МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: "АНАЛІЗ ТА ОЦІНКА ВРАЗЛИВОСТЕЙ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ (IOT) ТА РОЗРОБКА МЕТОДІВ ЇХ ЗАХИСТУ"

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олексій МИКОЛАЄНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Олексій МИКОЛАЄНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Олександр ПОРОХНИЦЬКИЙ
Ім'я, ПРІЗВИЩЕ

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Миколаєнку Олексію Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Аналіз та оцінка вразливостей в мережах інтернету речей (IoT) та розробка методів їх захисту.”,
керівник кваліфікаційної роботи ПОРОХНИЦЬКИЙ Олександр
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “__“ _____ 2024 р. №__.

2. Строк подання кваліфікаційної роботи “20” травня 2024 р.
3. Вихідні дані до кваліфікаційної роботи: Огляд і аналіз проблем і загроз Інтернету речей; визначення функцій на кожному рівні і аналіз загроз безпеці; розробка рекомендацій і практичних кроків щодо застосування методів захисту даних і пристроїв в системах Інтернету речей; проектування систем Інтернету речей і впровадження в них пропонованих методів забезпечення безпеки..
4. Перелік питань, які мають бути розроблені:
   4.1 Проаналізувати історію виникнення та розвиток Інтернету речей (IoT), розглянути ключові етапи його становлення та визначити технологічні досягнення, що сприяли його розвитку.
   4.2. Дослідити принципи роботи та використання IoT у сучасному світі, зокрема, розглянути основні компоненти систем IoT.
   4.3. Проаналізувати загрози безпеці та протоколи захисту в IoT, включаючи сучасні проблеми інформаційної безпеки, та представити протоколи захисту.
   4.4. Розглянути архітектуру IoT, визначити її основні рівні та функції, проаналізувати особливості та загрози безпеки на кожному рівні архітектури IoT та розробити методику захисту.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз принципів та особливості роботи IoT.	08.04.2024	
4.	Дослідження основних загроз безпеки та протоколів захисту.	22.04.2024	
5.	Вивчення інструментів та методів реалізації IoT на різних рівнях та вибір відповідного методу.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Олексій МИКОЛАЄНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачка Миколаєнко О.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Аналіз та оцінка вразливостей в мережах інтернету речей (IoT) та розробка методів їх захисту ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач МИКОЛАЄНКО Олексій у кваліфікаційній роботі проаналізував особливості розвитку та вразливості в роботі Інтернету речей, дослідив основні принципи роботи та використання IoT в сучасних умовах, проаналізував відповідні загрози та протоколи захисту, розглянув архітектуру та визначив основні рівні та функції та розробив на основі наявних інструментів та задач метод захисту IoT.

МИКОЛАЄНКО Олексій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, продемонстрував володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача МИКОЛАЄНКО Олексія на оцінку “_____” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Миколаєнко О.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти МИКОЛАЄНКО Олексій
на тему “ Аналіз та оцінка вразливостей в мережах інтернету речей (IoT) та розробка методів їх захисту ”

Актуальність. З кожним роком питання захисту інтернет речей стає все більш важливим та критичним. В особливості для різних сфер виробництв та домашнього використання які потребують економії часу на простих буденних завданнях або ж автоматизованої точності. Відповідно IoT потребує відповідний захист в практичній та актуальній формі з врахуванням наявних вразливостей.

З огляду на зазначене дослідження вразливостей IoT і відповідно методу їх захисту є актуальним науковим завданням.

Позитивні сторони.

1. У роботі були досліджені основні аспекти інтернету речей, їх принципи та особливості роботи в сучасному світі, загрози безпеки та відповідні їм протоколи захисту.
2. Кваліфікаційна робота була оформлена відповідно вимог.
3. Автор опрацював значну кількість англомовних джерел.
4. За результатами дослідження запропоновано метод на основі існуючих засобів та інструментів.

Недоліки.

Доцільно було б приділити більше уваги в третьому розділі і більш комплексніше розглянути та звернути увагу на нюанси взаємозв’язку інструментів та деталей усієї системи що включена в наданий метод.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач МИКОЛАЄНКО Олексій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню проблем забезпечення інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 14 рисунків, висновків та списку використаних джерел, що містить 40 найменуваннь. Загальний обсяг роботи становить 64 аркуша, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження засад забезпечення інформаційної безпеки IoT. Для цього у роботі використовуються методи системного аналізу та теорії інформаційної безпеки.

Об'єктом дослідження є забезпечення інформаційної безпеки.

Предмет дослідження - особливості забезпечення інформаційної безпеки підприємства.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки.

Як результат у роботі проведено аналіз основних характеристик, в тому числі досліджено особливості управління інформаційною безпекою підприємства в умовах інформаційного протиборства, зокрема представлено схему актуальних загроз інформаційній безпеці підприємства з урахуванням зазначеної специфіки; визначено напрями та методи забезпечення інформаційної безпеки підприємства у процесі інформаційного протиборства відповідно до запропонованої класифікації загроз.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті протидії загрозам, пов'язаним із веденням інформаційного протиборства.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

TCP - Transmission Control Protocol (Протокол управління передачею)

UDP - User Datagram Protocol (Протокол користувальницьких дейтаграм)

DDoS - Distributed Denial-of-Service (Розподілена атака відмови в обслуговуванні)

Dyn - Originally Dynamic Network Services (Спочатку Dynamic Network Services)

DNS - Domain Name System (Система доменних імен)

ARPA - Address and Routing Parameter Area (Область адресних і маршрутних параметрів)

PC - Personal computer (Персональний комп'ютер)

LAN - Local Area Network (Локальна вичислительна мережа)

ID - Identifier (Ідентифікатор)

RFID - Radio-Frequency Identification (Радіочастотна ідентифікація)

IP - Internet Protocol (Інтернет-протокол)

NFC - Near Field Communication (Комунікація ближнього поля)

IoT - Internet of Things (Інтернет речей)

M2M - Machine-to-Machine

TLS/SSL - Transport Layer Security/Secure Sockets Layer (Транспортний рівень безпеки/Безпечний рівень сокетів)

API - Application Programming Interface (Інтерфейс програмування додатків)

SOA - Service-Oriented Architecture (Сервісно-орієнтована архітектура)

WSN - Wireless Sensor Network (Бездротова мережа датчиків)

MEMS - Microelectromechanical Systems (Мікроелектромеханічні системи)

LPWAN - Low-Power Wide-Area Network (Мережа низького енергоспоживання великої площі)

IT - Інформаційні технології

QoS - Quality of Service (Якість обслуговування)

MITM - Man-in-the-Middle (Атака Людина посередині)

MQTT - Message Queue Telemetry Transport (Протокол транспортування даних телеметрії за допомогою черги повідомлень)

TPM - Trusted Platform Module (Модуль довіреної платформи)

ВСТУП

Актуальність Інтернет речей можна вважати новим витком розвитку інтернету, де відбувається обмін даними між об'єднаними в мережу фізичними об'єктами, де кожний пристрій може взаємодіяти самостійно та об'єднуватися з мільярдами інших об'єктів, що значно спростить життя, оскільки люди зможуть виконувати різні завдання, перебуваючи у віддалених місцях.

Інтернет речей стрімко поширюється в багатьох сферах діяльності. Ця концепція використовується в "розумних" будинках, транспортних системах і "розумних" містах. Завдяки цій системі різні промислові структури та системи охорони здоров'я зробили крок уперед, забезпечивши більший контроль над різними структурами та процесами. Штучний інтелект використовується для збору та обробки даних, які постійно аналізуються.

Ці можливості безсумнівно привертають увагу, оскільки IoT-системи дедалі більше розвивають свої переваги у взаємодії з інтелектуальними системами за рахунок розвитку різних розумних датчиків, різних технологій бездротового зв'язку, хмарних обчислень і аналітики. Згідно з інформацією, наданою різними сайтами зі збору статистики, станом на 2021 рік кількість під'єднаних до IoT пристроїв у світі перевищить чисельність населення планети, досягнувши 10,07 мільярда підключень. Ба більше, прогнози на 2030 рік показують, що кількість унікальних підключень сягне 25,44 мільярда. Ці цифри свідчать про те, що в майбутньому напрямок IoT-систем стане ще більш важливим аспектом реалізації рішень у різних інфраструктурних комплексах. Однак Інтернет речей стикається з безліччю труднощів і невирішених проблем.

Одне з ключових питань - безпека: атака ботнету Mirai викликала суспільний резонанс і змусила всіх звернути на себе увагу. Жертвами цієї атаки стали багато недорогих пристроїв зі стандартними паролями.

Зрештою винуватцем стала розподілена атака типу "відмова в обслуговуванні" (DDoS) на Dyn, провайдера системи доменних імен (DNS), яка

є частиною інтернет-інфраструктури багатьох великих американських компаній, що призвело до перебоїв з доходами і клієнтами.

Безпека мережі, додатків та інфраструктури має розглядатися на постійній основі. В іншому разі втрати будуть дуже великими. Однак на цьому етапі виробники не прагнуть захищати свої пристрої. Не варто забувати, що ціна впровадження методів інформаційної безпеки в їхніх рішеннях відповідно зросте. Ще одна причина відмови - висока вартість забезпечення високопродуктивних обчислень.

Усе середовище IoT, включно з розробниками і користувачами, потребує численних поліпшень у сфері безпеки IoT. За такого ставлення зростання цієї галузі може зупинитися в найближчі кілька років. Використання Інтернету IoT є

Використання може значно поліпшити багато сфер життя, але важко говорити про довіру, якщо безпека IoT не є повною.

Метою даної роботи є розробка системи забезпечення безпеки даних і пристроїв у системах Інтернету речей.

Для досягнення мети дослідження необхідно вирішити такі завдання

- Огляд та аналіз проблем і загроз Інтернету речей;
- Виявлення та аналіз характеристик загроз безпеки на різних рівнях;
- Порівняльний аналіз методів забезпечення безпеки IoT.

Область наукових інтересів: інформаційна безпека Інтернету речей.

Дослідницьке питання: способи та засоби захисту систем Інтернету речей.

Практична цінність дослідження полягає в проєктуванні IoT-систем, що знижують вплив кіберзагроз, на основі аналізу загроз і методів захисту.

РОЗДІЛ 1 АСПЕКТИ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Історія виникнення

Хоча приклади взаємопов’язаних електронних пристроїв існують ще на початку 19 століття, з винаходом телеграфу та його здатністю передавати інформацію за допомогою кодованого сигналу на відстань, витоки IoT відносяться до кінця 1960-х років. Саме тоді група видатних дослідників почала досліджувати шляхи з’єднання комп’ютерів і систем. Яскравим прикладом такої роботи була ARPANET, мережа, створена Агентством передових дослідницьких проектів (ARPA) Міністерства оборони США; ця мережа була попередницею сучасного Інтернету. Наприкінці 1970-х років підприємства, уряди та споживачі почали досліджувати способи підключення персональних комп’ютерів (ПК) та інших машин один до одного. До 1980-х років локальні мережі (LAN) забезпечували ефективний і широко використовуваний спосіб обміну документами, даними та іншою інформацією між групою ПК у режимі реального часу. До середини 1990-х років Інтернет розширив свої можливості в глобальному масштабі, і дослідники та інженери почали вивчати способи ефективнішого з'єднання.

У 1997 році британський технолог Кевін Ештон, співзасновник Auto-ID Center в Массачусетському технологічному інституті, почав досліджувати технологічну структуру, радіочастотну ідентифікацію (RFID), яка дозволила б фізичним пристроям з’єднуватися через мікрочіпи та бездротові сигнали, і це було у промові у 1999 році Ештон ввів фразу «Інтернет речей». Протягом кількох років смартфони, хмарні обчислення, прогрес у обчислювальній потужності та вдосконалені алгоритми програмного забезпечення створили основу для збору, зберігання, обробки та обміну даними більш надійним способом. У той же час з’явилися складні датчики, які могли вимірювати рух, температуру, рівень вологості, напрямок вітру, звук, світло, зображення, вібрацію та багато інших

умов, а також здатність точно визначити людину чи пристрій за допомогою геолокації. Ці розробки зробили можливою можливість спілкуватися як з цифровими пристроями, так і з фізичними об’єктами в реальному часі. Наприклад, додавши чіп відстеження, такий як Apple AirTag, до такого об’єкта, як гаманець або валіза, можна переглянути його місцезнаходження. Той самий чіп, вбудований у цифровий пристрій, може відстежувати його місцезнаходження в разі втрати чи викрадення. Потім, із широким розповсюдженням мобільних пристроїв, таких як смартфони та планшети, і впровадженням повсюдного бездротового зв’язку, стало можливим з’єднувати людей і речі майже всюдисущим способом. У результаті розумні транспортні мережі, підключені резервуари для зберігання та промислові роботизовані системи стали нормою.

IoT продовжує розвиватися, сьогодні він підтримує низку варіантів використання, включаючи штучний інтелект, який використовується для ультраскладного моделювання, системи датчиків, які виявляють забруднюючі речовини у водопостачаннях, і системи, які спостерігають за сільськогосподарськими тваринами та посівами. Наприклад, тепер можна відстежувати місцезнаходження та стан здоров’я тварин і дистанційно вносити оптимальні рівні води, добрив і пестицидів до посівів.

Високопідключені системи дозволяють судноплавним компаніям і авіакомпаніям враховувати погодні та механічні проблеми, а потім оптимізувати флот для максимального навантаження та ефективності. IoT надає автомобілістам карти в режимі реального часу та навігаційні пропозиції, які прокладають і змінюють маршрути на основі поточних схем руху. Ці системи зменшують затори та забруднення та економлять час і гроші. [1,2,3,4]

1.2 Принцип роботи IoT

В основі IoT лежить Інтернет-протокол (IP) і протокол керування передачею (TCP). Ці стандарти та правила є основою для датчиків, пристроїв і систем для з'єднання з Інтернетом і один з одним. IoT обробляє дані з пристроїв і передає інформацію через дротові та бездротові мережі, включаючи Ethernet, Wi-Fi, Bluetooth, стільниковий зв'язок 5G і LTE, радіочастотну ідентифікацію (RFID) і зв'язок ближнього поля (NFC). Як правило, пристрої IoT підключаються до шлюзів IoT або периферійних пристроїв, які збирають дані. Вони передають дані в хмарні обчислювальні середовища та з них, які зберігають і обробляють інформацію. Широкий набір мережевих стандартів гарантує, що даними можна ділитися та досягати правильної «речі», таким чином з'єднуючи фізичний світ із цифровим.

Існує два основних типи підключених пристроїв: спочатку цифрові та фізичні. Перший складається з машин і пристроїв, спеціально розроблених із вбудованим підключенням, таких як смартфони, потокові медіаплеєри, мобільні платіжні термінали, сільськогосподарські комбайни та реактивні двигуни. Цифрові пристрої генерують дані та спілкуються з іншими машинами за допомогою міжмашинного зв'язку (M2M). З іншого боку, до фізичних пристроїв належать мікрочіп або датчик із можливостями зв'язку. Наприклад, брелок, транспортний засіб або медичний пристрій у лікарні може містити чіп, доданий після його виготовлення, який робить новий об'єкт або продукт функціональним і доступним для відстеження. Деякі спостерігачі класифікують продукти відповідно до більш детального спектру інтерактивності, що складається не з двох категорій, а з п'яти, починаючи від чисто цифрових (за якими йдуть перш за все цифрові, подвійного використання та перші фізичні) до чистих пристроїв (без будь-яких цифрових можливостей).

IoT дозволяє людям і системам обмінюватися даними та контентом через соціальні мережі та інші онлайн-методи; віддалено контролювати події; і взаємодіяти з іншими через мобільні пристрої та інші системи, ігрові пристрої.

Наприклад, під час пандемії підключені термометри дозволили епідеміологам краще зрозуміти поширення COVID-19, відстежуючи людей з лихоманкою. [1,5,6,4,7]

1.3 Інтернет речей у сучасному світі

Будь-який фізичний об'єкт, що взаємодіє один з одним або із зовнішнім середовищем за допомогою передавання даних мережею, можна назвати Інтернетом речей. У сучасному світі Інтернет речей може використовуватися для взаємодії між машинами (M2M), між людьми і машинами. З появою нових протоколів і зростанням кількості "розумних" пристроїв IoT буде змушений вибрати напрямок конвергенції між "розумними" і автономними мережами; впровадження людини в системи IoT принесе користь у галузі охорони здоров'я та готовності до надзвичайних ситуацій. Таким чином, Інтернет речей сформує систему, яка зможе реагувати на різні події, використовуючи датчики для передачі інформації. Ця система вплине на підприємства, системи охорони здоров'я, якість життя і бізнес, використовуючи і забезпечуючи такі функції:

- Забезпечення інтегрованого середовища для взаємодії між фізичними об'єктами шляхом розширення каналів зв'язку датчиків з такими даними, як пульс, положення і частота серцевих скорочень;

- полегшення взаємодії між менеджерами і фізичними об'єктами за допомогою віддаленого доступу завдяки спрощенню процесів автоматизації та управління;

- знизити витрати на розгортання, впровадження та обслуговування різних систем завдяки наданню різних вимірювань та інших корисних даних через віддалений доступ до пристроїв.

Приклади сучасних застосувань і реалізацій IoT-систем:

- Підключені дороги.

Важливою галуззю, в якій починають впроваджувати системи IoT, є під'єднані дороги. Такі проєкти, як самохідні автомобілі Google, Uber і Yandex,

вимагають впровадження Інтернету речей. Така інтеграція дасть змогу поліпшити взаємодію з транспортною системою завдяки обміну даними і поліпшити зв'язок із водіями, зокрема

Поліпшення взаємодії з транспортною системою за рахунок обміну даними і поліпшення зв'язку з водіями та іншими безпілотними автомобілями.

- Підключені заводи.

Багато традиційних заводів починають перетворюватися на підключені фабрики:

- Проблеми простою на заводах;

- Проблеми з якістю роботи.

- Проблема пошуку причин різних виробничих неефективностей.

- Проблеми з виготовленням бракованого продукту.

- Розумні підключені будівлі.

Розумні підключені будівлі - свідчення успішного впровадження Інтернету речей. У будівлях такого типу використовуються різні сенсорні системи для підвищення продуктивності та обміну інформацією, що дає змогу отримувати відомості про те, що відбувається між різними системами.

Ця інформація може бути використана для автоматизації різних процесів, також вона може бути використана для автоматизації процесів, наприклад ручне та автоматичне управління кліматом в домі, освітленням, побутовою технікою та мультимедіа. А під безпекою розуміють захист дому (квартири, дачі, гаража) від пожежі, злодіїв та інших кримінальних елементів, які можуть бути небезпечними для життя чи майна (рис 1.1).

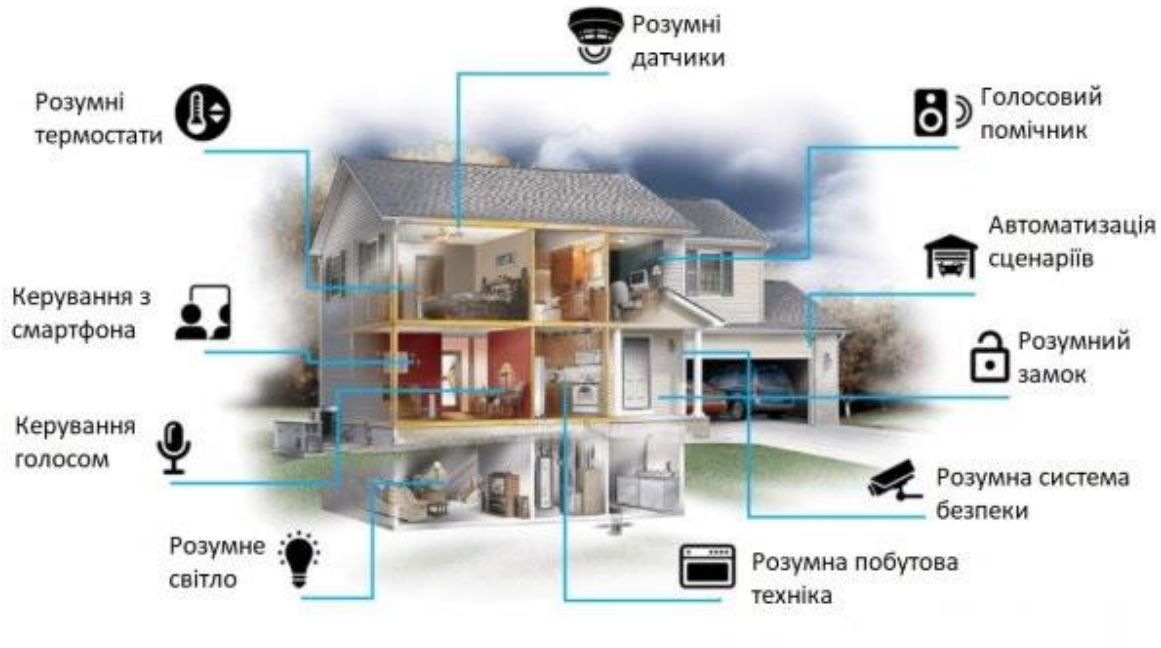

Рис. 1.1 Приклад розумного будинку

Власник будинку може налаштовувати та керувати такою розумною системою зі мобільного телефона, планшета, комп’ютера, дистанційних пультів або окремої сенсорної панелі, або керувати за допомогую голосового помічника. При цьому інформація про стан речей у цьому домі може віддалено передаватись власникові на мобільний додаток. [8,9]

Сільське господарство (рис 1.2)

Розумне сільське господарство часто не враховується в бізнес-критеріях для рішень Інтернету речей. Однак на ринку існує ряд інноваційних продуктів, орієнтованих на просунутих фермерів. Деякі з них використовують розподілену мережу розумних датчиків для моніторингу різних умов навколишнього середовища, таких як вологість, температура і якість ґрунту, крім того деякі з них використовуються для автоматизації систем зрошення.

Розумні зрошувальні системи використовують погодні дані в режимі реального часу для створення оптимальної програми поливу для саду система складається з інтелектуального контролера на базі Bluetooth і мобільного пристрою, його легко встановити, налаштувати та керувати

Рис. 1.2. Приклад IoT у сільському господарстві

Хоча продукт спочатку був розроблений для використання в домашніх умовах, подібні рішення можна застосовувати і до більших масштабів. [10]

1.4 Особливості роботи IoT

Основні елементи Інтернету речей включають в себе віддалені сервісні виклики, різноманітні сенсорні пристрої, комунікаційні мережі та контекстну обробку подій IoT прагне уявити себе як єдину мережу розумних предметів і людей, що можуть взаємодіяти та спілкуватися один з одним IoT прагне уявити себе як єдину мережу розумних предметів і людей, що можуть взаємодіяти та спілкуватися один з одним IoT прагне уявити себе як єдину мережу розумних предметів і людей, що можуть взаємодіяти та спілкуватися один з одним. Необхідною умовою для розподіленого середовища є повний взаємозв'язок між об'єктами, гарним прикладом якого є IoT. Архітектура, що являє собою цілісну систему, повинна гарантувати бездоганну роботу власних компонентів (надійність розглядається як основний елемент проєктування) і з'єднувати фізичні та віртуальні області. Основними вимогами до цілісної системи є ретельне опрацювання питань аварійного відновлення і масштабованості під час проектування.

Крім того, оскільки динамічне визначення місця розташування і мобільність є ключовими аспектами Інтернету речей, де смартфони використовуються повсюдно, сучасні архітектури повинні прагнути включати в себе точний рівень адаптивності для правильного опрацювання різних динамічних взаємодій в рамках екосистеми. Вона повинна прагнути до цього. Забезпечуючи вищий рівень абстракції.

Надання більш високого рівня абстракції, який може приховати деякі деталі та обмеження реалізації, безумовно можна вважати перевагою еталонних архітектур і моделей.

IoT-ARM (IoT Architecture Reference Model) орієнтована на розробку та перевірку інтегрованих мережевих архітектур для Інтернету речей (рис. 1.3).

IoT-ARM відображає різні рівні обслуговування та представлення. Рівень послуг охоплює обробку й аналіз подій на фізичному та комунікаційному рівнях, системи виявлення послуг і управління ресурсами, служби об'єднання повідомлень і корпоративні сервісні шини (ESB). Архітектура також охоплює управління API, необхідне для визначення та спільного використання системних сервісів, і веб-панель для управління та доступу до цих API. [5,11]

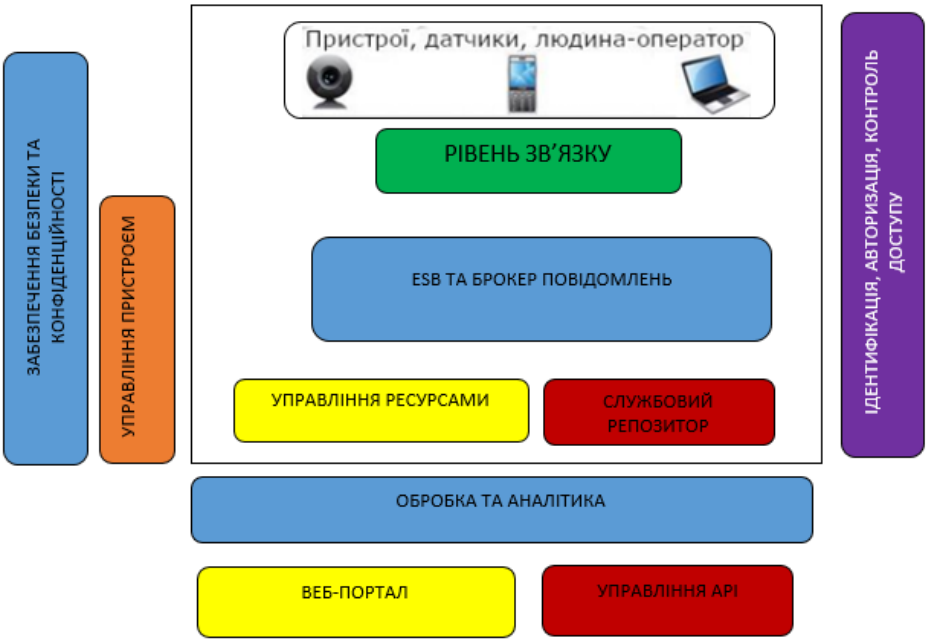

Рис. 1.3 Еталонна архітектура IoT

Зважаючи на важливість управління пристроями, забезпечення безпеки та конфіденційності на різних рівнях, а також можливості унікальної ідентифікації об'єктів і контролю рівнів доступу до них, ці компоненти в цій архітектурі є незалежними та сфокусованими.

Аналіз сервіс-орієнтованої архітектури (SOA).

Для багатьох постачальників послуг і користувачів архітектура SOA має велике значення при використанні Інтернету речей. Ця архітектура забезпечує взаємодію між безліччю різних пристроїв. Загальний вигляд сервіс-орієнтованої архітектури

Загальний вигляд сервіс-орієнтованої архітектури складається з чотирьох шарів, кожен з яких виконує такі функції

- Рівень датчиків тісно взаємодіє з наявними апаратними об'єктами для визначення стану речей;

- Мережевий рівень являє собою повну інфраструктуру, необхідну для підтримки дротового та бездротового підключення;

- Сервісний рівень дає змогу створювати та керувати послугами, необхідними користувачам і застосункам;

- Інтерфейсний рівень забезпечує різні способи взаємодії користувачів і додатків.

При використанні цієї архітектури система ділиться на слабопов'язані підсистеми.

Фокус на компонентах. За такого підходу функціональність архітектури дає змогу частинам системи продовжувати функціонувати в разі відмови конкретного компонента. Для архітектур, у яких надійність має першорядне значення, така можливість

функціональність надзвичайно важлива.

Система має досить високий рівень абстракції та широко використовується у WSN (Wireless Sensor Networks).

З WSN пов'язані різні переваги. Таким чином, IoT може використовувати SOA. Це пов'язано з тим, що ця архітектура покращує взаємодію і

масштабованість між об'єктами. Завдяки цій архітектурі користувачам простіше взаємодіяти з протоколами і рівнями системи.

У SOA Інтернет речей використовує всі свої сильні сторони. Це пов'язано з тим, що об'єднання функцій системи дає змогу створювати різноманітні та складні сервіси, які потім можна розділити на завдання. [12,13,14]

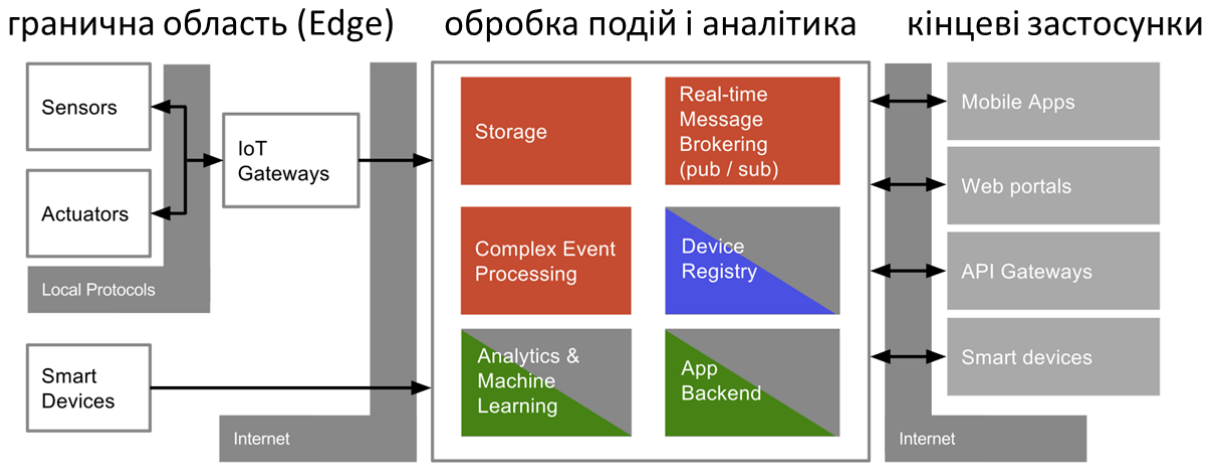

Рис 1.4. Сервіс-орієнтована архітектура для IoT

Компоненти Інтернету речей (рис 1.4).

- Одним із ключових компонентів системи IoT є датчик, який містить операційну систему з мінімальним відгуком, розташовану в критичних місцях, різні джерела збирання, аналізу та оброблення інформації, МЕМС і вбудовані системи;

- Системи зв'язку з датчиками. До них належать персональні мережі радіо-доступу та мережі зі слабкими каналами зв'язку.

- Взаємодіючі локальні мережі на основі IP. Найбільш часто використовуваний стандарт - 802.11 WiFi.

- Шлюзи і маршрутизатори, що забезпечують взаємодію в масштабах мережі;

- Глобальні обчислювальні мережі: оператори мобільного зв'язку, LPWAN, провайдери супутникових мереж тощо;

- Хмари, що виконують функції постачальників послуг, виробників баз даних, обробки та аналітики даних. [5,11]

- Безпека також є одним із компонентів систем IoT, включно з повною інтеграцією архітектури IoT, що має гарантувати автентичність, цілісність та інформаційну безпеку.

Еталонні моделі для Інтернету речей

На сьогоднішній день не існує остаточної або стандартизованої версії моделі IoT, проте компанія Cisco запропонувала еталонну модель, що складається з семи рівнів (таблиця 1). Підхід, що використовується в цій моделі дає змогу розділити процеси, що відбуваються на кожному рівні, на прості та складні.

Модель описує, як простота може бути досягнута шляхом вирішення завдань на кожному рівні, підтримуючи такі важливі етапи, як масштабованість і підтримка в Інтернеті речей.

Ця модель визначає функціональність, необхідну для функціонування Інтернету речей. Модель являє собою рівень абстракції та описує системи IoT шляхом відображення їхніх функціональних інтерфейсів; архітектура IoT дає змогу обробляти дані, створювати інформацію та керувати ними на основі контексту, що призводить до створення чудових рішень IoT.

Таблиця 1

Еталонна модель IoT

Рівні	**Характеристики**
Фізичні пристрої та контролери	Пристрої кінцевої точки, експоненціальне зростання, різноманітні
Зв’язок	Надійність, своєчасна передача, комутація та маршрутизація
Туманні обчислення	Перетворення данних в інформацію, яке може бути ефективною
Накопичення данних	Зберігання даних, постійні та перехідні дані

Продовження таблиці 1

Рівні	**Характеристики**
Абстракція данних	Семантика даних, цілісність даних ло програми, стандартизація даних
Додатки	Значуші інтерпретації та дії даних
Співробітництво і процеси	Люди, процеси, розширення можливостей та співпраця

Для проєктування IoT необхідні комунікаційні протоколи та інфраструктура. Рівень 3 називається туманними обчисленнями, основними функціями яких є перетворення та аналіз даних. Для отримання цих даних виконується обробка інформації, і наші подальші дії ґрунтуються на цих даних.

Перші три рівні моделі належать до рухомих даних, а наступні - до отриманої інформації. Безперервна обробка даних у туманних обчисленнях може здійснюватися в режимі реального часу. Такий підхід збільшує рівень цінності, на якому процеси і люди виконують дії в системах IoT. [15]

Висновки до розділу 1

Розглянувши історію виникнення Інтернету речей, принцип його роботи та його роль у сучасному світі, можна зробити висновок, що IoT став не лише технологічним досягненням, але й значною частиною нашого повсякденного життя. Перші спроби створення мережі об'єктів з'єднання почалися ще у 20-ому столітті, але справжня революція відбулася з появою мікроелектроніки та бездротових технологій у другій половині минулого століття.

Принцип роботи Інтернету речей полягає в узгодженому зборі та обміні даними між фізичними пристроями, які мають вбудовані сенсори та здатність до комунікації через Інтернет. Цей процес включає в себе збір інформації, передачу даних через мережу, їх аналіз та використання для прийняття рішень або автоматизації певних функцій.

У сучасному світі Інтернет речей використовується в різних сферах життя, від промисловості до домашнього господарства. У промисловості він забезпечує підвищення продуктивності та ефективності виробництва через автоматизацію процесів та моніторингу стану обладнання. У домашньому середовищі IoT дозволяє створювати "розумні" системи, які забезпечують комфорт, безпеку та ефективне використання енергії.

Проте, разом із вигодами, Інтернет речей також стикається з викликами. Зокрема, це питання безпеки даних та приватності, оскільки зі збільшенням кількості підключених пристроїв зростає ймовірність кібератак. Також важливо вирішити питання стандартизації, щоб забезпечити сумісність та взаємодію між різними пристроями та системами.

У цілому, Інтернет речей відкриває безліч можливостей для покращення якості нашого життя, але вимагає уваги до вирішення питань безпеки, приватності та стандартизації для подальшого стабільного розвитку.

РОЗДІЛ 2 АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ТА ПРОТОКОЛИ ЗАХИСТУ НА РІЗНИХ РІВНЯХ OSI

2.1 Сучасні проблеми інформаційної безпеки

Майже всі під'єднані пристрої IoT мають доступ до інфраструктури IoT і персональних даних; ризики, пов'язані з IoT, досягли нового рівня завдяки інтероперабельності, застосункам і автономному ухваленню рішень, водночас з'являються різноманітні шпарини в системі безпеки та потенційні вразливості. Тому питання безпеки та конфіденційності даних набувають критичного значення (рис. 2.1).

Рис. 2.1 Проблеми безпеки IoT

Поєднання мобільних мереж, соціальних мереж, Інтернету та різноманітних "розумних" об'єктів можна вважати Інтернетом речей, де користувачам пропонуються різноманітні послуги та додатки. [16]

Безпека на різних рівнях безпосередньо впливає на успіх систем IoT, оскільки підвищує безпеку, надійність і сумісність взаємодії об'єктів. Інтернет

речей досяг того рівня, коли різні простори (наприклад, цифровий і фізичний) можуть бути пов'язані між собою (рис. 2.2).

Різні датчики взаємодіють з фізичним простором. Ці датчики вже використовуються практично в усьому, від іграшок до систем охорони здоров'я і промислового сектору, і є прикладом того, як різні вразливості цифрового світу починають впливати на реальний світ.

Система вважається успішною тільки в тому разі, якщо вона здатна забезпечити захист від уразливостей, успіх додатків та інфраструктури Інтернет речей значною мірою залежить від безпеки та захисту від вразливостей.

Інтернет речей являє собою безліч нових інструментів, які інтегруються в організації і навіть системи. Кожен підключений пристрій - це потенційний шлюз до інфраструктури Інтернету та персональних даних. Дані з таких пристроїв можуть бути проаналізовані та використані. Аналіз цих даних може призвести до створення невидимих зв'язків, що зачіпають приватне життя людей і організацій.

Хоча питання безпеки та конфіденційності дуже важливі, потенційні ризики для об'єктів вийдуть на новий рівень, оскільки інтероперабельність, гібридні додатки та незалежне ухвалення рішень створюють складнощі, прогалини в безпеці та потенційні вразливості, це пов'язано зі створенням і потенційними вразливостями.

Ризики захисту даних виникають у сфері IT, оскільки складність може створити високу вразливість при підключенні сервісів. В Інтернеті речей більша частина інформації належить до особистих даних, таких як дата народження, місце розташування, бюджет тощо. Ризик неправомірного використання всіх наборів даних - один з аспектів проблеми великих даних. Інтернет речей має бути реалізований юридично, етично, соціально і політично прийнятним чином, з урахуванням правових, системних підходів, технічних і ділових питань.

Безпека - одна з головних проблем, але поки що немає чіткого визначення того, що є найбільш важливими питаннями безпеки даних і конфіденційності. [15]

Питання безпеки та конфіденційності даних не є чимось новим для Інтернету речей, оскільки подібні проблеми вирішувалися ще на зорі розвитку RFID, це пов'язано з тим, що ризики, пов'язані з Інтернетом речей, вийдуть на новий рівень у міру того, як сумісність гібридних застосунків і вразливості автономної системи безпеки стануть невід'ємною частиною процесу прийняття рішень. Нижче наведено діаграму кількості підключених пристроїв IoT (рис. 2.2).

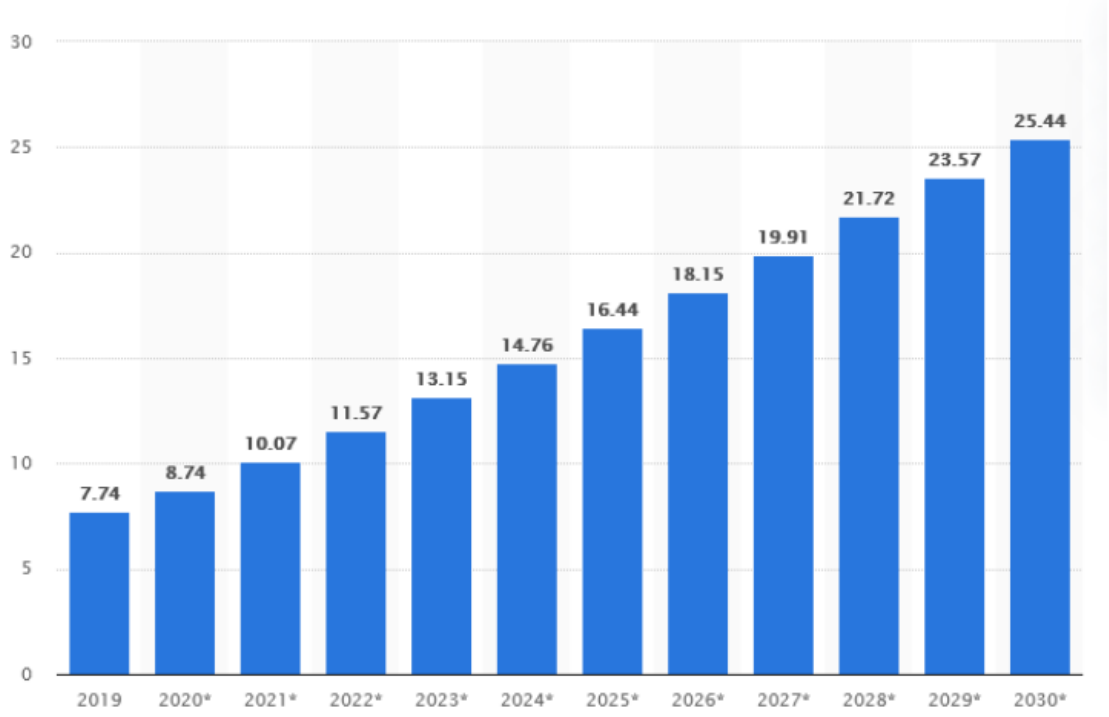

Рис 2.2 Діаграма оцінки кількості підключених IoT пристроїв по всьому світу з 2019 до 2030 року за даними сайта statista.com

2.2 Питання безпеки інтернету речей

На рисунку 2.3 представлено вимоги до безпеки системи, що включають шість основних критеріїв:

- Критерій конфіденційності (1) - дані захищаються уповноваженими особами;

- Критерій цілісності (2) - даним можна довіряти;

- Критерій доступності (3) - дані доступні, коли і де вони необхідні;

- Критерій надійності (4) - сервіс забезпечує надійний аудиторський слід;

- Критерій надійності (4) - сервіс забезпечує надійний аудиторський слід;

- Критерій конфіденційності (6) - сервіс не переглядає дані клієнта автоматично.

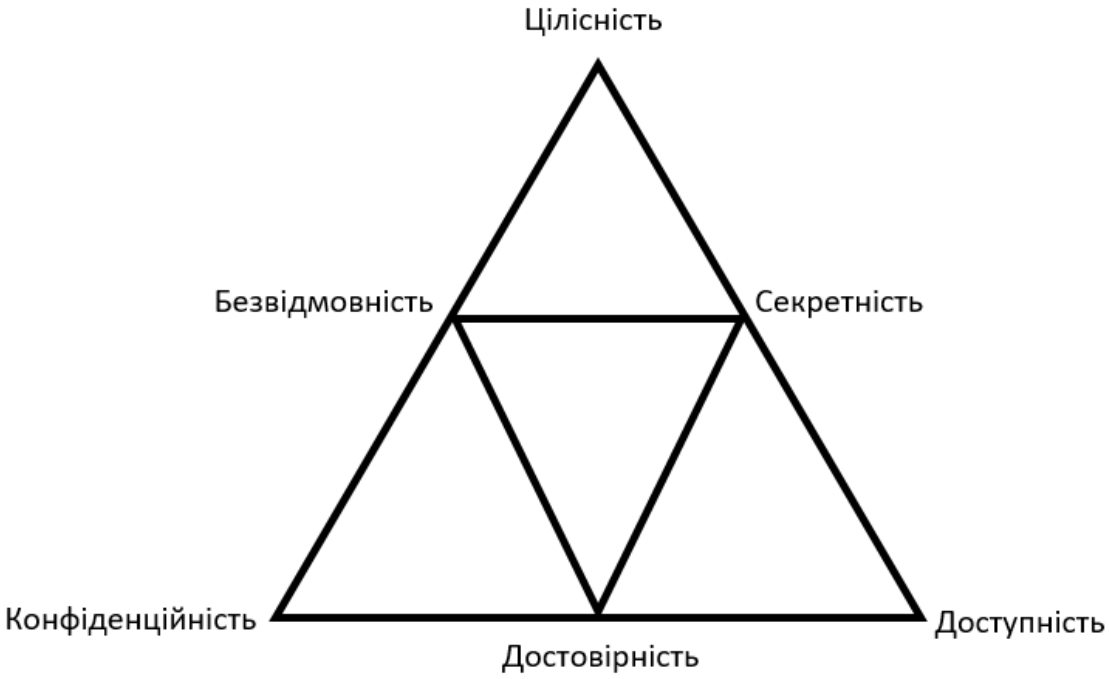

Рис 2.3 Вимоги безпеки IoT

Ризики захисту даних виникають, коли об'єкти Інтернету речей збирають і агрегують фрагменти, пов'язані з даними. Персональні дані перетворюються шляхом зіставлення певної кількості точок, так що місце розташування, час і частота забезпечують контекст для перегляду подій. Це один з аспектів проблеми великих даних, і фахівці з безпеки повинні переконатися, що вони продумали потенційні ризики конфіденційності, пов'язані з усім набором даних. Головне в сценаріях IoT. [17]

Основні проблеми безпеки в сценаріях IoT включають конфіденційність даних, конфіденційність і довіру.

Конфіденційність даних:

- Неадекватна аутентифікація/автентичність;

- Небезпечні інтерфейси (наприклад, інтернет, мобільний телефон);

- Відсутність транспортного шифрування;

- Підтримка конфіденційності;

- Контроль доступу.

Конфіденційність:

- Конфіденційність; Захист даних; Управління ризиками інформаційної безпеки.

Безпека;

- Конфіденційність за замовчуванням;

- Політика конфіденційності;

- Відстеження/профілювання/незаконна обробка.

Довіра:

- Системи управління ідентифікацією;

- Небезпечне програмне забезпечення/прошивка;

- Забезпечення безперервності та доступності послуг;

- Шкідливі атаки на пристрої та системи IoT;

- Втрата автентифікації користувача/скрута в ухваленні рішень.

Щоб проілюструвати вимоги до безпеки в IoT, змодельовано архітектуру IoT, що складається з чотирьох рівнів: рівня датчиків, мережевого рівня, рівня сервісів і рівня інтерфейсів.

Кожен рівень може забезпечувати відповідні засоби контролю безпеки, включно з контролем доступу, засобами автентифікації, цілісністю та конфіденційністю даних, доступністю та можливістю захисту засобів IOT від вірусів і атак.

У сучасних виробничих комплексах і "розумних" містах, під'єднаних до єдиної платформи, головною вимогою є створення оптимізованої архітектури безпеки для пристроїв, що входять до Інтернету речей. Створена система безпеки повинна відстежувати кожен під'єднаний до мережі пристрій окремо і попереджати про можливий шкідливий доступ, за необхідності захищати пристрій або відключати його у відповідь на загрози. Таким чином розробка і використання стандартів - найважливіший процес для Інтернету речей.

На всіх рівнях Інтернету речей найактивніша робота ведеться в галузі стандартизації. Наразі розробленням стандартів займаються кілька великих організацій: IEEE (Інститут інженерів електротехніки та електроніки) та ISO/IEC (Міжнародна електротехнічна комісія).

2.3 Безпека на сенсорному рівні

Цей рівень характеризується перетином людей, місць і предметів. Це можуть бути прості інструменти, як-от термометр або лампочка, або складні пристрої, як-от медичне обладнання чи виробничі прилади.

Щоб безпеку було реалізовано повною мірою, вона має бути закладена в обладнання і використовуватися. Це означає, що засоби IoT повинні перевіряти особистість для підтримки надійності, підписувати і шифрувати дані для забезпечення їхньої цілісності, а також обмежувати локальне зберігання даних для захисту персональних даних.

Модель безпеки пристрою має бути дуже суворою, щоб запобігти несанкціонованому використанню, але досить гнучкою, щоб тимчасово підтримувати безпечну, спеціальну взаємодію між людьми та іншими пристроями.

В таблиці 2 наведено найважливіші питання безпеки в IoT.

Таблиця 2

Найчастіші вразливості в інтернеті речей на всіх рівнях архітектури

Проблеми безпеки	**Рівень інтерфейсів**	**Рівень служб**	**Мережевий рівень**	**Сенсорний рівень**
Небезпечний веб-інтерфейс	+	+	+	
Недостатня автентифікація авторизація	+	+	+	+
Небезпечні мережеві послуги		+	+	
Відсутність транспортного шифрування		+	+	
Проблеми конфіденційності		+	+	+

Продовження таблиці 2

Небезпечний хмарний інтерфейс	+			
Небезпечний мобільний інтерфейс	+		+	+
Небезпечність конфігурації	+	+	+	
Небезпечне програмне за безпечення / прошивка	+		+	
Погана фізична безпека			+	+

Пристрої IoT стали повсюдно поширені в навколишньому середовищі, і в якості інструменту IoT завдання полягає у створенні систем, що захищають від несанкціонованого доступу до пристроїв. Це знижує ймовірність отримання конфіденційної інформації, як-от персональні дані, ключі шифрування та автентифікаційна інформація Пристрої IoT мають тривалий термін служби,

Тому під час випуску конкретного пристрою необхідно включати оновлення програмного забезпечення, щоб уникнути різних експлойтів. [18,19,20,21]

2.4 Безпека мережевого рівня

Цей рівень являє собою комунікацію та обмін повідомленнями між речами і хмарними сервісами. Оскільки інтернет-комунікації зазвичай об'єднують приватні та публічні мережі, безпека, як зрозуміло, має велике значення.

Цей рівень найбільш зрозумілий для розуміння безпеки IoT, оскільки такі технології, як шифрування TLS/SSL, ідеально підходять для вирішення цього завдання. [22]

Основні труднощі виникають при розгляді криптографічних питань у пристроях з обмеженими ресурсами, тобто у 8-бітних мікроконтролерах з обмеженою оперативною пам'яттю. Наприклад, Arduino Uno може витратити до трьох хвилин на шифрування тестового корисного навантаження з використанням 1024-бітного RSA-ключа, тоді як алгоритм цифрового підпису на основі еліптичної кривої з аналогічною довжиною RSA-ключа може зашифрувати те саме корисне навантаження за 0,3 секунди. Це означає, що

виробники пристроїв не можуть використовувати обмеженість ресурсів як виправдання для обходу безпеки своїх продуктів. [18,19,20,21]

2.5 Постановка задачі безпеки на рівні служб

Цей рівень являє собою систему управління IOT і відповідає за організацію автоматизації між пристроями і користувачами, політиками і правилами та пристроями. На цьому рівні важливо забезпечити високий рівень контролю доступу для управління різними пристроями та користувачами, а також авторизованими діями.

Для забезпечення відшкодування витрат важливо вести журнал аудиту всіх змін користувачів і пристроїв, щоб дії, зроблені в системі, не могли бути спростовані. Ці дані спостереження також можуть бути використані для виявлення потенційно небезпечних пристроїв при виявленні аномальної поведінки. Аналіз великих даних, отриманих у результаті роботи IoT, часто називають найціннішим аспектом Інтернету речей.

Збереження конфіденційності також є одним із головних пріоритетів для урядових установ, і для IoT Федеральна торгова комісія (FTC) і Агентство мережевої та інформаційної безпеки Європейського союзу (ENISA) випустили рекомендації.

(ENISA) випустили рекомендації з безпеки IoT. Вони включають в себе такі вимоги до безпеки, як

надання чіткого повідомлення про використання даних за наявності чіткого контролю над ними; передача даних у хмарні сервіси; зберігання даних клієнтів у хмарних сервісах в ізольованому і/або зашифрованому вигляді; використання ключів, що надаються клієнтами; агрегування даних від клієнта до клієнта, анонімізація даних під час їх аналізу. [18,19,20,21]

2.6 Безпеки рівня інтерфейсів

Існує також низка питань на рівні інтерфейсів, де необхідно забезпечити безпеку IoT, оскільки на кожному рівні існують свої специфічні проблеми. Перш за все, у пристроях IoT має бути реалізовано надійний захист. Навіть у невеликих інструментах з обмеженими ресурсами.

Вони також повинні забезпечувати конфіденційність, цілісність і надійність під час обміну даними мережею. Нарешті, необхідно зрозуміти баланс між конфіденційністю споживача і конфіденційністю бізнесу, а також важливість величезної кількості даних, які генерує IoT. [18,19,20,21]

2.7 Моніторинг проблем безпеки даних та пристроїв інтернету речей

Немає сумнівів у тому, що переваги та можливості нових технологій будуть швидко поширюватися. Концепція "Інтернету речей" застосовується до таких технологічних інновацій і, в ширшому сенсі, до "розумних міст",

Поряд з очевидними перевагами, це має вирішити проблеми, пов'язані з широким розповсюдженням таких технологій. Однією з таких проблем є те, що виробники інтернет-компонентів не вважають за потрібне приділяти достатню увагу питанням інформаційної безпеки, пов'язаним з повсякденним використанням окремих компонентів системи та всіх програмно-апаратних комплексів. Інтернет-компоненти.

З виходом на ринок численних виробників термінального, комунікаційного та керуючого обладнання все більшої актуальності набуває питання сумісності компонентів зі складними структурами і можливості роботи без ризику несанкціонованого доступу до систем, витоку і розповсюдження службової інформації.

Речі представляють собою різноманітні інструменти, які перевершують за кількістю ПК, ноутбуки та смартфони за межами захищеного корпоративного кордону. Незважаючи на це, безпека довгий час залишалася невирішеною

проблемою, але в останні роки спостерігається зростаючий інтерес до Інтернету речей.

В опитуванні, проведеному компанією Microsoft у 2019 році, 19% експертів зазначили, що безпека є однією з найважливіших проблем, яку необхідно вирішувати. Наразі існує чотири основні проблеми - пошук специфічних рішень для IP, виділення нових коштів для спеціалізованих працівників, брак знань з цього питання та складність у пошуку та виборі відповідних рішень - які мають певні наслідки у створенні та порушенні систем безпеки IP.

Що стосується питань безпеки, то опитані експерти Microsoft розташували їх так, як показано на рисунку 2.4

У більшості випадків безпека на рівні мережі викликала занепокоєння у 43% респондентів.

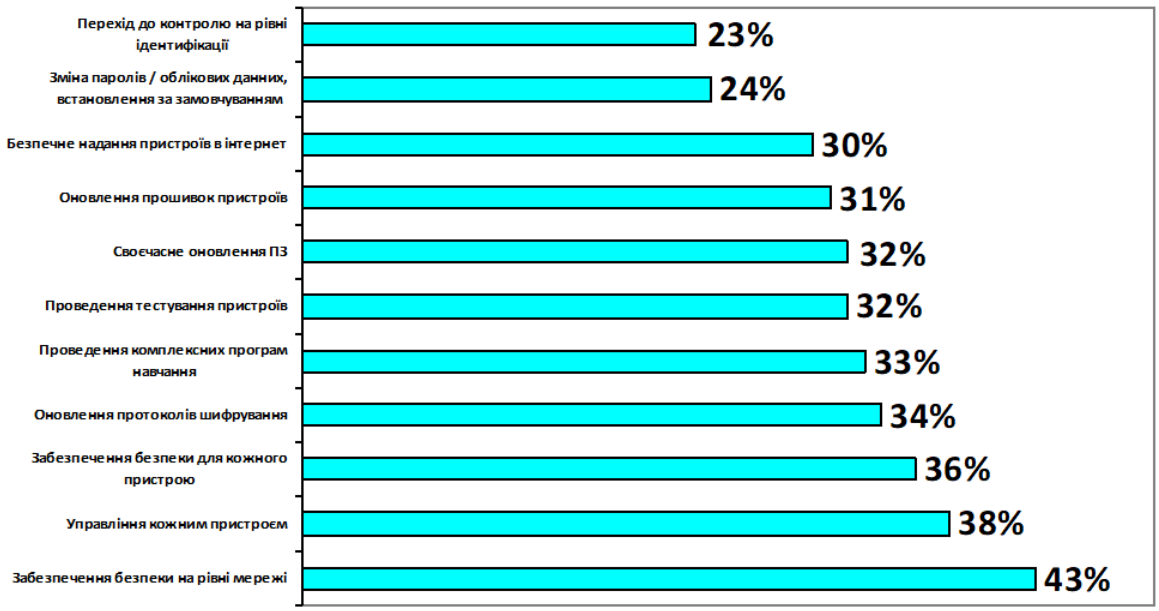

Рис 2.4 Актуальність проблем безпеки згідно дослідження експертів

Багато незахищених пристроїв полегшують DDoS-атаки, а різні пристрої можуть використовуватися для атак на корпоративні системи. Останні часто працюють з паролями "за замовчуванням". Ця вразливість створила ботнет Mirai.

Інтенсивність складної атаки Mirai на сайт журналіста Б. Кребса, створений для розслідування продажу послуг ботнету, сягнула піку в 665 Гбіт/с за допомогою лінивої та інтелектуальної відеокамери.

Таким чином, ми можемо працювати над створенням дослідницьких цілей, орієнтованих на загрози безпеці IoT, в результаті чого буде сформовано список рекомендацій щодо захисту систем Інтернету речей.

Сьогодні ми живемо в світі, де пристроїв, підключених до Інтернету речей, більше, ніж людей.

Ми живемо у світі, де пристроїв, підключених до Інтернету речей, більше, ніж людей. Це можуть бути розумні годинники або зчитувачі RFID, які відстежують певні дані. Взаємодія через різні мережі і хмарні платформи, пов'язані з Інтернетом речей, відбувається через різні пристрої, підключені до цієї системи.

Вона відбувається через різні пристрої, підключені до цієї системи.

Інформація в режимі реального часу стає умовою трансформації всієї сфери IoT. Інтернет речей викликає багато позитивних змін, які знаходять своє відображення в сферах охорони праці та безпеки, а також у бізнесі. Він сприяє підвищенню продуктивності виробництва та сприяє вирішенню глобальних екологічних і гуманітарних проблем. Приклади цієї технології спрямовані на використання великих обсягів низькоенергетичних з точки зору обчислювальних та енергетичних засобів для подібних простих завдань. Ця технологія використовується, наприклад, в розумних будинках і розумних містах. [23]

Вона також може бути застосована до інших розподілених систем (наприклад, географічних інформаційних систем). У цих випадках управління різними пристроями відрізняється. Це пов'язано з тим, що при використанні комп'ютерів та інших розумних пристроїв ними повинна керувати людина, тоді як при використанні M2M участь людини абсолютно непотрібна.

Останні прогнози щодо Інтернету речей підтверджують, що до кінця 2021 року інтеграція величезної кількості пристроїв і систем IoT перевищить 16 мільярдів.

Це еквівалентно подвійному населенню світу. Багато виробничих галузей і галузей життєзабезпечення (через величезне поширення цієї технології по всьому світу) стурбовані безпекою сучасних систем Інтернету речей. [20,24]

Це пов'язано з тим, що питання безпеки тепер стосується не тільки кінцевих користувачів цієї технології, а й величезних потоків даних, які виникають під час M2M-взаємодій.

Виробники всіх компонентів IoT наразі ігнорують безпеку систем, які вони виробляють; однією з причин невпровадження безпеки в компоненти IoT є висока кошторисна вартість. Це тягне за собою додаткові витрати на електроенергію і завдає шкоди системі IoT в цілому. Крім того, застосування безпекового підходу до систем IoT безпосередньо збільшує ціну всіх рішень на ринку. Розглянувши різні питання, можна сформулювати основні загрози, присутні в IoT.

Різноманітні проблеми, які часто виникають при використанні пристроїв, змусили багатьох дослідників в області інформаційної безпеки серйозно поставитися до питань безпеки. Порушення принципу наскрізної інформаційної безпеки першими помітили фахівці в цій галузі, і ця умова рекомендована для всіх систем IoT та інших сервісів.

Принцип наскрізної ІБ для різних пристроїв і сервісів у сфері "Інтернету речей" повинен існувати з ранніх стадій розробки продуктів, а після отримання готових пристроїв підтримка ІБ повинна забезпечуватися до останнього дня роботи таких "речей", вважає група дослідників HPE, виявила низку проблем, які виникають між розробниками та споживачами послуг Інтернету речей. Було виявлено такі проблеми, пов'язані з безпекою

- Незнання вимог безпеки власниками пристроїв.

Однією з найпоширеніших і найпростіших проблем є нездатність власників пристроїв змінити свої паролі після придбання та активації IoT-пристрою. У більшості випадків заводські паролі часто дублюються, що створює серйозну лазівку для зловмисників для використання пристрою. Тому власникам пристроїв рекомендується ретельніше ставитися до захисту своїх пристроїв.

Це пов'язано з тим, що багато "речей" не мають систем безпеки, що робить пристрої легкими воротами для мережевих вторгнень, які в кінцевому підсумку можуть призвести до значних збитків.

- Проблеми з шифруванням трафіку

Опитування, проведене HPE, показало, що приблизно 70% проаналізованих пристроїв не шифрують свій бездротовий трафік. Дослідження показало, що в 70% випадків трафік, що проходить між різними пристроями IoT, не був повністю захищений, з наступними проблемами

системи взагалі не захищені або не зашифровані.

- Багато xss уразливостей у веб-додатках пристроїв

Більшість (60%) веб-додатків на пристроях IoT мають різні небезпеки, пов'язані з міжсайтовим скриптингом (XSS) і неправильною організацією доступу.

- Багато паролів недостатньо надійні

- 90% різноманітної інформації збирається IoT-пристроями без відома власника

- Численні вразливості

Після детального аналізу різних типів IoT-пристроїв дослідники підрахували, що в різних пристроях IoT існує понад 20 вразливостей.

Висновок, до якого прийшла система IoT, був однозначним: безпека всіх компонентів IoT повністю відсутня. Нижче наведено короткий виклад висновків щодо типів виявлених вразливостей

- Електроживлення пристроїв

- Проблеми аутентифікації та стандартизації архітектури IoT та протоколів інформаційної безпеки;

- Проблеми з автентифікацією; Порушення принципів наскрізної ІБ; Розробники не підтримують свої продукти;

- Підвищення ризиків безпеки через відсутність нормальних оновлень програмного забезпечення та операційних систем; та

- Підвищена ймовірність успішних атак на мережу через нездатність пристроїв до самозахисту; [25,26,27,28]

- Використання незахищеної хмарної інфраструктури.

На початку 2019 року інша дослідницька група використовувала ресурси, призначені для приманки для зловмисників (HONIPOT), і отримала 276 000 унікальних і 105 мільйонів неунікальних атак. Як зазначають дослідники, кількість атак зросла в сім разів у порівнянні з 2018 роком. На даний момент злочинці створюють безліч бот-мереж, оскільки досі не існує рішення для вирішення величезної кількості проблем безпеки.

Кількість комп'ютерних атак стрімко зростає, оскільки користувачі та різні компанії займаються купівлею таких пристроїв, як роутери та камери, але байдуже ставляться до заходів протидії крадіжкам. Комп'ютерні злочинці здійснюють різні типи атак. Вони збирають багато заражених пристроїв з різних мереж для здійснення DDoS-атак або створюють власні проксі-сервери для інших шкідливих дій (таб. 3).

Таблиця 3

Ширина DDoS – атаки

		Пристрої які доступні					
		1%	10%	25%	50%	75%	100%
Використані прістрої	1%	36.28	362.78	906.96	1813.89	2720.83	3627.78
	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%	3627.78	36277.77	90694.43	181888.28	272083.28	362777.71

Оскільки більшість атак такого роду є дуже прихованими, малоймовірно, що користувачі будуть знати про них, враховуючи, що атаки на IoT не зачіпають складні та інтегровані системи. Примітно.

Це шкідливе програмне забезпечення засноване на використанні різних програм, які намагаються знайти вразливості в додатках і, в разі успіху, заразити пристрої. Після зараження пристрою ботнет використовує експлойти для подальшого контролю над ним.

Наступним за поширеністю виявився троян Nyadrop, на який припадає 38% усіх атак. Цей троянець використовує в своїх атаках методи грубої сили. Ще одним цікавим ботнетом був Gafgyt, на який припало 2% всіх атак.

Нижче наведено перелік різних методів (атак), які можуть бути використані для розробки пропозицій щодо посилення безпеки. [20]

- Методи "посилення", які використовують протоколи LDAP і TCP, атакують шляхом надсилання декількох повідомлень на сервер, які в кінцевому підсумку потрапляють на веб-сайт.

- У розподілених мережах поширеною атакою є модифікація інформації про маршрутизацію, де вузли мережі є маршрутизаторами, які можуть змінювати маршрути, збільшуючи таким чином час доставки пакетів.

- Загрози, основною метою яких є часткове видалення пакетів, називаються вибірковою передачею. Цей тип атаки залишає сліди на вузлах мережі, які потім можуть бути використані для подальших дій. Додавання різних атак, спрямованих на один вузол, до списку вибіркової передачі, основною метою яких є збір великих обсягів трафіку, підвищує ефективність атаки, тим самим створюючи такі проблеми, як

Знижує цілісність і доступність даних в мережі.

- Sinkhole-атаки - це метод збору трафіку шляхом отримання доступу до певного вузла. У разі успіху зловмисник може виконувати різні операції із захопленого вузла.

- Атаки Sybil використовуються для порушення маршрутизації та агрегації даних. Метою цієї атаки є отримання контролю над вузлом і використання псевдоідентифікаторів для видачі себе за кілька вузлів одночасно. Розподілене радіо.

Мережі з одноранговими вузлами є основними цілями цієї атаки.

- Атаки типу Wormhole спрямовані на перехоплення декількох вузлів мережі і, в разі успіху, створення маршруту для відправки перехоплених пакетів.

- Flood-атаки, які надсилають HELLO-пакети, відправляють велику кількість повідомлень в мережу, забиваючи фізичні характеристики пристрою.

Метою цієї атаки є перевантаження різних обчислювальних можливостей та інших критично важливих компонентів.

Формулювання рекомендацій з безпеки для користувачів IoT-систем.

- Зберігання довірених паролів.

За замовчуванням підключені IoT-пристрої мають однотипні стандартні паролі, тому основним захистом, який повинен здійснювати користувач, є надійне зберігання паролів. Вимогою в цьому випадку є зміна стандартного пароля. Якщо змінити пароль неможливо, пристрій не слід підключати до інфраструктури IoT.

- Надання повноважень.

Для забезпечення належної роботи IoT-пристрою та безпеки необхідно надати базовий рівень авторизації.

- Тестування пристрою

Перед підключенням пристроїв до мережі слід виконати повну перевірку працездатності. Як додатковий захід безпеки, протестуйте локальні та хмарні сервіси.

- Ізоляція IoT

Щоб ізолювати деякі IoT-пристрої від критичних мережевих ресурсів, слід створити додаткові мережі для взаємодії різних пристроїв і використовувати брандмауери.

- Управління трафіком IoT.

Весь небажаний вхідний трафік слід блокувати або сканувати відкриті порти пристрою, щоб з'ясувати, як зловмисник може скомпрометувати пристрій і закрити його.

- Використання шифрування

Використовуйте шифрування трафіку, якщо це можливо.

- Купуйте лише ті продукти, які підтримують оновлення.

2.8 Аналіз особливостей та загроз безпеки рівнів архітектури

Сенсорний рівень

Пристрої, які є частиною багаторівневої мережі, де інформація постійно збирається та обмінюється, роблять це завдяки взаємодії між смарт-мітками та мережею на рівні датчиків. На цьому рівні відбувається взаємодія з мережею.

Заради його визначення слід виділити наступні можливості

- При проектуванні систем IoT основними питаннями є ресурси, розмір, вартість і енергоспоживання, оскільки можуть використовуватися різноманітні RFID-мітки, RFID-зчитувачі та інші сенсорні пристрої;

- Наступною ключовою можливістю є розгортання, оскільки кінцеві точки Інтернету речей вимагають розгортання різноманітних сенсорних пристроїв;

- Інтернет речей наповнений різними пристроями, гібридними мережами і речами; такі системи повністю гетерогенні;

- Бездротові сенсорні мережі, SCADA, бездротові mesh-мережі та інші гібридні мережі;

Основною проблемою на рівні датчиків є безпека; IIoT стрімко зростає і основною метою Інтернету речей є підключення до промислових мереж для отримання різних інтелектуальних сервісів,

Це тягне за собою нові виклики при взаємодії з пристроями. Одним із прикладів є визначення довіреної особи, яка взаємодіє з даними користувача для аутентифікації та визначає рівень довіри до додатку.

Необхідність судити і приймати рішення самостійно, знати, що в один момент часу потрібно прийняти команду, а в інший - виконати завдання, є високим пріоритетом для моделі безпеки IoT.

Всі пристрої сенсорного рівня описуються такими характеристиками, як обмежений зв'язок і низьке енергоспоживання. Ця величезна кількість додатків Інтернету речей піднімає низку питань безпеки.

Проблеми безпеки.

На цьому рівні проблеми безпеки можна розділити на дві основні категорії

- Для кінцевих вузлів систем IoT безпека включає в себе наступні вимоги: аутентифікація, конфіденційність, цілісність, доступність, фізичний захист і управління контролем доступу;

- На рівні датчиків - автентифікація джерел і пристроїв, конфіденційність; і на цьому рівні необхідні автономність, доступність і цілісність.

На цьому рівні необхідні автономність, доступність і цілісність. На таблицях 4 і 5 показані найпоширеніші потенційні загрози і вразливості безпеки для кінцевих точок IoT.

Таблиця 4

Загрози безпеки та вразливості на кінцевому вузлі 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

Мережевий рівень

Мережевий рівень є невід'ємною частиною архітектури, оскільки він дає змогу всім об'єктам IoT отримувати інформацію про своє оточення через мережу. Цей рівень відповідає за передачу агрегованих даних на рівні датчиків і сервісів.

З огляду на те, що Інтернет речей складається з безлічі гібридних мереж, виникає безліч проблем, пов'язаних із мережевою взаємодією, безпекою та комунікаційними питаннями.

Таблиця 5

Аналіз загроз безпеки та вразливостей на сенсорному рівні

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

Для скоординованого виконання завдань мережевий рівень повинен враховувати вимоги до управління, планування та розгортання мережі:

- Технології для повного контролю та управління бездротовими, мобільними та фіксованими мережами

- Підвищення ефективності роботи мережі

- Пошук рішень проблем, пов'язаних із вимогами до якості обслуговування (QoS).

- Питання конфіденційності інформації.

- Питання безпеки та конфіденційності.

У перерахованих вище питаннях варто приділити особливу увагу недоторканності приватного життя людини, безпеці та конфіденційності даних, оскільки технології безпеки в IoT забезпечують лише базовий захист, у цій галузі залишається багато відкритих питань, і вирішення цих проблем має першорядне значення.

Нижче наведено вимоги до безпеки на мережевому рівні.

- До вимог безпеки на мережевому рівні належать: конфіденційність даних, конфіденційність і захист людини, цілісність, автентифікація, доступність і захист ключів;

- Витік конфіденційності - ще одна основна вимога безпеки. У ситуаціях, коли різні об'єкти IoT розташовані в доступних і ненадійних місцях, у разі фізичного контакту зловмисника з об'єктом у системі IoT може виникнути

проблема витоку інформації. Прикладом може слугувати ідентифікація користувача;

- Цілісність і конфіденційність при передачі сигналу між різними IoT-мережами створюють вимоги до безпеки зв'язку;

- Наступна за важливістю вимога - надмірність з'єднань, яка створює проблеми безпеки, пов'язані з DoS-атаками (через перевантаження мережі) і проблемами безпеки ключів (через високе споживання мережевих ресурсів). Ці проблеми виникають, коли користувачі втрачають контроль;

- Атаки типу "людина посередині" (Man-In-The-Middle, MITM) - це процес створення незалежних з'єднань між жертвою і зловмисником для передачі повідомлень. Атакуючого змушують повірити, що між жертвою і зловмисником існує приватне з'єднання, але в кінцевому підсумку жертва перебуває під контролем зловмисника;

Можливість запобігти створенню хибних сигналів для експлуатації пристрою - ще одна вимога безпеки проти підроблених мережевих повідомлень.

На таблицях 6 і 7 показано загрози та вразливості безпеки мережевого рівня.

Таблиця 6

Загрози безпеки на мережевому рівні

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 безпеки	Опис
Загрози передачі	Загрози передачі, такі як переривання, блокування, маніпулювання даними, підробка і т. д.
Маршрутна атака	Атаки на шлях маршрутизації

Слід також додати, що існують проблеми, пов'язані з безпекою протоколів систем IoT і мережевої інфраструктури. До числа проблем, для яких наразі не існує рішень, належать:

- Уразливості в паролях і засобах контролю доступу, що забезпечують аутентифікацію та авторизацію;

- Забезпечення шифрованої передачі даних на мережевому рівні;

Таблиця 7

Загрози безпеки та вразливості на мережевому рівні

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

Слід також додати, що існують проблеми, пов'язані з безпекою протоколів систем IoT і мережевої інфраструктури. До числа проблем, для яких наразі не існує рішень, належать:

- Уразливості в паролях і засобах контролю доступу, що забезпечують аутентифікацію та авторизацію;

- Забезпечення шифрованої передачі даних на мережевому рівні;

Рівень інтерфейсів

Концепція "розумного будинку", RFID-мітки, реалізується за допомогою стандартних протоколів Інтернету речей і технологій сервісних компонентів і розглядається на рівні інтерфейсу. Цей рівень залежить тільки від застосунку і тому вимагає дотримання таких вимог безпеки:

- Завантаження та оновлення програмного забезпечення, виправлення, необхідні для підтримання безпеки, та аутентифікація адміністратора;

- цілісність, конфіденційність, аутентифікація та авторизація.

На рівні інтерфейсу під час розроблення системи мають бути дотримані такі вимоги безпеки

- Безпека має бути реалізована в системах IoT, де кінцеві пристрої працюють без нагляду;

- При виборі рішення щодо забезпечення безпеки слід звернути увагу на збір енергоефективних методів;

- Приділяти достатню увагу прийняттю рішень для різних частин системи, враховуючи, що різні кінцеві точки можуть мати різні схеми захисту.

На таблицях 8 та 9 наведено загрози та вразливості безпеки на рівні інтерфейсу.

Таблиця 8

Загрози безпеки 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

Таким чином, інтерфейсний рівень виступає посередником між системою IoT і різними додатками. Цей рівень забезпечує легітимність взаємодії між додатками та системами.

Таблиця 9

Загрози безпеки та вразливості на рівні інтерфейсів

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

Таким чином, інтерфейсний рівень виступає посередником між системою IoT і різними додатками. Цей рівень забезпечує легітимність взаємодії між додатками та системами. [29,30]

Особливості рівня служб

Технологія Middleware - один з основних і найважливіших інструментів для підтримки сервісів і додатків. Сервісний рівень забезпечує економічно ефективну платформу для цієї системи, де апаратне та програмне забезпечення може бути використано повторно. Інтернет речей спирається на проміжне програмне забезпечення і являє собою діяльність, здійснювану з використанням різних стандартів, розроблених постачальниками послуг та організаціями.

Під час розроблення сервісного рівня враховували формування загальних вимог до API, додатків і сервісних протоколів. Такі ключові компоненти, як сервіси інтеграції та аналізу, сервіси опрацювання подій та аналогічні сервіси безпеки, забезпечують обмін даними між сервісами, а також обмін та опрацювання інформації, що відповідає діям на рівні сервісів.

Нижче наведено перелік послуг, що виконуються на цьому рівні

- Сервіси виявлення - це компоненти, що дають змогу знаходити конкретну інформацію та сервіси шляхом пошуку в ефективній інфраструктурі;

- сервіси збірки забезпечують можливість повної взаємодії між підключеними об'єктами; основна ідея полягає у створенні сервісів, які відповідають вимогам і вирізняються підвищеною надійністю;

- Здатність розуміти інструкції пристроїв, що надаються різними сервісами, і сприймати достовірну інформацію,

- Формування управління надійністю;

- Вимоги, які висуває користувач до забезпечення взаємодії між сервісами, виконуються сервісними API.

Було проведено багато досліджень, присвячених рішенням і міркуванням щодо поліпшення сервісного рівня:

- Архітектура SOCRADES була використана для підвищення ефективності між прикладним і сервісним рівнями;

- Об'єкти IoT представлені на нижніх рівнях, наприклад, служби виявлення мереж і служби обміну даними;

- Сервіси, що забезпечують взаємодію між додатками та іншими компонентами, також надаються на рівні сервісів.

Для вибору ефективної стратегії розв'язання проблеми необхідно дотримуватися таких вимог безпеки

- Нижче наведено вимоги безпеки для вибору ефективної стратегії розв'язання проблеми: автентифікація, тобто автентифікація послуг;

- Цей рівень вимагає дотримання вимог до захисту цілісності та конфіденційності, безпеки ключів і відмовостійкості;

- На цьому рівні основною проблемою є витік конфіденційності;

- зловживання послугами, наприклад, використання непідписаних послуг;

- Кінцеві вузли IoT, здатні виявляти маскувальні атаки;

- DoS-атаки;

- Захист від повторних атак;

- Аналізатори трафіку та інформаційні операції.

Щоб ухвалювати правильні рішення, система безпеки на рівні послуг повинна вміти захищати різні операції від загроз. На таб. 10 показано узагальнений список загроз безпеки.

На цьому рівні застосування безпеки має вирішальне значення. Існує безліч стандартів, протоколів і власних рішень, що конкурують один з одним; тут на перший план виходять архітектури SOA, оскільки вони можуть підвищити рівень безпеки, але сервісний рівень залишається проблемою безпеки під час передавання даних між різними рівнями та сервісами. Інші компоненти безпеки, контроль доступу та управління безпекою сервісів також повинні вирішувати ці проблеми.

Міжрівневі загрози

Архітектури SOA дають змогу забезпечити використання інформації на всіх чотирьох рівнях, щоб підвищити рівень сумісності між різними сервісами та пристроями. Впровадження такої функціональності ставить низку проблем, зокрема.

питання безпеки, пов'язані з конфіденційністю користувачів і їхніх даних, обміном даними через захищені ієрархії та надійністю.

У даній архітектурі IoT обмін інформацією між різними рівнями призводить до виникнення декількох загроз безпеці. [12,13,14]

Таблиця 10

Загрози безпеки на рівні служб

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

Методи забезпечення безпеки IoT мають свої відмінності та вимоги залежно від рівня, на якому вони використовуються. Використовувані рівні можна розділити на три типи. Сенсорний рівень є першим типом і в основному представлений фізичними об'єктами (датчиками, сенсорами), що використовують бездротові сенсорні мережі, Bluetooth, RFID та інші методи.

Таблиця 11

Загрози безпеки між рівнями в IoT архітектурі

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

Методи забезпечення безпеки IoT мають свої відмінності та вимоги залежно від рівня, на якому вони використовуються. Використовувані рівні можна розділити на три типи. Сенсорний рівень є першим типом і в основному представлений фізичними об'єктами (датчиками, сенсорами), що використовують бездротові сенсорні мережі, Bluetooth, RFID та інші методи.

Виходячи з вимог до безпеки IoT, визначених раніше, на цьому рівні висуваються такі вимоги, як конфіденційність, секретність, доступність, автентичність і цілісність. На таблиці 12 представлено порівняльний аналіз можливих методів забезпечення безпеки на рівні датчиків.

На мережевому рівні, де розташовані мобільні мережі та Інтернет, також існують свої методи забезпечення безпеки. Нижче представлено зображення методів забезпечення безпеки на мережевому рівні (таб. 12).

Забезпечення безпеки в Інтернеті речей (IoT) є критично важливим завданням у зв'язку зі зростанням кількості підключених пристроїв і збільшенням потенційних загроз. Для забезпечення безпеки IoT існують різні методи, які варіюються в залежності від конкретних вимог і характеристик системи. Одним з таких методів є шифрування даних, яке дозволяє захистити інформацію від несанкціонованого доступу шляхом перетворення її в незрозумілий формат без ключа доступу. [31,32,33]

Таблиця 12

Методи безпеки даних на рівні сенсорів

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 ін)	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 (RCS, 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 невиявлено, безпечна (дорога) передача даних не потрібна	Більшість таких алгоритмів потребує багато енергії та часу

Продовження таблиці 12

IDS/IPS	Забезпечують більшість вимог безпеки	Використовується для виявлення і запобігання більшості підозрілих користувачів і атак	Використовується для виявления 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, в другий рівень для шифрування даних RFID	Підвищує рівень безпеки для RFID даних та сигналів	Споживає потужність з час
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

Висновки до другого розділу

У другій частині було досліджено сучасні проблеми інформаційної безпеки в контексті розвитку технологій, зокрема Інтернету речей (IoT). Виявлено, що інтеграція великої кількості пристроїв у повсякденне життя створює нові загрози, які вимагають ефективних заходів захисту на різних рівнях архітектури.

Сучасні проблеми інформаційної безпеки включають зростаючу кількість кібератак, що націлені на крадіжку даних, порушення конфіденційності та експлуатацію вразливостей систем.

Питання безпеки Інтернету речей (IoT) є особливо актуальними, оскільки велика кількість з'єднаних пристроїв збільшує площу потенційних атак. Неналежна безпека цих пристроїв може призвести до серйозних наслідків, включаючи вторгнення у приватне життя та компрометацію критично важливих систем.

Безпека на сенсорному рівні полягає у захисті даних, що збираються сенсорами. Це включає шифрування даних, автентифікацію пристроїв та забезпечення цілісності інформації.

Безпека мережевого рівня спрямована на запобігання несанкціонованому доступу до мережевих ресурсів. Використовуються методи шифрування, управління доступом, а також розгортання систем виявлення та запобігання вторгнень.

Постановка задачі безпеки на рівні служб передбачає розробку та впровадження політик і процедур, які гарантують безпечну роботу сервісів, що використовуються в IoT-інфраструктурі.

Безпека рівня інтерфейсів включає захист комунікаційних протоколів і інтерфейсів між пристроями та системами. Забезпечення захисту від підробки даних та атаки типу "людина посередині" (MitM) є критично важливим.

Моніторинг проблем безпеки даних та пристроїв Інтернету речей передбачає постійне відстеження стану безпеки пристроїв та аналіз даних для виявлення аномалій та потенційних загроз.

Аналіз особливостей та загроз безпеки рівнів архітектури дозволяє ідентифікувати специфічні ризики, притаманні кожному рівню IoT-архітектури, і розробити відповідні захисні заходи.

РОЗДІЛ 3 РОЗРОБКА МЕТОДУ ЗАХИСТУ НА ПРИКЛАДІ ВІРТУАЛЬНОГО IoT ПРИСТРОЮ

3.1 Постановка задачі до проектування IoT системи

При проектуванні мережі Інтернету речей необхідно враховувати 2 компоненти:

- Проектування фізичної мережі;
- Проектування логічної мережі;

Фізичне проектування включає в себе все обладнання яке використовується, від маршрутизаторів, до кабелів.

Логічне проектування включає в себе деталі побудови мережі починаючи з L2, L2+, L3, L4 рівнями OCI, закінчуючи побудовою резервних каналів, та розширенням каналів.

Для спілкування IoT пристроям із сервером використовують протоколи різних рівнів, з допомогою яких буде змоге керувати IoT пристроями, та отримувати від них команди (рис. 3.1) [25,21,34]

Рис. 3.1 Протоколи які використовуються в IoT

На канальному рівні використовуються такі протоколи, що перелічені нижче:

1. WiFi, або 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
2. WiMAX - це стандарт для бездротових мереж метрополітену (WMAN), розроблений робочою групою № 16 IEEE 802, що спеціалізується на бездротовому широкосмуговому доступі від точки до багатоточок.
3. 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.
4. 2G/3G/4G - Це різні типи телекомунікаційних поколінь. Пристрої IoT на основі цих стандартів можуть обмінюватися даними через стільникові мережі.

На мережевому рівні загалом використовують IPv4 так як IPv6 наразі не надає ні один провайдер в Україні.

На транспортному рівні протоколи поділяються на 2 типи:

1. **Протокол керування передачею (TCP)**: Цей протокол забезпечує надійну передачу даних між двома хостами. Він гарантує, що дані будуть доставлені без помилок і в правильному порядку, навіть якщо в мережі виникають помилки. TCP використовується для таких програм, як веб-браузери, електронна пошта та передача файлів.
2. **Протокол користувацьких дейтаграм (UDP)**: Цей протокол не забезпечує надійності передачі даних. Дані надсилаються без гарантії доставки або правильного порядку. UDP використовується для таких програм, як потокове відео та онлайн-ігри, де швидкість і час очікування є більш важливими, ніж надійність.

Протоколи рівня додатків:

1. HTTP - Протокол передачі гіпертексту (HTTP) це протокол прикладного рівня для передачі гіпермедійних документів, таких як HTML.
2. 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.

3. 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.

4. MQTT - це протокол підключення машина до машини (M2M) Інтернет речей.

5. XMPP - це комунікаційний протокол для орієнтованого на повідомлення проміжного.

6. DDS - протокол проміжного програмного забезпечення та стандартом API для підключення, орієнтованого на дані, від Object Management Group.

7. AMQP - IoT складаються з жорстких компонентів, які маршрутизують і зберігають повідомлення в операторі брокера, з набором політик для з'єднання компонентів разом. [35,36,37]

Логічне проектування - це абстрактне розуміння суті і процесу.

Логічне проектування складається з:

- функціональний блок IoT;
- комунікаційна модель IoT;
- API зв'язку IoT.

Функціональні блоки IoT складаються з пристроїв, комунікацій, послуг, управління та додатків.

Функціональний блок пристрою відповідає за функції виявлення, моніторингу та контролю.;

- Функціональний підрозділ комунікацій відповідає за управління комунікаціями в системі Інтернету речей.

- Блок функціонального управління забезпечує різні функції управління системою Інтернет речей;

- Блок функціональної безпеки відповідає за захист системи Інтернету речей.

- Функціональний блок програми відповідає за управління різними аспектами Інтернету речей.

Модель комунікації IoT:

- модель відповіді на запит, в якій відбувається взаємодія клієнт-сервер;
- двотактна модель;
- Кілька моделей.

API зв’язку IoT. Найчастіше використовуються два API:

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

3.2 Побудова IoT системи

У систему Інтернету речей входять наступні пристрої:

- Інтелектуальний дверний замок (1);

- Інтелектуальна лампа (2) ;

- Датчик оптичного перемикання (2);

- Базові станції, шлюзи (1);

Використовуються наступні протоколи:

- - На канальному рівні для всіх датчиків використовується технологія WiFi;

- На мережевому рівні використовується протокол Ipv4;

- Транспортний рівень підтримує протоколи TCP і UDP;

На прикладному рівні використовуються протоколи-Mqtt і WebSocket.

На малюнку 3.2 показана топологія системи IOT, створеної за допомогою PacketTracer:

Топологія показує, що мережеве з'єднання між усіма датчиками в системі IOT забезпечує шлюз, відповідальний за маршрутизацію та передачу даних. Інтернет речей ізольований і має мережу 192.168.25.1/24. Система використовує модель "запит-відповідь" та посилання на основі REST та WebSockets.

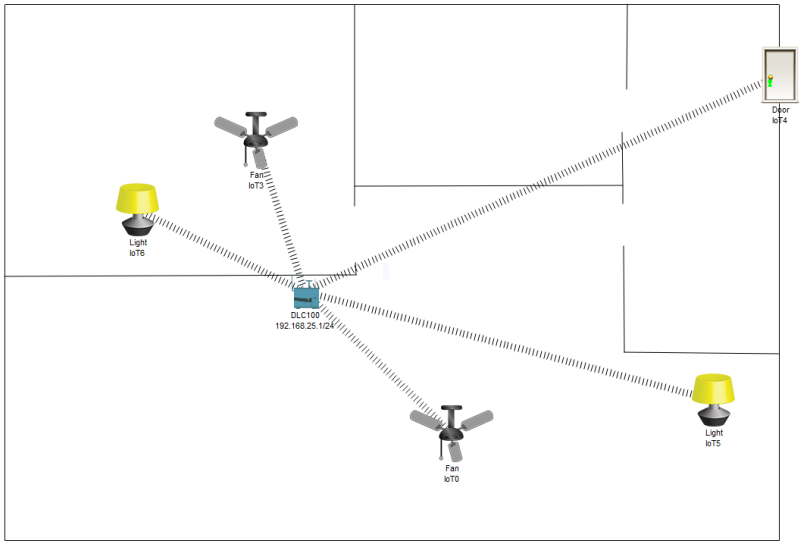

Рис. 3.2 Топологія інтернету речей

3.3 Вибір методів безпеки та їх реалізація

Використання аутентифікації TLS / SSL поверх MQTT (рис 3.3 та 3.4)

Використовуйте метод автентифікації, щоб додати автентифікацію TLS/SSL. На прикладному рівні, де в проектованої системі Інтернету речей використовується протокол MQTT, додана захист SSL/TLS, реалізована в платформі IBM Watson IOT.

Це пов'язано з системою Інтернету речей, створеною для об'єднання датчиків і хмари. Платформа Інтернету речей знаходиться між рівнем датчиків і рівнем додатків.

Замість датчиків ваш буде наведено приклад підключення віртуального IoT пристрою до платформи IBM Watson IOT.

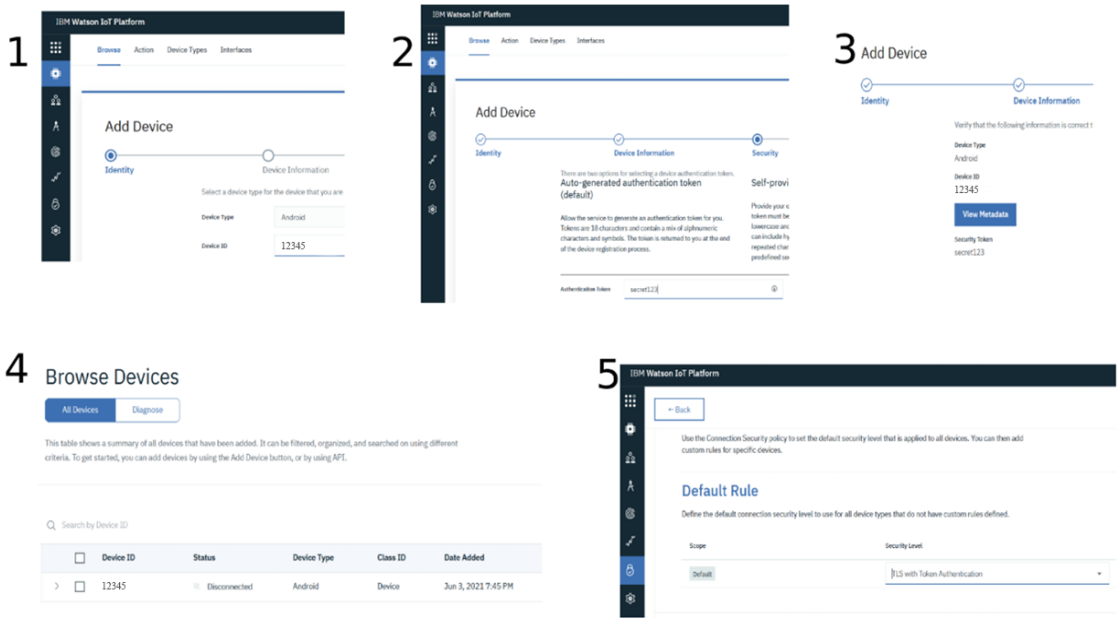

Рис. 3.3 Створення пристрою в IoT-плаформі

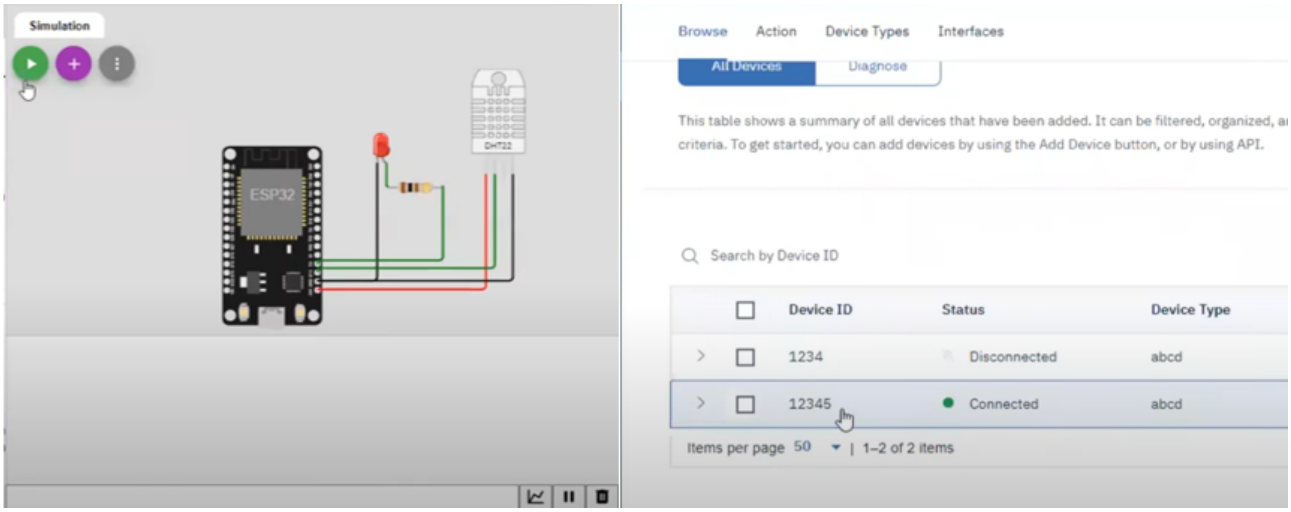

Рис. 3.4 Аутентифікація пристроя

Впровадження апаратних методів захисту.

Для підвищення безпеки обміну інформацією між об'єктами Інтернету речей реалізований модуль генерації ключів шифрування.

Найкращим рішенням є модуль TPM, оскільки він має багато спільних функцій (рис. 3.5):

- Забезпечує цілісність обладнання;
- Може працювати в безпечному режимі, щоб зменшити шкоду, заподіяну зараженням шкідливими програмами;
- Встановіть рівень довіри

Рис. 3.5 TPM модуль

Забезпечують зв'язок. Дослідження показують, що практично всі системи Інтернету речей не шифрують трафік. Тут необхідно визначити основні аспекти впровадження системи Інтернету речей:

- Шифрування трафіку;
-Аутентифікація;

Впровадження пропонованого рішення в систему Інтернету речей:

При проектуванні мережі для шифрування трафіку був обраний і використовувався метод Oval encryption, оскільки його швидкість є вигідною в порівнянні з іншими методами на слабкому чіпі.

Сертифікати безпеки 2.X. 509 забезпечують унікальну ідентифікацію пристроїв, дозволяють дізнатися, яким пристроям слід довіряти, і підвищують безпеку мережі. Аутентифікація відіграє важливу роль, оскільки допомагає обмежити доступ до мережі різних неперевірених пристроїв і служб.

Захист пристроїв на рівні коду. Щоб пристрій не став частиною ботнету і не брав участі в інших діях, запланованих зловмисником, він повинен виконувати

тільки ті функції, які покладені на пристрій на програмному рівні.Тобто в першу чергу необхідно створити захист для коду пристрою Інтернету речей.

Впровадження запропонованого рішення в систему Інтернету речей:

1.При проектуванні системи була обрана бібліотека OpenSSL для перевірки надійності і верифікації необхідного коду виконання пристрою.

Безпека при використанні пристрою. У розділі 2 обговорювалися численні загрози, що нависають над кінцевими точками Інтернету речей, такі як шкідливе програмне забезпечення, яке створює загрозу для пристроїв або використовує вразливості. [16,38]

Впровадження пропонованого рішення в систему Інтернету речей:

1. Впровадження систем контролю доступу. При впровадженні такої системи існує повне обмеження між усіма мережевими підключеннями і додатками. Впровадження системи контролю доступу підвищило захист від різних експлойтів.

Безпека управління пристроями. Незалежно від рівня безпеки мережі Інтернету речей, потенціал для загроз зберігається. На даному етапі забезпечення безпеки необхідно використовувати систему для аналізу інформаційної безпеки.

Впровадження пропонованого рішення в систему Інтернету речей:

1. Впровадження системи безпеки UBA analysis для виявлення аномальної поведінки користувачів. Система збирає різноманітну інформацію, будує поведінкові моделі і визначає аномальну активність.

Додаткові методи підвищення безпеки:

- Системні оновлення. Щоб мати можливість вчасно встановлювати виправлення від різних вразливостей, необхідно підтримувати постійні оновлення пристроїв Інтернету речей.

Також перед запуском системи необхідно виконати безпечне завантаження, яка представляє собою перевірку вбудованого програмного забезпечення системи.

- Впровадження програмного забезпечення для захисту від різних типів вірусів. Система проектування IoT забезпечує встановлення та використання антивірусного програмного забезпечення Symantec.

- Впровадження комплексу для проведення аудитів; щомісяця проводиться аудит мережевої інфраструктури за допомогою розробленої системи IoT. Рішенням для проведення аудиту був AWS IoT device Defender, сервіс аудиту Інтернету речей.

- Впровадження брандмауерів для поліпшення контролю вхідного і вихідного трафіку на пристроях Інтернету речей.

- Створення надійних і унікальних паролів і їх постійна зміна.

- Створення ізольованих мереж для Інтернету речей. Компанія має ізольовану мережу 192.168.25.1 / 24, що ускладнює зловмисникам доступ до неї. Нижче наведено графічне представлення методів захисту, що використовуються в проектованій системі Інтернету речей (рис. 3.6). [39,40]

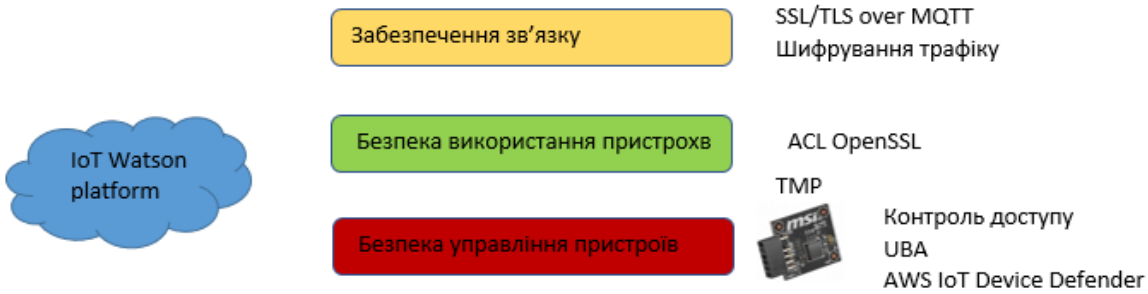

Рис. 3.6 Система методів безпеки для спроектованої системи IoT

Висновок до третього розділу

В даний час немає чітко визначених умов або вимог, тому кожна система Інтернету речей потребує свого власного комплексного рішення. При проектуванні мережевої безпеки Інтернету речей інформаційну безпеку необхідно розглядати з різних точок зору.Тому що в іншому випадку це буде неефективно, і зловмисник скористається слабкою стороною такої системи.

У цьому розділі основна увага приділяється наступним компонентам:

- Побудова і проектування системи Інтернету речей;
- Описується метод забезпечення безпеки в системі Інтернету речей.

Далі, при створенні методу мережевої безпеки, ми сформулювали концепцію конкретної системи Інтернету речей і запропонували наступні функції інформаційної безпеки:

- Забезпечення зв'язку;
- Безпека пристрою на рівні коду;
- Безпека при використанні пристрою;
- Безпека управління пристроєм.

Крім того, були запропоновані різні існуючі рішення для забезпечення безпеки та додаткові методи підвищення безпеки.

Ви виконали наступні завдання:

Були визначені основні компоненти Інтернету речей.

Було проведено аналіз загроз безпеці та вразливостей на кожному рівні для вивчення способів підвищення безпеки на різних рівнях.

Ми провели порівняльний аналіз методів забезпечення безпеки Інтернету речей.

Розроблено систему Internet of Things та запропоновано метод забезпечення безпеки для проектованої системи Internet of Things.

Надано рекомендації щодо застосування методів забезпечення безпеки в системі Internet of Things.

ВИСНОВОК

В першому розділі було піднято такі теми, як:

Історія виникнення та розвиток Інтернету речей (IoT). У цій частині визначено ключові етапи становлення та розвитку IoT, а також проаналізовано технологічні досягнення, що сприяли його появі та розвитку. Це дозволяє зрозуміти фундаментальні основи та еволюцію цієї технології.

Принципи роботи та використання IoT у сучасному світі. Тут досліджено основні принципи роботи IoT, включаючи компоненти систем IoT та їх взаємодію. Також розглянуто приклади застосування IoT у різних галузях, таких як промисловість, розумний дім, що демонструє широкі можливості та переваги цієї технології в сучасному світі.

В другому розділі було піднято такі теми, як:

Аналіз загроз безпеці та протоколи захисту в IoT. Було проведено аналіз основних загроз безпеки, що існують для IoT, а також сучасних проблем інформаційної безпеки. Представлено протоколи захисту, які використовуються на кожному рівні моделі OSI, що дає розуміння, як забезпечити безпеку даних та збереження конфіденційності в IoT.

Архітектура IoT та особливості безпеки на різних рівнях. Розглянуто загальну архітектуру IoT, визначено основні рівні та функції кожного з них. Проаналізовано особливості та загрози безпеки на кожному рівні архітектури IoT, що дає можливість детально оцінити ризики та розробити відповідні заходи захисту.

В третьому розділі показано модель побудови IoT та її захист. Наведено просту модель побудови IoT та визначено протоколи її захисту. Визначено ефективні заходи забезпечення безпеки в моделях IoT, що дозволяє впроваджувати надійні та захищені IoT-системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Greengard S. Internet of Things | Definition, History, Examples, & Privacy Concerns. Encyclopedia Britannica. URL: https://www.britannica.com/science/Internet-of-Things (date of access: 19.05.2024).
2. Major Milestones in IoT Technology History - IoT Marketing. IoT Marketing. URL: https://iotmktg.com/major-milestones-iot-technology-history/ (date of access: 19.05.2024).
3. Pieters N. The History of IoT. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/history-iot-nick-pieters?trk=article-ssr-frontend-pulse_more-articles_related-content-card (date of access: 19.05.2024).
4. What is Internet of Things | IGI Global. IGI Global: International Academic Publisher. URL: https://www.igi-global.com/dictionary/internet-of-things/15436 (date of access: 19.05.2024).
5. Architectural reference model. SlideShare. URL: https://www.slideshare.net/slideshow/architectural-reference-model/54761902 (date of access: 19.05.2024).
6. Kuruvilla G. Learn about the "Internet of Things" (IoT) in 3 minutes. Rumie. URL: https://learn.rumie.org/jR/bytes/learn-about-the-internet-of-things-io-t-in-3-minutes/?gad_source=1&gclid=Cj0KCQjwxqayBhDFARIsAANWRnTaF963ZB44lZKMDoYjjjpYJSUSM1C49YE9hKf22y9bG3NK0X91rKUaAlApEALw_wcB (date of access: 19.05.2024).
7. Top 7 enterprise cybersecurity challenges in 2024 URL: https://www.techtarget.com/searchsecurity/tip/Cybersecurity-challenges-and-how-to-address-them (date of access: 19.05.2024).
8. Розумний будинок - Безпека та відеоспостереження. Безпека та відеоспостереження. URL: https://oxorona.com/smart-home/ (дата звернення: 19.05.2024).
9. IoT Security Issues, Threats, and Defenses - Security News. Trend Micro (DE)|Branchenführende Plattform für Cybersicherheit. URL: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses (date of access: 19.05.2024).
10. Internet of Things (IoT) Security Challenges and Best Practices - Apriorit. Apriorit. URL: https://www.apriorit.com/white-papers/513-iot-security (date of access: 19.05.2024).
11. Architecture Reference Model. IOT notes by Parita. URL: https://iotnotesbyparita.wordpress.com/architecture-reference-model/ (date of access: 19.05.2024).

12. A Research Agenda for Service-Oriented Architecture (SOA): Maintenance and Evolution of Service-Oriented Systems. SEI Digital Library. URL: https://insights.sei.cmu.edu/library/a-research-agenda-for-service-oriented-architecture-soa-maintenance-and-evolution-of-service-oriented-systems/ (date of access: 19.05.2024).

13. Rhodes J. Microservices vs Service-Oriented Architecture (SOA): A Comparative Analysis. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/microservices-vs-service-oriented-architecture-soa-analysis-rhodes-bisrc (date of access: 19.05.2024).

14. Unveiling Market Trends. Service-Oriented Architecture (SOA) Market Report: 2031 Summary. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/service-oriented-architecture-soa-market-report-gjhge (date of access: 19.05.2024).

15. Gillis A. S. What is IoT (Internet of Things) and How Does it Work? | Definition from TechTarget. IoT Agenda. URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (date of access: 19.05.2024).

16. Internet of Things (IoT). SCIRP. URL: https://www.scirp.org/journal/paperinformation?paperid=108574 (date of access: 19.05.2024).

17. Information Security: Principles, Threats, and Solutions. HackerOne | #1 Trusted Security Platform and Hacker Program. URL: https://www.hackerone.com/knowledge-center/principles-threats-and-solutions (date of access: 19.05.2024).

18. IoT Reference Model / M. Bauer et al. SpringerLink. URL: https://link.springer.com/chapter/10.1007/978-3-642-40403-0_7 (date of access: 19.05.2024).

19. Academy B. I. 7 LAYERS OF CYBER SECURITY YOU SHOULD KNOW | Bilginç IT Academy. Bilginç IT Academy. URL: https://bilginc.com/en/blog/7-layers-of-cyber-security-you-should-know-5933/ (date of access: 19.05.2024).

20. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. PubMed Central (PMC). URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10136937/ (date of access: 19.05.2024).

21. Network Security – Network Layer. Online Tutorials, Courses, and eBooks Library|Tutorialspoint.URL: https://www.tutorialspoint.com/network_security/network_security_layer.htm (date of access: 19.05.2024).

22. Network Layer Security | SSL Protocols - javatpoint. www.javatpoint.com. URL: https://www.javatpoint.com/network-layer-security-ssl-protocols (date of access: 19.05.2024).

23. IoT Basics – IoT Connections. Telenor IoT. URL: https://iot.telenor.com/iot-insights/what-is-iot-connections/ (date of access: 19.05.2024).

24. Wrixte. IoT Security Monitoring: Protecting Your Connected Devices URL: https://www.linkedin.com/pulse/iot-security-monitoring-protecting-your-connected-devices-wrixte-co (date of access: 19.05.2024).

25. Contributors to Wikimedia projects. Link layer security - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Link_layer_security (date of access: 19.05.2024).

26. Hacker) G. E. (. E. Modern Problems in Cybersecurity and Innovative Solutions. LinkedIn: URL: https://www.linkedin.com/pulse/modern-problems-cybersecurity-innovative-solutions-giridaran-e (date of access: 19.05.2024).

27. Henke C. IoT Security: Risks, Examples, and Solutions | IoT Glossary. emnify | IoT Solution Provider. URL: https://www.emnify.com/iot-glossary/iot-security (date of access: 19.05.2024).

28. Hettema H. Implementing Security as a set of services. URL: https://www.linkedin.com/pulse/implementing-security-set-services-hinne-hettema (date of access: 19.05.2024).

29. Dac-Nhuong Le IoT: Security and Privacy Paradigm / Dac-Nhuong Le, Souvik Pal : CRC Press, 2020. – 399 p

30. Varadharajan, V., & Bansal, S. (2016). Data Security and Privacy in the Internet of Things (IoT) Environment. Connectivity Frameworks for Smart Devices, 261–281.

31. D. Wyatt, T. Choudhury, and J. Bilmes. 2007. Conversation detection and speaker segmentation in privacy-sensitive situated speech data. InInterspeech.

32. Network Setup, Configuration, Security and Support | Bajardo. Home | Bajardo. URL: https://bajardo-italia.it/contatti/network-setup-configuration-security-and-support/?gad_source=1&gclid=Cj0KCQjwxqayBhDFARIsAANWRnRhTt-fj59tpEWGOhzIMd1ZmaY6QdUuyQH0TRpTtgRT3s32J4tVuE4aAso8EALw_wcB (date of access: 19.05.2024).

33. 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.

34. What Are The Layers Of Network Security?. It Support Company | Managed Service Provider | Cyber Security. URL: https://computronixusa.com/what-are-the-layers-of-network-security/ (date of access: 19.05.2024).

35. Virtualization of Event Sources in Wireless Sensor Networks for the Internet of Things. PubMed Central (PMC). URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4299036/ (date of access: 19.05.2024).

36. 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.

37. Practical IoT Hacking / Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods : No Starch Press, 2021. – 434 p.

38. IOT BASED SMART IRRIGATION SYSTEM BY EXPLOITING DISTRIBUTED SENSORIAL NETWORK. SlideShare. URL: https://www.slideshare.net/slideshow/iot-based-smart-irrigation-system-by-exploiting-distributed-sensorial-network/250631374 (date of access: 19.05.2024).

39. Federated Cloud-Sharing Tool Is Own-Cloud, Produced by Own-Cloud.org. URL: https://owncloud.com/features/federated-cloud-sharing

40. Tschofenig, H., et al. (2015) Architectural Considerations in Smart Object Networking. Internet Architecture Board. URL: https://www.rfc-editor.org/rfc/rfc7452.txt