішень. Нижче наведено діаграму оцінки кількості підключених IoT пристроїв (рис. 2.2).

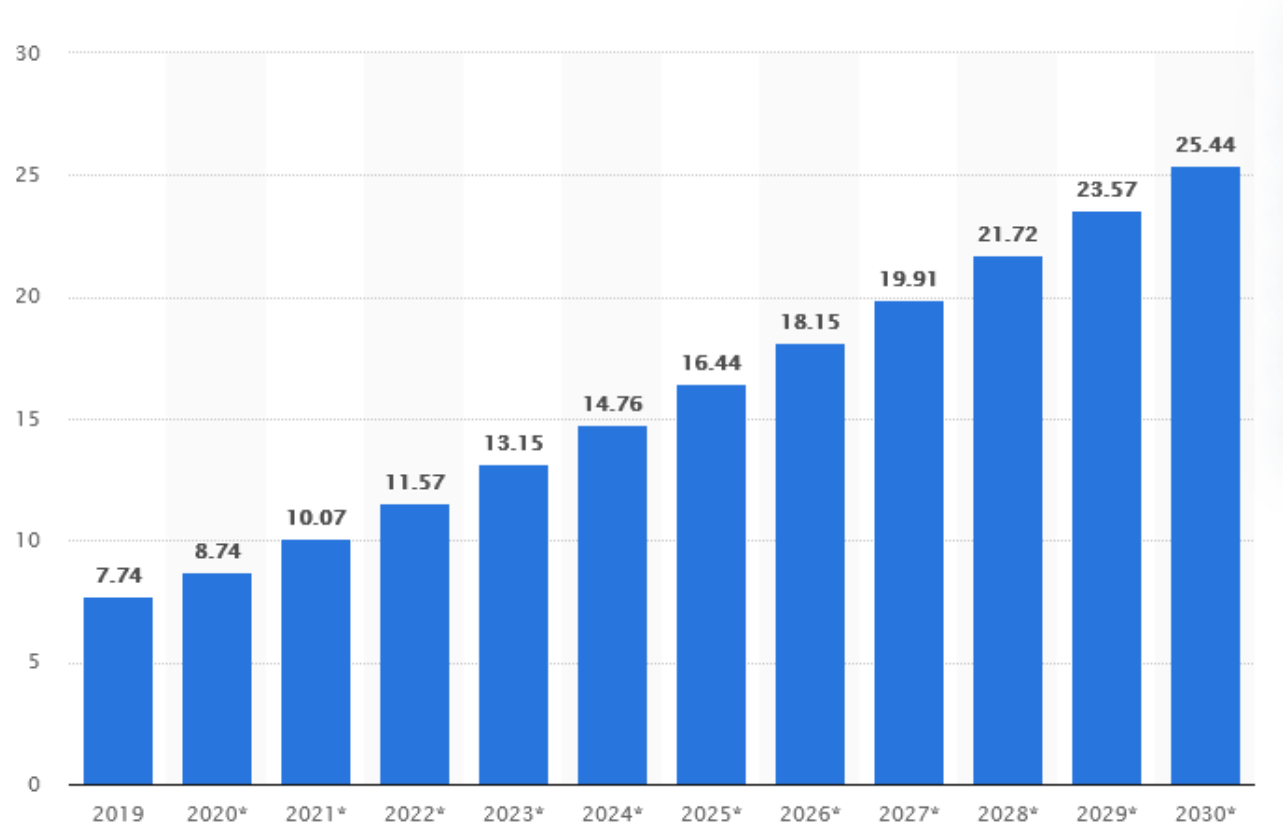

Рис 2.2. Діаграма оцінки кількості підключених IoT пристроїв по всьому світу з 2019 до 2030 року за даними сайта statista.com

2.1.1 Питання безпеки інтернету речей

На рис. 2.3 відображені вимоги до безпеки системи, що складається з 6 основних критеріїв:

- критерій конфіденційності (1) - дані, захищені уповноваженими;
- критерій цілісності(2) - дані надійні;
- критерій доступності(3) - дані доступні, коли і де це потрібно;
- критерій безвідмовності(4) - послуга забезпечує надійний аудиторський шлях;
- критерій достовірності(5) - компоненти можуть підтвердити свою ідентичність;
- критерій секретності(6) - служба автоматично не бачить дані клієнтів.

Рис 2.3. Вимоги безпеки IoT

Ризики захисту даних виникають, коли об`єкти в інтернеті речей збирають та узагальнюють фрагменти, пов'язані з даними. Особиста інформація перетворюється через зіставлення певної кількості точок, тому що місце, час, періодичність є контекстом для перегляду подій. Це один із аспектів виклику ве-

ликих даних, і фахівці з безпеки повинні забезпечити, щоб вони продумали потенційні ризики конфіденційності, пов’язані з усім набором даних. Основні проблеми безпеки в сценарії IoT включають конфіденційність даних, секретність та довіру.

Конфіденційність даних:

- недостатня аутентифікація / достовірність;
- небезпечні інтерфейси (Інтернет, мобільний телефон тощо);
- відсутність трансортного шифрування;
- збереження конфіденційності;
- управління доступом.

Секретність:

- секретність, захист даних та управління ризиками інформаційного забезпечення ;
- секретність за замовчуванням ;
- політика конфіденційності ;
- відстеження / профілювання / незаконна обробка.

Довіра:

- система управління особистості ;
- небезпечне програмне забезпечення / прошивка ;
- для забезпечення безперервності та доступності послуг ;
- виконання шкідливих атак на пристрої та системи інтернету речей;
- втрата перевірки користувача / складність у прийнятті решінь.

Для того, щоб продемонструвати вимоги до безпеки в Інтернеті речі, ми моделюємо IOT архітектуру, яка складається з чотирьох рівнів: сенсорний рівень, мережевий рівень, рівень служб та рівень інтерфейсів.

Кожен рівень може забезпечити адекватне управління безпекою, такі як контроль доступу, інструменти автентифікації, цілісність даних та конфіденційність, наявність та можливість захисту інструментів IOT для вірусів та атак. На рис. 2.4 наведено узагальнені та найбільш важливі проблеми безпеки в IoT.

Сучасні виробничі об’єкти та смарт-міста, які з’єднані в єдину платформу в першу чергу вимагають створення оптимальної архітектури безпеки пристроїв в інтернеті речей. Створювана безпека повинна відстежувати кожен підключений до мережі пристрій окремо, попереджати про можливий зловмисний доступ, або захищати чи відключити пристрої в міру необхідності та загрози. Тому, вкрай важливий процес для інтернету речей - це розробка і використання стандартів.

В області стандартизації, на всіх рівнях інтернету речей, ведеться найактивніша робота. В наш час розробкою стандартів займається деякі великі організації: IEEE (Institute of Electrical and Electronics Engineers) і ISO / IEC (International Electrotechnical Commission).

2.1.2 Забезпечення безпеки на сенсорному рівні

Цей рівень характеризується як перехрестя людей, місць і речей. Це може бути прості інструменти, наприклад термометри, лампочки або складні пристрої, такі як медичні пристрої та виробниче обладнання.

Щоб забезпечити повну реалізацію безпеки, потрібно, щоб вона була розроблена та використана у пристроях. Це означає, що інструменти IoT повинні мати можливість підтвердити свою ідентичність, щоб зберегти довіру, підписання та шифрування для цілісності даних та обмеження локально збережених даних для захисту ваших особистих даних.

Модель безпеки пристроїв повинна бути дуже суворою для того, щоб запобігти несанкціоноване використанням, але досить гнучкою, щоб тимчасово підтримувати безпечну, спеціальну взаємодію між людьми та іншими пристроями.

Проблеми безпеки	Рівень інтерфейсів	Рівень служб	Мережевий рівень	Сенсорний рівень
Небезпечний веб-інтерфейс	+	+	+	
Недостатня автентифікація авторизація	+	+	+	+
Небезпечні мережеві послуги		+	+	
Відсутність транспортного шифрування		+	+	
Проблеми конфіденційності		+	+	+
Небезпечний хмарний інтерфейс	+			
Небезпечний мобільний інтерфейс	+		+	+
Небезпечність конфігурації	+	+	+	
Небезпечне програмне забезпечення / прошивка	+		+	
Погана фізична безпека			+	+

Рис 2.4. Найчастіші вразливості в інтернеті речей на всіх рівнях архітектури

Пристрої інтернету речей будуть існувати скрізь у навколишньому середовищі, в якості інструментів IoT буде поставлена проблема про створення системи захисту від несанкціонованого доступу до пристроїв. Це зменшує можливість отримання конфіденційної інформації для перснальних даних, криптографічних ключів та облікових даних. Пристрої IoT мають довгий термін служби, тому треба включити оновлення ПО, щоб уникнути різних експлойтів після випуску певних пристроїв.

2.1.3 Безпека мережевого рівня

Цей рівень представляє зв'язок та обмін повідомленнями між речами та хмарними службами. Зв'язок в Інтернеті, як правило, пов'язано з поєднанням приватних та громадських мереж, тому зрозуміло, що безпека стає важливою. Цей рівень надає найбільшої ясності про розуміння безпеки інтернета речей, бо технологія, як шифрування TLS / SSL, ідеально підходить для вирішення проблеми.

Основна складність виникає при розгляді проблем криптографії на пристроях з обмеженими ресурсами, тобто 8-бітових мікроконтролерах з обмеженою оперативною пам'яттю. Наприклад, Arduino Uno займає до 3 хв для шифрування тестового корисного навантаження при використанні 1024-бітових ключів RSA, однак алгоритм цифрового підпису еліптичної кривої зі схожою довжиною ключа RSA може зашифрувати те саме корисне навантаження за 0,3 с. Це означає, що виробники пристроїв не можуть використовувати обмеження ресурсів як привід, щоб уникнути безпеки своїх продуктів.

2.1.4 Постановка задачі безпеки на рівні служб

Цей рівень представляє собою систему управління IOT та несе відповідальність за вбудовування пристроїв і користувачів, політик та правил та організацій автоматизації на різних пристроях. Досягнення високого контролю доступу для управління ідентифікацією різних пристроїв і користувачів та дії які мають дозвіл та є критично важливими на цьому рівні.

Для того, щоб досягти відшкодування, важливо вести аудиторський слід змін для всіх користувачів та пристроїв, щоб неможливо було спростувати дії, вжиті в системі. Ці дані моніторингу також можуть бути використані для виявлення потенційно скомпрометованих пристроїв при виявленні аномальної поведінки. Аналіз великих даних сукупних даних, створених IOT, часто може бути призначений найціннішим аспектом інтернету речей.

Підтримка конфіденційності також є головним пріоритет державних установ, коли Федеральна торгова комісія (FTC) та Агентство Європейського Союзу випускає відповідні інструкції щодо мережевої та інформаційної безпеки

(ENISA) для Захист IoT. Це включає в себе захищені вимоги безпеки, таких як: забезпечення чіткого сповіщення про використання даних, де існує видимість про чіткий контроль над даними, надсилання до хмарної служби, зберігаючи дані клієнтів, що зберігаються в хмарній службі, відокремленими та / або зашифрованими. за допомогою ключів, наданих замовником, і при аналізі сукупних даних між клієнтами дані повинні бути анонімізовані.

2.1.5 Безпеки рівня інтерфейсів

Велика кількість проблем так само існує на рівні інтерфейсів, де потрібно надати забезпечення безпеки IoT, враховуючи що проблеми кожного рівня унікальні на кожному рівні. В першу чергу, необхідно впроваджувати надійну безпеку в пристроїв інтернету речей. Навіть невелікі інструменти з обмеженими ресурсами також повинні буті реалізовані для підтримки конфіденційності, цілісності та Довірі при обміні данимі в мережі. Нарешті, існує баланс між конфіденційністю споживачів та конфіденційності бізнесу, а також розуміння значення велічезної кількості даних, створених IoT.

2.2 Моніторинг проблем безпеки даних та пристроїв інтернету речей

Переваги та можливості для нових технологій швидко ввійдуть у своє життя, без сумніву. Концепція інтернету речей також застосовується до таких нововведень та у більш широкому сенсі відноситься до інтелектуального міста, яке повинно бути приділено проблемам поширення таких технологій разом з усіма очевидними перевагами. Одна така проблема полягає в тому, що виробники інтернет-компонентів не думають, що потрібно давати належну увагу до питань інформаційної безпеки, пов`язаних з повсякденним використанням, окремих компонентів системи та всіх апаратних програмних пакетів. З випуском великої кількості виробників, що мають кінцеве, комунікаційне та контрольне обладнанням, питанням суміжності компонентів складної структури та можливість їх роботи без ризику несанкціонованого доступу, витоку або доставки системи циркулюючої інформації.

Речі представляють собою ряд інструментів, що перевищує кількість ПК, ноутбуків та смартфонів за межами захищеного корпоративного краю. Не зважаючи на це, питання безпеки вже багато часу залишається невирішеною проблемою, але за останні роки можна побачити більшу зацікавленість в цій сфері IoT.

У дослідженні Microsoft 2019 року, 19% експертів відзначили, що безпека одна з найважливіших проблем, яку потрібно вирішувати. Зараз існую чотири головних проблеми, а саме пошук певних IP-рішень, виділення нових коштів на спеціалізованих робітників, недоліки в кількості знань на дану тематику і складність в пошуку та виборі правильних рішень мають певні наслідки у створенні та порушенні IP-систем безпеки.

Що стосується питань безпеки речей, експерти Microsoft, що проводили досліди, розмістили питання безпеки як зображено на рис. 2.5.

Більшу частину часу хвилює безпеку мережевого рівня, з числом респондентів 43%

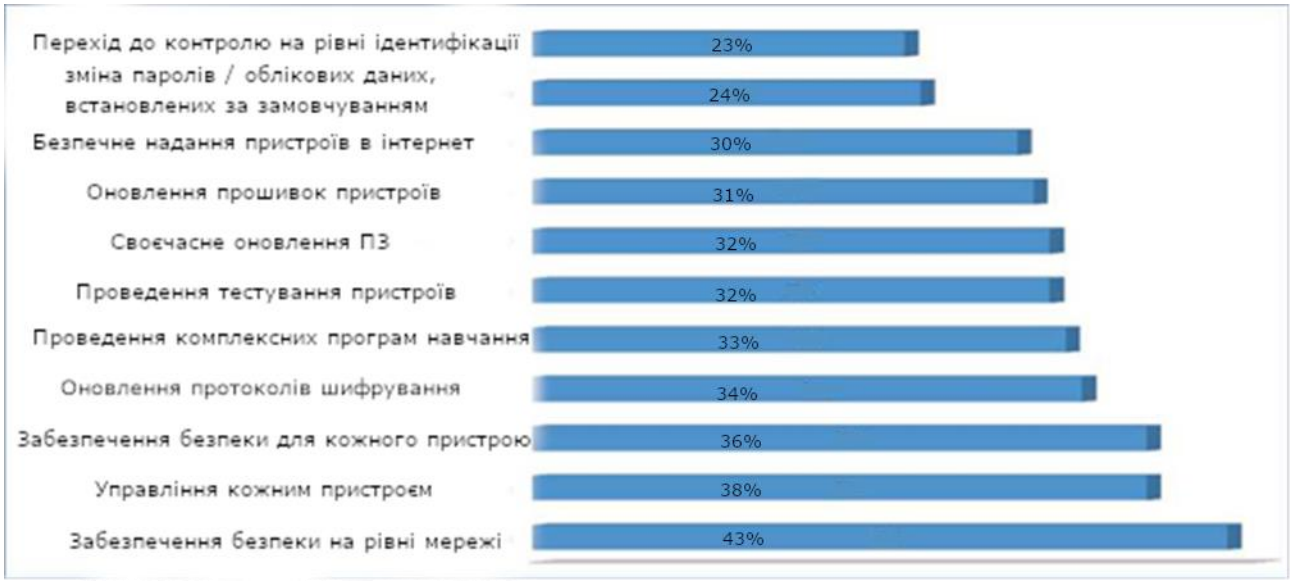

Рис 2.5. Актуальність проблем безпеки згідно дослідження експертів

Багато недостатньо захищених пристроїв полегшує атаки DDoS, де різні пристрої можуть бути використані для атаки корпоративних систем. Останні часто працює з паролем "за замовчуванням". Ця уразливість викликала Mirai ботнети.

Сила упорядкованої атаки Mirai на веб-сайт журналіста B.Krebs, який створив його для розслідування продажу послуги бонтнетів, пік якохї досяг 665 Гбіт/с , де використовувались лиже інтелектуальні відокамери.

Таким чином можна підійти до створення мети дослідження, що буде фіксуватись на загрозах безпеки IoT, результатом якої стане перелік рекомендацій для забезпечення системи інтернету речей.

Сьогодні ми перебуваємо в світі, де пристрої, підключені до IOT,перевищили кількість людей. Ці інструменти можуть бути інтелектуальний годинник або відстеження певних даних через RFID зчитувач. Обмін через різні мережеві та хмарні платформи , що пов`язані з інтернетом речей відбувається через різні пристрої, що підключені до цієї системи.

Інформацію, що можна отримати в реальному часі стає умовою трансформування усієї сфери IoT. Інтернет речей викликає багато позитивних змін, які відображаються у сферах охорони праці та здоров'я, у сфері бізнесу. Він сприяє покращенню показників виробництва та вирішення глобальних екологічних та гуманітарних проблем. Цей приклад технології спрямован на використання великої кількості низької енергії для обчислення та енергії з точки зору обчислювальних та енергетичних інструментів для подібних простих завдань. Така технологія застосовується, наприклад в розумному будинку чи розумному місті.

Сферою застосування також може бути інші розподілені системи (геоінформаційні та інші).У цих випадках управління для різних пристроїв відрізняється, бо при використанні комп'ютера або іншого розумного пристрою управління потребує людини , але при використанні M2M участь людини становиться зовсім непотрібна.

Останні прогнози, які стосуються сфери інтернету речей підтверджують те, що до кінця 2021 року інтеграція між величезною кількістю пристроїв і IoT системами перевищить кордон в 16 мільярдів, що в два рази більше населення нашої планети. Безліч галузей виробництва і життєзабезпечення (обумовлених колосальним поширенням в усьому світі даної технології) стурбоване безпекою сучасної системи інтернету речей, адже тепер проблема безпеки є не тільки у

кінцевих користувачів, що використовують цю технологію, але і наданням безпеки величезним потоком даних, що виникає при M2M взаємодії.

Виробники усіх компонентів інтернету речей на даний момент ігнорують безпеку в системах, які вони виробляють. Однією з таких причин відмови і ігнорування впровадження систем безпеки в свої компоненти IoT полягає в великих розрахункових витратах, що несе за собою додаткові витрати на електроенергію і призводить до шкоди всі системі інтернету речей, адже автономність роботи компонентів такої системи має високий рівень важливості, наприклад акумуляторні батареї. Більш того, якщо застосувати підхід з безпекою в IoT системах, це безпосередньо підвищить ціну всіх рішень на ринку. Після розгляду безлічі проблем, можна спробувати сформувати основні загрози присутні в IoT.

При використанні пристроїв, часто відображається великий спектр проблем, які змусили безліч дослідників в сфері Інформаційної безпеки серйозно зайнятися вирішенням проблем безпеки. Порушення наскрізного принципу інформаційної безпеки - перше що помітили експерти в цій галузі, адже ці умови були рекомендовані для всіх систем інтернету речей та інших послуг.

Принцип наскрізної ІБ різних пристроїв і послуг в сфері інтернету речей повинен бути присутнім на ранніх етапах створення продукту, а після отримання готового пристрою необхідно забезпечити підтримку ІБ до останніх днів роботи таких "речей" . Ряд проблем виникають між розробниками і клієнтами послуг інтернету речей були помічені групою дослідників в HPE. Були відзначені такі проблеми, пов'язані з безпекою:

- Ігнорування вимог безпеки з боку власників пристроїв

Однією з найпомітніших і простих проблем стала нездатність власника пристрою замінити пароль після покупки і запуску пристрою IoT. В більшості своїй заводській пароль часто дублюється, що ставати великий лазівкою для зловмисника по експлуатування пристрою, саме тому власникам пристроїв радять з більшою обережністю ставитися до захисту пристроїв, адже безліч "речей" не мають системи безпеки, тому легко можуть змусити пристрої стати

шлюзом для вторгнення в мережу, що в кінцевому рахунку призводить до великої пошкоди.

- Проблеми з шифруванням трафіку

В ході проведеного HPE дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротової трафік. Дослідження показало, що в 70% випадках трафік, який проходь між різними пристроями IoT систем повністю незахищений і не має шифрування

- Безліч xss вразливостей в веб-додатках пристроїв

Велика частина веб-додатків (60%) IoT пристроїв має різні небезпеки, пов'язані з міжсайтовий скріптингом (XSS) і неправильною організацією доступу.

- Безліч паролів мають малу стійкість
- 90% різної інформації IoT пристрої збирають без відома власника
- Велика кількість вразливостей

При детальному розборі різних типів пристроїв інтернету речей, дослідники підрахували, що різні пристрої інтернету речей мають більше 20 вразливостей.

Висновок, який отримала IoT система виявився очевидним - повна відсутність безпеки всіх компонетов інтернету речей. Нижче наведені сумарні висновки щодо встановлення типів вразливостей.

- живлення пристроїв;
- проблеми сертифікації та стандартизації IoT архітектур і протоколів інформаційної безпеки;
- проблеми аутентифікації порушення принципу наскрізної ІБ, розробник не підтримують свій продукт;
- відсутність нормального оновлення ПЗ і ОС, що підвищує ризики пов'язані з безпеку;
- нездатність пристроїв до захисту, у разі чого підвищується шанс успішної атаки зловмисника на мережу;
- використання незахищеної хмарної інфраструктури.

На початку 2019 року, інша дослідницька група, за допомогою ресурсів, призначених як приманка для зловмисника (хоніпот) отримали 276 тисяч унікальних і 105 мільйонів не унікальних атак. Як помітили дослідники, кількість атак збільшилася в порівнянні з 2018 роком приблизно в 7 разів. На даний момент все ще немає рішень для боротьби з величезний безліччю проблем безпеки, тому злочинці створюють багато ботнетів.

Кількість комп'ютерних атак швидко збільшується, оскільки користувачі, різні підприємства беруть участь у покупці пристроїв, наприклад, маршрутизатори або камери та інші, але не піклуються про захист від крадіжки. Комп'ютерні зловмисники використовують різни типи атак. Вони збирають багато заражених пристроїв із різних мереж для проведення DDoS атак або створення власних проксі-серверів для інших шкідливих дій (рис. 2.6).

		Доступні пристрої					
		1%	10%	25%	50%	75%	100%
Використання пристроїв	1%	36.28	362.78	906.96	1813.89	2720.83	3.627.78
	10%	362.78	3.627.78	9069.44	18138.89	27208.33	36277.77
	25%	906.96	9069.44	22673.61	45347.21	68020.82	90694.43
	50%	1813.89	18138.89	45347.21	90694.43	136041.64	181888.28
	75%	2720.83	27208.33	68020.82	136041.64	204062.46	272083.28
	100%	3.627.78	36277.77	90694.43	181888.28	272083.28	362777.71

Рис. 2.6 Ширина DDoS – атаки

Більшість атак в своєму роді досить потайливі, тому можливість помітити таку атаку користувачем дуже мала, враховуючи той факт, що IoT атаки не вдають із себе складні і комплексні системи. Слід зазначити, що велику частку від усіх атак приймає на себе сімейство шкідливого ПО Mirai, суть яких полягає у використанні різних програм, які намагаються знайти вразливе місце в додатку і в разі успіху пристрій вдається інфікувати. Ботнет, після інфікування пристрою, використовує застосовані експлойти для подальшого управління на ним. Наступну велику частку від усіх атак прийняв на себе троян Nyadrop, з відсотковою часткою від усіх атак - 38%. Цей троян використовує метод брутфорса в

своїх атаках. Ще один ботнет, який привернув до себе увагу називаєтья Gafgyt, його відсотковою часткою від усіх атак було 2% .

Завдяки дослідженням експертів в області ІБ, вдалося скласти порівняльний аналіз між різними країнами і відсотком атак на них в 2019 і 2018 році (рис. 2.7).

1 половина 2018		1 половина 2019	
Бразилія	28%	Китай	30%
Китай	14%	Бразилія	19%
Японія	11%	Єгипет	12%
США	5%	Росія	11%
Греція	5%	США	8%
Туреччина	4%	В'єтнам	4%
Мексика	4%	Індія	4%
Росія	3%	Греція	4%
Південна Корея	3%	Південна Корея	4%
Італія	2%	Японія	4%

Рис. 2.7. Країни та процент атак на них

Можна побачити, що найбільша кількість атак в 2018 році припало на Бразилію, Китай і Японію, з часткою від усіх атак 28%, 14%, 11% відповідно. В 2019 ситуація трохи змінилася, і найбільш кількість атак довелося на Китай, Бразилію і Єгипет (30%, 19%, 12%).

Нижче буде наведено список різних технологій (атак), на підставі якого будуть створені пропозиції щодо посилення безпеки.

- Технологія «Amplification», яка використовує LDAP і TCP протоколи, виробляє свою атаку за допомогою відправки на сервер безлічі повідомлень, які в кінцевому рахунку надходять до веб-сайту.
- Для розподіленої мережі частою атакою виступає зміна інформації маршрута, же вузли мережі є маршрутизаторами, які здатні змінювати собі свої маршрути, тим самим збільшуючи час доставки пакета.
- Загроза, в якій головною метою є часткове видалення пакетів називається вибіркової розсилкою. Такий тип атаки залишає слід на вузлі мережі і проводить з ним подальші дії. Якщо до вибіркової розсилки, яка фокусується на вузлі, додати різні атаки, головною метою яких є збір

великого трафіку, ефект атаки підвищується, тим самим зменшуючи цілісність і доступність даних в мережі.

- Технологія «Sinkhole Attack» застосовується для збору трафіку, при отриманні доступу до конкретного вузла. При успіху, зловмисник може робити різні махінації від вузла, який він захопив.
- Технологія «Sybil attack» застосовується для створення збоїв роботи маршрутизації, агрегації данних. Ціль даної атаки - отримання контролю над вузлом і використання псевдоідентифікаторів, які допомагають робити вигляд декількох вузлів одночасно. Розподілені та бездротові мережі з рівноправними вузлами є головною ціллю цієї атаки.
- Атака червоточини націлена на захоплення декількох вузлів мережі, які в разі успіху створюють шлях, куди відправляється перехоплені пакети.
- Флуд атака з відправкою HELLO пакетів, яка відправляє безліч повідомлень в мережу, забиваючи фізичні характеристики пристроїв. Ціль атаки полягає в тому, щоб створити навантаження на різні обчислювальні потужності і інші важливі компоненти.

Формування рекомендацій щодо забезпечення безпеки для користувачів IoT системі.

- Надійне збереження паролів.

Елементарний захист, який повинен виконувати користувач - це надійне зберігання паролів, бо за замовчуванням підключенні пристрої IoT мають однотипні стандартні паролі. Вимогою в цьому випадку стає заміна стандартних паролей. Якщо немає можливості замінити пароль, то пристрій не слід підключати до інфраструктури IoT.

- Надання привілеїв

Для нормальної роботи пристроїв інтернету речей і надання безпеки необхідно надавати базовий рівень привілеїв.

- Тестування пристроїв

При підключенні пристрою до мережі необхідно провести повну перевірку на справність. Додатковим заходом безпеки буде перевірка локальних і хмарних сервісів.

- Ізоляція IoT

Для того, щоб ізолювати деякі пристрої IoT від критично важливих ресурсів в мережі, необхідно створити додаткову мережу для взаємодії різних пристроїв і використовувати міжмережевий екран.

- Керування трафіком IoT

Необхідно заблокувати весь небажаний вхідний трафік або просканувати пристрій на відкриті порти, щоб дізнатися як зловмисник може викликати компроментацію пристрою, після чого закрити їх.

- Використання шифрування

Використовувати можливість шифрування трафіку, якщо вона є.

- Купувати тільки ті продукти, оновлення яких ще підтримується.2.3

2.3 Аналіз особливостей та загроз безпеки рівнів архітектури

2.3.1 Сенсорний рівень

Пристрої, які є частиною багаторівневої мережі, де відбувається постійний збір інформації, обмін даними, роблять це за допомогою взаємодії між інтелектуальними мітками і мережами на сенсорному рівні. На цьому рівні слід виділити такі можливості для його визначення:

- зменшення кількості ресурсів і вартості при проектуванні IoT системи, де основною проблемою стають ресурси, розміри, вартість і енергоспоживання, тому що можуть використовуватися різні речі, наприклад RFID-мітки, RFID - зчитувачі та інші сенсорні пристрої;
- наступна ключова можливість - розгортання, бо кінцеві вузли інтернету речей вимагають розгортання різних сенсорних пристроїв, яке може відбуватися в різні моменти часу (поетапно, одночасно);

- інтернет речей переповнює різні безлічі пристроїв, гібридних мереж, речей, що робить таку систему повністю неоднорідною;
- бездротові сенсорні мережі, SCADA, бездротові ніздрюваті мережі та інші гібридні мережі;

Головною проблемою, на сенсорному рівні стає безпека. Стрімке зростання набуває IIoT, в якому головною метою такого інтернету речей стане підключення до промислових мереж для отримання безлічі інтелектуальних послуг, що тягне за собою нові проблеми при взаємодії з пристроями. Прикладом може вважатися визначення довіреної особи, яка взаємодіє з одними даними для аутентифікації і визначає рівень довіри до додатка.

Необхідність у прийнятті власних суджень і рішень для того, щоб знати, що в один момент часу потрібно приймати певну команду, а в інший виконати завдання, є високим пріоритетом для моделі безпеки системи інтернету речей.

Всі пристрої на сенсорному рівні описуються такими характеристиками як обмежені можливості підключення і низьке енергоспоживання. За рахунок настільки величезної кількості додатків IoT з'явилася велика кількість проблем безпеки.

На цьому рівні проблеми безпеки можна розділити на дві основні категорії:

- для кінцевого вузла в системі інтернету речей, безпека має такі вимоги: аутентифікація, конфіденційність, цілісність, доступність, фізичний захист і управління контролем доступу;
- для сенсорного рівня вимоги висуваються для аутентифікації джерела і пристроїв, їх конфіденційність, на цьому рівні необхідна автономність, доступність, цілісність.

На рис. 2.8 та 2.9 відображені найбільш часті потенційні загрози і вразливості безпеки для кінцевого вузла IoT.

Загрози безпеки	Опис
Несанкціонований доступ	Через фізичне захоплення або логічної атаки, конфіденційна інформація на кінцевих вузлах захоплюється зловмисником.
Доступність	Кінцевий вузол перестає працювати, оскільки фізично захоплений або логічно атакований
Spoofing атака	За допомогою вузла шкідливого ПО зловмисник успішно маскується під кінцеве пристрій IoT, кінцевий вузол або кінцевий шлюз шляхом фальсифікації даних.
Selfish загроза	Деякі кінцеві вузли Інтернету речей перестають працювати, щоб заощадити ресурси або пропускну здатність, щоб викликати збій мережі.
Шкідливий код	Вірус, троян і небажані повідомлення, які можуть викликати збій програмного забезпечення
DoS	Спроба зробити ресурс кінцевого вузла Інтернету речей недоступним для користувачів.
Загрози передачі	загрози передачі, такі як переривання, блокування, маніпулювання даними, підробка і т. Д.
Маршрутна атака	Атаки на шлях маршрутизації

Рис 2.8. Загрози безпеки та вразливості на кінцевому вузлі IoT

Загрози та вразливості кінцевих вузлів IoT	Кінцеві пристрої IoT	Кінцевий вузол IoT	Кінцевий шлюз IoT
Несанкціонований доступ	+	+	+
Selfish загроза		+	+
Spoofing атака		+	+
Шкідливий код	+	+	+
DoS	+	+	+
Загрози передачі		+	+
Маршрутна атака	+	+	+

Рис 2.9. Аналіз загроз безпеки та вразливостей на сенсорному рівні

2.3.2 Мережевий рівень

Мережевий рівень є невід'ємною частиною архітектури, так як дозволяє всім об'єктам IoT розпізнавати своє оточення за допомогою мережі. Цей рівень служить для передачі агрегованих даних на сенсорний та службовий рівень. Виходячи з того, що інтернет речей складається з безлічі гібридних мереж, з'являється велика кількість складнощів пов'язаних з мережевими проблемами, проблемами безпеки і зв'язком.

Для виконання завдань спільними зусиллями, необхідно враховувати, що мережевий рівень потребує управління, планування і розгортання мереж. для виконання усіх функцій, цей рівень вимагає вирішення наступних проблем:

- технології для повного контролю і управління бездротовими, мобільними і фіксованими мережами;
- підвищення ефективності мережі;
- пошук рішення проблем з вимогами до якості обслуговування (QoS)
- проблеми конфіденційності інформації;
- проблеми безпеки та конфіденційності.

У наведених вище проблемах варто акцентувати увагу на конфіденційності і безпеці людини та конфіденційності даних. Вирішення цих проблем є першочерговою важливістю, так як технології в сфері безпеки забезпечують лише базовий рівень захисту в IoT, тому існує багато невирішених завдань в цій області.

Наведемо вимоги безпеки на мережевому рівні:

- набір базових вимог до безпеки, а саме: конфіденційність даних, людини та їх захист; цілісність; аутентифікація;доступність; захист ключів;
- витік конфіденційності теж є одним з основних вимог до безпеки. Ситуації, коли різні об'єкти IoT знаходяться в легкодоступних, ненадійних місцях і можуть створювати проблеми розкриття інформації при фізичному

контакті зловмисника з об'єктом IoT системи. Прикладом може бути ідентифікація користувача;

- цілісність і конфіденційність при передачі сигналів між різними мережами інтернету речей створюють вимоги безпеки зв'язку;
- наступною важливою вимогою вважається надмірність підключень, при якій з'являються проблеми безпеки пов'язані з DoS атаками (викликані перевантаженнями мережі) і проблема безпеки ключів (викликані високим споживанням мережевих ресурсів). Такі проблеми виникають при втраті контролю над користувачами;
- атака типу Man-In-The-Middle (MITM), при якій відбувається процес передачі повідомлень між жертвою і зловмисником шляхом створення незалежних з'єднань. Зловмисник змушує жертв повірити, що між ними існує приватне зв'язок, але в кінцевому рахунку жертви перебувають під контролем зловмисника;

Можливість запобігання створенню підроблених сигналів для неправильного використання пристроїв - теж є вимогою безпеки від підроблених мережевих повідомлень.

На рис. 2.10 та 2.11 наведені загрози безпеки та вразливості мережевого рівня.

Загрози безпеки	Опис
Порушення даних	Передача захищеної інформації в ненадійну середу
Відкритий і закритий ключ	Складається з ключів в мережах
Шкідливий код	Virus, троян і небажане повідомлення, яке може викликати збій програмного забезпечення
DoS	Спроба зробити ресурс кінцевого вузла IoT недоступним для користувачів
Загрози передачі	Загрози передачі, такі як переривання, блокування, маніпулювання даними, підробка і т. д.
Маршрутна атака	Атаки на шлях маршрутизації

Рис. 2.10. Загрози безпеки на мережевому рівні

	Витік конфіденційності	Конфіденційність	Цілісність	DoS	PKI	MITM	CSRF
Фізичний захист	+	+					+
Безпека передачі		+	+	+	+	+	+
Переповнення підключень			+	+	+		
Міжрівневе з'єднання	+	+				+	+

Рис. 2.11. Загрози безпеки та вразливості на мережевому рівні

Слід так само додати, що є проблеми, пов'язані з безпекою протоколів і мережевою інфраструктурою в системі IoT. Проблеми, які на даний момент не мають рішення, представлені нижче:

- уразливості пароля і контролю доступом, які надають доступ до аутентифікації і авторизації;
- створення зашифрованої передачі даних на мережевому рівні;

2.3.3 Рівень інтерфейсів

Концепції розумного будинку, RFID - мітки, які реалізуються за допомогою стандартних протоколів інтернету речей і службово-складових технологій, розглядаються на рівні інтерфейсів. Цей рівень має залежність тільки від програм, тому повинні бути наступні вимоги безпеки:

- завантаження і оновлення ПЗ, патчі, які необхідні для підтримки безпеки і аутентифікація адміністратора;
- цілісність, конфіденційність, аутентифікацію та авторизацію.

На рівні інтерфейсів необхідно дотримуватися наступних вимог безпеки при розробці системи:

- необхідно впроваджувати безпеку в системи IoT, де кінцеві вузли працюють без нагляду;
- необхідно звертати увагу на збір енергоефективних способів при підборі рішень для безпеки;
- необхідно приділяти належну увагу в прийнятті рішень на різні частини системи, враховуючи, що схема захисту на різних кінцевих вузлах може відрізнятися.

На рис. 2.12 та 2.13 узагальнено загрози безпеки та вразливості на рівні інтерфейсів.

Загрози безпеки	Опис
Віддалена конфігурація	Не вдалося провести налаштування на інтерфейсах
Неправильна конфігурація	Неправильна конфігурація на віддаленому кінцевому вузлі IoT, кінцевому пристрої або кінцевому шлюзі
Управління безпекою	Витік логів та ключів
Система управління	Збій системи управління

Рис 2.12. Загрози безпеки на рівні інтерфейсів

	Несанкціонований доступ	Помилка вузла	Masquerade атака	Selfish загроза	Троян, вірус, спам	Витік конфіденційності
Фізичний захист безпеки	+		+			
Антивірус, брандмауер				+		
Управління доступом	+	+	+			+
конфіденційний		+	+			+
Цілісність даних		+	+	+	+	
Наявність						
Аутентифікація	+	+	+			+
Не відмова	+	+	+			+

Рис. 2.13. Загрози безпеки та вразливості на рівні інтерфейсів

Таким чином, інтерфейсний рівень є посередником між IoT системою і різними додатками. Цей рівень надає гарантію того, що взаємодія між додатками і системою є законною.

2.3.4 Особливості рівня служб

Технологія міжрівневого ПЗ – один із основних і найважливіших інструментів, що сприяє підтримці служб і програм. Службовий рівень забезпечує цій системі ефективну, з точки зору економії, платформу, де можна використати повторно апаратні та програмні засоби. Інтернет речей залежить від середніх технічних характеристик та ілюструє діяльність, яка виконується за допомогою різних стандартів, розробленими постачальниками послуг та організаціями.

Формування загальних вимог для API, додатків і службових протоколів, враховувалися при розробці службового рівня. Такі ключові компоненти, як служби інтерграції і аналітики, служби обробки подій і аналогічні їм служби безпеки дозволяють виконувати обмін даними між службами, обмін і обробку інформації, які відповідають діям на службовому рівні.

Нижче наведено перелік служб, які виконуються на даному рівні:

- служба виявлення - компонент, який дозволяє отримати певну інформацію і послуги, шляхом пошуку ефективної інфраструктури;
- служба складання дає можливість для повноцінної взаємодії між підключеними об'єктами, де головною ідеєю є створення служб, які більше підходять за вимогами і визначаються більшим ступенем надійності;
- вміння і можливість розуміти доручення пристроїв, що надається різними службами, та розуміння довіреної інформації,
- формування управління надійністю;
- вимоги, що ставить користувач для надання взаємодії між службами, виконують службові API.

Зараз існує багато доробок, які стосуються рішень і роздумів стосовно покращення службового рівня:

- для підвищення ефективності між додатками і службовим рівнем стали використовувати архітектуру SOCRADES;
- об'єкти IoT були представлені більш низьким рівнем, де існує, наприклад, служби виявлення мережі та служби обміну даними;
- служби, які дають можливість взаємодії між додатками і іншими компонентами, так само надані на рівні служб.

Нижче буде наведено вимоги до безпеки для підбору ефективної стратегії боротьби с проблемами:

- набір основних вимог, а саме авторизація, службова аутентифікація;
- на цьому рівні необхідно збереження цілісності і дотримання захисту конфіденційності, безпеки ключів і відмовостійкість;
- витік конфіденційності є основною проблемою на цьому рівні;
- зловживання службами, наприклад використання непідписаних служб;
- кінцевий вузол IoT, який зможе визначити атаку типу masquerade;
- DoS-атака;
- захист від повторних атак;
- аналізатор трафіку і маніпулювання інформацією.

Для прийняття правильного рішення, безпека на службовому рівні повинна бути здатна захистити різні операції від загроз. На рис 2.14 показано узагальнений список загроз для безпеки.

Застосування безпеки має велике значення на цьому рівні. Існує багато стандартів, протоколів, пропрієтарних рішень, які складають конкуренцію між собою. Тут архітектура SOA повністю розкривається, тому що вона здатна підвищити рівень безпеки, але рівень служб все ще має проблеми безпеки передачі даних між різними рівнями і службами. Безпека, контроль доступу та інші складові управління безпекою служб так само потребують рішення цих проблем.

2.3.5 Міжрівневі загрози

Архітектура SOA дає можливість надавати використання інформації для всіх чотирьох рівнів, тому що це підвищує рівень сумісності між різними службами і пристроями. Представлення таких можливостей створює ряд проблем безпеки з конфіденційністю користувачів і так само їх даних, проблеми безпечного міжрівневого обміну даними і гарантія довіри.

В цій архітектурі IoT обмін інформацією між різними рівнями призводить до деяких загроз безпеки, які наведені нижче, на рис. 2.15.

Загрози безпеки	Опис
Загрози конфіденційності	Витік конфіденційності або зловмисне відстеження місцезнаходження
Зловживання службами	Послуги несанкціонованого доступу користувачів або уповноважені користувачі отримують доступ до послуг, на які немає підписки
Маскування особистості	Кінцевий пристрій IoT, вузол або шлюз маскуються зловмисником
Маніпулювання службовою інформацією	Зловмисник маніпулює інформацією в службах
Відмова	Відмова від операцій
DoS	Спроба зробити ресурс кінцевого вузла IoT недоступним для своїх користувачів
Повтор атаки	Атака повторно надсилає інформацію для підробки одержувача
Маршрутна атака	Атака на шлях маршрутизації

Рис 2.14. Загрози безпеки на рівні служб

Загрози безпеки	Опис
Витік конфіденційної інформації	Конфіденційна інформація може бути не захищена на межі різних рівнів
Підміна особистості	Особистість на різних рівнях має різні пріорітети
Конфіденційна інформація поширюється між рівнями	Конфіденційна нформація поширюється на різних шарах і спричиняє витік інформації

Рис. 2.15. Загрози безпеки між рівнями в IoT архітектурі

Методи забезпечення безпеки інтернету речей мають свої відмінності і вимоги в залежності від рівня на якому вони використовуються. Умовно рівні,

на яких вони використовуються можна розділити на 3 типи. Сенсорний рівень це першим тип, який в більшості своїй має фізичними об'єктами (сенсорами, датчиками) які в більшості своїй використовують бездротові сенсорні мережі, Bluetooth, RFID та інші методи.

Виходячи з вимог до безпеки IoT, які були визначені раніше, на цьому рівні вимогами є конфіденційність, таємність, доступність, достовірність і цілісність. На рис 2.16. зображений порівняльний аналіз можливих методів безпеки на сенсорному рівні, їх переваги та недоліки.

На мережевому рівні, де присутні мережі мобільного зв'язку та інтернет теж є свої методи безпеки. Нижче представлений малюнок методів безпеки на мережевому рівні(рис. 2.17).

Методи	Вимоги	Використання	Переваги	Недоліки
Управління ключами	1,3,5	Він використовується для забезпечення генерації ключів і поновлення алгоритмів безпеки з використанням розподілу ключів(PKI та інші)	Легкий механізм захисту	Займає багато часу при конфігуруванні
Захищені алгоритми ключів (SKA)	1,5,6,2	Для інтернету речей використовуються симетричні та асиметричні алгоритми ключів(RC5, AES та інші)	Менше споживання енергії, вартості та часу роботи вузлів завдяки симетричним алгоритмам ключів	Асиметричні алгоритми ключів споживають більше енергії та часу
Протокол безпечної маршрутизації	1,2,5	Безліч алгоритмів безпечної маршрутизації, таких як об'єднання даних, маршрутизація з декількома переходами і ключові механізми, наприклад SNEP який використовується для WSN, забезпечує багатоточкову трансляцію аутентифікації	До тих пір, поки вторгнення не виявлено, безпечна(дорога) передача даних не потрібна	Більшість таких алгоритмів потребує багато енергії та часу
IDS/IPS	Забезпечують більшість вимог безпеки	Використовується для виявлення і запобігання більшості підозрілих користувачів і атак	Використовується для виявлення і запобігання більшості підозрілих користувачів і атак.	IDS вимагає визначення політики безпеки, щоб гарантувати, що загрози та атаки обробляються відповідно до керівних принципів корпоративної політики безпеки
IPSec	1,2,5,6	Метод надає два рівня безпеки: аутентифікація і механізми шифрування, де аутентифікація використовується для визначення користувача, а другий рівень для шифрування даних RFID	Підвищує рівень безпеки для RFID даних та сигналів	споживає потужність і час

Рис. 2.16. Методи безпеки даних на рівні сенсорів

Методи	Вимоги	Використання	Переваги	Недоліки
Наскрізна автентифікація та управління ключами	1,2	Пристрої IoT мають бути автентифіковані за допомогою механізму автентифікації, PKI та наскрізного шифрування	Забезпечує наскрізну автентифікацію та шифрування	Важкий механізм безпеки
Криптографічна система	2	Використовується для перевірки передачі даних через інші вузли та виявлення будь-якої помилки в мережі	Може виявити помилку мережі та перевірити дані. Криптографія симетричного ключа споживає мало енергії та часу	Асиметрична криптографія витрачає ресурси і час
Секретність даних і цілісність	2,6	Він використовується для виявлення та контролю будь-якої помилки, якавідбувається в мережі. Цілісність даних використовує алгоритми шифрування перевірки вихідних даних, які надсилаються	використовується для перевірки вихідних даних	Витрачає багато часу

Рис. 2.17. Методи безпеки даних на мережевому рівні

2.4 Висновки до другого розділу

У другому розділі було зосереджено увагу на таких проблемах:

- Сучасні проблеми інформаційної безпеки;

- Моніторинг проблем з безпеки даних та пристроїв інтернету речей

- Визначення особливостей та порівняльній аналіз загроз безпеки на кожному рівні архітектури

При дослідженні проблем інформаційної безпеки було складено: спектр загрог IoT, дослідження вимог до безпеки інтернету речей і визначення питань безпеки на кожному рівні.

У другій частині розділу було розглянуто актуальність проблем безпеки і аналіз існуючих атак, їх принцип роботи, після чого були сформовані рекомендації по безпеці грунтуючись на тенденції атак.

Кінець розділу є дослідницької частиною, де був проведений аналіз загроз безпеки та вразливостей на кожному рівні та розглянуті способи поліпшення безпеки на різних рівнях.

РОЗДІЛ 3. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ IoT СИСТЕМИ

3.1 Постановка задачі до проектування IoT системи

При проектуванні мережі інтернету речей необхідно включати дві складові:

- фізичне проектування мережі;
- логічне проектування мережі;

Фізичне проектування мережі включає в себе пристрої IoT і протоколи. Протоколи IoT .

Для успішної взаємодії і установки зв'язку IoT пристроїв і сервера існує безліч протоколів різних рівнів, які дають можливість управляти IoT пристроями і отримувати від них команди через Інтернет (рис. 3.1-3.5).

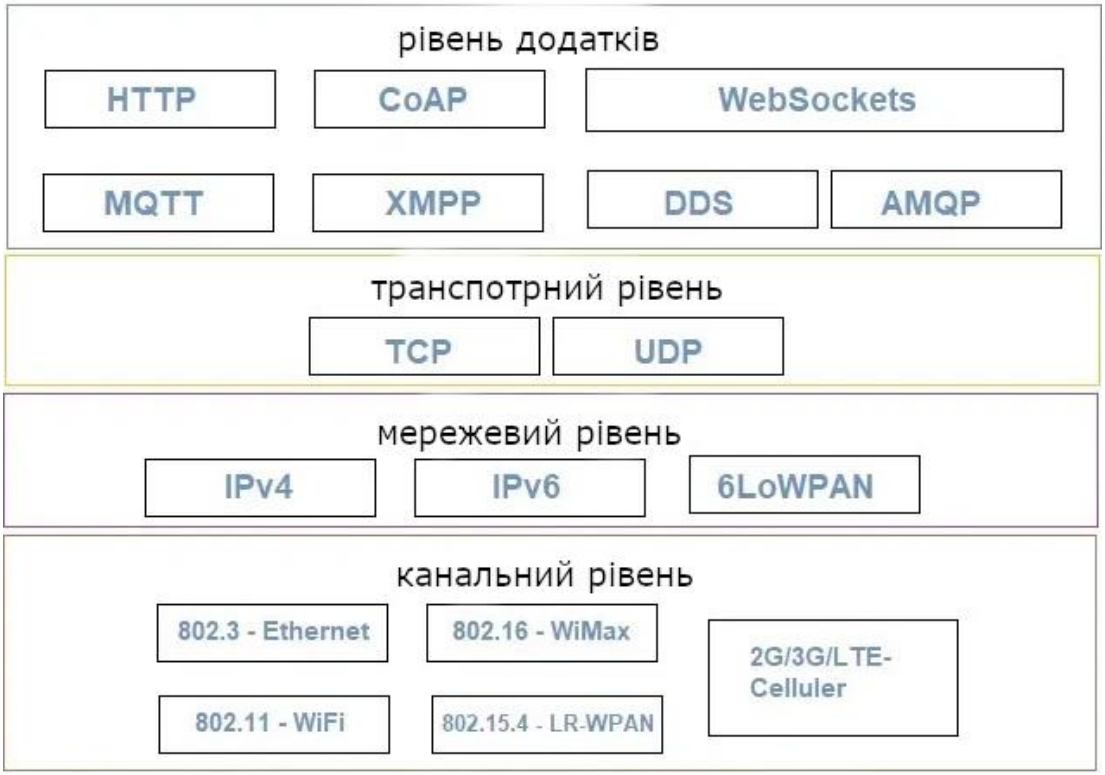

Рис 3.1. Протоколи IoT

Назва	Опис
Ethernet	Ethernet - це сукупність технологій та протоколів, які використовуються переважно в локальних мережах.
WiFi	IEEE 802.11 є частиною набору протоколів локальної мережі IEEE 802 і визначає набір протоколів управління доступом до мультимедіа (MAC) та протоколів фізичного рівня (PHY) для реалізації бездротової локальної мережі (WLAN) Wi-Fi комп'ютерного зв'язку на різних частотах, включаючи але не обмежуючись діапазонами частот 2,4 ГГц, 5 ГГц і 60 ГГц.
Wi-Max	Стандарт технології WiMAX - це стандарт для бездротових мереж метрополітену (WMAN), розроблений робочою групою № 16 IEEE 802, що спеціалізується на бездротовому широкосмуговому доступі від точки до багатоточок.
LR-WPAN	Збірник стандартів для низькошвидкісної бездротової персональної мережі. Стандарт IEEE 802.15.4 визначає рівень MAC і PHY, який використовується, але не обмежується, мережевими специфікаціями, такими як протоколи Zigbee, 6LoWPAN, Thread, WiSUN та MiWi . Стандарти забезпечують недорогий та низькошвидкісний зв'язок для пристроїв з обмеженою потужністю.
2G / 3G / 4G - мобільний зв'язок	Це різні типи телекомунікаційних поколінь. Пристрої IoT на основі цих стандартів можуть обмінюватися даними через стільникові мережі.

Рис. 3.2. Протоколи канального рівня

Назва	Опис
IPv4	Адреса Інтернет-протоколу (IP-адреса) - це числова мітка, присвоєна кожному пристрою, підключеному до комп'ютерної мережі, яка використовує Інтернет-протокол для зв'язку. IP-адреса виконує дві основні функції: ідентифікацію хоста або мережевого інтерфейсу та адресацію місцезнаходження. Інтернет-протокол версії 4 (IPv4) визначає IP-адресу як 32-розрядний номер.
IPv6	Інтернет-протокол версії 6 (IPv6) є останньою версією Інтернет-протоколу (IP), протоколу зв'язку, що забезпечує систему ідентифікації та розташування комп'ютерів у мережах та маршрутизує трафік через Інтернет.
6LoWPAN	6LoWPAN - це скорочення від IPv6 від малопотужних бездротових персональних мереж. 6LoWPAN - це назва робочої групи, яка укладена в Інтернеті IETF. 6LoWPAN - це дещо викривлене скорочення, яке поєднує останню версію Інтернет-протоколу (IPv6) та малопотужні бездротові персональні мережі (LoWPAN).

Рис. 3.3. Протоколи мережевого рівня

Назва	Опис
TCP	TCP (Transmission Control Protocol) - стандарт, який визначає, як встановити та підтримувати мережеву розмову, за допомогою якої прикладні програми можуть обмінюватися даними.
UDP	User Datagram Protocol (UDP) - це протокол транспортного рівня. UDP є частиною пакету протоколів Інтернету, який називається пакетом UDP / IP. На відміну від TCP, це ненадійний і безпровідний протокол. Отже, немає необхідності встановлювати зв'язок до передачі даних.

Рис. 3.4. Протоколи транспортного рівня

Назва	Опис
HTTP	Протокол передачі гіпертексту (HTTP) - це протокол прикладного рівня для передачі гіпермедійних документів, таких як HTML.
CoAP	Протокол обмежених додатків CoAP - це спеціалізований протокол інтернет-додатків для обмежених пристроїв, як визначено у RFC 7252. Він дозволяє пристроям здійснювати зв'язок через Інтернет.
WebSocket	Протокол WebSocket забезпечує двосторонній зв'язок між клієнтом, що запускає ненадійний код у контрольованому середовищі, із віддаленим хостом, який увійшов у зв`язок із цим кодом.
MQTT	MQTT - це протокол підключення 'машина до машини' (M2M) / 'Інтернет речей'.
XMPP	Розширюваний протокол обміну повідомленнями та присутності (XMPP) - це комунікаційний протокол для орієнтованого на повідомлення проміжного програмного забезпечення на основі XML
DDS	Служба розподілу даних (DDS) є протоколом проміжного програмного забезпечення та стандартом API для підключення, орієнтованого на дані, від Object Management Group
AMQP	Протоколи AMQP - IoT складаються з жорстких компонентів, які маршрутизують і зберігають повідомлення в операторі брокера, з набором політик для з'єднання компонентів разом.

Рис. 3.5. Протоколи рівня додатків

Логічне проектування представляє абстрактне розуміння сутностей та процесів.

Логічне проектування складається з:

- функціональних блоків IoT;
- модель зв`язку IoT;
- API зв`язку IoT.

Функціональні блоки IoT складаються з пристроїв, зв`язку, послуг, управління та додатків.

Функціональний блок пристроїв відповідає за можливості зондування, моніторингу та управління;

- Функціональний блок зв`язку відповідає за обробку зв`язку в системі IoT;
- Функціональний блок управління забезпечує різні функції управління системою інтернету речей;
- Функціональний блок безпеки відповідає за захист системи IoT;
- Функціональний блок додатків відповідає за контроль різних аспектів IoT.

Модель зв`язку IoT:

- модель запит-відповідь, в якій відбувається взаємодія між клієнтом і сервером;

- модель Push-Pull;
- модель пар.

API зв'язку IoT. Найбільш частіше використовується два API:

- API зв'язку на основі REST;
- API зв`язку на основі WebSocket.

3.2 Побудова IoT системи

IoT система має наступні пристрої:

- розумний дверний замок (3);
- датчик відкриття вікна (3);
- розумна лампа (2) ;
- датчик включення світла (3);
- базова станція, шлюз (1);

Використовуються наступні протоколи:

- на канальному рівні використовується технологія WiFI для всіх сенсорів;
- на мережевому рівні використовується IPv4 протокол;
- на транспортному рівні існує підтримка TCP та UDP протоколів;
- на рівні додатків використовуються протоколи MQTT, WebSocket.

На рис. 3.6 наведено топологію IoT системи, яка була створена за допомогою PacketTracer:

У топології видно, що підключення до мережі між усіма сенсорами в IoT системі забезпечує шлюз, який несе відповідальність за маршрутизацію даних і їх відправку. Інтернет речей ізольований і має мережу 192.168.25.0/24. В системі обрана модель запит-відповідь і API зв'язку на підставі REST і WebSocket.

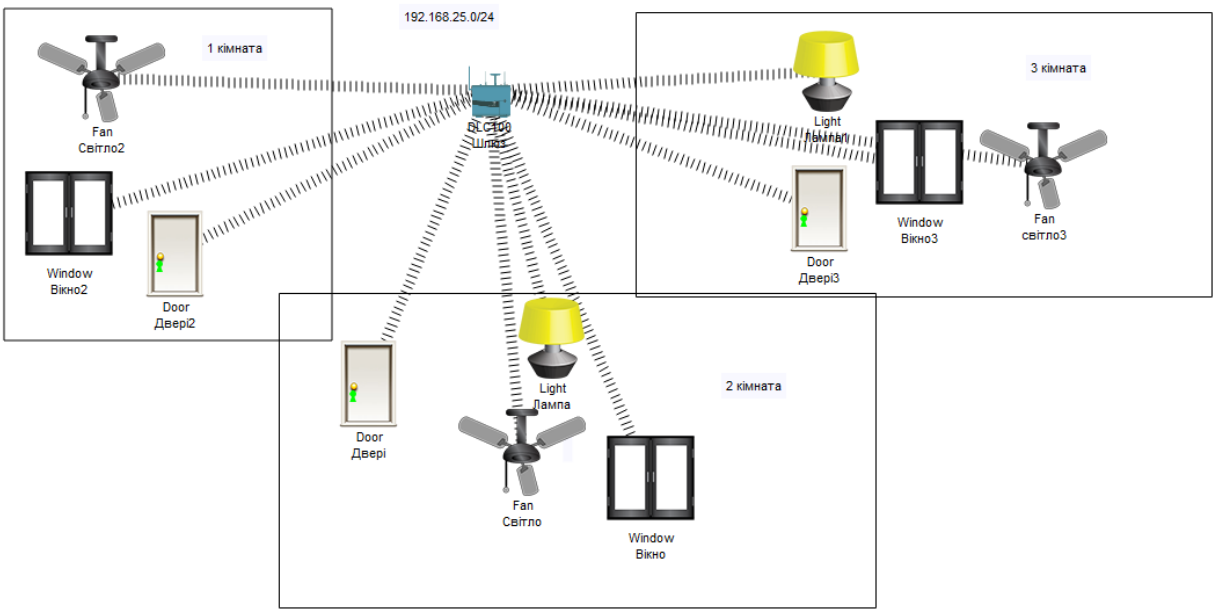

Рис 3.6. Топологія інтернету речей

3.3 Вибір методів безпеки та їх реалізація

Застосуємоо TLS/SSL аутентифікацію поверх MQTT (рис. 3.7-3.8)

Використовуємоо метод автентифікації, до якого додаємо TLS/SSL аутентифікацію. На рівні додатків, де в спроектованій системі IoT використовується протокол MQTT, додаємо SSL/TLS захист, реалізований на платформі IBM Watson IoT Platform.

Це ПО системи інтернету речей, яке створено для того, щоб поєднати сенсори з хмарою. IoT-платформи знаходяться між рівнем сенсорів та додатків. Замість датчика, ініціювати підключення до хмари буде смартфон. Після створення пристрою, завантажуємов додаток на смартфон та проходимо етап аутентифікації для підключення до платформи

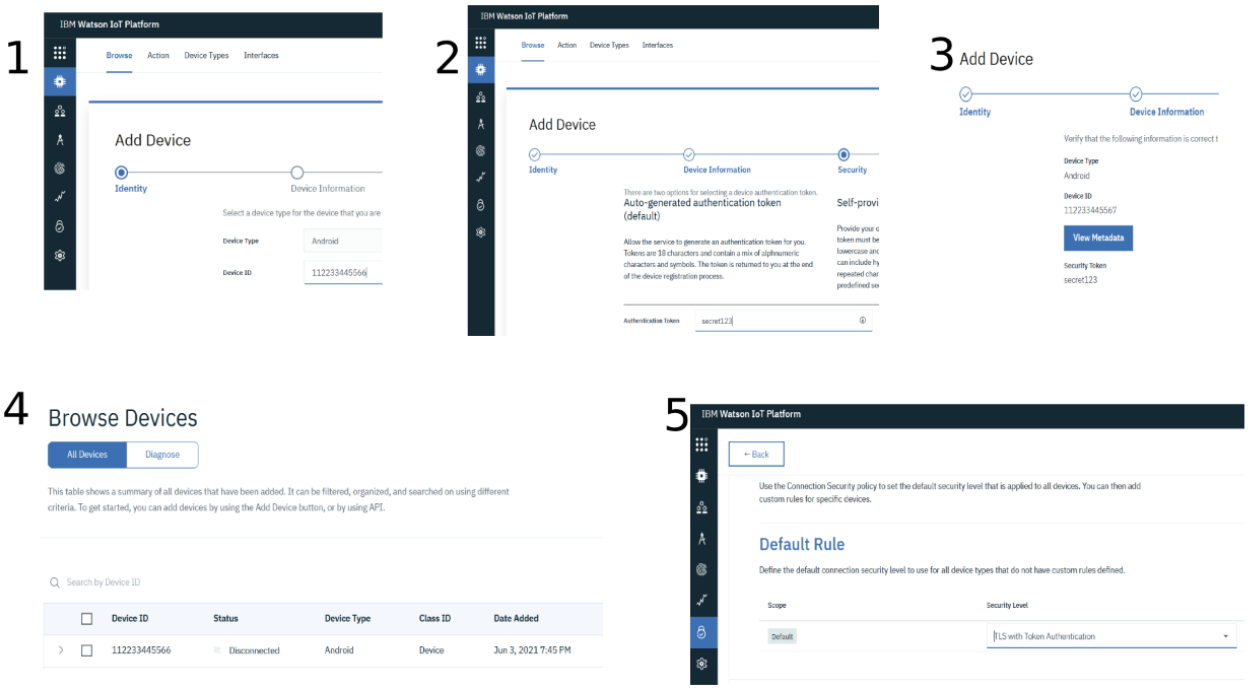

Рис. 3.7 Створення пристрою в IoT-плаформі

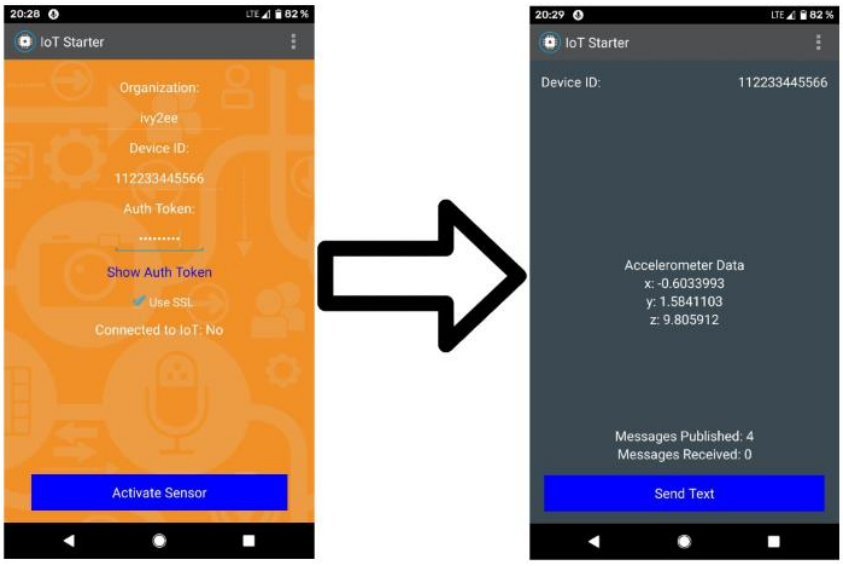

Рис. 3.8 Аутентифікація пристроя

Впровадження контролю доступу для пристроїв (рис. 3.9).

Створюємо нову роль та надаємо певні права для неї, відредагувавши права для шлюза та користувача.

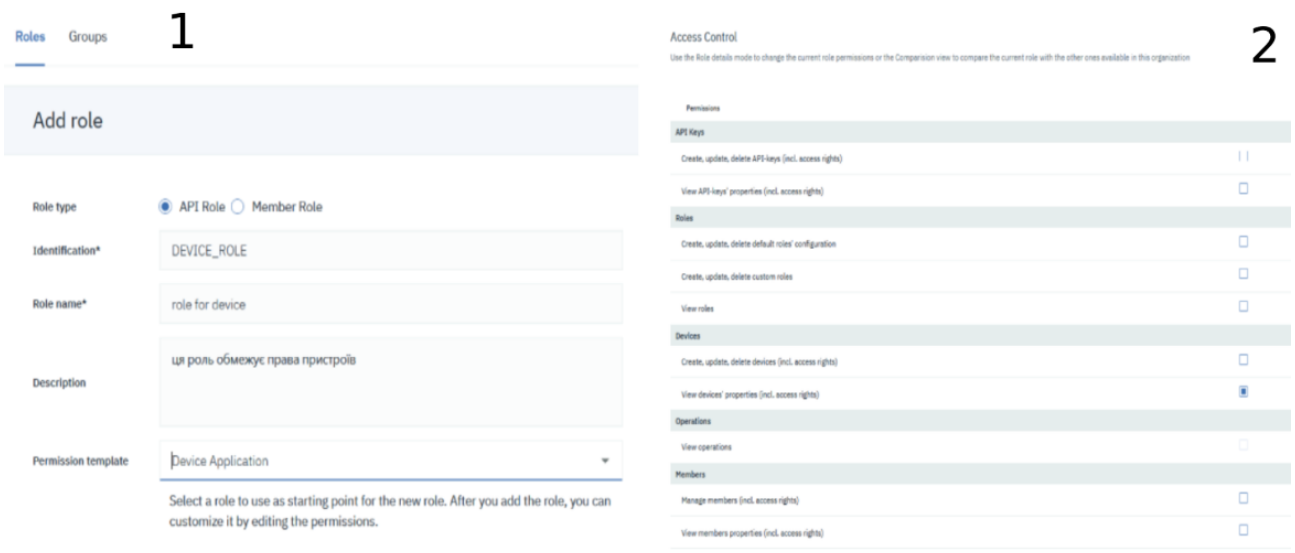

Рис. 3.9. Створення контролю доступу для пристроїв

Впровадження апаратного методу безпеки.

Для підвищення безпеки при обміні інформацією між об'єктами інтернету речей був впроваджений модуль створення ключів шифрування.

Оптимальним рішенням є TPM модуль так як має ряд затребуваних функцій (рис. 3.10):

- надає цілісність пристрою;
- може працювати в безпечному режимі для зменшення шкоди при зараженні шкідливим ПЗ;
- встановлює корінь довіри;

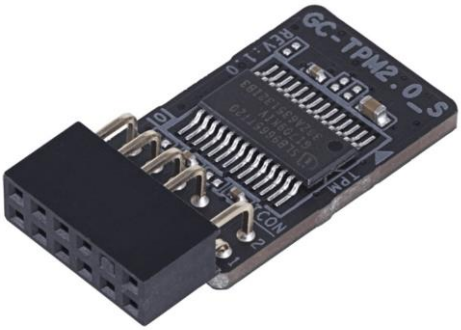

Рис. 3.10. TPM модуль

Автор виділяє такі рівні забезпечення безпеки системи інтернету речей.

Забезпечення зв'язку. Дослідження показали, що практично всі IoT системи не шифрують трафік. Тут необхідно визначити головні аспекти щодо впровадження в IoT системи:

- шифрування трафіку;
- перевірка автентичності;

Реалізація запропонованих рішень в IoT системі:

1. У проектуванні мережі для шифрування трафіку був обраний і використаний метод Еліптичної криптографії, так як він дає перевагу в швидкості в порівнянні з іншими методами на слабких чіпах.
2. У систему були впроваджений сертифікат безпеки X.509, для надання унікальної ідентифікації пристрою, щоб знати яким пристроям слід довіряти і підвищення безпеки в мережі. Перевірка справжності має важливу роль, тому що допомагає обмежити мережу від різних неперевірений пристроїв і сервісів.

Безпека пристроїв на рівні коду. Для того, щоб пристрої не стали частиною ботнету і не брали участь в інших діях, які планують зловмисники, необхідно щоб на програмному рівні пристрій виконував тільки задані йому функції, іншими словами першою необхідністю потрібно ставити створення захищеності коду IoT пристроїв.

Реалізація запропонованих рішень в IoT системі:

1. При проектуванні системи була обрана бібліотека OpenSSL для перевірки автентичності та підтвердження необхідного виконавчого коду пристрою.

Безпека при використанні пристроїв. У другому розділі був описаний ряд загроз, які нависають над кінцевими вузлами IoT, такими як шкідливе ПЗ, за допомогою компрометації пристрою і використання вразливостей.

Реалізація запропонованих рішень в IoT системі:

1. Впровадження системи розмежувань доступа. При впровадженні такої системи відбувається повне обмеження між усіма мережевими підк-

лученнями і додатками. Впровадження системи розмежувань доступу підвищило захист від різних експлойтів.

Безпека управління пристроїв. Незалежно від безпеки мережі IoT, шанс появи загрози залишається. На цьому етапі безпеки необхідно використати систему для аналітики ІБ.

Реалізація запропонованих рішень в IoT системі:

1. Впровадження аналітичної системи безпеки UBA, яка виявляє аномальну поведінку користувача. Ця система збирає різну інформацію, вибудовує модель поведінки і визначає аномальну активність.

Додаткові практики щодо поліпшення безпеки:

- Оновлення системи. Необхідно підтримувати постійні оновлення IoT пристроїв, щоб встигати вчасно встановлювати патчі від різних вразливостей. Необхідно так само виконання безпечного завантаження, яке представляє собою перевірку прошивки системи перед завантаженням системи.

- Впровадження захисного ПЗ від різного роду вірусів. В системі проектування IoT передбачена установка і використання антивірусного програмного забезпечення Symantec .

- Впровадження комплексу з проведення аудитів. Щомісяця в спроектованій системі IoT буде відбувається аудит інфраструктури мережі. Рішенням для виконання аудиту став AWS IoT Device Defender, який представляє собою сервіс по проведенню аудитів інтернету речей.

- Впровадження брандмауера для поліпшення контролю вхідного і вихідного трафіку на пристроях IoT.

- Створення надійніх та унікальніх паролів та їх постійна зміна.

- Створення ізольованої мережі для IoT. У компанії присутня ізольована мережу 192.168.25.0/24, яка підвищує складність отримання доступу до неї зловмисникам. Нижче наведено графічне зображення використаних методів безпеки для спроектованої системи IoT(рис 3.11).

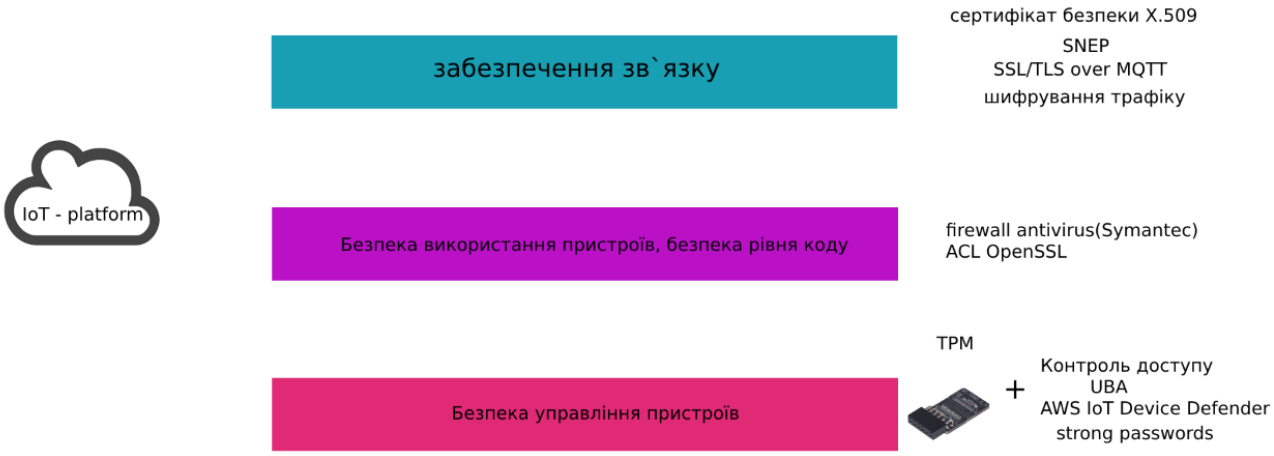

Рис. 3.11 Система методів безпеки для спроектованої системи IoT

3.4 Висновок до третього розділу

На кожну систему IoT необхідно своє комплексне рішення, так як на сьогоднішній день немає чітко сформованих умов і вимог. ІБ необхідно розглядати з різних сторін при проектуванні безпеки мережі IoT, бо в іншому випадку вона стане неефективною і будь-який зловмисник скористається слабкою стороною такої системи.

У цьому розділі увага було зосереджена на таких компонентах:

- Створення і проектування системи IoT;
- Запропонування методів безпеки в системі інтернету речей.

У свою чергу, при створенні методів безпеки мережі була складена концепція для конкретної системи IoT, в якій були запропоновані наступні можливості забезпечення інформаційної безпеки:

- Забезпечення зв`язку;
- Безпека пристроїв на рівні коду;
- Безпека, при використанні пристроїв;
- Безпека управління пристроїв.

Крім цього були запропоновані різні існуючі рішення для безпеки та додаткові практики щодо поліпшення безпеки.

Були виконані наступні завдання:

- Було визначено основні компоненти інтернету речей.
- Проведен аналіз загроз безпеки та вразливостей на кожному рівні та розглянуті способи поліпшення безпеки на різних рівнях.
- Проведено порівняльний аналіз методів безпеки IoT.
- Спроектовано систему інтернету речей та запропоновано методи безпеки для спроектованої системи інтернету речей.
- Надано рекомендації стосовно застосування методів безпеки в системі інтернету речей.

ВИСНОВКИ

Дипломна робота присвячена методам безпеки даних та пристроїв інтернету речей для побудованої системи IoT. В процесі отримані наступні результати:

1. Визначено основні компоненти інтернету речей. В процесі було розібрано еталонну архітектуру , SOA архітектуру.
2. При дослідженні проблем інформаційної безпеки було складено: спектр загроз IoT, дослідження вимог до безпеки інтернету речей і визначення питань безпеки на кожному рівні.
3. Був проведений порівняльний аналіз методів безпеки IoT.
4. Спроектовано систему інтернету речей та запропоновано методи безпеки для спроектованої системи.
5. Надано рекомендації стосовно застосування методів безпеки в системі інтернету речей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Varadharajan, V., & Bansal, S. (2016). Data Security and Privacy in the Internet of Things (IoT) Environment. Connectivity Frameworks for Smart Devices, 261–281.
2. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges [Електронний ресурс]. –2019. –Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S22108327193028193.
3. Flynn D. IoT considerations —cloud services —IaaS, PaaS, SaaS, build your own [Електронний ресурс] / Des Flynn. –2015. –Режим доступу до ресурсу: https://medium.com/lattice-research/iot-considerations-server-side-iaas-paas-saas-1f55afc03185.
4. What Is Platform-as-a-Service (PaaS)? [Електронний ресурс] –Режим доступу до ресурсу: https://www.cloudflare.com/learning/serverless/glossary/platform-as-a-service-paas/.
5. H. Haddadi, H. Howard, A. Chaudhry, J. Crowcroft, A. Madhavapeddy, and R. Mortier, “Personal Data: Thinking Inside the Box,” CoRR, ArXiv e-prints, 2015.
6. M. Mun, S. Hao, N. Mishra, K. Shilton, J. Burke, D. Estrin, M. Hansen, and R. Govindan, “Personal Data Vaults:A Locus of Control for Personal Data Streams,” in Proceedings of the 6th International COnference, ser. Co-NEXT ’10. New York, NY, USA: ACM, 2010, pp. 17:1–17:12.
7. Jaimunk, J. (2019). Privacy-Preserving Cloud-IoT Architecture (Abstract). 2019 IEEE/ACM 6th International Conference on Mobile Software Engineering and Systems (MOBILESoft).
8. K. Alanezi and S. Mishra, “A privacy negotiation mechanism for the internet of things,” in IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2018, pp. 512–519.
9. JA Stankovic. 2014. Research directions for the internet of things. IEEE Internet of Things Journal 1, 1 (2014), 3–9.
10. L. Cranor. 2002. Web privacy with P3P. " O’Reilly Media, Inc."

A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satyanarayanan. 2017. Assisting Users ina World Full of Cameras: A Privacy-Aware Infrastructure for Computer Vision Applications. In CVPRW. IEEE, 1387–1396.

11. D. Wyatt, T. Choudhury, and J. Bilmes. 2007. Conversation detection and speaker segmentation in privacy-sensitive situated speech data. InInterspeech.
12. PE Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In SOUPS.
13. What is AWS [Електронний ресурс] –Режим доступу до ресурсу: https://aws.amazon.com/what-is-aws/.
14. Пороло Є. Удосконалена архітектура мережі для хмарного Інтернету речей / Є. Пороло, В. Курдеча // ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ / Є. Пороло, В. Курдеча. –м. Київ, Україна: ISSN(print) 2663-502X, ISSN(online) 2664-3057, 2020. –С. 219–221.
15. Пороло Є. Застосування концепції Data Bank в мережі хмарного IoT / Євгеній Пороло // ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ / Євгеній Пороло. –м. Київ, Україна: ISSN (print)2663-502X, ISSN (online) 2664-3057, 2020. –С. 368.
16. Practical IoT Hacking / Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods : No Starch Press, 2021. – 434 p.
17. Rakjumar Buyya Internet of Things / Rajkumar Buyya, Amir Vahid Dastjerdi : Morgan Kaufmann, 2016. – 378 p.
18. IoT Security / Madhusanka Liyanage, An Braeken, Pardeep Kumar, Mika Ylianttila : Wiley, 2020. – 304 p.
19. Claire Rowland User Experience Design for the Internet of Things / Claire Rowland : O'Reilly Media, Inc., 2015.
20. Barry Haughian Design, Launch, and Sacle IoT Services: A Practical Business Approach / Barry Haughian : Apress, 2018. – 292 p.
21. Gilad Rosner Privacy and the Internet of Things / Galid Rosnar : O'Reilly Media, Inc., 2016.
22. Brian Russel Practical Internet of Things Security / Brian Russel, Drew Van Duren : Packt Publishing, 2018. – 382 p.
23. Demystifying Internet of Things Security: Design a security framework for an Internet connected ecosystem / Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler : Apress, 2019. – 382 p.
24. Sravani Bhattacharjee / Practical Industrial Internet of Things Security: A Practitioner's Guide to Securing Connected Industries / Sravani Bhattacharjee : Packt Publishing, 2018. – 324 p.
25. Dac-Nhuong Le IoT: Security and Privacy Paradigm / Dac-Nhuong Le, Souvik Pal : CRC Press, 2020. – 399 p.
26. Fei Hu Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations / Fei Hu : CRC Press, 2016. – 604 p.