МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Система безпроводового зв’язку розумного будинку»

Виконавець: _____ Олександр ХРИСТЕНКО
(підпис)

Керівник: _____ Георгій КОНАХОВИЧ
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Христенка Олександра Ігоровича

(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Система безпроводового зв’язку розумного будинку» затверджена наказом ректора від «07» вересня 2022 р. №1321/ст

2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.

3. Вихідні дані до роботи розумний будинок, IoT, DDoS, WEP, WPA, Wi-FI

4. Зміст пояснювальної записки

Розділ 1 “Основні проблеми інтернету речей”

Розділ 2 “Проблеми безпеки IoT та технологій”

Розділ 3 “Методи підвищення захисту IoT та розумного будинку”

Розділ 4 “Вдосконалення генерації паролів для Wi-Fi”

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: 8 рисунків

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Основні проблеми інтернету речей	12.09.2022-05.10.2022	Виконано
4	Проблеми безпеки IoT та технологій	06.10.2022-15.10.2022	Виконано
5	Методи підвищення захисту IoT та розумного будинку	17.10.2022-29.11.2022	Виконано
6	Вдосконалення генерації паролів для Wi-Fi	30.10.2022-5.11.2022	Виконано
7	Охорона праці	07.11.2022-12.11.2022	Виконано
8	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Георгій КОНАХОВИЧ
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Олександр ХРИСТЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Система безпроводового зв’язку розумного будинку» містить 111 сторінок, 8 рисунків, 5 таблиці, 42 використаних джерел.

Ключові слова: розумний будинок, IoT, DDoS, WEP, WPA, Wi-FI

Об’єкт дослідження – безпека пристроїв IoT.

Предмет дослідження – розумні пристрої.

Мета кваліфікаційної роботи – Розробити методи підвищення ступеня захисту пристроїв розумного будинку.

Метод дослідження – для досягнення поставлених цілей в роботі використано: порівняльний метод, статистичний аналіз, структурний аналіз, прийоми аналізу наукової літератури, порівняльний метод.

Матеріали кваліфікаційної роботи рекомендується використовувати при розробці систем IoT та при впровадженні в домашніх умовах

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

DoS – Denial of Service

DDoS – Disturbed Denial of Service

OTA – Over-the-Air

RFID – Radio frequency identification

QoS – Quality of Service

IP – Internet Protocol

WEP – Wired Equivalent Privacy

WPA – Wi-Fi Protected Access

Wi-Fi – Wireless Fidelity

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

IoT – Internet of Things

MCU – Microcontroller Unit

RFID – Radio Frequency IDentification

SSL – Secure Sockets Layer

TLS – Transport Layer Security

SHA – Secure Hash Algorithm

HTTP – HyperText Transfer Protocol

ВСТУП

Актуальність теми. З поширеністю IoT ризики безпеки зростають, а особливості цих пристроїв роблять їх уразливими до кібератак. Один скомпрометований об'єкт мережі IoT робить вразливими усі інші притстрої всередині мережі. Оскільки IoT являє собою сукупність пристроїв або датчиків, об'єднаних у мережу, то всі загрози безпеці, які стосуються бездротових сенсорних мереж (WSN), Інтернету та Cloud, мають відношення до мереж IoT. Інтернет речей відкриває величезні можливості із супутнім ризиком. Відсутність надійної автентифікації пристроїв IoT, шифрування даних, управління ключами, тощо роблять мережу IoT вразливою для зовнішніх атак і загроз.

Мета і завдання дослідження. Мета кваліфікаційної роботи полягає в тому щоб розробити методи підвищення ступеня захисту пристроїв розумного будинку.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Дослідити основні проблеми безпеки розумних пристроїв
2. Розробити методи підвищення захисту IoT
3. Вдосконалити генерацію паролів для Wi-Fi

Об'єктом дослідження – безпека пристроїв IoT.

Предметом дослідження – розумні пристрої.

Методи досліджень. Для досягнення поставлених цілей в роботі використано: порівняльний метод, статистичний аналіз, структурний аналіз, прийоми аналізу наукової літератури, порівняльний метод.

Наукова новизна отриманих результатів. Методи захисту систем IoT та розумного будинку. Вдосконалення генерації паролей для бездротових мереж.

Практичне значення отриманих результатів. Матеріали кваліфікаційної роботи рекомендується використовувати при розробці систем IoT та при їх впровадженні в домашніх умовах або підприємстві.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2022 р.

РОЗДІЛ 1
ОСНОВНІ ПРОБЛЕМИ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Що таке Інтернет речей

Інтернет речей — це сучасний термін, який набув великої популярності в останні кілька років. Цю назву придумав Кевін Ештон у 1999 році під час презентації компанії Procter and Gamble (P&G) про підключення технології RFID до Інтернету.

Інтернет речей описує систему, в якій предмети у фізичному світі та датчики всередині цих елементів підключаються до Інтернету через бездротові та дротові Інтернет з'єднання. Ці датчики можуть використовувати різні комунікаційні технології, такі як RFID2, NFC3, Wi-Fi, Bluetooth, Zigbee або Thread. Мета цієї системи полягає в тому, щоб використовувати датчики для збору та аналізу даних, щоб надавати нову інформацію або підвищити ефективність існуючих систем, а також створити автономне середовище, де пристрої та людина безперебійно співпрацюють.

Завдяки швидко вдосконалюваним технологіям бездротового зв'язку з низьким енергоспоживанням, потужним, але відносно дешевим мікроконтролерам, машинному навчанню та хмарним технологіям, IoT може поширюватися у все більших сферах. Розумні будинки дозволяють заощаджувати електроенергію за рахунок більш ефективного використання електроенергії та систем контролю температури, а також забезпечують своїм власникам підвищений комфорт завдяки автоматичному освітленню, контролю за домом через телефон, та кращій безпеці. У сфері охорони здоров'я медичні системи в лікарнях можуть стати більш досконалими, оснастивши пацієнтів пристроями, які повідомляють про стан здоров'я або місцезнаходження безпосередньо своїм лікарям. Industry 4.0 [3] використовує переваги Інтернету речей для модернізації автоматизації на підприємствах, забезпечення зв'язку "машина-машина", а також моніторингу використання

обладнання та потреб у обслуговуванні. Сільськогосподарська промисловість може використовувати дані датчиків для кращого та ефективнішого догляду за тваринами та рослинами.

1.2 Технології IoT

Успіх Інтернету речей залежить від широкого спектру технологій. Серед них апаратні компоненти, такі як датчики або мікроконтролери, які мають бути енергоефективними, якщо використовуються для кінцевих пристроїв, або достатньо потужними, щоб підтримувати велику мережу IoT або навіть обробляти вихідні дані мережі. Крім того, програмні технології, які забезпечують функціональність і комунікаційні можливості для цих MCU, також повинні відповідати цим вимогам, тому за останні два десятиліття з'явилося так багато нових комунікаційних технологій і протоколів, орієнтованих на IoT, з низьким енергоспоживанням. Також, з'являються спрощені версії IoT поширених операційних систем, які можна використовувати на розумних шлюзах.

Крім того, хмарні обчислення набули великої популярності, оскільки вони надають можливість обробляти та зберігати величезні обсяги даних, створених мережами IoT та забезпечувати автоматизацію шляхом аналізу даних і управління кінцевими пристроями без необхідності компаніям підтримувати власні сервери. Однак останнім часом периферійні обчислення почали ставати новою нормою, оскільки мікроконтролери стають все потужнішими та можуть самостійно впоратися зі складністю обробки даних. Технології штучного інтелекту також відіграватимуть важливу роль у можливому загальному впровадженні Інтернету речей у світі, оскільки вони можуть забезпечити ефективність і автономність мереж Інтернету речей.

Іншою важливою сферою є конфіденційність і безпека мереж IoT, яка включає як програмне забезпечення, наприклад, у формі криптографічних алгоритмів, так і апаратне забезпечення, яке можна використовувати для безпечного зберігання ключів та паролів, що використовуються для захисту доступу до мережі та зв'язку.

За останні три десятиліття було розроблено широкий спектр технологій підключення, корисних для IoT. Деякі з попередніх включають RFID, Bluetooth і Wi-Fi, серед більш сучасних – NFC, Zigbee, Thread і Bluetooth Low Energy. Zigbee і Thread засновані на стандарті IEEE 802.15.4, який зосереджується на низькошвидкісних бездротових персональних мережах з пристроями з низьким споживанням енергії. Bluetooth Low Energy - це нова версія Bluetooth, яка також була створена з урахуванням низького енергоспоживання.

Протоколи зв'язку з великими накладними витратами, такі як TCP/IP, не підходять для малопотужних мікроконтролерів. Завдяки цьому були винайдені більш ефективні комунікаційні протоколи, орієнтовані на IoT, такі як CoAP, MQTT, AMQP або XMPP-IoT.

1.2.1 Zigbee

Технологія Zigbee розроблена членами Zigbee Alliance. Вони зосереджені на створенні стандарту для Інтернету речей. Zigbee 3.04 - це їхнє останнє уніфіковане рішення, яке базується на IEEE 802.15.4, Zigbee PRO та бібліотеці кластерів Zigbee. Zigbee підтримує великі мережі з низьким енергоспоживанням, що працюють у діапазоні нижче 1 ГГц локально та 2,4 ГГц у глобальному масштабі. Zigbee PRO підтримує чотири типи пристроїв - кінцеві пристрої, маршрутизатори, які обслуговують мережу, координатори, які створюють, підтримують і захищають мережу, і шлюзи, що забезпечують підключення до Інтернету. Пристрої можуть підтримувати Zigbee Green Energy, яка є технологією накопичення енергії, що дозволяє використовувати невеликі датчики або пристрої без батареї або дротового джерела живлення. Пристрої Zigbee обмінюються даними через протокол прикладного рівня під назвою Dotdot і у співпраці з Thread Group, Dotdot може використовуватися з пристроями Thread для інтеграції підключення IPv6 до мереж Zigbee. [1]

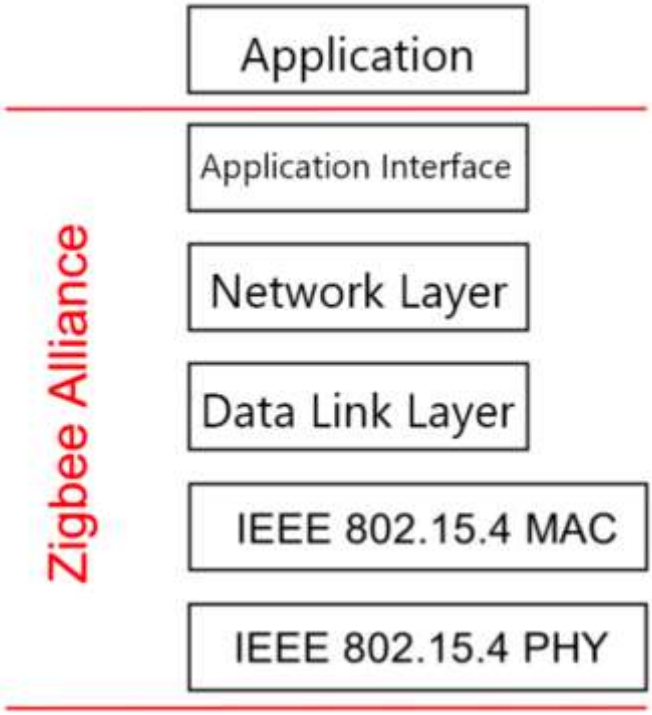

Рис 1.1 Архітектура Zigbee

1.2.2 Bluetooth

Bluetooth - це технологія, створена в 1994 році, яка забезпечує бездротову передачу даних між пристроями, такі як передач музики до навушників або зв'язок між телефоном та автомобілем. У 2011 році Bluetooth Low Energy був випущений з упором на малопотужні пристрої та Інтернет речей. Пристрої, які використовують BLE, проводять більшу частину свого робочого часу в режимі сну, що забезпечує низьке споживання енергії. У 2017 році BLE було розширено через специфікацію Bluetooth Mesh Profile. [2]

1.2.3 Thread

Thread - це протокол бездротового mesh зв'язку, винайдений і підтримуваний Thread Group. Основними напрямками цієї технології є розумні будинки та розумні комерційні будівлі. Він розроблений як малопотужний, безпечний та заснований на IEEE 802.15.4. Thread забезпечує зв'язок IPv6 з пристроями через 6LoWPAN, відкритого стандарту рівня адаптації для транспортування пакетів IPv6 у мережах IEEE 802.15.4. Thread підтримує кілька типів пристроїв у своїх мережах:

прикордонний маршрутизатор, кінцевий пристрій відповідний маршрутизатору, кінцевий пристрій і кінцевий пристрій у режимі сну. [3]

Прикордонний маршрутизатор - це особливий тип маршрутизатора, який забезпечує підключення мережі 802.15.4 до мереж на інших фізичних рівнях, як-от Wi-Fi або Bluetooth. Вони також обслуговують мережу 802.15.4 і надають різноманітні послуги, наприклад маршрутизацію для операцій поза мережею. Одна мережа Thread може мати кілька прикордонних маршрутизаторів. В такому випадку, мережа не має єдиної точки збою для підключення за межами Thread.

Маршрутизатори забезпечують служби маршрутизації, підключення та служби безпеки для мережевих пристроїв і пристроїв, які намагаються приєднатися до мережі. Відповідний маршрутизатору, кінцевий пристрій за потреби може стати маршрутизатором або його роль може бути знижена і він стане звичайним кінцевим пристроєм. Після пониження вони не пересилають повідомлення та не надають зазначені послуги. Підвищенням і пониженням ролі кінцевих пристроїв, керує мережа Thread без необхідності взаємодії з користувачем. Ці пристрої не можуть переходити в режим сну для економії енергії.

Кінцеві пристрої в режимі сну не надають жодних мережевих послуг і потребують головного маршрутизатора, щоб мати можливість спілкуватися з рештою мережі. Проте більшу частину свого часу вони проводять в режимі сну, таким чином зберігаючи енергію та гарантуючи, що вони можуть працювати роками, використовуючи батарейку типу «таблетка».

Коли принаймні два маршрутизатори знаходяться в мережі, стек Thread утворює mesh топологію. Якщо присутній лише один маршрутизатор або прикордонний маршрутизатор, мережа працює з базовою зіркоподібною топологією. Mesh Thread є самовідновлюваним і не має єдиної точки збою, що означає, що коли один із маршрутизаторів зникає, пристрої, які їх потребували, автоматично знаходять заміну та виявляють альтернативні маршрути для підтримки повної функціональності.

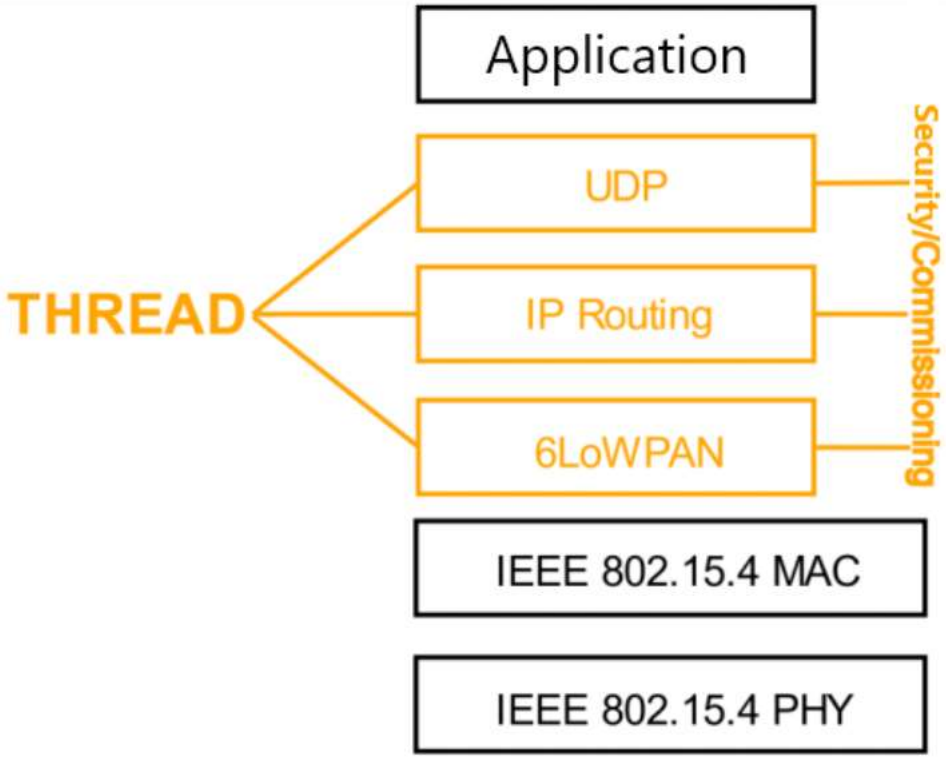

Рис 1.2 Архітектура Thread

Стек Tread описує три фази підключення нових пристроїв до мережі. Спочатку пристрій переходить у фазу виявлення, під час якої він виявляє мережу Thread і встановлює контакт з маршрутизатором для введення в експлуатацію. Це робиться шляхом сканування всіх доступних каналів, надсилання запитів маяків на кожен і очікування потенційних відповідей. Після виявлення маршрутизатора пристрій починає обмінюватися даними з ним, щоб можна було розпочати етап введення в експлуатацію. Якщо пристрій уже введено в експлуатацію, йому взагалі не потрібно переходити у фазу виявлення.

На етапі введення в експлуатацію пристрій або використовує інформацію, надану йому методом Out-of-band, щоб підключитися до мережі Thread, або встановлюється сесія введення в експлуатацію між пристроєм та програмою для введення в експлуатацію на смартфоні, планшеті або сервісом в Інтернеті. Через цю сесію пристрій отримує необхідну інформацію для підключення до мережі. На етапі введення в експлуатацію пристрою потрібен правильний попередній спільний ключ для пристрою (PSKd) і головний ключ мережі, щоб отримати дозвіл на приєднання.

Нарешті, пристрій підключається до мережі, обмінюється конфігураційними повідомленнями зі своїм головним маршрутизатором і отримує мережеву адресу від маршрутизатора.

Таблиця 1.1

Порівняння технологій

	Thread	Zigbee 3.0	Bluetooth Low energy
Стандарт	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.1
Частота	2.4 ГГц	2.4 ГГц, до ГГц	2.4 ГГц
Радіус	20-30 м	10-20 м	200 м
Швидкість передачі	250 Кб/с	250 Кб/с	до 2 Мб/с
IPv6	Так, 6LoWPAN	Ні	Ні
Макс к-сть пристроїв	250	65000	Без обмежень
Топологія	Mesh, Star	Mesh, Star, Tree	Mesh, Point-to-Point, Broadcast
Підключення до хмари	Border Router, Gateway	Mesh, Star, Tree Gateway	Mesh, Point-to-Point, Broadcast Smartphone, Gateway

1.2.4 Хмарні обчислення

Хмарні обчислення - це модель обчислень на вимогу, що складається з автономних мережевих IT (апаратних та/або програмних) ресурсів. Головна перевага цієї моделі полягає в тому, що організаціям більше не потрібно володіти та підтримувати власні центри обробки даних, а натомість вони можуть отримувати ресурси за запитом від постачальника хмарних обчислень. Ці хмари швидко масштабуються, дозволяють об’єднувати ресурси, де кілька споживачів

використовують один і той самий пул ресурсів. Вони також прості у використанні, оскільки їхні постачальники зазвичай пропонують доступ до графічного інтерфейсу користувача та посібники з розробки, а також на основі підписки, що дозволяє споживачам платити лише за той час і ресурси, які їм потрібні.

Хмарні платформи часто поділяють на три категорії: програмне забезпечення як сервіс (SaaS), платформа як сервіс (PaaS) та інфраструктура як сервіс (IaaS). Інфраструктура як послуга надає споживачам доступ до обробки, зберігання, мереж та інших ресурсів, де споживач може розгортати та запускати довільне програмне забезпечення. Платформа як послуга дозволяє споживачам використовувати мови програмування, бібліотеки, сервіси та інструменти, які підтримуються постачальником, для розгортання в хмарній інфраструктурі. Програмне забезпечення як послуга надає користувачам можливість використовувати програми, що працюють у хмарній інфраструктурі.

Хмарні обчислення є дуже важливою частиною Інтернету речей. Це дозволяє датчикам збирати дуже великі обсяги даних і зберігати їх у базах даних із високим ступенем масштабування. Він надає засоби для проведення глибокої аналітики таких даних, використання машинного навчання для підвищення ефективності систем Інтернету речей. У попередні роки тенденція полягала в тому, щоб використовувати обчислювальні можливості хмари для вдосконалення малопотужних пристроїв із низькою продуктивністю та виконання більшої частини обробки на хмарних платформах. Однак із зростанням занепокоєння щодо конфіденційності даних і вдосконаленням мікроконтролерів Edge computing стає новою популярною ідеєю. Edge computin використовують сильні сторони шлюзів або навіть кінцевих пристроїв, оснащених потужнішими мікроконтролерами, щоб зробити велику частину обчислень локальними, зменшуючи затримку, покращуючи конфіденційність і зменшуючи залежність мережі від хмари.

1.2.5 Edge Computing

Переваги Edge Computing включають можливість обробки масивних даних, створених пристроями на межі мережі, замість передачі їх у централізовану хмару.

Воно може надавати послуги з швидшою відповіддю та кращою якістю і його можна вважати інфраструктурою Інтернету речей майбутнього. Вони також описують різні підходи до периферійних обчислень, які реалізуються сьогодні.

Cloudlets - це невеликі центри обробки даних, розташовані на межі Інтернету. Вони спрямовані на покращення наскрізного реагування між мобільним пристроєм і хмарою. Вони складаються з потужних комп'ютерів, які надають потужні обчислювальні ресурси найближчим мобільним пристроям із меншою затримкою. Вони можуть служити посередником між мобільними пристроями та хмарою. Cloudlets повинні бути набагато гнучкішими у своєму забезпеченні, оскільки мобільні пристрої підключаються до них динамічно завдяки мобільності користувачів. Технологію передачі віртуальної машини потрібно використовувати для передачі необхідних служб між Cloudlets під час руху користувача. Мобільні пристрої повинні виявити Cloudlets, оскільки вони є невеликими, територіально розподіленими центрами обробки даних. Вони можуть покращити надійність усієї системи IoT, додавши рівень між потенційними кібератаками та хмарою та інкапсулюючи середовище кожного користувача в окрему віртуальну машину.

Mobile edge networking визначається як технологія, яка забезпечує середовище IT-послуг і можливості хмарних обчислень на межі мобільної мережі. Це може бути представлено програмами, що працюють як віртуальна машина на потужній мобільній периферійній платформі. Його можна використовувати для керування потоковими відеосервісами в розумних містах, доповненій реальності чи розумних автомобілях. Він може збирати, класифікувати та аналізувати потоки даних IoT, керувати протоколами, розповсюдженням повідомлень і обробкою аналітики.

Нарешті, Fog Computing спрямований на розподіл ресурсів і послуг від хмари до речей, використовуючи потужніші кінцеві вузли, де це можливо, і невеликі хмари на межі. Він може забезпечити взаємодію з IoT, 5G, віртуальною реальністю та іншими додатками. Він створює ієрархічну мережу Fog, яка може спілкуватися між собою та з хмарою. Кожен Fog може самостійно збирати та обробляти дані або передавати їх за ієрархією за потреби.

1.2.6 Операційна система

З появою таких пристроїв, як Raspberry Pi і збільшенням кількості потужних мікроконтролерів з низьким енергоспоживанням на ринку, постачальники ОС почали розробляти простіші або менш ресурсомісткі версії своїх систем, які можна використовувати для пристроїв IoT. Серед них Ubuntu Core, Windows 10 IoT і Android Things. Ці операційні системи мають деякі спільні атрибути, важливі для пристроїв IoT: вони створені для більшої безпеки, дозволяють оновлення по повітрю та швидку розробку. Крім того, Windows 10 IoT можна легко інтегрувати з хмарною платформою Microsoft Azure, тоді як Android Things так само можна інтегрувати з Google Cloud.

Розробники мають вибір між запуском цих ОС на потужних кінцевих пристроях і підключенням їх безпосередньо до Хмари або використанням шлюзу, який запускає ОС і спілкується з Хмарою від імені кінцевих пристроїв.

Android Things - це операційна система, створена компанією Google і призначена для пристроїв Інтернету речей. Вона базується на Project Brillo, яка була іншою операційною системою від Google, і хоча обидві мають одне ядро, Brillo була зосереджена на розробці C++, тоді як Android Things підтримує Android SDK. Android Things розширює основну структуру Android і дає розробникам можливість розробляти за допомогою Android SDK і Android Studio, отримати доступ до апаратного забезпечення через інфраструктуру Android, інтегрувати додаткові периферійні пристрої через Peripheral I/O API і використовувати консоль Android Things для надсилання через повітря функціонал та оновлення безпеки. Він підтримується кількома наборами для розробки, включаючи NXP Pico i.MX7D і Raspberry Pi 3 Model B. [4]

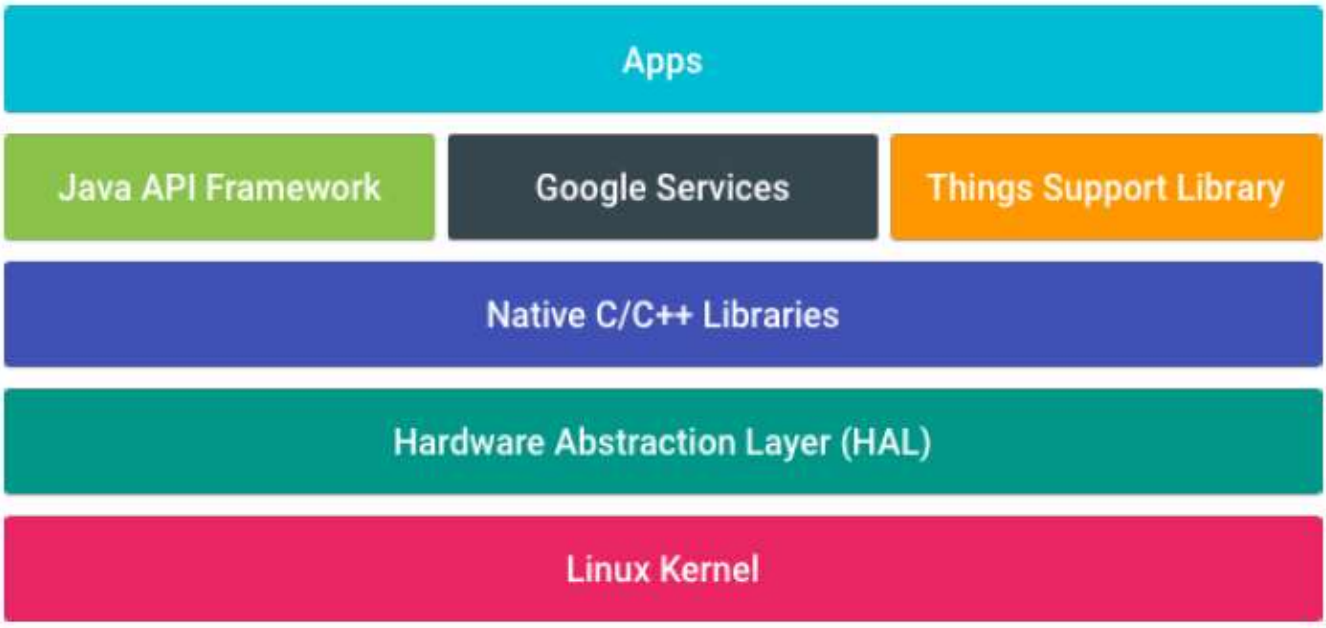

Рис. 1.3. Архітектура платформи Android Things

1.2.7 Обладнання

Пристрої, які використовуються для IoT, можна загалом розділити на дві категорії: малопотужні пристрої з меншою обчислювальною потужністю, але кращим енергозбереженням, які використовують такі технології, як Zigbee або Thread і потужніші пристрої з операційними системами IoT, як-от Windows 10 IoT або Android Things які зазвичай підключаються до Інтернету безпосередньо.

Кілька компаній зосереджені на створенні малопотужних мікроконтролерів, придатних для розробки IoT. Серед них Texas Instruments із бездротовим мікроконтролером CC2650, здатним спілкуватися через Bluetooth Low Energy, Zigbee та 6LoWPAN. STMicroelectronics пропонує серію багатопротокольних пристроїв STM32WB55xx, які також можуть обмінюватися даними через Bluetooth Low Energy та протоколи на основі IEEE 802.15.4. Компанія NXP Semiconductors також виробляє пристрої KW41Z з наднизьким споживанням енергії, використовуючи підключення Bluetooth Low Energy і IEEE 802.15.4.

Розробні плати та невеликі комп’ютери, такі як Raspberry Pi, Qualcomm DragonBoard або NXP Pico, є достатньо потужними, щоб повністю використовувати вищезазначені операційні системи і тому можуть діяти як потужні, але більш

енергоємні кінцеві пристрої або мережеві шлюзи, підключаючи малопотужні мережі до Інтернету.

1.2.8 Криптографія

Основними поняттями криптографії, є приватність/конфіденційність, автентифікація, цілісність, неспростовність та обмін ключами. Приватність гарантує, що лише призначений отримувач може прочитати дані повідомлення, автентифікація - це процес підтвердження особи, цілісність - це гарантія того, що передане повідомлення не підроблено, неспростовність - це механізм перевірки того, що відправник дійсно надіслав повідомлення, а обмін ключами - це метод обміну криптографічними ключами між відправником і одержувачем. Криптографічні алгоритми класифікуються на три категорії: криптографія секретного ключа, криптографія відкритого ключа та хеш-функції.

Криптографія із секретним ключем використовує один ключ як для шифрування, так і для дешифрування повідомлень. Відправник бере повідомлення у відкритому вигляді, шифрує його за допомогою секретного ключа та надсилає як зашифрований текст одержувачу. Потім одержувач використовує той самий ключ, щоб розшифрувати зашифрований текст назад до читабельного відкритого тексту. Оскільки обидві сторони використовують однаковий ключ, цей метод також називають симетричним шифруванням. Метод працює або в режимі потокових шифрів, або в режимі блочних шифрів. Потокові шифри працюють з окремими бітами, байтами або комп’ютерними словами за раз і використовують механізм зворотного зв’язку, щоб забезпечити постійну зміну ключа. З іншого боку, блокові шифри оперують блоками даних, використовуючи щоразу один і той самий ключ. Загалом відкритий текст, зашифрований потоковим шифром, щоразу шифруватиме інший зашифрований текст, тоді як відкритий текст блокового шифру завжди шифруватиме той самий зашифрований текст.

Криптографія з відкритим ключем залежить від математичних функцій, які називаються односторонніми функціями, які легко обчислити, але зворотні функції яких важко обчислити. У схемі використовуються два математично пов’язані ключі,

але один не можна використовувати для визначення іншого. Один із ключів можна використовувати для шифрування відкритого тексту, а інший – для розшифровки отриманого зашифрованого тексту і це не має значення, який ключ застосовано першим. Оскільки відправник і одержувач використовують різні ключі, цей підхід називається асиметричним шифруванням. Одним із найбільш часто використовуваних алгоритмів відкритих ключів є алгоритм RSA, який можна використовувати для обміну ключами, цифрових підписів або шифрування невеликих блоків даних.

Хеш-функції або дайджести повідомлень або одностороннє шифрування - це алгоритми, які не використовують жодних ключів. Замість цього вони використовують хеш-значення фіксованої довжини, обчислене на основі відкритого тексту, що робить його таким, що неможливо відновити ні вміст, ні довжину оригінального відкритого тексту. Вони часто використовуються для шифрування паролів, для цифрового друку пальців або для забезпечення цілісності комп'ютерного файлу. Оскільки це односторонні алгоритми шифрування, зашифрований текст неможливо розшифрувати. Сьогодні широко використовувані алгоритми хешування включають алгоритми дайджесту повідомлень (MD), які є серією байтових алгоритмів, які створюють 128-бітне значення хешування з повідомлення довільної довжини, і алгоритми безпечного хешування (SHA).

Рівень захищених сокетів (SSL) і захист транспортного рівня (TLS) - це протоколи, які забезпечують безпечні транзакції через протоколи зв'язку, такі як HTTP. SSL використовує сертифікати RSA для автентифікації та початкового рукостискання, після чого обидві кінцеві точки зв'язку узгоджують схему шифрування. Після того, як було виявлено, що SSL скомпрометований, протокол TLS став новим популярним протоколом. Він розширюється та має зворотну сумісність із SSL, підтримує додаткові криптографічні схеми та використовується для зв'язку HTTPS. Зв'язок між клієнтом і сервером ініціюється після рукостискання протоколу TLS, яке має три фази. Спочатку виконується незашифрований обмін ключами. Після цього весь зв'язок шифрується, починаючи з другої фази рукостискання, де сервер надсилає параметри сервера, які визначають додаткові параметри рукостискання.

Нарешті, сервер і, за бажанням, клієнт проходять автентифікацію, ключі підтверджуються, а цілісність рукостискання гарантується.

1.3 Еволюція автономних систем

Однією з найбільших переваг Інтернету речей є автономні системи, які керують цілими мережами пристроїв на основі власних рішень за допомогою машинного навчання або попередньо запрограмованих правил, щоб забезпечити ефективність і підвищити якість життя всюди, починаючи з фабрик і промислових підприємств. рослин для сільського господарства, міст, будинків тощо. Початковий підхід до цієї концепції полягав у повній інтеграції Інтернету речей із хмарними обчисленнями та залишення більшої частини обробки даних, створених мережами IoT, у хмарі. Дослідники зосередилися на труднощах впровадження розширених функцій, таких як обробка даних, на слабких обчислювальних пристроях, і проаналізували тенденції та технології, які використовувалися на той час. Вони запровадили нову парадигму, яку назвали CloudIoT, яка об’єднує хмару та IoT для покращення їх обох. З їхньою пропозицією хмара принесе кращі ресурси зберігання для IoT, оскільки величезні обсяги неструктурованих або напівструктурованих даних, створених пристроями IoT, можна буде зберігати на практично безмежних хмарних серверах. Крім того, це забезпечить набагато більші та більш масштабовані обчислювальні ресурси та дозволить обробку даних, що було не дуже можливо зробити на місці. Нарешті, хмара слугувала б свого роду комунікаційним центром, де всі пристрої та програми могли б підключатися та спілкуватися один з одним. Документи також пропонують можливі застосування CloudIoT, наприклад, в охороні здоров’я, розумних містах або розумних будинках. Наприкінці вони також коротко згадують Fog Computing, який є підмножиною Edge Computing, показуючи, як швидко IoT продовжує розвиватися та змінюватися.

Тенденція до інтеграції цих двох областей також була очевидною з того, як постачальники хмарних платформ рекламували свої рішення та які вони пропонували способи їх використання. Наприклад, Google Cloud раніше рекомендував надсилати

всі дані своєму брокеру MQTT і використовувати їхні хмарні сервіси для аналізу та обробки даних і відповіді на пристрої новими командами, як можна побачити на малюнку 1.4.

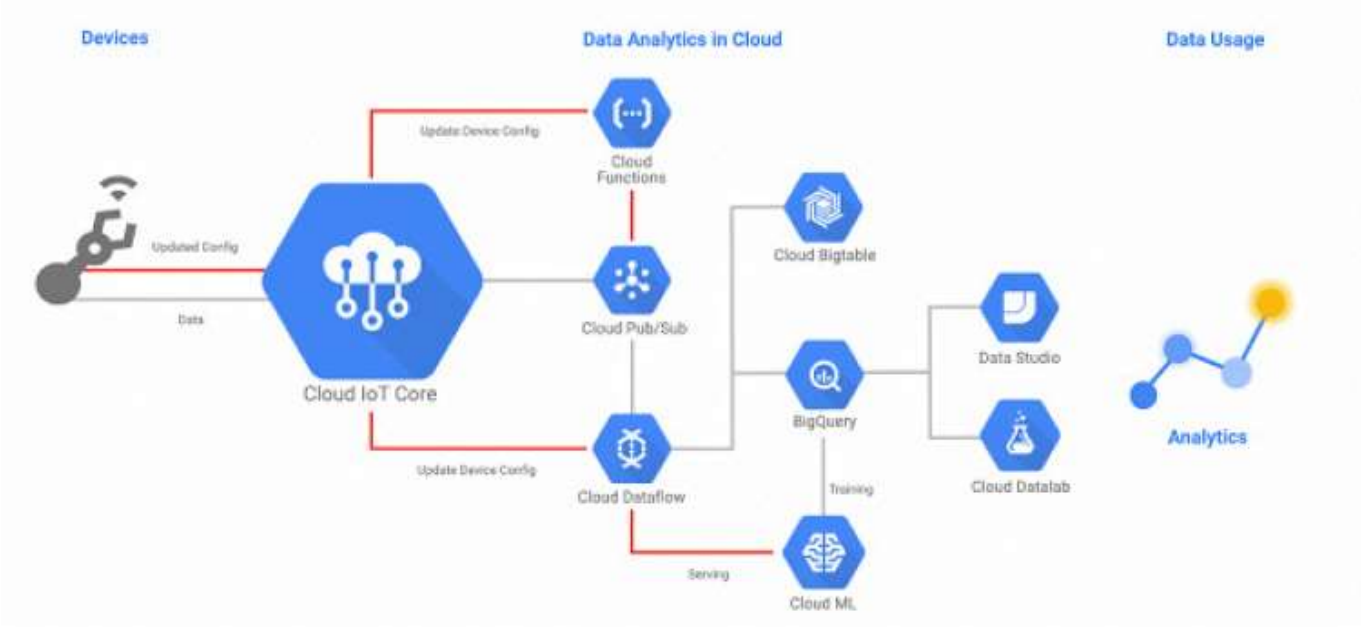

Рис. 1.4. Старий підхід Cloud IoT Core

Однак цей підхід створює велику затримку зв’язку як між пристроями, так і між алгоритмом обробки даних і пристроями, якими він керує. Крім того, вся система повністю залежить від підключення до Інтернету та підключення до використовуваної хмарної платформи, що робить її вразливою та потенційно небезпечною.

Наприклад, розумний будинок, який використовує термостати для керування нагріванням і охолодженням повітря всередині та виконує обробку даних виключно в хмарі, може, у найкращому випадку, повністю припинити нагрівання та охолодження без підключення до Інтернету, а в гіршому випадку може застрягти в одній із цих операцій і поставити під загрозу життя його мешканців.

Щоб знайти рішення цих проблем, дослідження та розробки IoT перейшли до нової парадигми, Edge Computing. Існує багато досліджень і статей, присвячених периферійним обчисленням, де порівнюється хмарні обчислення з периферійними обчисленнями і пояснюється, чому децентралізована ідеологія периферійних

обчислень набуває популярності. Одними з найважливіших переваг є висока чутливість хмарних служб, які надаються Cloudlets, кращий захист конфіденційності та маскування збоїв у хмарі завдяки підтримці функціональності системи навіть без підключення до хмари. Команда дослідників представляє проблеми рішень хмарних обчислень, як-от високу затримку зв'язку та значне навантаження на мережеві з'єднання з хмарою через усі дані, створені пристроями IoT. Вони представляють Edge Computing та його корисність у кількох різних сферах технологій, включаючи Інтернет речей, і, нарешті, вони описують свою експериментальну оцінку мобільних ігор із використанням Edge Computing.

Проблеми залежності від хмари також згадувалися в різних засобах масової інформації, як-от Medium, який опублікував статтю, в якій досліджуються значні недоліки систем, які повністю залежать від Інтернету та хмари щодо їх функціональності, і пропонується перелік кроків, які можна зробити, щоб позбутися надмірної залежності від Cloud. Подібним чином у networkworld є стаття, в якій розповідається про важливість периферійних обчислень для еволюції IoT і про важливі покращення, які Edge Computing може привнести в IoT. [5]

Зрештою, зміни у філософії також можна помітити в тому, як змінилися посібники від постачальників хмарних платформ за останні два роки. Всупереч попередньому менталітету переміщення всього в хмару, як згадувалося раніше та показано на малюнку 1.4, сьогодні вони пропонують різні типи платформ периферійних обчислень, які можна використовувати на місці на досить потужних пристроях і які можуть подбати про мережу- підключення до хмари та обмін даними та інформацією.

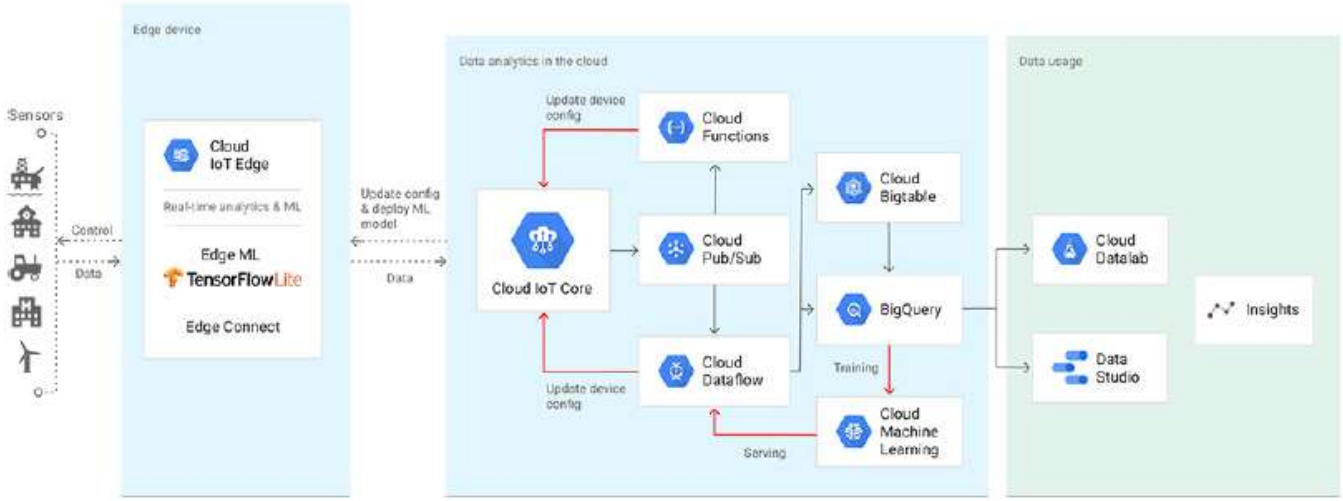

Рис. 1.5. Новий підхід Cloud IoT Core

Тепер Google пропонує використовувати пристрій Edge зі своїми службами Cloud IoT Edge, щоб виконувати аналіз у реальному часі та машинне навчання, використовуючи хмару для зберігання даних, перенавчання моделей машинного навчання та надання онлайн-аналітики у формі графіків даних.

1.4 Сучасні автономні рішення та їх проблеми

Як згадувалося раніше, оригінальні рішення Cloud Computing мають багато проблем, і сьогодні навіть постачальники хмарних платформ змінюють свої пропозиції щодо мереж Інтернету речей, як-от Google зі своїм Cloud IoT Edge або Amazon і Amazon IoT Edge.

Серед рішень домашньої автоматизації на ринку було кілька невдалих продуктів. Revolv16 був розумним домашнім центром, призначеним для керування різноманітними гаджетами за допомогою програми для смартфона. Однак хаб повністю залежав від хмарної служби компанії-розробника. Згодом Revolv був куплений компанією Nest, а згодом хмарний сервіс було закрито, через що всі хаби Revolv перестали працювати. Іншим продуктом зі схожою долею став Emberlight, розумна розетка, призначена для роботи зі звичайними лампочками. Його мета полягала в тому, щоб дозволити мобільному додатку керувати звичайними лампочками замість того, щоб купувати спеціальні та дорогі. Проблема полягала в

тому, що всі елементи керування здійснювалися через хмарну службу, яку знову було закрито. [6]

Ще одним прикладом є керування домом за допомогою розумних помічників, таких як Alexa в Echo Amazon або Google Assistant в Google Home. Ці продукти використовують розпізнавання голосу в хмарі, щоб розуміти команди та спілкуватися з людьми. Старіші версії не підтримували офлайн-розпізнавання мовлення, що могло призвести до повної втрати контролю над розумними будинками, які покладалися на них. Один досвід із цією критичною несправністю описано в статті Mashable, де автор не міг керувати своїм пристроєм Alexa, через що вони не могли навіть увімкнути світло в будинку.

Ідея Edge Computing була досліджена, з метою впровадження інтелектуального шлюзу електронної охорони здоров'я для впровадження Інтернету речей у охорону здоров'я. Стаття зосереджена на винайденні архітектури системи, яка б дозволила створити безпечну мережу з локальним сховищем, фільтрацією даних і аналітикою. Результатом їхньої роботи став UT-GATE, функціональний шлюз із сервером WebSocket, який забезпечує локальне обслуговування під час зв'язку з віддаленою хмарною платформою для отримання покращених правил обробки, отриманих завдяки глибшій аналітиці.

Різні команди дослідників намагалася вирішити ці проблеми, запропонувавши ієрархічну архітектуру туманних обчислень, яка medє гнучкою, масштабованою та наближає обчислювальні ресурси до кінцевих пристроїв. Архітектура складається з мережі обчислювально потужних вузлів туману, кожен з яких може підключитися до хмарного сервера, щоб розвантажити свою роботу, якщо це необхідно. Отримана конструкція може суттєво зменшити навантаження на трафік у мережах і затримку зв'язку, яка може бути проблемою в системах, заснованих виключно на хмарних обчисленнях.

На ринку вже є продукти, які пропонують часткову або навіть повну функціональність підключених мереж навіть без підключення до Інтернету. Останній Amazon Echo Plus, наприклад, дозволяє обмежено використовувати центр управління домом з голосовим керуванням в автономному режимі. Phillips Hue Bridge є ще одним

прикладом, оскільки йому потрібне підключення до Інтернету лише для дистанційного керування, але локально може працювати повністю в автономному режимі, як пояснюється в статті howtogeek. Hubitat - це платформа домашньої автоматизації, створена з урахуванням офлайн-функціональності. Незважаючи на можливість використовувати підключення до Інтернету для оновлень і спілкування в хмарі, підключення до Інтернету не потрібне для виконання будь-яких основних функцій. Це робить всю систему більш безпечною, приватною та усуває затримку.

1.5 Безпека та конфіденційність

Коли IoT став популярним, багато виробників зосередилися на продуктивності та зручності використання пристроїв IoT і проігнорували заходи безпеки та механізми шифрування, зробивши свої пристрої вразливими. У звіті Forbes прогнозується, що до 2025 року до Інтернету буде підключено понад 80 мільярдів розумних пристроїв. Така величезна кількість потенційно небезпечних пристроїв буде дуже небезпечною не лише для їхніх власників, але й для Інтернету та всього світу.

Вже було багато випадків, які доводять масштаби цієї проблеми, від зламу казино через їхній резервуарĄsh до серцевих пристроїв, якими хакери могли зловживати, щоб спричинити неправильний темп або удари, підключений транспортний засіб вразливий до захоплення, та дозволяючи хакерам заглушити двигун автомобіля або скоротити перерви, до масової DDoS-атаки через бот-мережі Mirai, яка заразила десятки мільйонів пристроїв IoT і залишила недоступною велику частину Інтернету на східному узбережжі США. [8]

Окрім контролю над уразливими пристроями, хакери також можуть прослуховувати їхні повідомлення та викрадати чи зловживати їхніми даними. Це може призвести до проблем із конфіденційністю, наприклад використання розумних камер для віддаленого стеження за будинками або витоку важливої особистої інформації, як-от медичні записи чи періоди часу, коли будинок чи будівля часто порожні, і їх легше зламати.

Зважаючи на важливість цих питань, уряди та дослідницькі групи світу зосереджуються на визначенні належних запобіжних заходів і принципів безпеки для боротьби зі зростаючим ризиком, який представляє незахищений Інтернет речей. Наприклад, у Японії, щоб зміцнити безпеку своєї країни перед Літніми Олімпійськими іграми 2020 року, уряд перевірив і зламав сотні мільйонів пристроїв, таких як маршрутизатори та веб-камери, використовуючи їхні паролі за замовчуванням, які користувачі часто залишають незмінними. Вони планують скласти список потенційно скомпрометованих пристроїв і повідомити про них владі.

У статті, опублікованій на міжнародній конференції в 2012 році, група китайських дослідників дослідила та проаналізувала стан безпеки в Інтернеті речей і запропонувала найважливіші проблеми, які ще потрібно подолати. Вони розділили IoT на чотири рівні, описані на малюнку 1.6. [9]

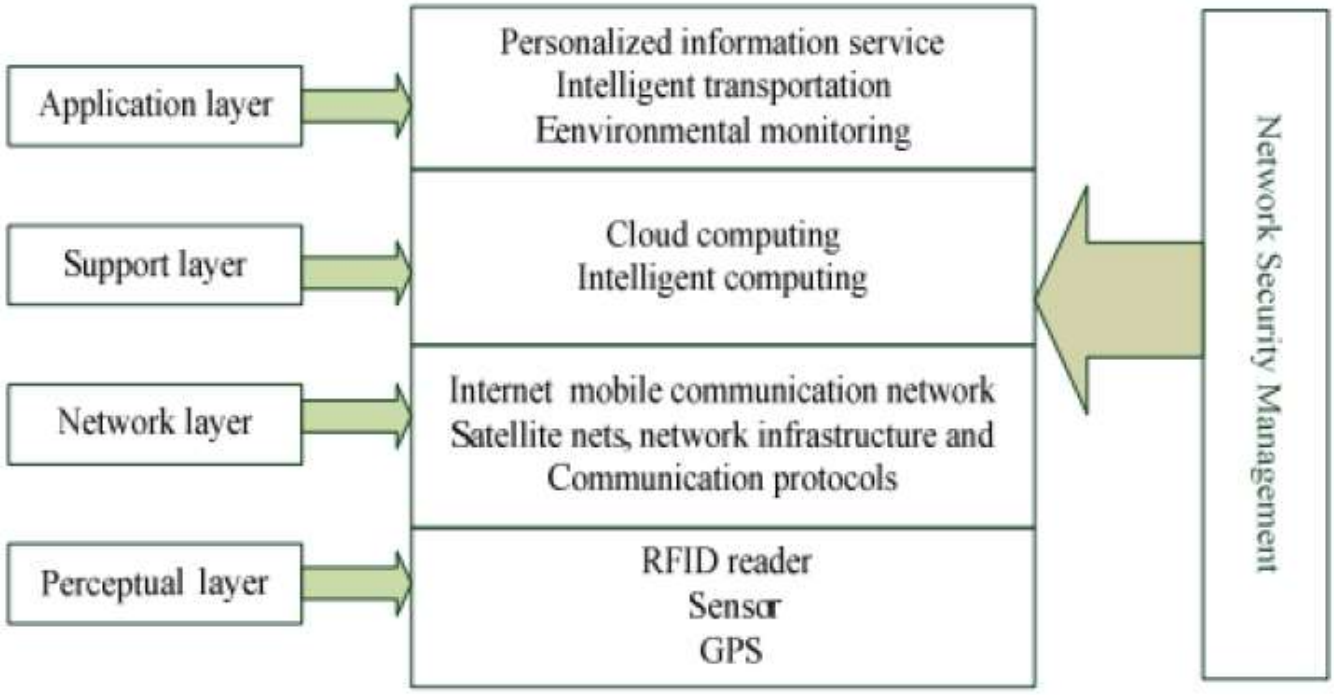

Рис. 1.6. Архітектура безпеки

Вузли на фізичних рівнях мають обмежену обчислювальну потужність і пам’ять, але в той же час вони повинні підтримувати автентифікацію, щоб запобігти незаконному доступу. На мережевому рівні атаки типу “man in the middle" становлять небезпеку, і також необхідно запобігати DDoS-атакам. Рівень підтримки має бути

захищений від зловмисної інформації та використовувати потужніші технології безпеки системи та антивірусні програми. Для прикладного рівня потреби в безпеці залежать від типу програми, але здебільшого стосуються конфіденційності даних і контролю доступу.

Останній огляд безпеки IoT за 2017 рік показує, що, незважаючи на те, що всі технології, пов'язані з IoT, розвиваються, проблем із безпекою залишається надто багато навіть через п'ять років. Серед обмежень пристроїв вони перераховують короткий час автономної роботи пристроїв IoT і легкі обчислювальні можливості, через які звичайна криптографія не може працювати в системах IoT. Безпека IoT залежить від технологій, протоколів і механізмів безпеки, які впроваджують виробники, і в окремих випадках створені пристрої можуть бути вразливими до певних типів атак. Наразі існує нагальна потреба в розробці загальної політики безпеки та стандартів для продуктів IoT. [10]

Існують також механізми, за допомогою яких можна переконатися, що в разі зламу програмного забезпечення на пристрої або криптографічних ключів все ще є спосіб відновити уражені пристрої. Серед них – оновлення по повітрю (OTA) і автоматична ротація криптографічного ключа. Оновлення OTA – це оновлення програмного забезпечення, які можна налаштувати та надіслати на пристрої через Інтернет без необхідності взаємодії з користувачем. OTA матиме вирішальне значення для IoT, оскільки або неоновлення пристроїв взагалі, або користувачі оновлюють їх вручну, становлять ризики для безпеки та дають зловмисникам можливість назавжди захопити пристрій або перехопити фізичний носій, який використовується для транспортування оновленого програмного забезпечення та втручатися в нього, перш ніж воно досягне призначених користувачів. Android Things підтримує OTA через консоль Google, яку можна однаково використовувати для всіх пристроїв Android. [11]

Ротація криптографічного ключа має дуже схожу мету з OTA. Коли ключ пристрою викрадено, якщо пристрій налаштовано на автоматичне видалення поточних ключів і реєстрацію нових через певний період часу, то зловмисник може отримати доступ до мережі лише через пристрій протягом цього періоду. Ось чому

Google Cloud IoT Core та інші хмарні платформи підтримують перемикання ключів або навіть використання кількох одночасно, щоб згладити ротацію та звести перебої в доступі до мінімуму.

1.6 Ініціалізація пристрою

Ініціалізація є важливою частиною або терміном служби пристрою. І необхідно виконати при першому підключенні до мережі або після скидання настройок на пристрої. Є кілька рівнів ініціалізації. По-перше, пристрою необхідно використовувати деякі початкові значення і стани, які можуть бути попередньо запрограмовані, або динамічно налаштовані за допомогою будь-якого зв'язку. Далі пристрою необхідно встановити з'єднання з незалежно від того, до якої мережі він підключається, та ресурси для пристрою повинні бути виділені та підготовлені в іншій частині системи, яка у разі цієї тези буде шлюзом та хмарою.

До найчастіше використовуваних технологій цієї мети сьогодні відносяться, наприклад, QR-коди, мітки RFID і мітки NFC29. QR-коди – це двовимірні коди, які можна роздрукувати на наклейці, а потім відсканувати мобільним додатком або будь-яким іншим зчитувачем.

Це дуже просте та недороге рішення для одностороннього зв'язку. RFID – це технологія, яка використовує електромагнітні поля замість сканування зображення, і її ефективний діапазон може становити від кількох сантиметрів до кілометра. RFID також може використовуватися тільки як односторонній зв'язок. NFC походить від RFID і призначений для роботи тільки на близькій відстані для підвищення безпеки. На відміну від RFID та QR-кодів, NFC підтримує обмін інформацією між пристроями.

Дослідження у цій галузі шукають ще більше способів виконання ефективної ініціалізації. Одна з таких концепцій - BlinkComm, включає зв'язок за допомогою видимого світла. Наразі розглядаються питання схем ініціалізації, які використовуються у сучасних продуктах. В деяких випадках завдання вимагає дуже складних процедур або навіть кабельного з'єднання, що не дуже зручно для користувача, особливо з великою кількістю пристроїв, які повинні стати частиною

Інтернету речей у найближчому майбутньому. Також в дослідженнях обговорюють безпеку різних методів ініціалізації та говорять про декілька вразливостей у системах, які, наприклад, використовують встановлені секретні ключі для своєї фази ініціалізації, що є небезпечним, оскільки компрометація одного такого пристрою може поставити під загрозу всю мережу. Мета дослідження полягала в тому, щоб представити рішення, яке пропонує прості та безпечні початкові налаштування пристроїв IoT без необхідності використання спеціалізованого обладнання. Вони оцінюють супутні рішення та розраховують теоретичну пропускну здатність каналу зв'язку з видимим світлом, а також впроваджують методи кодування, які забезпечують більш ніж утричі більшу швидкість порівняно з конкурентами за мінімальних апаратних вимог, таких як один світлодіод та один фотодіод.

Ті ж дослідники, які написали статтю, згадану в попередньому абзаці, продовжили свої дослідження ініціалізації на основі видимого світла і винайшли дві нові багатоканальні схеми розгортання ключів, які називають LISA і LISAT, в яких використовується джерело світла, таке як смартфон. планшет або сенсорний екран для безпечної взаємодії з пристроями з обмеженими ресурсами. LISA розшифровується як "Легка ініціалізація та аутентифікація на основі SMS", LISAT - "Ініціалізація на основі Light та аутентифікація на основі SMS" за участю довіреної третьої сторони. Різниця між ними полягає в тому, що з LISAT користувач може ініціювати два бездротові пристрої, один поряд з собою, а інший у географічно віддаленому місці, використовуючи свій смартфон як довірена третя сторона. Протоколи використовують видиме світло, що генерується, наприклад, екраном смартфона, для передачі інформації зі смартфона на пристрій, що ініціалізується, і пристрій відповідає смартфону за допомогою зашифрованих SMS-повідомлень. У LISAT смартфон також зв'язується з віддаленим пристроєм через SMS. Хоча протоколи були реалізовані для використання SMS, вони можуть бути адаптовані для підтримки інших технологій, таких як LoRaWAN, Sigfox, NB-IoT або навіть BLE, Wi-Fi та NFC. Протоколи були реалізовані на комерційно доступній платформі та протестовані 34 користувачами, які надали відгуки, які дослідники планують використовувати для покращення своїх майбутніх версій протоколу. [12]

1.7 Потужність

Пристрої в Інтернеті речей можна розділити на дві категорії, коли йдеться про енергоспоживання. Існують шлюзи та інші обчислювально потужні пристрої, які споживають занадто багато енергії, щоб отримувати живлення від батарей а, отже, вимагають постійного джерела живлення, а також більш ефективні та менш обчислювально потужні кінцеві пристрої, які мають бути бездротовими, але водночас мають працювати довго протягом місяців чи навіть років без підзарядки. Тому було проведено безліч досліджень і кілька різних підходів до того, як такі кінцеві пристрої можуть живитися і як зробити їх максимально енергоефективними, надаючи необхідні послуги IoT. [13]

Щоб зробити пристрої енергоефективними, були винайдені нові стандарти та протоколи зв'язку, такі як IEEE 802.15.4 та 6LoWPAN. Пристрої, що взаємодіють за допомогою технологій, заснованих на таких стандартах та протоколах, економлять енергію, передаючи обмежені обсяги даних, максимально зменшуючи накладні витрати пакетів, використовуючи невелику швидкість передачі на невеликих відстанях та меншу смугу пропускання. Як правило, вони працюють в одноранговій, пористій або зіркоподібній топології.

Ще один важливий спосіб економії енергії - використання різних сплячих режимів, що відключають апаратні компоненти, щоб пристрій споживав енергію тільки тоді, коли це необхідно. Мікроконтролер KW41Z, що продається NXP Semiconductors, наприклад, має чотири основних режими STOP, які варіюються від зупиненого ЦП зі збереженням всіх станів введення-виводу, логіки та пам'яті та деяких периферійних пристроїв в асинхронному режимі до вимкненого ЦП з тільки I/O та невеликий регістр зберігаються, і працює дуже мало периферійних пристроїв в асинхронному режимі, в той час як решта MCU вимкнена. Чотири основні режими: нормальна зупинка, зупинка при дуже низькій потужності, зупинка при малому витоку і зупинка при дуже низькому витоку. [14]

Роблячи пристрої енергоефективними, можна також зосередитися на різних стратегіях їх живлення. Одним з них є збір енергії, який використовує енергію з навколишнього середовища або інших джерел енергії та перетворює її на електричну енергію. Деякі методи можуть перетворювати сонячну енергію, в той час як інші використовують енергію вітру або механічну енергію, наприклад, коли механічна напруга застосовується до п'єзоелектричних матеріалів або коли важіль, що обертається, з'єднується з генератором. Навіть самі люди можуть бути джерелом енергії завдяки рухам тіла, кров'яному тиску, руху пальців та іншим засобам. Збирання енергії можна розділити на дві архітектури: збір-використання або збір-складування-використання. Пристрої на основі Harvest-Use живляться безпосередньо від системи і можуть працювати тільки під час перетворення певної форми енергії. Пристрої Harvest-Store-Use можуть зберігати зібрану енергію та використовувати її пізніше.

Збір бездротової енергії для пристроїв IoT досліджується. Цей підхід називається Wireless Energy Harvesting IoT чи WEH-IoT. Сенсорні пристрої з підтримкою WEH складаються з антени, приймача, блоку WEH, блоку управління живленням (PMU), блоку датчика/процесора і, опціонально, акумулятора. Для збору енергії необхідні два основні модулі: блок WEH, який збирає радіочастотну енергію, та PMU, який керує пристроєм та керує споживанням енергії. Джерела енергії класифікуються на дві категорії: виділені джерела, які є РЧ-джерелами, що використовуються для забезпечення передбачуваної подачі енергії на пристрої, та навколишні джерела, серед яких широкомовні радіоприймачі, телевізори, точки доступу Wi-Fi та інші. Зрештою, вони представляють та оцінюють можливі реалізації цієї системи.

На ринку вже є продукти, де використовуються різні схеми збору енергії. Серед них мітки Williot30, які використовують Bluetooth та збирають навколишню радіочастотну енергію від стільникового зв'язку, Bluetooth, Wi-Fi та інших технологій підключення 2,4 ГГц, навіть Zigbee та Thread. Ці теги підключаються до хмарної служби Williot для забезпечення безпечної автентифікації та обробки датчиків. Ще одна технологія збору енергії IoT - це Zigbee Green Power31, яка дозволяє

використовувати пристрої Zigbee PRO без батареї, збираючи енергію від вимикачів світла, п'єзоелектричних елементів та динамо-або електромеханічних перетворювачів.

1.8 Майбутнє Інтернету речей

Хоча майбутнє Інтернету речей може здатися світлим, Cisco оцінює 50 мільярдів підключених пристроїв до 2020, а IDC прогнозує 80 мільярдів пристроїв до 2025року, залишається ще багато проблем, які необхідно вирішити. У міру того, як мікроконтролери стають більш енергоефективними, машинне навчання стає більш досконалим, протоколи зв'язку та технології підключення стають більш уніфікованими та стандартизованими, IoT швидко розширюватиметься і швидше за все, стане важливою частиною повсякденного життя. Однак, хоча це майбутнє обіцяє більший комфорт і найкраще життя, існує також небезпека великомасштабних зламів та атак на вразливі та погано захищені пристрої та мережі. Якщо ці небезпеки не будуть усунені в найближчому майбутньому, IoT може відкрити двері для великої шкоди від проблем з конфіденційністю у будинках людей, до проблем зі здоров'ям через підключене медичне обладнання та надзвичайно великих DDoS-атак, що наражають на небезпеку весь Інтернет. [15]

У своєму нинішньому стані Інтернет речей далекий від того, щоб бути прийнятим та включеним у життя мільярдів людей. Однак, дослідження її проблем та пошук обґрунтованих рішень ведуться дуже інтенсивно. Навіть виробники MCU і пристроїв, тепер усвідомлюють помилки останніх кількох років і працюють над згаданими вище проблемами, особливо над граничними обчисленнями та безпекою мереж IoT.

Схоже, що наступні кілька років матимуть вирішальне значення для переконання людства в тому, що IoT зробить світ кращим, безпечнішим та комфортнішим для життя, а не повністю контрольоване середовище, яке позбавляє їх вибору та перебуває під загрозою захоплення та неправильного використання шкідливими сторонами щодня. Зрештою, жити в будинку, який економить енергію,

піклується про потреби його мешканців і робить їх життя зручнішим у багатьох відношеннях - приваблива перспектива, але життя в будинку, який бажає нашкодити його мешканцям, звучить швидше як жах.

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому розділі було розглянуто ідею IoT. Розгянуто та порівняно між собою основні протоколи (ZigBee, Bluetooth Thread). Розглянуто популярні операційні системи IoT. Розглянуто категорії обладннаня пристроїв IoT за їх потужністю. Порівняно старий та новий підхід до побудови архітекутери IoT та перспективи розвитку.

ОЗДІЛ 2
ПРОБЛЕМИ БЕЗПЕКИ IOT ТА ТЕХНОЛОГІЙ

2.1 Суть проблеми безпеки IoT

Існує понад мільярди пристроїв IoT, бізнес-процесів і систем з елементом IoT. Ці дані, доступні в екосистемі, необхідно зафіксувати та проаналізувати, щоб побачити, чи можна отримати будь-яку функціональну інформацію, яка є корисною для клієнта чи бізнесу. Основними елементами IoT є люди, речі, дані та процеси. Системи IoT спрямовані на об’єднання цих елементів у мережу, які спілкуються один з одним через дротове або бездротове середовище. Пристрої IoT згруповані як датчики, які збирають дані, приводи, які виконують дії і шлюзи, які діють як інтерфейси для зв’язку та автоматизації. У структурі IoT дані збираються з датчиків, обробляються мікроконтролерами, такими як Raspberry Pi або Arduino, зберігаються в хмарній базі даних, а аналіз даних із зібраних великих даних виконується за допомогою будь-яких інструментів або мов, таких як python або java. IoT розроблений для посилення зв’язку між пристроями (D2D), «людина-пристрій» (H2D), «людина-людина» (H2H) і «пристрій-людина» (D2H).

З поширеністю Інтернету речей ризики безпеки зростають. Доступність даних у будь-якому місці робить їх уразливими для загроз безпеки та атак. У цьому розділі розглядаються основні проблеми, проблеми та рішення для забезпечення безпеки IoT. Один скомпрометований об'єкт мережі IoT робить вразливими інші об'єкти. Оскільки IoT являє собою сукупність пристроїв або датчиків, об'єднаних у мережу в хмарі для надання інформаційних послуг, всі загрози безпеці, які застосовуються до бездротових сенсорних мереж (WSN), Інтернету та хмари, мають відношення до мереж IoT. Інтернет речей відкриває величезні можливості для бізнесу із супутнім ризиком. Відсутність надійної автентифікації пристроїв IoT, шифрування даних IoT, управління ключами тощо робить мережу IoT вразливою для зовнішніх атак і загроз.

2.2 Вимоги до безпеки Інтернету речей

Безпека повинна забезпечуватись протягом усього життєвого циклу пристрою IoT. Розглянемо вимоги до безпеки, які необхідно перевіряти на різних етапах життєвого циклу, щоб пом'якшити атаку на IoT:

Криптографічні алгоритми. Симетричні алгоритми мають невелику вагу у порівнянні з асиметричними алгоритмами а, отже, рекомендуються для захисту передачі даних. Однак у них є проблеми з обміном ключами, конфіденційністю, цифровим підписом та автентифікацією повідомлень. Отже, рекомендуються алгоритми з відкритим ключем, оскільки вони можуть забезпечити керування ключами, автентифікацію вузлів, масштабованість та безпеку.

Методи керування ключами. Керування ключами – важлива функція безпеки в IoT. Для безпечного зв'язку потрібен полегшений безпечний розподіл ключів.

Схеми розподілу ключів, що використовуються в WSN, є широкомовною розсилкою, групове, основне і спільне поширення ключів. Основна увага в дослідженнях управління ключами приділяється зниженню складності, енергоспоживанню та безпеці. [16]

Алгоритми захищеної маршрутизації – традиційні протоколи мережної маршрутизації не можуть використовуватись для мережі IoT. Протокол маршрутизації повинен гарантувати справжність інформації, що маршрутизується, а при обміні даними через бездротове середовище має уникати перехоплення. Протоколи маршрутизації повинні бути захищені для запобігання таким атакам, як Dos, Worm hole, black hole та вибіркова переадресація. [17]

Класифікація даних - дані, що переміщуються у мережі IoT, можуть бути функціональними або пов'язаними з людьми, або підприємством. Ступінь захисту, що потрібна для даних, залежить від ступеня конфіденційності даних. Дані можуть бути захищені з урахуванням класифікації конфіденційності. Отже, для постачальника IoT надаються такі рекомендації:

- Визначте схему класифікації даних на основі конфіденційності даних.
- Визначте всі дані та групи даних у мережі IoT та класифікуйте їх.

- Розробіть функцію безпеки, яка захищає перегляд та редагування даних на основі їх рівню класифікації. [18]

Захист пристроїв під час виробництва. Пристрої IoT можуть бути захищені під час виробництва. Будь-який інтерфейс, який використовується під час виробництва, має бути видалено перед розгортанням. Усі порти до пристроїв IoT повинні мати належний контроль доступу. Пристрої, розміщені у відкритих місцях, повинні мати захист від несанкціонованого доступу та екранування, щоб уникнути атак сторонніми каналами.

Надійна поетапна послідовність завантаження. Надійна поетапна послідовність завантаження забезпечує безпеку пристрою IoT. Однак перша послідовність вкрай важлива а, отже, має ініціюватися захищеним заблокованим кодом. Рекомендується використовувати безпечний модуль, у якому зберігаються криптографічні алгоритми та пов'язані з ними ключі. На кожному етапі завантажувального коду рекомендується перевіряти надійність завантажувального коду, достовірність апаратного забезпечення та завершення попереднього коду.

Захищена операційна система. Операційна система IoT повинна мати обмежені права доступу та зменшувати видимість системи. Операційна система повинна бути спроектована таким чином, щоб мати лише ті компоненти, пакети та бібліотеки, які необхідні для роботи пристрою IoT. Оновлення повинні надаватись протягом усього терміну служби розгорнутого пристрою. Порти, протоколи та служби, що не використовуються, повинні бути відключені. Мають бути надані окремі права доступу для користувачів та адміністраторів для доступу до файлів та каталогів. Має використовуватися зашифрована файлова система.

Безпека програм. Питання безпеки повинні бути невід'ємною частиною розробки додатків та не повинні додаватися окремо. Шлюз програм повинен перевіряти всі зібрані дані перед їх обробкою. Усі облікові записи користувачів та паролі мають бути видалені. Облікові дані програми повинні бути поміщені в безпечне сховище. Будь-які помилки програми не повинні розкривати подробиці базової архітектури. Рекомендується використовувати захищену процедуру життєвого циклу розробки програмного забезпечення.

Управління обліковими даними. Облікові дані, такі як паролі, криптографічні ключі та цифрові сертифікати користувача та процесу, які використовуються для доступу до даних, повинні зберігатися у захищеному місці, до якого не можуть отримати доступ зовнішні об'єкти. Паролі, що використовуються для аутентифікації, повинні бути надійними, зашифрованими та мати стандартну хеш-функцію. Для керування доступом може використовуватися двохфакторна автентифікація. Рекомендується використовувати унікальний цифровий сертифікат для кожного пристрою, і цей сертифікат необхідно захищати та регулярно оновлювати.

Шифрування. Для мережі IoT рекомендується найнадійніше та найновіше шифрування, якщо воно доступне за ціною. Стандарт шифрування повинен відповідати ступеню конфіденційності даних, що захищаються. Слід уникати використання глобальних ключів. Закритий ключ пристрою ніколи не слід передавати. Ключі шифрування повинні мати можливість віддаленої заміни. Ключі шифрування повинні зберігатись у довірених ключових модулях.

Мережеві підключення. Кількість інтерфейсів до пристрою IoT, через яке він підключається до зовнішньої мережі, має бути мінімальною. Доступ до пристрою має бути можливим лише через мінімальний порт, інтерфейс та сервіси. Для захисту з'єднань повинні використовуватися безпечні протоколи, такі як https та SFTP. Машина-одержувач має бути аутентифікованим перед відправкою будь-яких конфіденційних даних.

Оновлення програмного забезпечення. Перед будь-яким оновленням програмного забезпечення необхідно виконати аутентифікацію джерела, яке виконує аутентифікацію, за допомогою перевіреного сертифіката, отриманого від авторизованого центру сертифікації. Пакети оновлення програмного забезпечення мають бути підписані. Захищене ведення журналу подій - ведення журналу подій має бути захищеним від хакерів, змін або видалень.

Журнали подій зазвичай зберігаються в централізованому пулі журналів далеко від пристрою IoT і, отже, повинні передаватися окремими каналами. Журнали необхідно періодично аналізувати для виявлення будь-яких помилок та вжиття негайних заходів. Файли журналу повинні зберігатися в окремих розділах файлової

системи. Права доступу до лог-файлу мають бути обмежені. Жодні конфіденційні облікові дані, такі як паролі, не повинні зберігатися в журналах.

2.3 Виклики для покращення безпеки IoT

Проблеми, пов'язані з безпекою IoT – це не лише проблеми, пов'язані з безпекою бездротового середовища, WSN та Інтернету, але також питання контролю доступу, автентифікації та конфіденційності, пов'язані з IoT.

Вбудований пристрій з низьким енергоспоживанням – пристрої IoT мають меншу обчислювальну потужність та ємність пам'яті. Він часто вбудований у більше обладнання або пристрій, де важко виконувати алгоритми безпеки, які зазвичай мають велику вагу і є дорогими для пристрою з обмеженими ресурсами.

Управління довірою. Управління довірою потрібне на етапах збирання та розсіювання даних аутентифікації даних, для яких рекомендуються надійні криптографічні методи або цифрові підписи. [17]

Гетерогенність IoT є інтеграцією різних гетерогенних мереж а, отже, має свої проблеми із сумісністю та безпекою. Важкою задачею є ідентифікація довірених вузлів у гетерогенному середовищі. Неоднорідність, управління ідентифікацією, стійкість до відмови конфіденційності. [18]

Захищений контроль доступу. Захищений контроль доступу є серйозною проблемою мережі IoT. Зазвичай до інформації у хмарі звертаються різні сутності та процеси. Також рівень деталізації для доступу до тих самих даних відрізняється для різних отримувачів. Тому визначення політики управління доступом та забезпечення безпеки доступу є одним із основних завдань. [18]

Керування ідентифікацією - потрібна унікальна ідентифікація пристрою IoT та забезпечення автентифікації та авторизації для кожного пристрою. Аутентифікація забезпечує достовірність даних, що проходять через пристрій, а авторизація забезпечує безпечний контроль доступу. Об'єкти мережі IoT можуть додаватися динамічно а, отже, управління ідентифікацією з автентифікацією стає ще складнішим.

Конфіденційність – важливо забезпечити конфіденційність мільярдів користувачів у мережах IoT. Анонімність користувача має бути збережена. Список контролю доступу повинен підтримуватися будь-яким постачальником послуг. Конфіденційності необхідно приділяти належну увагу протягом усього життєвого циклу IoT.

Управління довірою. Управління довірою відіграє життєво важливу роль в обміні даними між об'єктами та між об'єктом та користувачем. Розрахунок репутації необхідний для прийняття рішення про довіреність об'єкту. Колективне уявлення центрального об'єкта допомагає розрахунку репутації інших об'єктів. Невідповідність у значенні репутації може бути усунена шляхом спільного використання інформації про довіру від різних центральних об'єктів.

Розподілена мережа IoT - централізована або підключена мережа IoT має окремі пасивні об'єкти збору даних, які передають зібрані дані до централізованої хмарної служби, яка виконує роботу з агрегування, обробки, аналізу та розподілу. Більше того, потік інформації до центрального вузлу слідує ієрархічному зразку. Це забезпечує кращий централізований контроль безпеки, але як тільки виникає вразливість, вся система наражається на ризик. У розподіленій мережі IoT кожен об'єкт має право виконувати роботу зі збирання, обробки, аналізу та розповсюдження інформації а, отже, є вектором атаки. [18]

Проте зловмисник зможе отримати від атакованого об'єкта лише часткову інформацію, яка також може бути важливою необхідною інформацією. Прикордонний інтелект на стороні постачальника послуг для запиту інформації локальним користувачем без втручання будь-якого зовнішнього об'єкта має потенційну вразливість, яку слід контролювати, надаючи функції суворої автентифікації та авторизації.

2.4 Проблеми безпеки Інтернету речей

Проблеми безпеки IoT, засновані на обмеженнях обладнання, програмного забезпечення, мережевих підключень. До апаратних обмежень належать

обчислювальні та енергетичні обмеження, обмеження пам'яті та захищене від несанкціонованого доступу пакування. Обмеження програмного забезпечення – це вбудоване програмне обмеження та динамічне виправлення безпеки. Обмеження на мережеві з'єднання включають мобільність, масштабованість, безліч пристроїв та засобів зв'язку, багатопротокольні мережі та топологію мережі. [19]

2.4.1 Апаратне забезпечення Інтернету речей

Апаратне забезпечення IoT включає датчики, пристрої, цифрові гаджети, мікроконтролери, такі як Arduino, Raspberry pi і вбудоване обладнання. Апаратні пристрої IoT присутні у клієнтів, вбудовані в будь-який інший пристрій і можуть використовуватися як пристрої, що носяться, або можуть бути постійно підключені до Інтернету. Отже, ці пристрої вразливіші для атак безпеки і можуть бути легко підроблені. Виробники апаратних пристроїв більше переймаються аспектами дизайну пристроїв IoT, ніж аспектами безпеки, а отже, клієнти наражаються на більший ризик. Зменшений розмір та можливості обробки обмежують функції безпеки пристрою IoT. Через переважання апаратного забезпечення IoT важко надати програмне виправлення для оновлення безпеки. Через відсутність стандартизації перед виробництвом обладнання IoT також піддається загрозам безпеці. Залізо IoT піддається атакам, яким піддаються всі пристрої, підключені до Інтернету, такі як DOS і DDoS.

Щоб захистити обладнання, необхідно вирішити такі питання, як життєвий цикл обладнання, оновлення програмного забезпечення, контроль доступу та автентифікація пристрою. Підприємства повинні взяти на себе ініціативу щодо перевірки конфігурації всіх IoT-пристроїв, виконати сканування вразливостей та перевірити мережеві підключення. Безпека вбудованих систем є серйозною проблемою зростання IoT. Різні консорціуми IoT працюють над визначенням фреймворку для одноманітної реалізації ідентифікації, виявлення пристроїв, автентифікації та контролю безпеки. Потрібно потурбуватися про захист особистих даних, що зберігаються в апаратному забезпеченні, до того, як їх буде видалено. При виборі апаратної платформи необхідно перевірити такі аспекти безпеки, як унікальна

ідентифікація та захищене сховище для ключів шифрування. Необхідно виконати оцінку, щоб перевірити, наскільки складно змінити облікові дані, що зберігаються в апаратному забезпеченні.

2.4.2 Програмне та мікропрограмне забезпечення Інтернету речей

Програмний компонент IoT включає вбудоване програмне забезпечення, операційні системи, що використовуються в IoT, такі як Android і Tiny OS, і хмарне програмне забезпечення, таке як Nimbis і Hadoop. Більшість програмного забезпечення IoT займається збором даних, інтеграцією пристроїв, інтерфейсом додатків і процесів, а також аналітикою в реальному часі. Пристрої IoT, підключені до Інтернету, мають вбудовану операційну систему як прошивки. Ці операційні системи не розроблялися з урахуванням вимог безпеки а, отже, вразливі до атак шкідливих програм. Вбудовані дані в побутові прилади, мобільні телефони і пристрої з мережевими можливостями більш вразливі для зовнішніх атак. Це пов'язано з тим, що вони обмінюються даними з іншими підключеними пристроями, а вбудовані дані зберігаються довше, ніж обладнання. Аспект безпеки нехтується підприємством, оскільки вартість апаратного забезпечення набагато менша, ніж вартість оновлення програмного забезпечення та безпеки. Неправильно налаштовані пристрої зберігання даних, підключені до мережі та будинків, також є основним джерелом загроз. Ці пристрої генерують величезні обсяги даних. Важко вирішити, чи мають бути дані захищені чи ні. Трояни або черв'яки можуть використовуватися для впровадження шкідливого коду програмного забезпечення. [20]

Найбільш економічним рішенням для захисту вбудованого програмного забезпечення є моніторинг та захист трафіку на шлюзі. Загрози безпеки для пристроїв, що використовуються в охороні здоров'я та виробництві, можна звести до мінімуму, відключивши їх зв'язок через Bluetooth, геозонуючи зв'язок, обмеживши і контролюючи доступ за допомогою зовнішніх програм. Для забезпечення безпеки слід уникати застарілих операційних систем та програмного забезпечення без виправлення.

2.4.3 Небезпека мережевого зв'язку

Через величезну кількість пристроїв IoT, підключених до мережі, традиційні механізми мережевої безпеки, ідентифікації та управління ключами важко реалізувати. Будь-який пристрій або процес, підключений до IP-адреси або URL-адреси, пов'язаний із ризиком. Помістити весь підключений IoT-пристрій під кордон контрольованого брандмауера складно, оскільки зловмисник може використовувати один скомпрометований вузол для бічної атаки на всю мережу. Моніторинг та ізоляція пристроїв IoT, задіяних у приватній VLAN або сегменті мережі, може знизити загрозу безпеці. Як рішення пропонується комірчаста мережа для підключення пристроїв IoT, оскільки вона самоорганізується, самовідновлюється і масштабується. Раптове збільшення вимог до пропускної здатності через великий обсяг даних, що генеруються сайтами соціальних мереж та IoT, імітуватиме атаку, таку як DoS. Бездротовий зв'язок між вузлами IoT піддає їх як активним, так і пасивним атакам. Комірчаста мережа формується шляхом підключення бездротових пристроїв без будь-якої інфраструктури. Сітка в IoT дозволяє елементам IoT взаємодіяти між собою за відсутності фіксованої інфраструктури для зв'язку. Це надзвичайно корисно у разі додатків з низьким енергоспоживанням та низькою швидкістю передачі даних у додатках охорони здоров'я, промислової та домашньої автоматизації. Мережа IoT на підприємстві піддається вразливості, якщо не визначено належну політику управління мобільністю підприємства (EMM) для зниження ризику витоку життєво важливих корпоративних даних у зовнішній світ. [20]

2.4.4 Витік даних з хмари

Дані зберігаються у хмарі з метою спільного використання. Очікується, що автентифіковані джерела у списку управління доступом отримають доступ до даних. Постачальник послуг несе відповідальність за будь-який витік даних з хмари. Неправильно налаштована хмара призведе до витоку даних. Зовнішній доступ до конфіденційних даних та журналів має бути обмеженим. Вороже настроєний співробітник може отримати доступ до будь-якого внутрішнього сервера та

підприємств, передати певні послуги на аутсорсинг з потенційною загрозою витоку даних. Хмарне середовище потребує постійного моніторингу та виявлення вторгнень. Для цього потрібний моніторинг та реєстрація журналів віртуальних машин та загальних служб. Щоб уникнути витоку даних рекомендуються системи виявлення та запобігання вторгненням.

2.4.5 Загрози та вектори атак

Зловмисник, націлений на IoT зможе використовувати MAC-адресу, щоб зрозуміти цільову платформу та перепроектувати програмне забезпечення, щоб знайти ключі шифрування. Вектори атаки - це шлях, який використовується хакером для отримання доступу до захищеної системи. Оскільки вектори атак, доступні для зловмисників, зростають з кожним днем через глобальне підключення і доступність, необхідно забезпечити відмовостійкість. Дані та метадані IoT є потенційними векторами атаки для будь-якого хакера. Нижче наведено деякі загрози в IoT,

Denial of Service - DoS-атака в IoT спрямована на виснаження ресурсів постачальників послуг та пропускну здатність мережі. Заглушення каналу бездротової мережі також є різновидом DoS-атаки. Оскільки пристрої IoT зазнають активних зловмисників, це також призводить до атак типу DoS.

Підслуховування - пасивні зловмисники націлюються на канал зв'язку, а підслуховувачі скидають дані та отримують інформацію. Активний зловмисник може захопити вузол, відкритий для довкілля, щоб отримати доступ до даних сховища.

Керування об'єктом IoT – активний зловмисник може отримати контроль над об'єктом IoT через шлях атаки. Цей тип атаки отримує контроль як над даними, так і над службами з даними.

Атака MQTT - сервери IoT, що використовують Message Queuing Telemetry Trans- port (MQTT) в Інтернеті, зазнають атак через неавторизований і незашифрований зв'язок. Сервери MQTT також уразливі для SQL-ін'єкцій та cross-side скриптів. Сервери MQTT, які використовуються для оновлення програмного забезпечення, можуть використовуватися для оновлення шкідливого коду.

Програма-вимагач - мережа IoT зазнає атаки програми-вимагача, за якої вони крадуть дані з будь-якого інтерфейсного шлюзу або хмарного агрегатора і вимагають за це гроші. При атаці програми-вимагача зловмисник зазвичай отримує важливі дані, наприклад, у лікарнях, які необхідні для повсякденної діяльності організації і вимагає грошей у тій чи іншій формі за розголошення даних. Атака програмами-вимагачами у середовищі IoT призводить до втрат для бізнесу.

Підробка запитів IoT. Зловмисник намагається атакувати IoT-пристрої, підключені до корпоративної мережі, замість зламати кілька рівнів безпеки.

Шкідливе програмне забезпечення для носимих пристроїв – пристрої, що носяться, діють як вектор атаки шкідливого програмного забезпечення та забезпечують авторизований доступ до підключеної мережі IoT, ботнети можуть атакувати мережу IoT як групу.

Загрози віртуалізації. Хост-комп'ютер, на якому запущено програмне забезпечення віртуалізації, може бути атакований кодом у віртуальному середовищі, який імітує атаку "man in middle".

2.4.6 Архітектура протокол Інтернету речей

Застосовувані протоколи та заходи безпеки, що надаються, залежать від того, чи є вузол обмеженим або необмеженим [21].

Wireless Hart – це протокол безпеки, який працює на кількох рівнях з використанням кількох ключів та захищає трафік, шифруючи корисне навантаження та забезпечуючи аутентифікацію повідомлень. Окремі ключі використовуються на мережному рівні для аутентифікації наскрізного зв'язку та на рівні каналу передачі даних для аутентифікації міжсегментного зв'язку.

LoRaWAN - це варіант для дального зв'язку що забезпечує захищений двосторонній зв'язок, мобільність та послуги локалізації. Він надає унікальний мережевий ключ для безпеки на мережному рівні, унікальний ключ програми для забезпечення наскрізної безпеки на рівні програм, а також ключ для конкретного пристрою.

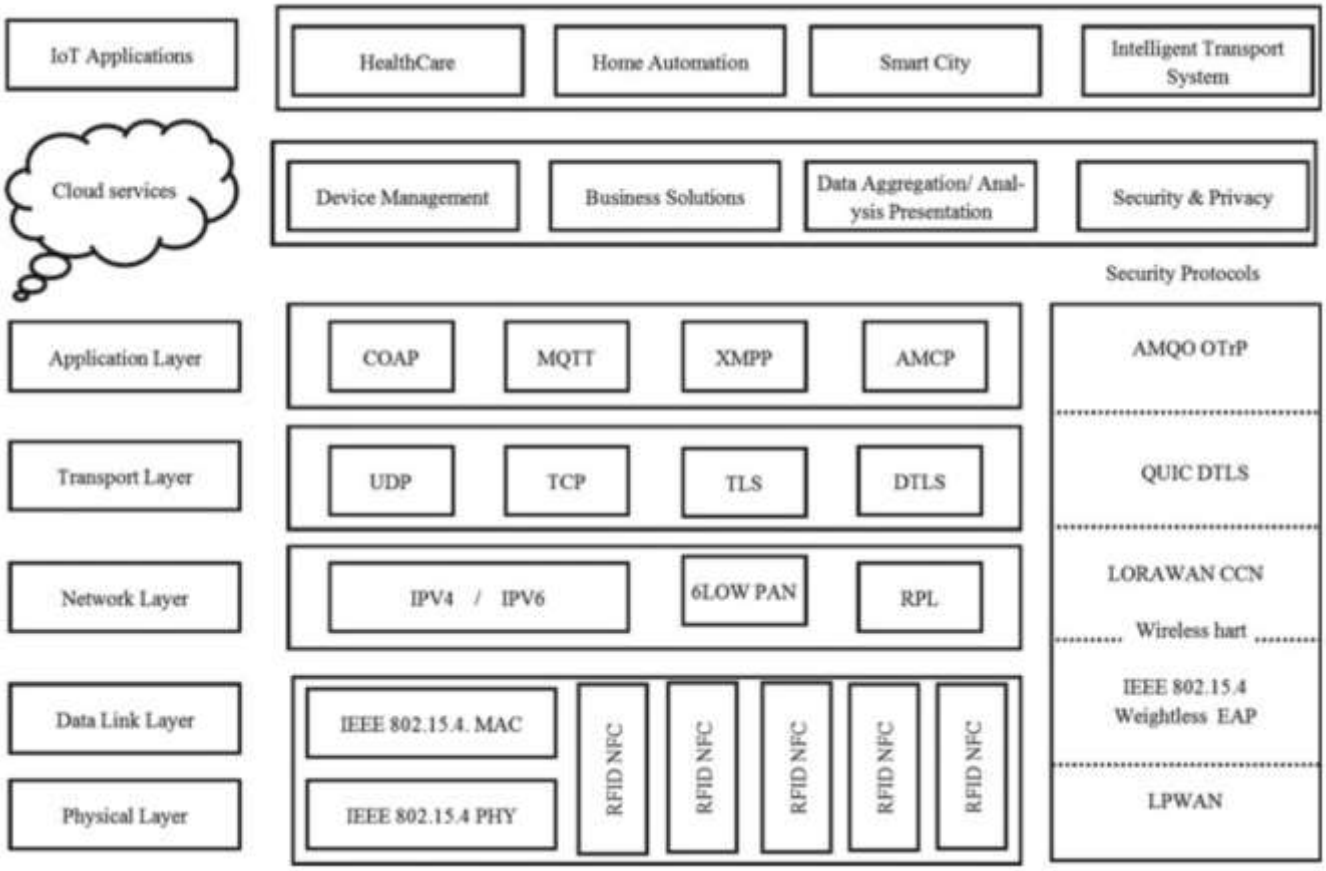

Рис .2.1. Архітектура IoT та стек протоколів

Фізичний рівень - цей рівень орієнтований на дані та відповідає за збір даних із пристроїв IoT. Параметри, які необхідно враховувати фізичному рівні IoT - це потужність, пропускна здатність і енергоспоживання. Пристрої, підключені до цього рівня, піддаються загрозам безпеки, таким як фізичне втручання у пристрої, прослуховування та зміна даних. Криптографічні алгоритми відіграють важливу роль у безпеці фізичного рівня. Глобальна мережа з низьким енергоспоживанням (LPWAN) використовується IoT для передачі невеликих даних на великі відстані з ефективним використанням батареї. Технологія підключення до Інтернету речей IoT може бути обрана на основі пропускної здатності каналу, QoS, надійності, діапазону, часу автономної роботи, безпеки, вартості та стандарту [15].

Канальний рівень - збільшення потужності передачі також збільшує швидкість передачі даних бездротового зв'язку. Можна використовувати будь-який протокол бездротового зв'язку, наприклад Bluetooth, Wi-Fi, Zigbee. IEEE802.15.4 використовується для забезпечення безпеки канального рівня. Він захищає кадри

MAC за допомогою криптографічних методів із симетричним ключем. Сюди входять Zigbee, 6LoWPAN, Wireless-HART. Weightless – це стандарт, який використовується для безпечного обміну даними між базовими станціями та кількома пристроями IoT. EAP (Extensible Authentication Protocol) підтримує кілька методів аутентифікації та працює незалежно від IP.

Мережевий рівень - на цьому рівні безпека зазвичай забезпечується протоколами 6LoWPAN та IPSec. Обмежений вузол використовує 6LoWPAN, а необмежений пристрій використовує IPv6 для адресації IoT. 6LoWPAN спеціально розроблений для забезпечення безпеки пристроїв з низьким енергоспоживанням та обчислювальними можливостями у WSN та Інтернеті. Тому криптографічні алгоритми поєднують методи RSA та ECC. 6LoWPAN повинен супроводжуватися методами IDS для моніторингу трафіку на предмет будь-якої зловмисної поведінки [16].

CCN (Content Concentric Networking) - це протокол, який використовується для доставки контенту у вигляді пакетів та розроблений для забезпечення масштабованості, мобільності та безпеки. IP Sec (безпека інтернет-протоколу) призначений для забезпечення автентифікації даних відправника та інкапсуляції корисних даних безпеки для забезпечення шифрування даних та автентифікації відправника.

Транспортний рівень - протокол QuiC [21] забезпечує мультиплексні з'єднання UDP і забезпечує захист, аналогічний TLS/SSL, для зменшення затримки з'єднання. Протокол DTLS (транспортний рівень дейтаграм) забезпечує конфіденційність зв'язку між клієнтом та сервером. Це запобігає падінню карнизу, фальсифікації та підробці. IPSec на транспортному рівні забезпечує конфіденційність та цілісність.

Прикладний рівень - до проблем безпеки рівня належать автентифікація користувачів, конфіденційність, контроль доступу, безпека проміжного програмного забезпечення. Обмежений вузол використовує CoAP, а необмежений вузол використовує HTTP як протокол прикладного рівня. Обмежений вузол також автентифікується шлюзом. Необмежений вузол доручає роботу з генерації головного сеансового ключа та автентифікації довіреного шлюзу. Криптографічні ключі

генеруються та обмінюються на основі еліптичної кривої – обміну ключами Деффі-Хеллмана. AMQP (Advanced Message Queuing Protocol) - це протокол проміжного програмного забезпечення, орієнтованого на повідомлення, який призначений для забезпечення маршрутизації, надійності та безпеки черги повідомлень.

Відкритий протокол довіри (OTrP) - це протокол для встановлення, оновлення та видалення програм, а також для керування конфігурацією безпеки у довіреному середовищі виконання (TEE). X.509 – це стандарт інфраструктури відкритого ключа (PKI) для керування цифровими сертифікатами та шифруванням з відкритим ключем. Ключова частина протоколу безпеки транспортного рівня використовується для захисту веб-комунікацій та електронної пошти.

2.5 Типи атак на IoT

Важлива особливість про IoT полягає в тому, що він робить речі розумними, вбудовуючи датчики та приводи. Збільшуючи можливості підключення, дозволяючи використовувати нові послуги. З іншого боку, обсяг даних, що генеруються IoT, збільшується, що призводить до атак на безпеку.

Тому з’являються такі питаня:

- Чому безпека важлива в IoT?
- Що може зробити зловмисник, атакуючи пристрій?
- Чому важливо враховувати атаку на пристрій?
- Чи може мій пристрій надсилати особисті дані зловмисникам?

Інтернет речей включає різні датчики, носимі пристрої, мобільні телефони і побутову техніку. У більшості випадків пристрої виготовляються виробниками, які не знають про безпеку. Коли користувач зберігає в своєму мобільному телефоні особисті дані, такі як поштові паролі, банківські реквізити тощо, він зазвичай вважає, що вони зберігаються в його локальній пам'яті. Насправді дані зберігаються у хмарному сховищі. Це дозволяє хакеру легко атакувати дані в хмарі та використовувати їх не за призначенням. Саме тому безпека в IoT вважається важливішою.

Може з’явитися таке питання, зазвичай люди зберігатимуть дані лише у своїх мобільних телефонах, тоді навіщо потрібний захист сенсорних пристроїв та іншої побутової техніки?

Справа в тому, що коли пристрій, скажімо, камера відеоспостереження, підключена до будинку, зазнає атаки, хакер може чітко знати можливість пограбування будинку. Це також запросить до будинку невідомих.

Наприклад якщо розумний холодильник, який замовляє продукти буде зламаний, то він зможе замовити будь-яку продуктів речей або може генерувати спам. У такій ситуації користувач або втратить гроші за непотрібні йому продукти або розлютиться і вимкне пристрій. Важливо те, що атакований пристрій підключено до наших мобільних телефонів та інших пристроїв. Таким чином, коли атакований простий пристрій хакер може легко отримати доступ до пристроїв, які містять захищені дані. Ось чому безпека вважається важливою у IoT.

2.5.1 Атаки на прошивку

Прошивка - це не що інше, як програмне забезпечення, яке використовується для керування апаратними пристроями. З початку 90-х почалися атаки на прошивки пристроїв. Зазвичай прошивка зберігається в незалежній пам'яті. Хакери зазвичай додають у цю незалежну пам'ять якийсь шкідливий код, роблять його частиною прошивки і починають керувати пристроєм. Ще одна причина, через яку люди віддають перевагу атакам на вбудоване ПЗ, полягає в тому, що їх важче виявити, оскільки вони запускаються до запуску антивірусної програми.

Хакери атакують прошивки з трьох основних причин [22]:

1. Стійкість: шкідливі програми часто можна видалити за допомогою антивірусного програмного забезпечення, а прошивку – ні.
2. Захист: такі механізми, як антивірусне програмне забезпечення, не перевірятимуть прошивку, що дозволить приховати шкідливой код та використовувати протягом тривалого часу.
3. Авторизація: додаючи шкідливий код, хакер зможе отримати повну авторизацію для доступу до системи.

Популярність цього типу атаки полягає в тому, що програмне забезпечення прошивки часто буває застарілим.

Більшість людей не знають про оновлення програмного забезпечення пристрою. Звичайно, виробник пристрою не є експертом у галузі безпеки, що призводить до вразливості пристрою.

Тим не менш, навіть остання прошивка не надасть повну безпеку. Більшість пристроїв, які виробляються останнім часом, оснащені операційною системою десятирічної давності. Крім того, прошивка не підтримується фахівцями з безпеки, що призводить до легших атак на них.

Але оновлювати пристрої та підтримувати їх у актуальному стані в будь-якому випадку необхідно. Від виробників потрібно вимагати, щоб вони більше піклувалися про безпеки пристроїв. Це можливо лише тоді, коли IT-фахівці, галузеві експерти та фахівці з кібербезпеки працюють разом.

2.5.2 Атаки на дані

IoT дозволяє підключати все більше і більше пристроїв, що призводить до більшої кількості вразливих систем безпеки. Підключені пристрої (як показано на рис. 2) можуть включати всі об'єкти, які ми використовуємо в повсякденному житті.

Ми зберігатимемо дані від температури до наших конфіденційних даних, таких як паролі. Це там захищено?

Ні. Ми вважаємо, як пов'язаний об'єкт може надавати інформацію. Розглянемо камеру спостереження, яка записує дані про теракт. Якщо людина може легко зламати її, вона може змінити записи. Тепер ви знаєте важливість даних? Знову ж таки, ви можете здивуватися, що камеру спостереження набагато легше атакувати? Він може бути захищений, але підключений до нього маршрутизатор або підключений до нього датчик можуть легко атакуватися. Таким чином, Інтернет речей надає хакерам більше можливостей для крадіжки інформації. Розрахункова кількість пристроїв з оцінки CISCO може досягти 50 мільярдів до 2020 року, як показано на рис. 3. Якщо майже кожен пристрій буде вразливим для атаки, світу не буде. Якщо будь-які дані можна зламати простими засобами, немає сенсу підключатися.

Поясню на іншому прикладі. Ви зберегли свої банківські реквізити (конфіденційні дані) у мобільних телефонах. Ви думаєте, що він захищений паролями, відбитками пальців тощо, щоб його не можна було атакувати. Але коли ви намагаєтеся керувати вентилятором (в «Розумному домі» - IoT-додатку) з мобільного телефону, насправді це відбувається за допомогою датчика. Якщо датчик зламаний, шкідливий код автоматично переноситься на мобільні пристрої, що полегшує атаку. Тепер ви вважаєте, що це неможливо? Ви не можете. Інтернет речей дозволяє з'єднувати речі, але також створює безліч дірок у безпеці.

2.5.3 Атаки через TELNET

Telnet фактично надає шлюз для атак на Інтернет речей. IBM Security також випустила дослідження у якому чітко підкреслюється, що Telnet, дуже старий метод доступу до віддалених систем і може використовуватися для отримання несанкціонованого доступу. [23]

Багато вбудованих системних програм використовують його можливості віддаленого доступу. Якщо зловмисник може знайти відкритий порт telnet, він може виконати такі дії:

- Використовувати будь-які вразливості, пов'язані з пристроєм
- Отримати несанкціонований доступ до пристрою для крадіжки даних.
- Визначити, як інформація розподіляється між пристроями.
- Робити brute force атаки для отримання паролів.

Одним із прикладів такої атаки є атака Bricker Bot. Атака бота Bricker використала атаку Telnet Brute force для зламування пристроїв жертви. Завдяки цьому зловмисник отримав доступ до приєднаних пристроїв. Від атаки можна захиститися, відключивши Telnet та змінивши паролі за замовчуванням.

Ще одна причина важливості telnet полягає в тому, що більшість пристроїв матимуть стандартні ім'я користувача та пароль. Незважаючи на те, що людям, які використовують пристрої, дається вказівка змінити паролі, неясно, чи всі це роблять. Стандартні паролі не змінюються, тому до таких пристрояїв можна легко отримати віддалений доступ через Telnet та SSH.

2.5.4 DDOS-атака

Атака типу «Denial of Service Attack» – ще одна популярний тип атак. Атака типу "DoS" генерує велику кількість трафіку на сервер і перевантажує його, що призводить до проблем з роботою. Якщо DoS-атака виконується з допомогою величезного ботнета, вона називається «Distributed Denial of Service Attack». Ботнети IoT можуть складатися з веб-камер, телевізорів, відеореєстраторів, блоків налаштування тощо і використовуватися для DDoS-атак.

20 вересня 2016 «KrebsOnSecurity.com» став об'єктом масштабної DDoS-атаки, в результаті якої сайт був відключений. Спочатку веб-сайт був захищений від цієї атаки Akamai, постачальником послуг цифрової безпеки веб-сайту. Компанія вирішила відкликати свій безкоштовний захисний щит, оскільки масштаби атаки (приблизно 620 Гбіт/с) були надто великі, щоб витримати її, не торкнувшись інших клієнтів. Аналіз Akamai показав використання великого ботнету скомпрометованих пристроїв IoT. Після зняття захисту Akamai веб-сайт відключився, поки Google не запропонував свою службу запобігання DDoS-атакам Project Shield, щоб відновити його.

OVH, відомий провайдер веб-хостингу, також став жертвою ще більш масштабної DDoS-атаки, ніж та, що вразила KrebsOnSecurity. Згідно з повідомленням засновника OVH Октава Клаба від 22 вересня 2016 року, одночасна DDoS-атака зі швидкістю 990 Гбіт/с (у сукупності) була запущена ботнетом, що складається з більш ніж 145 000 скомпрометованих пристроїв IoT (IP-камери та відеореєстр). OVH повідомив, що витримав атаку.

Відразу після DDoS-атак на KrebsOnSecurity.com і OVH користувач на хакерському форумі опублікував вихідний код шкідливого ПЗ, що отримав назву Mirai. Він націлений на незахищені IoT-пристрої і перетворює їх на ботів. Зловмисник може запустити DDoS-атаку, керуючи всіма ботами через центральний сервер управління та контролю, як це робиться у звичайних ботнетах.

21 жовтня 2016 року DNS-провайдер Dyn зазнав масованої DDoS-атаки і спочатку стверджував, що атака була здійснена з десятків мільйонів IP-адрес по

всьому світу. У пізнішому оновленні від Dyn зазначалося, що кількість шкідливих кінцевих точок насправді оцінюється приблизно в 100 000. Атака викликала проблеми у деяких користувачів, які намагалися отримати доступ до популярних веб-сайтів, таких як Twitter, Amazon, Tumblr, Reddit, Spotify та Netflix протягом дня. Згідно з інформацією Dyn про інцидент, в частині атаки брали участь IoT-пристрої, заражені ботнетом Mirai. Після кількох годин та кількох хвиль атак Dyn вирішив інцидент.

Основні тези про масові DDoS-атаки IoT полягають у наступному:

Величезні обсяги трафіку на DNS-серверах призвели до того, що багато веб-сайтів перестали працювати. Ботнет складається з великої кількості незахищених пристроїв, таких як домашні маршрутизатори та камери спостереження.

Використання паролів за промовчанням є однією з основних причин цієї вразливості.

Для запобігання цьому треба:

• Оновлювати пристрої IoT за допомогою виправлень безпеки, коли виправлення стають доступними.

• Відключіть Universal Plug and Play (UPnP) на маршрутизаторах, якщо в цьому немає необхідності.

• Купувати пристрої IoT у компаній із репутацією постачальників безпечних пристроїв.

2.5.5 roBOT + NETwork (BOTNET)

Ботнети з використанням IoT не нова ідея. Ботнет - це логічне з'єднання компрометованих пристроїв, таких як маршрутизатори, смартфони або пристрої IoT. Ці скомпрометовані пристрої можна контролювати та використовувати для проведення DDoS-атак. Мета створення ботнета - заразити якнайбільше пристроїв. Як правило, ботнети IoT використовувалися для запуску гучних DDoS-атак на для атак на організації.

Деякі з відомих атак ботнета - Zeus, ботнет Srizbi, Gameover Zeus і т.д. Атака Zeus використовувала троянську програму для зараження вразливих пристроїв і створило Zbot, який можна використовувати для збору банківських облікових даних

та фінансової інформації. Ботнет Srizbi знову використав троянську програму. Ботнет Gameover Zeus генеруватиме доменні імена, які будуть служити точками зв'язку для заражених ботів. Заражений пристрій буде перебирати домени, поки не знайди активний домен, здатного видавати нові команди.

Шкідливе програмне забезпечення Mirai призначене для сканування Інтернету на наявність незахищентих підключених пристроїв, а також для уникнення IP-адрес, що належать великим корпораціям, таким як Hewlett-Packard і державним установам, таким як Міністерство оборони США. Виявивши небезпечний пристрій, шкідливе програмне забезпечення намагається увійти в систему, використовуючи ряд поширених паролів за замовчуванням, що використовуються виробниками. Якщо ці паролі не працюють, Mirai використовує атаку brute force, щоб підібрати пароль. Як тільки пристрій скомпрометований, він стає частиною DDoS атаки.

Заражені пристрої часто продовжують нормально функціонувати, що ускладнює виявлення активності ботнета Mirai. Для деяких пристроїв IoT, таких як цифрові відеомагнітофони, стандартний пароль жорстко закодований у прошивці пристрою і багато пристроїв не можуть оновлювати прошивку через Інтернет.

Пізніше код Mirai був опублікований, що дозволило будь-кому використовувати шкідливе програмне забезпечення для створення бот-мереж з використанням погано захищених IoT-пристроїв.

2.5.6 Шкідливе програмне забезпечення

Шкідливе програмне забезпечення - це програмне забезпечення, яке використовується для отримання доступу до пристрою та його зараження. Більшість атак IoT виконуються або за допомогою троянської програми, або за допомогою шкідливого програмного забезпечення. Атака BrickerBot та ботнет Mirai створюються шляхом додавання до них шкідливого програмного коду. У 2015 та 2016 роках було здійснено понад 8,5 мільйонів атак шкідливого ПЗ.

Чому ці пристрої такі вразливі для зараження шкідливим програмним забезпеченням? З ряду причин, але насамперед тому, що виробники поспішно створили незахищені продукти, прагнучи отримати вигоду з фінансових

можливостей, що надаються недорогими технологіями IoT. Під тиском необхідності бути конкурентоспроможними та швидко виводити продукти на ринок питанням безпеки приділяється дуже мало уваги. В результаті пристрою IoT зазвичай страждають від:

• Слабка автентифікація: паролі та облікові дані для входу часто залишаються за замовчуванням, багато з яких ненадійні та легко вгадуються. Деякі пристрої мають одиночні фіксовані паролі або взагалі не потребують автентифікації.

• Численні вразливості у системі безпеки. У багатьох випадках продукти розробляються інженерами з дуже невеликим досвідом у сфері безпеки. Історія неодноразово показувала, що будь-який код має вразливість. Програмне забезпечення, розроблене або створене поспіхом в умовах вкрай обмеженого бюджету, має ще більше вразливостей.

• Обмежені можливості оновлення: недорогі пристрої, як і багато продуктів IoT, часто мають дуже низький прибуток, що може ускладнити або навіть унеможливити виробникам дозволити собі оновлення мікропрограми або відправлення виправлень безпеки.

• Обмежене шифрування: значна частина пристроїв IoT повністю позбавлена шифрування ні при передачі, ні при зберіганні.

• Неправильні пріоритети. Небагато співробітників IT-безпеки витрачають сили на безпеку інтелектуальних термостатів, камер відеоспостереження, цифрових відеореєстраторів, торгових автоматів або інших «гаджетів», підключених до мережі компанії.

Смарт-гаджети, заражені шкідливим ПЗ, можуть завдати шкоди кількома способами, у тому числі такими:

• Атаки типу «DoS»

• Атаки програм-вимагачів

• Крадіжка особистих даних

• Захоплення облікового запису

• Крадіжка ІС

Настав час підприємствам серйозно поставитися до безпеки IoT та запровадити політики та інструменти для виявлення сучасних шкідливих програм, які вже існують чи намагаються закріпитися у їхніх організаціях.

Витративши розумну кількість часу та зусиль на запобігання шкідливим програмам IoT зараз, підприємства будуть набагато краще підготовлені до постійно зростаючої кількості вразливих пристроїв, які напевно підключатимуться до їхніх мереж.

ВИСНОВКИ ДО РОЗДІЛУ 2

У цьому розділі було розглянуто суть проблеми безпеки IoT, основні вимоги до безпеки, криптографічні алгоритми, методи керування ключами, алгоритми маршрутизації, основні вектори атак.

РОЗДІЛ 3
МЕТОДИ ПІДВИЩЕННЯ ЗАХИСТУ IOT ТА РОЗУМНОГО БУДИНКУ

Оскільки Інтернет речей складається з безлічі підключених пристроїв, таких як датчики та мітки RFID, важливо адаптувати ці пристрої для роботи у звичайному Інтернеті. Пристрої IoT часто обмежені в обчислювальній потужності та об'ємі пам'яті. Тому використання криптографічних алгоритмів, яким часто потрібно більше ресурсів, ніж усі крихітні пристрої разом узяті, є складним завданням. Ще одна проблема – оновлення пристроїв у польових умовах. Часто доступне лише ненадійне з'єднання, а важливі для безпеки речі вимагають негайних оновлень, які складно розгорнути на всіх пристроях одночасно. Крім того, завдання зробити безпеку інтуїтивно зрозумілою для користувача є актуальним як ніколи, тому що прийняття користувачами залежить від простоти встановлення та обслуговування.

Розглянемо протоколи та рішення для забезпечення безпеки, які можуть бути використані в IoT на різних рівнях.

3.1 Рішення для транспортного рівня

Транспортний рівень переважно включає два типи протоколів, TCP та UDP. На додаток до цих протоколів є інші протоколи, такі як Secure Socket Layer (SSL), Datagram Transport Layer Security (DTLS) та Quick UDP Internet Connections (QUIC).

3.1.1 Протокол керування передачею (TCP)

TCP є одним із найбільш широко використовуваних протоколів транспортного рівня, де потрібна надійність передачі даних. TCP працює за принципом тристороннього рукостискання. Він має фазу встановлення з'єднання, фазу передачі даних та фазу завершення з'єднання. Це допомагає досягти надійної передачі даних. TCP це протокол, орієнтований на з'єднання. Він визначає, як розбити ці програми на пакети, щоб їх можна було легко обробляти на мережному рівні. Через

перевантаження мережі деякі пакети можуть бути втрачені. TCP виявляє ці проблеми та повторно передає їх.

Він не забезпечує жодного механізму безпеки для запобігання крадіжці даних. Безпеку можна додати за допомогою SSL або TLS, які ми обговоримо в наступних розділах.

3.1.2 Secure Socket Layer (SSL)

TCP не забезпечує жодної безпеки даних. Для передачі приватних даних було створено SSL. SSL використовує криптографічну систему, яка використовує два ключі для шифрування даних – відкритий ключ та закритий ключ.

Коли веб-браузер намагається підключитись до веб-сайту за допомогою SSL, браузер спочатку запитує ідентифікацію веб-сервера. Це спонукає веб-сервер надіслати браузеру копію SSL-сертифіката. Браузер перевіряє, чи сертифікат SSL є довіреним. Якщо сертифікат SSL є довіреним, браузер надсилає повідомлення на веб-сервер. Потім сервер відповідає браузеру підтвердженням із цифровим підписом для запуску зашифрованого сеансу SSL. Це дозволяє обмінюватися зашифрованими даними між браузером та сервером.

Незважаючи на те, що SSL забезпечує безпеку, він як і раніше схильний до атак «man in the middle». Щоб подолати цю проблему був створений TLS.

3.1.3 Transport Layer Security (TLS)

SSL є попередником TLS. SSL має три версії, і всі вони вважаються небезпечними через недоліки в їх конструкції. TLS було створено для усунення недоліків протоколу SSL. Терміни SSL, TLS і SSL/TLS зазвичай використовуються в літературі як взаємозамінні.

TLS – це протокол, що забезпечує конфіденційність та цілісність даних між двома взаємодіючими додатками. Це найбільш широко використовуваний протокол безпеки, який використовується для веб-браузерів та інших програм, що вимагають безпечного обміну даними по мережі, таких як передача файлів, VPN-підключення, обмін миттєвими повідомленнями та передача голосу по IP.

Ключовими відмінностями між SSL і TLS, які роблять TLS безпечнішим та ефективнішим протоколом, є автентифікація повідомлень, генерація ключового матеріалу та підтримувані набори шифрів, при цьому TLS підтримує новіші та безпечніші алгоритми. TLS і SSL несумісні, хоча зараз TLS забезпечує деяку зворотну сумісність для роботи зі застарілими системами.

Хоча TLS забезпечує безпеку, було виявлено, що він підтримує з'єднання, навіть коли дані не передаються. TLS невразливий для атаки POODLE, оскільки він вказує, що всі байти заповнення повинні мати однакове значення і бути перевірені. Але є атаки які використовують певні реалізації протоколу TLS, які неправильно перевіряють заповнення шифрування. Це робить деякі системи вразливими для POODLE, навіть якщо вони відключають SSL - один із рекомендованих методів протидії атаці POODLE.

3.1.4 User Datagram Protocol (UDP)

UDP - це протокол без встановлення з'єднання. Він не має діалогів квитування і таким чином, наражає програму користувача будь-якої ненадійності основного мережевого протоколу. Немає жодних гарантій доставки, пакетів чи захисту від дублювання. UDP надає контрольні суми для перевірки цілісності даних та номери портів для адресації різних функцій у джерелі та одержувачі дейтаграми.

У порівнянні з TCP UDP краще підходить для пристроїв IoT через мінімальні накладні витрати. У багатьох системах, що вбудовуються з обмеженими ресурсами, відсутність накладних витрат в UDP має велике значення в пропускній здатності в порівнянні з TCP. UDP не вимагає встановлення з'єднання і, отже, не підтримує стан з'єднання, тому розмір/використання пам'яті не є великою проблемою. Оскільки для передачі UDP потрібні лише дві дейтаграми UDP, по одній у кожному напрямку, навантаження на мережу зводиться до мінімуму, що ще більше скорочує час відгуку.

3.1.5 Безпека транспортного рівня дейтаграм (DTLS)

DTLS - це комунікаційний протокол, який забезпечує безпеку додатків, що працюють з дейтаграмами, дозволяючи їм обмінюватися даними таким чином, щоб

запобігти прослуховуванню, фальсифікації або підробці повідомлень. Протокол DTLS заснований на потоковому TLS та призначений для забезпечення гарантій безпеки. Дейтаграма протоколу DTLS зберігає семантику базового транспорту - програма не страждає від затримок, пов'язаних із потоковими протоколами, але має справу з переупорядкуванням пакетів, втратою дейтаграми та даними, що перевищують розмір мережевого пакета дейтаграми.

DTLS складається з двох рівнів: нижній рівень містить Record протокол, а верхній рівень містить будь-який із трьох протоколів, а саме Handshake, Alert, Change Cipher Spec або дані програми. Специфікація зміни шифру використовується під час рукостискання, щоб просто вказати, що протокол запису повинен захищати наступні повідомлення за допомогою нещодавно узгодженого набору шифрів і ключів безпеки. DTLS використовує протокол Alert для надсилання повідомлень про помилки між одноранговими вузлами DTLS. Протокол Record є носієм протоколів верхнього рівня. Заголовок Record містить поля типу контенту та фрагмента. Залежно від значення типу контенту, поле фрагмента містить протокол Handshake, Alert, Change Cipher Spec або дані програми. Заголовок Record в першу чергу відповідає за криптографічний захист протоколів верхнього рівня або даних програми після завершення процесу рукостискання. Захист протоколу Record включає конфіденційність, захист цілісності та автентичність.

DTLS Record – це досить простий протокол, тоді як протокол Handshake – це складний діалоговий процес, який містить численні асинхронні обміни повідомленнями. Повідомлення рукостискання, зазвичай організовані в пакети, використовуються для узгодження ключів безпеки, наборів шифрів та методів стиснення. Обсяг цієї обмежений лише стиском заголовків, а не криптографічною обробкою протоколів Record та Handshake.

3.1.6 Quick UDP Internet Connections (QUIC)

QUIC - це ще один протокол, орієнтований на мультиплексування потоків через UDP. QUIC призначений для забезпечення безпеки, еквівалентної SSL/TLS. Основна мета цього протоколу – підвищити продуктивність порівняно з TCP.

Ключові переваги QUIC в порівнянні з TCP + TLS + HTTP2 включають:

• Менша затримка встановлення з'єднання

• Покращений контроль заторів

• Мультиплексування без блокування початку рядка

• Запобіжне виправлення помилок

• Міграція з'єднання.

3.2 Рішення для прикладного рівня

HTTP підходить для отримання інформації з використанням моделі запит-відповідь, але IoT підключено більше пристроїв і є потреба у міжмашинному взаємодії. Крім того, пристрої IoT продовжують передавати інформацію в хмару або сервери, які їм необхідно відправити. У такому разі HTTP не підходить. Крім того, HTTP використовує велику пропускну здатність через текстову модель запиту та відповіді, яка не підходить для пристроїв з низькою пропускною здатністю. Пам'ятаючи про це, було розроблено два протоколи: MQTT та COAP.

Ще одна причина популярності цих протоколів полягає в тому, що вони менші, ніж HTTP, призначені для міжмашинної взаємодії, якості обслуговування, а також терпимі до мереж із втратами.

3.2.1 CoAP (Constrained Application Protocol)

CoAP - це обмежений протокол додатків, сама назва говорить про те, що це протокол прикладного рівня. Прикладний рівень знаходиться трохи вище за транспортний рівень, де TCP і UDP є основними протоколами. Проблема з UDP полягає у тому, що він нестабільний. Оскільки HTTP не підходить для пристроїв з низьким енергоспоживанням та низькою пропускною здатністю потрібно шукати нові протоколи.

Протокол CoAP було запропоновано у 2014 році. Розробники CoAP розробили його таким чином, що він повинен включати функції HTTP, а також застосовуватися

для обмежених пристроїв. CoAP працює через UDP та заснований на архітектурі REST. Структура повідомлення CoAP показано на рис. 6.

CoAP використовує дворівневу структуру, де шарами є повідомлення та запит/відповідь. Рівень повідомлення складається з CON (confirmable), NON (non-confirmable), ACK (acknowledgement) та RST (reset). Він призначений для повторної передачі втрачених пакетів.

1. CON (Confirmable) - якщо потрібна надійність, використовуйте цей тип повідомлення. У цьому випадку на повідомлення відповідають підтвердженням

2. NON (non-confirmable) – якщо надійність не має великого значення, використовуйте цей варіант.

3. ACK (acknowledgement) - цей тип призначений для забезпечення надійності

4. RST (reset) - якщо щось піде не так, буде використано скидання.

Рівень запиту/відповіді містить такі методи, як GET, PUT, POST та DELETE. Протокол CoAP реалізує спеціальні функції недоступні у HTTP. Особливості:

(i) Observe flag . У HTTP складно визначити стан змінної, що не використовується. Цей прапор використовується разом із повідомленням GET. Щоразу, коли відбувається зміна прапора спостереження, воно надсилає повідомлення на пристрій.

(ii) Discovery - цей прапор пов'язаний із виявленням пристроїв навколо нас. Сервер може зберігати список пристроїв та типів носіїв, які вони підтримують.

Якість обслуговування (QoS) досягається за допомогою повідомлень, що підтверджуються і не підтверджуються.

Для захисту передачі CoAP як основний протокол безпеки було запропоновано DTLS. За аналогією з протоколом HTTP, захищеним TLS (HTTPs), протокол CoAP із захистом DTLS називається CoAPs. DTLS гарантує E2E-безпеку різних програм на одному комп'ютері, працюючи між транспортним та прикладним рівнями.

3.2.2 MQTT (Message Queue Telemetry Transport)

MQTT [24] - це полегшений протокол на основі TCP, в якому використовується шаблон обміну повідомленнями "publish-subscribe" (див. рис. 7). Будь-яке джерело,

наприклад датчик, може публікувати свої дані, і будь-який клієнт може підписатися на ці дані. Протокол MQTT призначений для пристроїв з обмеженими ресурсами, пропускна здатність яких є мінімальною. MQTT складається з трьох компонентів: брокера, видавця та підписника. Брокер відстежує всі публікації та підписки. Видавець публікує інформацію для всіх підписників через брокера. Брокер забезпечує безпеку, перевіряючи авторизацію видавців та підписників. Брокер також гарантує доставку повідомлення, тобто воно буде доставлено хоча б один раз або рівно один раз.

MQTT використовує двійковий формат, що вимагає мінімальної пропускної здатності. Фіксований заголовок складає всього два байти. Тип повідомлення вказує на різні повідомлення, включаючи CONNECT, CONNACK, PUBLISH та SUBSCRIBE. Поле DUP вказує, що повідомлення продубльовано, і одержувач міг отримати його раніше. Поле рівня QoS призначене для забезпечення доставки. MQTT підтримує три рівні рівнів QoS: "відправив і забув", "доставлений хоча б один раз" і "доставлений рівно один раз". Поле RETAIN інформує сервер про необхідність зберегти останні отримані повідомлення публікації.

Він не тільки використовує простий формат повідомлення, а й вимагає менше електроживлення. Спочатку MQTT був створений в 1999 для віддалених датчиків. Тепер він використовується для безпечного та надійного зв'язку між пристроями. MQTT заснований на протоколі TCP і може бути захищений за допомогою TLS. MQTT забезпечує мінімальну безпеку. Комунікації MQTT, засновані тільки на TCP, не зашифровані і схильні до атак «man in the middle», DDoS-атакам і атак переповнення буфера.

Наступна проблема з MQTT полягає в тому, що повідомлення MQTT надсилаються у відкритому вигляді. Отже, імена користувачів та паролі легко доступні. Для забезпечення підтримки процесу аутентифікації він використовує TLS. Шифрування транспорту за допомогою SSL та TLS може захистити дані при правильному застосуванні. Для захисту від загроз конфіденційні дані, включаючи ідентифікатори користувачів, паролі та інші типи облікових даних, завжди повинні бути зашифровані. Недоліком використання TLS, SSL та інших методів шифрування

є те, що вони можуть спричинити значні накладні витрати. Однак такі методи, як відновлення сеансу TLS можуть компенсувати деякі витрати на підключення TLS. Апаратне прискорення - ще один спосіб зменшення штрафу за розмір при шифруванні. Для складних програм на обмежених пристроях оптимізована бібліотека шифрування може бути дуже корисною. Коли код програми великий, бібліотека шифрування може зменшити обсяг пам'яті для обробки та підвищити продуктивність. Архітектура MQTT залежить від високої доступності брокерів. Використання сертифікатів X.509 для автентифікації клієнтів може заощадити ресурси на стороні брокера, коли багато клієнтів намагаються використовувати служби брокера, такі як пошук у базі даних або дзвінки веб-служб. Поєднання MQTT з найсучаснішими стандартами безпеки, такими як TLS, та використання сертифікатів X.509 також може допомогти підвищити безпеку та продуктивність. Шифрування даних для забезпечення безпеки та конфіденційності також має вирішальне значення для потоків доходів постачальників послуг у забезпеченні оптимальної якості обслуговування клієнтів.

Незважаючи на те, що MQTT розроблений, щоб бути легким, він має два недоліки для дуже обмежених пристроїв. Кожен клієнт MQTT повинен підтримувати TCP і зазвичай постійно підтримує з'єднання з брокером. Для деяких середовищ із високою втратою пакетів або нестачею обчислювальних ресурсів це проблема. Крім того, імена тем MQTT часто є довгими рядками. Обидві ці недоліки усуваються протоколом MQTT-SN (MQTT - Sensor Networks), який визначає UDP-порівняння MQTT і додає підтримку брокера для індексації імен тем.

3.2.3 Secure MQTT (SMQTT)

MQTT та MQTT-SN використовують SSL/TLS для забезпечення безпеки. Але насправді надати сертифікати безпеки всім пристроям неможливо. Також SSL/TLS страждає від таких атак, як BEAST, CRIME і т. д. Для подолання цієї проблеми пропонується Secure MQTT, який доповнює функцію безпеки для існуючого протоколу MQTT. У цьому протоколі використовуються різні типи повідомлень, які відрізняються за типом повідомлення в заголовку MQTT. Тип повідомлення "0000"

зарезервований на майбутнє. Заголовок змінної містить прапорець імені користувача та пароля (може полегшити аутентифікацію користувача), після їх встановлення відповідні значення також включаються в корисне навантаження. Однак ці значення не зашифровані в повідомленні а, отже, небезпечні. Протокол SMQTT доповнює функцію безпеки існуючого MQTT, пропонуючи нову публікацію повідомлень MQTT із зарезервованим типом повідомлення "0000", де повідомлення зашифровані за допомогою ABE (шифрування на основі атрибутів). Видавець використовує команду Spublish для публікації зашифрованого повідомлення за допомогою ABE. Отже, підписники, які відповідають політиці доступу, можуть розшифрувати повідомлення. Перевага ABE полягає в тому, що він підтримує широкомовне шифрування, що підходить для пристроїв IoT. ABE бувають двох типів: ABE на основі політики шифрованого тексту (CP-ABE) та ABE на основі політики ключів (KPABE). [25]

У безпечному протоколі MQTT є три сутності:
(i) Видавничий пристрій публікує дані на задану тему.
(ii) Абонентський пристрій отримує дані з тієї ж теми через брокера.
(iii) PKG або брокер є довіреною третьою стороною.

У протоколі чотири фази. На етапі налаштування виконується реєстрація та керування ключами. На етапі шифрування дані шифруються, а на етапі публікації Publisher публікує зашифровані дані під заданим ім'ям теми та надсилає їх брокеру. На етапі розшифровки дані розшифровуються підписаними пристроями.

3.3 Рішення для мережного рівня

Пристрої в Інтернеті - це пристрої з обмеженими ресурсами, що означає потужність та обсяг пам'яті обмежені. У цьому розділі буде розглянуто протоколи IPv6 та 6LowPAN. IPv6 може підтримувати адресний простір усіх задіяних пристроїв IoT. 6LoWPAN спеціально розроблений для пристроїв із низьким енергоспоживанням.

3.3.1 IPv6

IPv4 - мережна адресація, що широко використовується. Це 32-бітна адреса, яка може підтримувати до 4 мільярдів пристроїв. У світі Інтернету речей кожен пристрій підключено до Інтернету, але це можна зробити лише тоді, коли IP-адреси виділені для всіх пристроїв. IPv4 недостатньо при такій величезній кількості пристроїв. Отже, переходимо на IPv6.

IPv6 – це 128-бітна адреса. Він може виділяти до 2128 діапазонів адрес. Це дозволяє виділити всю кількість пристроїв, підключених у світі IoT. Основні особливості, які роблять його вигідним у порівнянні з IPv4, полягають у наступному:

1. Масштабованість. Оскільки це 128-бітна адреса, ми можемо призначити IP-адресу кожному пристрою.

2. Можна забезпечити справжній наскрізний зв'язок

3. Коефіцієнти використання адресного простору IPv6 невеликі.

4. IP Sec є вимогою IPv6, яка дозволяє двом або більше вузлам безпечно обмінюватися даними шляхом автентифікації та шифрування кожного IP-пакету сеансу зв'язку.

3.3.2 6LoWPAN

Незважаючи на те, що IPv6 забезпечує платформу адресації, він не підходить для малопотужних пристроїв, що використовуються в IoT. Для підтримки цих пристроїв нам потрібний інший протокол. Low power Wireless Personal Area Networks (WPANs), на які можуть спиратися багато комунікації IoT, мають деякі особливі характеристики, відмінні від колишніх технологій канального рівня, такі як обмежений розмір пакета (наприклад, максимум 127 байтів для IEEE 802.15.4), різна довжина адреси та низька пропускна спроможність. Таким чином, виникла потреба у створенні рівня адаптації, який узгоджував пакети IPv6 зі специфікаціями IEEE 802.15.4. Робоча група IETF 6LoWPAN розробила такий стандарт у 2007 році. 6LoWPAN – це специфікація мапінгу сервісів потрібних IPv6 over WPAN з низьким енергоспоживанням для підтримки мережі IPv6. Стандарт забезпечує стиснення заголовків для зменшення накладних витрат під час передачі, фрагментацію для

відповідності вимогам IPv6 Maximum Transmission Unit (MTU) та пересилання на канальний рівень для підтримки доставки з кількома переходами. Дейтаграми, укладені в 6LoWPAN, супроводжуються комбінацією деяких заголовків. Ці заголовки бувають чотирьох типів, що ідентифікуються двома бітами:

- (00) - NO 6LoWPAN Header
- (01) - Dispatch Header
- (10) - Mesh Addressing
- (11) - Fragmentation

За заголовком NO 6LoWPAN пакети, що не відповідають специфікації 6LoWPAN, будуть відкидатися. Стиснення заголовків IPv6 або багатоадресне розсилання виконується шляхом вказівки заголовка Dispatch. Заголовок Mesh Addressing ідентифікує пакети IEEE 802.15.4, які мають бути перенаправлені на канальний рівень. Для дейтаграм, довжина яких перевищує один кадр IEEE 802.15.4, слід використовувати заголовок Fragmentation. 6LoW-PAN усуває безліч накладних витрат IPv6 таким чином, що в кращому разі невелика дейтаграма IPv6 може бути відправлена через один перехід IEEE 802.15.4. Він також може стискати заголовки IPv6 до двох байтів.

ВИСНОВКИ ДО РОЗДІЛУ 3

У цьому розділі було розглянуто методи покращення безпеки на різних рівнях: транспортному, прикладному, мережевому. Розглянуто протоколи Constrained Application Protocol, Message Queue Telemetry Transport, SMQTT, IPv6, 6LoWPAN.

РОЗДІЛ 4
ВДОСКОНАЛЕННЯ ГЕНЕРАЦІЇ ПАРОЛІВ ДЛЯ WI-FI

4.1 Безпека мережі Wi-Fi

Оскільки бездротовий зв'язок використовує частину спектра радіочастот, радіосигнали доступні для будь-яких пристроїв в радіусі дії. Бездротові канали зв'язку не такі безпечні, як дротові, через більш вразливі середу, радіосигнали які передаються кожному бездротовому пристрої поблизу. У цих бездротових каналах використовуються попередньо визначені радіочастоти, відомі всім, тому зловмисники можуть перехоплювати пакети або видавати себе за комунікаційну сторону, наприклад, за допомогою атак типу "man in the middle". [26]

Подібно до традиційних провідних мереж, бездротові мережі також піддаються загрозам конфіденційності, цілісності та доступності, які будуть детально розглянуті нижче.

Конфіденційність. У бездротових мережах бездротові сигнали може приймати будь-яка людина в діапазоні передачі. Таким чином, зловмисники-хакери можуть легко перехопити конфіденційні дані, що передаються бездротовими каналами зв'язку. Характер бездротового зв'язку може бути конфіденційним, незалежно від мети передачі. Бездротовий зв'язок може використовуватися для надсилання електронних листів, запиту доступу до веб-сторінки, виконання однорангової мережі або для цілей керування бездротовою мережею. У разі зашифрованого бездротового трафіку механізми та алгоритми шифрування, які використовуються для зв'язку, чутливі. Таким чином, конфіденційність бездротового зв'язку можуть бути чутливими і повинні бути передбачені для ціль.

Цілісність. У бездротових мережах є два типи джерел загроз безпеці. З одного боку, існує кілька не зловмисних джерел вразливостей у бездротовому середовищі, такі як:

- неминучі перешкоди від інших вузлів;

- втрата або ослаблення сигналу, викликане різними рівнями перешкод (різні фонові шуми, будівлі, дерева) на шляху розповсюдження радіосигналу;
- проблеми з прийомом, спричинені поганими погодними умовами;
- випадкові збої зв'язку, викликані внутрішніми апаратними та програмними проблемами у бездротових пристроях.

З іншого боку, у бездротових мережах також є зловмисні джерела загрози безпеці. Цей тип порушень цілісності є зловмисними атаками з метою перевірки даних корисного навантаження перехоплених бездротових пакетів. Для незашифрованого бездротового трафіку хакер може видати себе за один кінець зв'язку та залучити до розмови іншого кінцевого користувача. Інша вразливість бездротових мереж полягає в тому, що коли користувач бездротової мережі отримує два радіосигнали, він зазвичай вибирає для використання сильніший. Таким чином, якщо бездротовий маршрутизатор хакера перехоплює радіосигнал від відправника, а потім видає себе за одержувача, щоб передати сильніший радіосигнал назад до відправника, який нібито походить від безпроводового маршрутизатора одержувача, тоді зловмисник може видати себе за одержувача і зв'язатися з відправником-жертвою.

Доступність. Існують три проблеми, пов'язані з доступністю бездротових мереж:

1. проблема доступності виникає, якщо апаратний або програмний компонент не працює. Наприклад, апаратне забезпечення з батарейним живленням розрядилося або програмний компонент застарів і має бути оновлений через якісь фатальні помилки;
2. проблема доступності виникає коли користувач втрачає доступ до певних мережних служб. Наприклад, повільні послуги, які пропонуються бездротовою мережею. Цьому може бути багато можливих причин: сильний фоновий шум від сусідніх вузлів, потреби в послугах, що перевищують можливості приймача і т.д.;

3. проблема доступності виникає через можливість неавторизованого бездротового підключення. Наприклад, приватні власники особистих точок доступу Wi-Fi не хочуть ділитися своїм доступом з іншими в радіусі дії.

4.2 Протоколи безпеки Wi-Fi

WEP. Першим протоколом для захисту бездротових мереж є протокол WEP, випущений 1997 році. WEP, призначений для радіозв'язку, має забезпечити конфіденційність, еквівалентну традиційним мережам проводового зв'язку. WEP був розроблений для запобігання перехопленню зловмисниками бездротових даних під час їх передачі між бездротовими хостами та точками доступу. Однак від початку розробки WEP не вистачало необхідних контрзаходів для досягнення цієї мети. Експерти з кібербезпеки виявили в 2001 році кілька серйозних недоліків WEP, що призвело до рекомендацій усієї галузі не використовувати WEP для забезпечення безпеки бездротової мережі. Недоліки WEP настільки серйозні, що WEP-з'єднання може бути зламано за допомогою доступного програмного забезпечення за кілька хвилин. WEP використовує потоковий шифр RC4 (Rivest Cipher 4) для автентифікації та шифрування. Він використовує ключ шифрування, який спільно використовується користувачами бездротової мережі та точками доступу. Brute force атака може дуже швидко підібрати 40-бітний ключ. Навіть при довжині ключа 104 біта через недоліки потокового шифру RC4 можна легко зламано за допомогою деяких інструментів, таких як WEPCrack і aircrack-ng. Ось короткий виклад недоліків WEP: [26]

- У конструкції WEP не використовуються ефективні алгоритми шифрування;
- WEP неправильно автентифікує користувачів;
- WEP не має ефективного контролю за несанкціонованими доступ до даних у бездротових мережах;
- Доступність авторизованих користувачів не гарантується WEP.

Внаслідок цього безпека, що забезпечується протоколом WEP для бездротових мереж, неприйнятна.

WPA. У 2003 році Wi-Fi Alliance випустив WPA як тимчасовий стандарт, тоді як комітет зі стандартів IEEE працював над розробкою більш досконалого безпечного протоколу WPA2 як довгострокову заміну WEP. Протокол WPA призначений для подолання відомих недоліків, виявлених WEP. Багато функцій WPA безпосередньо усувають вразливість WEP. WPA виправляє багато недоліків протоколу WEP, використовуючи сильніше шифрування, ключі шифрування більшого розміру та безпечнішу перевірку цілісності.

WPA2. Як розширення протоколу WPA стандарт WPA2 був ратифікований комітетом зі стандартів IEEE у 2004 році як стандарт 802.11i. З моменту свого випуску WPA2 невпинно зростає у використанні. Подібно WEP та WPA, WPA2 також пропонує корпоративну та персональну версії. З тих пір WPA2 вважався найбезпечнішим стандартом бездротової безпеки, доступним для бездротової мережі. Подібність WPA та WPA2 полягає у використанні структури 802.1x/Extensible Authentication Protocol (EAP) як інфраструктури для забезпечення взаємної автентифікації та динамічного управління ключами, призначеної для захисту всіх версій пристроїв 802.11. [26]

Основна відмінність між WPA та WPA2 полягає в тому, що WPA2 використовує Advanced Encryption Standard (AES) для шифрування. AES – це блоковий шифр, тоді як RC4 – потоковий шифр.

Розмір блоку, який використовується в AES, становить 128 біт як для відкритого тексту, так і для зашифрованого тексту. Крім того, в AES використовуються ключі трьох різних розмірів: 128, 192 і 256 біт, кожен з яких використовується в різних раундах або ітераціях алгоритму, всього в AES задіяно 36 раундів. Шифрування, що забезпечується AES, настільки надійне, що потрібно мільйони років, щоб зламати шифрування AES методом brute force. Протокол WPA2 також замінює протокол Temporal Key Integrity Protocol (TKIP), що використовується в WPA, на більш досконалий механізм автентифікації – Cipher Block Chaining Message Authentication Code Protocol (CCMP).

Однак WPA2 також має вразливості, які виявили експерти з безпеки в бездротових мережах. Основною вразливістю WPA2 є те, що люди можуть зламати

парольну фразу WPA2-Personal, вгадуючи пароль, якщо користувач використовує простий пароль. Як тільки хакер правильно вгадає простий пароль, він зможе розшифрувати захоплені бездротові пакети. Тому, якщо користувач використовує простий пароль, то безпека, що забезпечується парольною фразою WPA2-Personal, може бути легко зламана хакерами. Ще одним недоліком WPA2-Personal є те, що користувач, що має парольну фразу, може проникнути та перехопити мережевий трафік інших користувачів, а потім запустити шкідливі

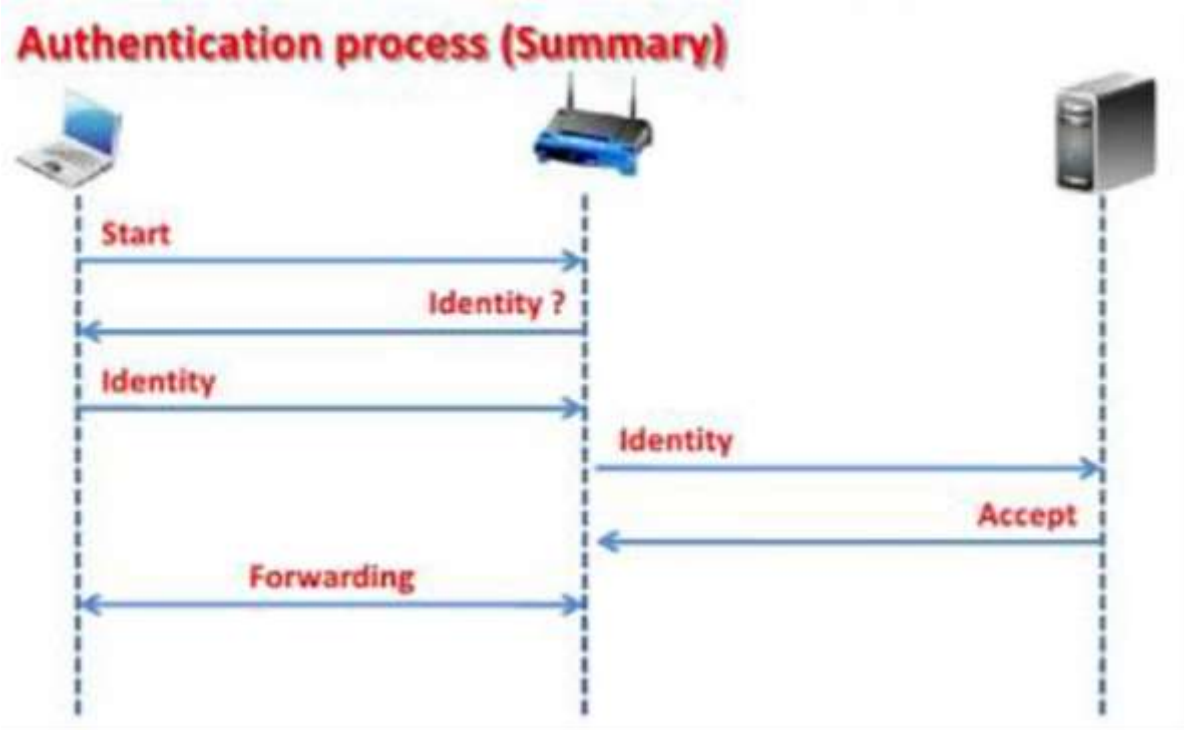

Рис. 4.1. Процес аутентифікації WPA2

WPA3. Найновішою технологією безпеки бездротових мереж є протокол WPA3, випущений у 2018 році. Важливими новими функціями, доданими до цього абсолютно нового протоколу безпеки для бездротових мереж, є кращий захист простих паролів, що використовуються користувачами, шифрування особистих і відкритих даних. мереж, призначених для індивідуальних користувачів, та для корпоративних мереж, у цій новій технології також реалізовано безпечніше шифрування. [26]

Таблиця 4.1

Порівняння WEP, WPA, WPA2 та WPA3

Стандарт	WEP	WPA	WPA2	WPA3
Реліз	1997	2003	2004	2018
Шифрування	RC 4	TKIP з RC 4	AES CCMP	AES CCMP і GCMP
Розмір ключа	64 і 128 біти	128 біти	128 біти	128 і 256 біти
Тип шифру	Потоковий	Потоковий	Блоковий	Блоковий
Аутентифікація	Open system and shared key	Pre-shared key and 802.1x with EAP variant	Pre-shared key and 802.1x with EAP variant	Simultaneous Authentication of Equals and 802.1x with EAP variant

WPA3-Personal. Протокол WPA3 пропонує шифрування на основі одночасної автентифікації рівних (SAE), замінюючи метод аутентифікації з попереднім загальним ключем (PSK), який використовували його попередники. SAE пропонує набагато надійніше шифрування, ніж PSK. Таким чином, якщо зловмисники використовують атаки грубої сили або словника, безпека WPA3 в особистих мережах працює добре і може відобразити ці атаки. Але якщо користувач бездротової мережі використовує дуже простий пароль, хакер може легко вгадати пароль та отримати несанкціонований доступ до приватної бездротової мережі.

WPA3-Personal пропонує шифрування в бездротових мережах для кожного окремого користувача. У бездротовій мережі WPA3-Personal користувач не може вкрасти або підслухати бездротовий трафік інших користувачів, захищений протоколом WPA3-Personal. Навіть якщо хакер успішно вгадав пароль користувача, він або вона не зможе отримати сеансові ключі, які використовуються для шифрування, і, отже, не

зможе розшифрувати будь-який бездротовий трафік. Таким чином, весь зашифрований бездротовий трафік, як і раніше, захищений.

WPA3-enterprise. Для кращого захисту бездротових мереж, що використовуються для бізнесу, в корпоративній версії WPA3 — WPA3-Enterprise — реалізовано додатковий рівень безпеки зі 192-бітним ключем. Ця нова функція безпеки важлива для тих корпоративних бездротових мереж, які розгорнуті у чутливому середовищі та потребують високого рівня безпеки та захисту.

Важливою функцією безпеки, що включена до WPA3-Enterprise, є Wi-Fi Enhanced Open. За допомогою цієї нової функції діалоги 802.11 між точками доступу та бездротовими хостами у відкритих мережах шифруються різними ключами для різних підключень. Шифрування для кожного бездротового з'єднання відрізняється. Базова технологія називається Opportunistic Wireless Encryption (OWE). У WPA3-Enterprise використовуються захищені кадри управління (PMF) для захисту бездротового трафіку операцій управління між бездротовими хостами та точками доступу. Ще одна функція Wi-Fi Enhanced Open полягає в тому, що вона захищає користувачів бездротової мережі від крадіжки мережевого трафіку або атаки один на одного. Таким чином, такі атаки як перехоплення сеансу не можуть бути виконані хакерами в бездротових мережах з реалізованим протоколом WPA3-Enterprise.

4.3 Вдосконалення генерації пароля

Сучасний домашній компьютер використовуючи лише ресурс CPU буде мати швидкість підбору 6000-7000 паролів за секунду, залежно від моделі CPU, але цю швидкість можна значно збільшити використовуючи GPU або навіть ферму з GPU

Таблиця 4.2

Кількість підібраних паролів за проміжок часу

	Кількість паролів		
Час	CPU	GPU	12 GPU
1 секунда	10^4	1,5·10^10	1,8·10^11
1 хвилина	6·10^5	9·10^11	1,08·10^13
1 година	3,6·10^7	5,4·10^13	6,48·10^14
1 доба	8,64·10^8	1,3·10^15	1,56·10^16
1 рік	3,15·10^11	4,73·10^17	5,68·10^18

Можна зробити висновок, чим довше триває підбор паролю, тим надійніше цей пароль та навпаки. Тому постає питання про формування парольних політик.

Математично парольні множини для парольних політик можна описати, як вибірку з певних символів:

- сполучення з символів для паролів (комбінація), коли з n елементів (кількості можливих символів) вибирають k (довжина обраного паролю), порядок не має значення;
- розміщення з символів для паролів, коли з n елементів вибирають k в певному порядку;

- розміщення з повтореннями з символів для паролів, коли число всіх розміщень з n елементів вибирають k, з повтореннями.

Статистичною (емпіричною) функцією розподілу вибірки множини паролів є закон зміни частоти події підбору пароля, при X<x:

$$F*(x) = \frac{a(x)}{a}\ , \tag{4.1}$$

де *a(x)* – число значень варіантів паролю, для яких $x \le X$,

X –випадкова величина множини паролів, розподіл якої невідомий;

a – об'єм вибірки множини паролів.

Аналогом теоретичної диференціальної функції (густини) розподілу є щільність відносної частоти:

$$f_i = \frac{w_i}{h}, \tag{4.2}$$

де *Wi* – відносна частота, *h* – інтервал підбору.

Середнє арифметичне спостережуваних значень випадкової величини множини паролів:

$$M*[X] = \frac{\Sigma_{i=1}^{k} x_i n_i}{n} = x_e, \tag{4.3}$$

де x_i – значення випадкової величини паролю,

$n = \Sigma_{i=1}^{k} n_i$ - число випробувань можливого підбору (об'єм вибірки).

Статистичні початкові та центральні моменти вибірки довільних порядків m:

$$M[(X - x_r)^m] = \frac{\Sigma_{i=1}^{k} (x_i - x_r)^m N_i}{N}, \tag{4.4}$$

При збільшенні числа спостережень вибірки множини паролів всі статистичні характеристики будуть збігатись за ймовірністю до відповідних числових характеристик генеральної сукупності їх множини. При $M \rightarrow Max$, $Pz \rightarrow 0$

Для даних паролів можливі деякі відмінності, за кількістю множини.

Сполучення множини паролів (комбінація). З n елементів вибирають k, порядок не має значення.

$$C_n^k = \frac{n!}{(n-k)!*k!}, \tag{4.5}$$

де n - кількість можливих символів;

k - довжина обраного паролю.

В даному випадку:

n=88 - ASCII: 26 прописних літер, 26 заголовних літер, 10 цифр, 26 спеціальних символів;

k=63 - кількість символів у паролі для WPA/WPA2.

Розміщення множини паролів. З n елементів вибирають k в певному порядку.

$$A_n^k = \frac{n!}{(n-k)!}, \tag{4.6}$$

де n- кількість можливих символів;

k- довжина обраного паролю.

Розміщення з повтореннями множини паролів. Число всіх розміщень з n по k з повтореннями.

$$A'^k_n = n^k, \tag{4.7}$$

де n- кількість можливих символів;

k- довжина обраного паролю [ДЖЕРЕЛО!].

Таблиця 4.3

Кількість паролів, що використовуються для захисту Wi-Fi

Варіанти захисту	Кількість символів в паролі	Кількість отриманих паролів для парольних політик		
		Сполучення	*Розміщення*	*Розміщення з повтореннями*
WPA/WPA2	64 шістнадцяткових символи	0	1.12·10^21	8.22·10^85
WPA/WPA2 (TKIP 128 біт)	63 символи ASCII	6.03·10^21	1.19·10^109	3.18·10^122
+WPS(QSS) Налаштування швидкого підключення, що несе уразливість	8 цифр, одна з яких відповідає за контрольну суму, тому підбирається 7, через помилку підбирається 4 перших, або 4 останніх з 7	6.05·10^5	10^4+10^3	10^7

З таблиці 5.3 можна зробити висновок, що знання зловмисником технологій формування парольних політик надасть йому перевагу в часі на підбір паролю без повторень приблизно у 5.27·10^100 разів.

Також важливо те, що кількість паролів для множини не дає оцінити стійкість паролю, так як вона залежить від способу створення паролю.

Для того щоб ускладнити підбір пароля, треба сформувати змінні правил ускладнення для сполучення множин паролів.

Із сполучення множини паролів Up відбирається множина Uz (рис. 4.2), що складається з паролів, які мають в собі 2 або 3 числа від двох до восьми цифр.

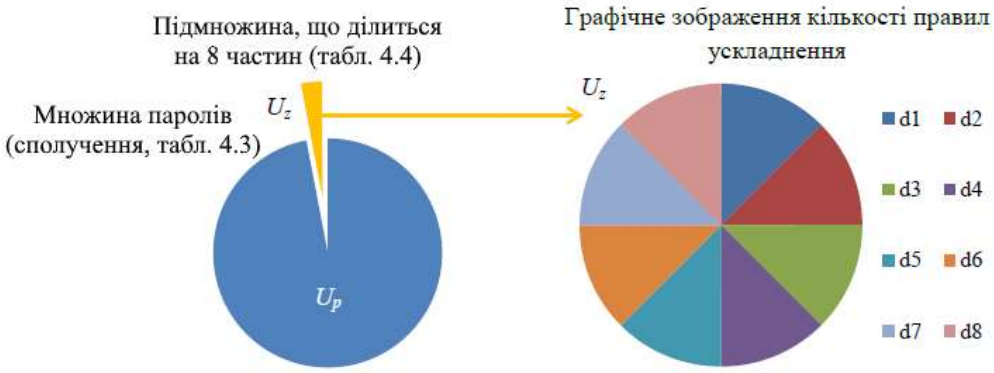

Рис 4.2. Кількість чисел, що можуть бути частиною паролю

До Uz потрапляють паролі, які містять 2 або 3 числа, довжиною від 2 до 8 цифр, або комбінацій набору символів, що можуть бути в словниках.

В свою чергу із множини Uz за певним правилом d (d1…d8), що визначається кількістю та довжиною чисел, виділяються 8 підмножин Ul(d), (від 2 до 8 цифр), що прописуються в кожному рядку таблиці 4.4.

Таблиця 4.4

Кількість чисел, що можуть бути частиною паролю

Ul(d)	Кількість чисел у паролі	Кількість цифр у числі				Кількість комбінацій
d1	3	3	3	3	1	*Ul (d1)*
d2	3	4	3	2	1	*Ul (d2)*
d3	3	4	3	3		*Ul (d3)*
d4	3	4	4	2		*Ul (d4)*
d5	2	5	5			*Ul (d5)*
d6	2	6	4			*Ul (d6)*
d7	2	7	3			*Ul (d7)*
d8	2	8	2			*Ul (d8)*

З підмножини Ul(d) відповідно до обраного номеру правила d обираються паролі, які додаються до множини (Up - Uz). Це, в свою чергу, створює множину Uk.

Даний підхід забезпечує трирівневе ускладнення паролю

Формула розрахунку кількості можливих комбінацій паролів матиме вигляд:

$$U_{l(d)} = C_l^m * C_{l-m}^m * C_{l-2m}^m * \dots * C_{l-rm}^m, \quad (4.8)$$

де l – кількість літер алфавіту;

m – кількість літер в слові (3…6);

r = 1…m, при умові: $m<rm<l$.

Загальна кількість паролів для парольної множини *Uz*

$$U_z = U_{l(d1)} + \cdots + U_{l(d16)}, \tag{4.9}$$

Значення ускладненої множини буде розраховуватись

$$U_k = (U_p - U_z) * U_z, \tag{4.10}$$

де *Uk* – кількість паролів для кінцевої, ускладненої, множини паролів;
Up – початкове значення кількості паролів (сполучення з таблиці 4.3);
Uz – значення кількості комбінацій чисел, формула (4.9).
Розрахунок ускладненої множини паролів, за одним із можливих правил *d*

$$U_{k(\text{в})} = (U_p - U_z) * U_{l(d)}, \tag{4.11}$$

де *Uk(d)* – ускладнена комбінація за обраним правилом *d*,
Up – початкове значення кількості паролів (сполучення з таблиці 4.3),
Uz – значення комбінацій чисел, з різної кількості цифр з формули (4.9),
Ul(d) – кількість комбінацій чисел, з кількості цифр, формула (4.8).

ВИСНОВКИ ДО РОЗДІЛУ 4

Була вдосконалена генерація випадкового паролю завдяки використанню інтегрованого підходу для генерування більш стійких паролів, а також урахуванню можливостей співпадіння з паролями системи словників та розширення множини U_z дозволяє створити пароль, ймовірність підбору якого буде мінімальною та збільшити кількість варіантів правила ускладнення *d* та кількість можливих комбінацій підбору, а також рівень невизначеності для зловмисника.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗИВИЧАЙНИХ СИТУАЦІЯХ

Кожен має право на належні, безпечні і здорові умови праці. Це гарантує нам Конституція України (ч. 4 ст. 43) [27].

Одним із найважливіших елементів будь-якого підприємства є робоче місце, в межах якого відбувається цілеспрямована діяльність (тобто праця) конкретного працівника. Робоче місце - це частина виробничого простору одного або групи працівників, оснащена основним і допоміжним технологічним обладнанням, інвентарем, інструментом, робочими меблями, необхідними для виробництва певного виду робіт. З розвитком виробничих процесів та інформаційні технології все частіше робочі місця працівників оснащуються персональним комп’ютером. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає удосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу на здоров'я робітників [28].

5.1. Охорона праці

При дослідженні методів та засобів будинку було здійснено розробку модулів системи РБ із дотриманням усіх норм та правил з охорони праці та техніки безпеки. Враховуючи той факт, що виконання досліджень вимагає використання засобів обчислювальної техніки, то необхідним є створенням безпечних умов праці при використанні персональної електронно-обчислювальної машини (ПЕОМ). Також потрібно приділити особливу увагу питанням електро- та пожежної безпеки.

З урахуванням вимог ДСанПіН 3.3.2.007-98 та НПАОП 0.00-7.15-18 необхідно визначити небезпечні і шкідливі фактори, які впливають на користувачів ВДТ (візуально дисплейний термінал) ПЕОМ при експлуатації, дослідити ці фактори,

розглянути їхній вплив, принципи їх нормування і способи запобігання їхнього шкідливого впливу на людину [29].

Основними шкідливими та небезпечними виробничими факторами, які пов’язані з використанням ПЕОМ, є такі:

- електромагнітне випромінювання радіочастотного діапазону;
- наявність іонізуючого рентгенівське випромінювання;
- випромінювання оптичного діапазону (ультрафіолетове, інфрачервоне і випромінювання видимого діапазону);
- електростатичне поле; недостатня освітленість робочої зони;
- підвищений рівень шуму;
- значна напруга зорових органів і пов’язане з цим перевтомлення користувача ПЕОМ;
- значне навантаження на пальці і кисті рук, що при відсутності профілактики і медичного контролю, може викликати професійні захворювання;
- тривале перебування в одному й тому ж самому положенні сидячи, що викликає застійні явища в організмі людини;
- відблиски на екрані монітора;
- можливість ураження електричним струмом;
- можливість виникнення пожежі.

Робоче приміщення з ПЕОМ по рівню безпеки ураження людей електричним струмом згідно ПУЕ можна віднести, до помешкань без підвищеної небезпеки, тому що:

- відносна вологість повітря не перевищує 75%;
- матеріал підлоги (паркет) є діелектриком;
- температура повітря не досягає значень, більших +30 °С;
- відсутня можливість одночасного дотику людини до з'єднаних з землею металоконструкцій будівлі, технологічних апаратів, механізмів і т.п., з одного боку, і до металевих корпусів електроустаткування - з іншого боку;

- відсутні хімічно агресивні середовища.

Електромережа трьохфазна з глухозаземленою нейтраллю, із зануленням і повторним заземленням нульового дроту відповідно до вимог ПУЕ (правил улаштування електроустановок). Мережа обладнана автоматом струмового захисту, розрахованого на струм 12 А. Час спрацювання автомату 0,1 с.

Для того, щоб не допустити ураження працівника електричним струмом при виникненні аварійних ситуацій, необхідно заземлити все обладнання, що працює від мережі 220 В, 50 Гц. Опір нульового дроту повинен бути таким, щоб при замиканні на корпус або нульовий дріт; виникав струм короткого замикання, сила якого повинна перевищувати в 1,4 рази номінальний струм спрацювання автомата струмового захисту (при струмі короткого замикання менше 100 А).

Тобто струм короткого замикання при виникненні аварійної ситуації в рази перевищує номінальний струм спрацювання автомату, що задовольняє встановленим нормам К>1,4. Виконано всі необхідні заходи щодо електробезпеки відповідно до ДНАОП 0.00-1.21-98, додаткових заходів по електробезпеці впроваджувати не потрібно.

Облаштування робочих місць, обладнаних відеотерміналами, повинно забезпечувати:

- належні умови освітлення приміщення і робочого місця, відсутність відблисків;
- оптимальні параметри мікроклімату (температура, відносна вологість, швидкість руху та рівень іонізації повітря);
- належні ергономічні характеристики основних елементів робочого місця.

А також необхідно вжити заходи проти таких небезпечних і шкідливих чинників, як наявність шуму та вібрації, електромагнітного, ультрафіолетового і інфрачервоного випромінювання, електростатичного поля між екраном монітору і оператором, наявність пилу, озону, оксидів азоту й аероіонізації.

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступеня вогнестійкості.

Службові приміщення, в яких розташовані ПЕОМ, не повинні межувати з приміщеннями, де рівні шуму та вібрації перевищують норму (механічні цехи, майстерні тощо) [30].

Відповідно до ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» площа приміщення, у яких розташовують відеотермінали, визначається, виходячи з розрахунку на одне робоче місце - не менше 6,0 кв. м, об'єм - не менше 20,0 куб. м, з урахуванням максимальної кількості осіб, які одночасно працюють у зміні [29].

Заземлені конструкції, що знаходяться в приміщеннях (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном тощо), мають бути надійно захищені діелектричними щитками або сітками від випадкового дотику. У приміщеннях з ПЕОМ слід щоденно проводити вологе прибирання, повинні бути медичні аптечки першої допомоги, а також система автоматичної пожежної сигналізації. [28].

Загальне освітлення має бути виконане у вигляді суцільних або переривчастих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників. Як джерело світла при штучному освітленні повинні застосовуватися, як правило, люмінесцентні лампи типу ЛБ. Допускається у світильниках місцевого освітлення застосовувати лампи розжарювання.

Рівень освітленості на робочому столі в зоні розташування документів має бути в межах 300-500 лк. У разі неможливості забезпечити даний рівень освітленості системою загального освітлення допускається застосування світильників місцевого освітлення, але при цьому не повинно бути відблисків на поверхні екрана та збільшення освітленості екрана більше ніж до 300 лк.

При дотриманні цих вимог, виконання всіх видів робіт на ПЕОМ при дослідженні методів та засобів адаптивної селекції каналів зв’язку для розумного будинку, є безпечним з точки зору охорони праці, техніки безпеки та протипожежної безпеки.

5.2. Оцінка надійності захисту виробничого персоналу об’єкта у воєнний час

При оцінці надійності захисту виробничого персоналу необхідно враховувати, що практично будь-які наслідки НС можуть призвести до ураження людей та стати причиною їхньої смерті або призвести до втрати працездатності на тривалий час. Надійність захисту виробничого персоналу є одним з важливих факторів, які визначають стійкість роботи підприємств у надзвичайних ситуаціях мирного та воєнного часів [31].

Найбільш ефективним заходом захисту є укриття людей в захисних спорудах (ЗС) при дотриманні таких умов: - загальна місткість ЗС дозволяє укрити всіх робітників та службовців, тобто весь виробничий персонал об’єкту; - захисні споруди задовольняють вимогам захисту від усіх небезпечних наслідків НС; - захисні споруди устатковані системами життєзабезпечення на необхідну тривалість перебування у них; - розміщення ЗС відносно робочих місць дозволяє своєчасно укритися всім робітникам за сигналами сповіщення про НС; - робітники та службовці своєчасно сповіщаються та навчені способам захисту та правилам дії за сигналами сповіщення. За показник надійності захисту робітників та службовців з використанням ЗС можна прийняти коефіцієнт надійності захисту КН.З., що показує яка частина робітників та службовців забезпечується надійним захистом від усіх небезпечних наслідків виникнення НС. Коефіцієнт надійності захисту визначається на основі окремих показників, що характеризують підготовленість об’єкту до виконання завдань захисту робітників та службовців за основними складовими задачами.

Оцінка надійності захисту виробничого персоналу проводиться в такій послідовності:

1. Оцінюється інженерний захист робітників та службовців об’єкта. Показником інженерного захисту є коефіцієнт КІНЖ. ЗАХ., що показує, яка частина виробничого персоналу працюючої зміни може укритися своєчасно в ЗС з достатніми захисними властивостями та системами життєзабезпечення, які

дозволяють укривати людей протягом встановленого терміну: КІНЖ. ЗАХ. = NІНЖ. ЗАХ. / N, де N – це чисельність найбільшої працюючої зміни;

2. Вивчається система сповіщення та оцінюється можливість своєчасного доведення сигналу сповіщення до робітників та службовців. Показником надійності з урахуванням сповіщення є коефіцієнт КСП : КСП = NСП / N;

3. Оцінюється навченість виробничого персоналу способам захисту та діям за сигналами сповіщення. Показник – коефіцієнт навченості КНАВЧ : КНАВЧ = NНАВЧ / N;

4. Визначається готовність сховища до прийому людей. Для цього визначається час, протягом якого сховища, що використовуються за подвійним призначенням, можуть бути підготовлені до прийому людей (звільнюються від сторонніх речей, поновлюється запас їжі, води, здійснюється перевірка герметичності, функціонування систем життєзабезпечення). Порівнюючи фактичний час підготовки сховища ТГ. ФАК. з потрібним ТГ. ПОТ., визначається готовність сховища до прийому людей. Для оцінки надійності захисту враховуються лише ті сховища, для яких: ТГ. ФАК. / ТГ. ПОТ. ≤ 1;

5. Показником надійності захисту з урахуванням готовності є коефіцієнт готовності КГОТ : КГОТ = NГОТ / N;

На основі окремих показників визначається коефіцієнт надійності захисту робітників та службовців КН. З. за мінімальним значенням окремих показників: КІНЖ.ЗАХ., КСП., КНАВЧ., КГОТ.. Визначаються слабкі місця в підготовці об’єкту до успішного вирішення задачі захисту виробничого персоналу у надзвичайних ситуаціях та передбачаються можливі шляхи підвищення показників надійності захисту [32].

У висновках вказується: надійність захисту робітників та службовців; необхідність підвищення захисних властивостей наявних захисних споруд та заходи для підвищення надійності; приміщення, які доцільно пристосувати під ЗС; кількість та тип ЗС, що швидко зводяться; заходи надійного захисту чергового персоналу; заходи з повного забезпечення персоналу ЗІЗ; заходи покращення умов зберігання, профілактики та ремонту ЗІЗ; заходи забезпечення об’єкту в умовах Р.Х.Б.З.

Інженерний захист – це захист з використанням інженерних споруд. Оцінка інженерного захисту полягає у визначенні показників, що характеризують здатність інженерних споруд забезпечити надійний захист людей: це показники за місткістю захисної споруди – КВМ., показник за здатністю захисної споруди відповідати

захисним вимогам – КЗ,Т,, показник за здатністю систем життєзабезпечення захисної споруди забезпечити усім необхідним тих хто укриваються протягом усього терміну укриття – КЖ.О., показник за здатністю виробничого персоналу своєчасно зайняти захисну споруду – КСВР. Вихідні дані для оцінки:

1. Вид можливої надзвичайної ситуації, значення параметрів її основних вражаючих факторів.
2. Віддаленість об’єктів від місця прояву надзвичайних ситуацій, км;
3. Метеоумови: VC.B. – середня швидкість вітру, км/годину, напрямок вітру, хмарність;
4. Кліматичні умови – кліматична зона – для України це 1V або V;
5. Загальна кількість робітників та службовців, яких треба укрити у сховищі, в тому числі жінок;
6. Розподіл робітників за робочими ділянками та їх віддаленість від ЗС.

Характеристики ЗС:

- розміщення ЗС відносно житлового або виробничого комплексу;
- тип ЗС (клас) – надмірний тиск, який витримують конструкції;
- КПОСЛ конструкцій або тип захисного матеріалу та товщина кожного шару захисного матеріалу укриття;
- основні та допоміжні приміщення в сховищі та їх розміри (площа - S, висота - h); тип і склад елементів системи повітропостачання;
- об’єм резервних ємностей систем водопостачання та ємностей для збору стічних вод – при відсутності виходу каналізації у міську каналізаційну мережу (не проточна каналізація); елементи санітарно-технічних пристроїв.

Місткість ЗС визначають відповідно до прийнятих норм за площею і об’ємом приміщень на одну людину. Розрахунок роблять окремо за кожною захисною

спорудою, а потім визначають загальну кількість місць в усіх сховищах на об’єкті і показник інженерного захисту за місткістю КМ [33].

При здійсненні оцінки надійності захисту виробничого персоналу спочатку визначають максимальні параметри тих вражаючих факторів, які можуть суттєво впливати на надійність захисту:

- для землетрусу – за інтенсивністю землетрусу визначають відповідну йому величину надмірного тиску;
- для аварії на атомної електростанції – визначають напрямок розповсюдження хмари зараженого повітря, розраховують час початку формування сліду радіоактивної хмари на об’єкті і рівень радіації на об’єкті на одну годину після аварії;
- для аварії на хімічно небезпечному підприємстві - визначають напрямок розповсюдження хмари зараженого повітря, глибину зони хімічного зараження, час підходу хмари зараженого повітря до об’єкта, тривалість дії джерела забруднення;
- для пожежі - визначають напрямок розповсюдження пожежі, час підходу пожежі до об’єкту, можливу тривалість горіння; для катастрофічного затоплення - визначають час підходу хвилі прориву до об’єкту, можливу висоту хвилі прориву на об’єкті, час спорожнення водосховища [31].

На заключному етапі аналізують результати оцінювання надійності захисту об’єкта, роблять висновки та висувають пропозиції, в яких зазначають:

- надійність захисту (коефіцієнт надійного захисту КН.З. – за мінімальним значенням з окремих показників: КМ., КЗ.В., КЖЗ., КСВ. УКР.);
- визначають слабкі місця в захисті;
- намічають заходи із вдосконалення інженерного захисту робітників і службовців об’єкта.

Об’єктивний стан захисту працівників слід відобразити в графічному документі «Плані укриття». На плані зазначають місце розташування захисних споруд, їх характеристики на підставі розрахунків, розподіл працівників за спорудами та

маршрути руху до них. Допустимо укривати на 5–7 % людей більше, ніж дозволяє розрахункова місткість сховища [33].

5.3. Організація протипожежного захисту та проведення протипожежної профілактики на промисловому підприємстві

Протипожежна профілактика - комплекс організаційних і технічних заходів щодо попередження, локалізації та ліквідації пожеж, а також щодо забезпечення безпечної евакуації людей та матеріальних цінностей у разі пожеж.

Пожежна безпека - це такий стан промислового об'єкта, при якому виключається можливість пожежі, а в разі його виникнення попереджається вплив на людей небезпечних факторів і забезпечується захист матеріальних цінностей. Пожежі завдають величезних матеріальних збитків, призводять до травм та загибелі людей, так як супроводжуються виникненням небезпечних чинників, таких як відкритий вогонь, підвищена температура, токсичні речовини, дим, недолік кисню, ушкодження і порушення будівель, споруд, вибухи технічного обладнання тощо. Тому виконання правил пожежної безпеки на підприємствах є обов'язковим для всіх посадових осіб і громадян. Основи пожежної безпеки закладаються на стадії проектування підприємства, будівлі, споруди, планування технологічного процесу, встановлення обладнання, тобто враховується інженерно - технологічними заходами, які представлені в проектах при розробці проектної документації на будівництво, і вимагає суворого дотримання протипожежних правил у процесі експлуатації [33].

Пожежна безпека промислових підприємств складається з системи попередження пожеж, системи пожежного захисту і організаційно-технічних заходів.

Система попередження пожеж - це комплекс організаційних і технічних засобів, спрямованих на виключення можливості виникнення пожеж, на запобігання утворення горючої і вибухонебезпечного середовища шляхом регламентації вмісту горючих газів, парів і пилу в повітрі, а також виключення можливості виникнення джерел загоряння або вибуху; забезпечення пожежної безпеки технологічних

процесів, обладнання, електрообладнання, систем вентиляції, збереження сировини та інших матеріалів [30].

Виключенню та запобігання пожеж сприяє: герметизація виробничого устаткування, заміна горючих речовин, які застосовуються в технологічних процесах на негорючі, обмеження обсягів речовин, які застосовуються і зберігаються на підприємстві; контроль над концентрацією речовин в повітрі в приміщеннях і технологічному обладнанні; застосування робочої та аварійної вентиляції; відвід займистою середовища в спеціальні пристрої та безпечні місця; застосування інгібуючих і флегматизуючих домішок; вибір безпечних швидкісних режимів руху середовища [31].

Система пожежної захисту забезпечується застосуванням архітектурно-проектних рішень, перешкод шляху поширення пожежі, вогневідсікних пристрої на технологічних комунікаціях, в системах вентиляції, повітряного опалювання і кондиціонування повітря.

Організаційно-технічні заходи пов'язані з системами попередження пожеж та системами протипожежного захисту і повинні включати: організацію пожежної охорони, організацію відомчих служб відповідно до законодавства України та рішеннями місцевих органів самоврядування; паспортизацію речовин, матеріалів, виробів, технологічних процесів, будівель і споруд в частині забезпечення [28].

Усі заходи пожежної безпеки виробництва за призначенням поділяються на чотири групи:

1. Заходи, які забезпечують пожежну безпеку технологічного процесу та обладнання, збереження сировини і готової продукції.
2. Будівельно-технічні заходи, спрямовані на виключення причин виникнення пожеж і на створення стійкості огороджувальних конструкцій і будівель, на запобігання можливості розповсюдження пожеж і вибухів.
3. Організаційні заходи, які забезпечують організацію пожежної охорони, навчання працюючих методів запобігання пожеж і застосування первинних способів гасіння пожеж.

4. Заходи щодо ефективного вибору способів гасіння пожеж, оснащення пожежного водопостачання, пожежної сигналізації, створення запасу засобів гасіння.

Протипожежний захист забезпечується:

- вибором класу вогнестійкості об'єкта і меж вогнестійкості будівельних конструкцій;
- обмеженням поширення вогню в разі виникнення вогнища пожежі;
- застосуванням систем проти димного захисту;
- забезпеченням безпечної евакуації людей; застосуванням засобів пожежної сигналізації, сповіщення та пожежогасіння; організацією пожежної охорони підприємства.

Згідно Закону України «Про пожежну безпеку», забезпечення безпеки підприємств, установ покладено на керівників або уповноважених ними осіб. Обов'язки власників підприємств щодо забезпечення пожежної безпеки визначені ст.5 даного Закону Україну [30].

Власники підприємств, установ і організацій, а також орендарі зобов'язані:

- Розробляти комплексні заходи щодо забезпечення профілактики пожежної безпеки;
- Відповідно до нормативних актів з пожежної безпеки розробляти, затверджувати положення, інструкції, інші нормативні акти, що діють в межах підприємства, здійснювати постійний контроль за їх виконанням;
- Забезпечувати виконання протипожежних вимог, норм та правил, а також виконання приписів і постанов органів державного пожежного нагляду;
- Організовувати навчання працівників правилам пожежної безпеки та пропагувати заходи щодо їх забезпечення;
- Утримувати у справному стані засоби протипожежного захисту і зв'язку, пожежну техніку, обладнання та інвентар, не допускати їх використання не за призначенням;

- Створювати у разі потреби, відповідно до встановленого порядку, підрозділи пожежної безпеки та необхідну для їх функціонування матеріально-технічну базу;
- Подавати на вимогу державної пожежної охорони відомості та документи про стан пожежної безпеки об'єктів і продукції, яка ними випускається;
- Проводяться заходи щодо впровадження автоматичних засобів виявлення та гасіння пожеж;
- Своєчасно інформувати пожежну охорону про несправність пожежної техніки, систем пожежогасіння, водопостачання і т.д. [31].

ВИСНОВКИ ДО РОЗДІЛУ 5

Приведені рекомендації щодо організації робочого місця на підприємстві дозволяють підвищити рівень безпеки праці, попередити виникнення надзвичайних ситуацій та надати першу медичну допомогу при виникненні надзвичайної ситуації. Служби охорони праці, а саме відповідні служби і структурні підрозділи підприємства повинні здійснювати постійний контроль за виконанням робіт у відповідності з вимогами з охорони праці, електро-, газо- і пожежобезпеки, не допускати до роботи осіб, які не пройшли інструктаж та не здали заліки по питаннях охорони праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників.

Перед початком роботи слід переконатися у справності електропроводки, вимикачів, штепсельних розеток, за допомогою яких обладнання включається в мережу, наявності заземлення комп'ютера, його працездатності.

Щоб уникнути пошкодження ізоляції проводів і виникнення коротких замикань не дозволяється: вішати що-небудь на дроти, зафарбовувати й білити шнури і дроти, закладати дроти і шнури за газові та водопровідні труби, за батареї опалювальної системи, висмикувати штепсельну вилку з розетки за шнур, зусилля повинне бути додане до корпусу вилки.

Для виключення ураження електричним струмом забороняється: часто вмикати і вимикати комп'ютер без необхідності, торкатися до екрану і до тильної сторони блоків комп'ютера, працювати мокрими руками, працювати на засобах обчислювальної техніки та периферійному обладнанні, що мають порушення 70 цілісності корпусу, порушення ізоляції проводів, несправну індикацію включення живлення, з ознаками електричної напруги на корпусі, класти на обладнання сторонні предмети.

Забороняється під напругою очищати від пилу і забруднення електрообладнання. Забороняється перевіряти працездатність електроустаткування в непристосованих для експлуатації приміщеннях з струмопровідними підлогами, сирих, не дозволяючи заземлити доступні металеві частини. Неприпустимо під напругою проводити ремонт засобів обчислювальної техніки і периферійного обладнання. Ремонт електроапаратури проводиться тільки фахівцями-техніками з дотриманням необхідних технічних вимог.

Після закінчення роботи необхідно знеструмити всі засоби обчислювальної техніки і периферійне устаткування. У разі безперервного виробничого процесу необхідно залишити включеними тільки необхідне обладнання.

Оцінка надійності захисту виробничого персоналу об’єкта у воєнний час та організація протипожежного захисту і проведення протипожежної профілактики на промисловому підприємстві проводиться згідно основних норм та вимог законодавства з охорони праці та техніки безпеки на підприємстві.

На основі окремих показників визначається коефіцієнт надійності захисту робітників та службовців. Визначаються слабкі місця в підготовці об’єкту до успішного вирішення задачі захисту виробничого персоналу у надзвичайних ситуаціях та передбачаються можливі шляхи підвищення показників надійності захисту. Вказується: надійність захисту робітників та службовців; необхідність підвищення захисних властивостей наявних захисних споруд та заходи для підвищення надійності; приміщення, які доцільно пристосувати під ЗС; кількість та тип ЗС, що швидко зводяться; заходи надійного захисту чергового персоналу; заходи

з повного забезпечення персоналу ЗІЗ; заходи покращення умов зберігання, профілактики та ремонту ЗІЗ; заходи забезпечення об’єкту в умовах Р.Х.Б.З.

Система пожежної захисту забезпечується застосуванням архітектурно-проектних рішень, перешкод шляху поширення пожежі, вогневідсікних пристрої на технологічних комунікаціях, в системах вентиляції, повітряного опалювання і кондиціонування повітря. Організаційно-технічні заходи пов'язані з системами попередження пожеж та системами протипожежного захисту і повинні включати: організацію пожежної охорони, організацію відомчих служб відповідно до законодавства України та рішеннями місцевих органів самоврядування; паспортизацію речовин, матеріалів, виробів, технологічних процесів, будівель і споруд в частині забезпечення.

РОЗДІЛ 6
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1. Зведення та первинне оброблення статистичних даних екологічної інформації

До найактуальніших проблем сьогодення, від яких залежить існування людства, є екологічні проблеми. Для їх вирішення, перш за все, необхідні нові підходи до природного середовища. Екологічна статистика є невід'ємним атрибутом системи управлінських рішень в охороні навколишнього середовища від невеликого локального екологічного об'єкту до глобального масштабу оцінки екологічного стану всієї біосфери. Сьогодні статистичні методи і моделі широко використовуються для діагностики стану довкілля, при вивченні причинно-наслідкового механізму формування варіації та динаміки екологічних явищ і процесів, у моніторингу навколишнього природного середовища, при прогнозуванні стану екологічних процесів і ситуацій та прийнятті оптимальних управлінських рішень [40].

Теоретичне узагальнення фактів є другим ступенем складнішого процесу пізнання світу, адже на цьому етапі здійснюється наукове узагальнення статистичних даних. Таке узагальнення дає можливість встановити внутрішні зв'язки між явищами, їх кількісно-якісні перетворення. Процес теоретичного узагальнення статистичних даних, зведення фактів у єдине ціле в статистиці називають зведенням статистичних даних [40].

Зміст і завдання статистичного зведення це первинне наукове оброблення даних спостереження для характеристики суцільного явища узагальнюючими показниками. Статистичне зведення являє собою сукупність прийомів, які дозволяють одержати узагальнюючі статистичні показники як зведені ознаки масових явищ, що характеризують стан, взаємозв'язки і закономірності розвитку явищ в цілому. Зведення являє собою другий ступінь статистичного дослідження і від його якості значною мірою залежить результат усієї статистичної роботи.

Етапи зведення. В цілому статистичне зведенню включає такі етапи:

- статистичне групування;
- підсумовування даних;
- табличне і графічне оформлення одержаних даних.

Одержана в процесі зведення система статистичних показників підлягає подальшому аналізу в наукових і практичних цілях. За допомогою статистичного зведення розв'язують такі завдання: групування даних, розроблення системи показників для характеристики груп і всієї статистичної сукупності, обчислення групових і загальних показників, зведення результатів обчислення у статистичних таблицях.

Одержана в процесі зведення система статистичних показників підлягає подальшому аналізу в наукових і практичних цілях. Завдання зведення за допомогою статистичного зведення розв'язують такі завдання: групування даних, розроблення системи показників для характеристики груп і всієї статистичної сукупності, обчислення групових і загальних показників, зведення результатів обчислення у статистичних таблицях [30].

Статистичні ряди і первинне оброблення статистичної інформації. У результаті обробки та систематизації статистичних матеріалів отримуємо ряди цифрових показників, які характеризують окремі сторони явищ, що вивчаються, в просторі або зміну цих явищ у часі. Тому побудова статистичних рядів є основою будь-якого первинного оброблення статистичної інформації.

Статистичні ряди - це ряди цифр, які характеризує окремі сторони екологічних явищ у просторі або в часі. їхнє значення полягає в тому, що вони використовуються як прийом первинної обробки цифрової інформації, як проміжна ланка при побудові угруповань, як самостійний прийом аналізу при вивченні закономірностей розвитку суспільних явищ [31].

Часові ряди представляють собою ряди статистичних даних, розташованих у хронологічному порядку. Ці ряди мають особливо важливе значення при вивченні динаміки явищ і розглядатимуться далі окремою темою «Елементи рядів». Усі ряди складаються з двох елементів: варіантів і частот.

Варіант - це окреме значення групувальної ознаки, частота число, яке показують, як часто варіант зустрічається в ряді. Замість частот може бути частка, виражена коефіцієнтом чи відсотком. Значення рядів розподілу багатогранне – це первинна обробка інформації при зведенні, проміжний прийом при побудові угруповань, спеціальний самостійний прийом для вивчення закономірності розподілу. Основні поняття, що використовуються при вивченні рядів розподілу: частковість нагромадження частот, обсяг ряду, інтервал, границі інтервалу, щільність розподілу. Побудова та аналіз статистичних рядів. Неупорядковані ряди - ряди чисел первинної інформації, отримані внаслідок спостереження. Вони служать джерелом інформації про стан явищ і однорідність сукупності, є початковим етапом статистичного аналізу.

Дані цього ряду характеризують стан, рівень явища, який склався в кожній одиниці сукупності. Однак, якщо ряд великий, то не можливо візуально узагальнити досягнуті рівні по різних об'єктах. Для великих сукупностей інформацію зручніше і наочніше представити графічно у вигляді поля розсіювання (діаграми казусів), побудованого в системі прямокутних координат, де на горизонтальній осі відкладаються номери об'єктів, а на вертикальній - назви показників. При цьому шкалу розмічають, починаючи не з нуля, а з мінімального і до максимального значення ознаки. Числові значення ознак конкретних об'єктів на координатне поле наносяться у вигляді точок, які відповідають номеру об'єктів [40].

Ранжируванний ряд - упорядкований ряд одиниць сукупності за зростанням чи спаданням ознаки. Він також складається з двох елементів: рангового номера об'єкту і ознаки, яка має здатність варіювати, побудованої за зростанням. Огіва може мати різні обриси залежно від характеру варіації ознаки. Отже ранжирування є як самостійним методом дослідження закономірності розподілу, так і початковим етапом побудови варіаційних рядів розподілу - дискретного та інтервального. Ряди розподілу, що засновані на признанні цієї мінливості, дозволяють систематизувати та узагальнити результати спостереження, а також встановити відповідності отриманого матеріалу з теоретичними розрахунками [31].

6.2. Роль матеріало- та ресурсозбереження у вирішенні екологічних проблем

Із розвитком цивілізації та науково-технічного прогресу, обсягів виробництва та його відходів проблеми стосунків між природою і суспільством дедалі загострюються. Основною причиною забруднення навколишнього середовища є ресурсоємні забруднюючі технології, що приводять до утворення відходів і їх величезного накопичення. Основний шлях вирішення еколого-енергетичних проблем - це енергозбереження. Перехід на інтелектуальні технології (комп'ютерні, телекомунікаційні, біогенні і ін.), як значно менш енергоємні, а також більш високорентабельні і екологічно чисті [33].

Одним із важливих чинників ефективної екологічної політики є впровадження в практику досягнень науково-технічного прогресу, це перш за все нової техніки і технології, прогресивної структури виробництва та ресурсозберігаючих технологій. Цей прогрес наглядно можна спостерігати на прикладі історії розвитку ЕОМ, що за весь час свого існування пройшли чотири покоління розвитку [33].

Перше покоління (кінець 40-х - кінець 50-х років XX ст.) ЕОМ виготовлені на основі електронних ламп. Вони мали невелику швидкодію - кілька тисяч операцій на секунду, потребували великої площі розміщення обладнання, а також великої енергоємності. Для введення програм у цих машинах використовувалася перфострічка, яку готували на телеграфних апаратах. Як пристрій управління використовувався виключно інженерний пульт, а єдиним пристроєм введення був ТБПМ, що видавав лише неформатовані числа.

Друге покоління (кінець 50-х - кінець 60-х років XX ст.) ЕОМ виготовлені на основі напівпровідникових транзисторів. Вони мали . на два-три порядки вищу швидкодію. Значно зменшили енергоємність (десятки кВт). Вперше з'явився пристрій АЦПУ, що давав змогу роздруковувати на рулонному папері літери і цифри рядками по 128 символів. Крім того, для введення інформації почали використовуватися паперові перфокарти, а для запам'ятовування інформації - магнітні стрічки.

Третє покоління (кінець 60-х - початок 80-х років XX ст.) ЕОМ виготовлені на основі інтегральних мікросхем. Вони мали швидкодію до 10 млн операцій на секунду. Деякі моделі ЕОМ мали розміри не більше за холодильник. Енергозатрати - не більше кількох кВт. Уперше почали використовувати відео термінали (дисплеї).

Четверте покоління (початок 80-х років XX ст. і донині). ЕОМ виготовлені на НВІС. Швидкодія - сотні млн. операцій на секунду. Переважно найпоширенішими стали персональні комп'ютери (ПК) як окремий клас машин із невеликими розмірами, достатніми для розміщення на столі. Енергоживлення - кілька сотень Вт.

Обмеженість ресурсів зумовлює необхідність їх ефективного використання. Одним зі способів такої діяльності є ресурсозбереження. Під ресурсозбереженням варто розуміти діяльність, яка пов’язана з економією та у вирішенні екологічних проблем, будь-яких видів ресурсів, тобто ресурсозбереження визначається конкретними формами прояву: матеріало-, земле-, трудо-, енергозбереженням та іншими ресурсами . Під економією ресурсів можна розуміти раціональне, комплексне використання та ощадливе споживання всіх видів ресурсів виходячи з наявного рівня розвитку техніки і технології за одночасного зниження впливу на навколишнє середовище з метою вирішенні екологічних проблем [33].

Згідно з Державним стандартом України (ДСТУ 3051-95), ресурсозбереження – це діяльність (організаційна, економічна, технічна, наукова, практична, інформаційна), методи, процеси, комплекс організаційно-технічних засобів, що супроводжують усі стадії життєвого циклу обкатів і спрямованих на раціональне використання та економне витрачання ресурсів [32].

Вирішення питань ресурсозбереження потребує розробки ефективної системи управління цими процесами і залежить від технології виробництва.

Для вирішення поставлених заходів по ресурсозбереженню необхідно:

- вдосконалення норм та нормативів, впровадження результатів науково-технічного прогресу;
- впровадження автоматизації виробничих процесів та вдосконалення матеріально-технічного постачання та забезпечення;

- організація розробки і реалізації галузевих і регіональних ресурсозберігаючих програм як основного документа в галузі створення високоефективних продукцій і технологій;
- розробка завдань по підвищенню ефективності використання матеріальних ресурсів з урахуванням використання відповідних видів вторинної сировини;
- встановлення граничних лімітів використання ресурсів для формування замовлень, посилення міжгалузевих зв'язків при розробці виробничих програм, балансів розподілу продукції з метою випуску найбільш економічної продукції і зняття з виробництва застарілих виробів, використання вторинних ресурсів;
- вдосконалення показників ефективності виробництва, в тому числі розрахованих на одиницю основного якісного параметра виробів, з наступним уточненням нормативів витрат ресурсів і застосування економічних нормативів;
- створення банку нормативної інформації ресурсозбереження [33].

Запровадження всебічної екологізації. Екологізація – це процес неухильного і послідовного впровадження систем технологічних, управлінських, юридичних та інших рішень, які дають змогу підвищувати ефективність використання природних ресурсів та умов поряд із поліпшенням або хоча б збереженням якості довкілля. Крім того, це поширення екологічних принципів та підходів на всі сфери життєдіяльності людського суспільства: культуру, науку, виробництво та соціальні явища. Передусім це стосується запровадження екологічної освіти та виховання для формування екологічно свідомого ставлення до навколишнього природного середовища, встановлення гармонійних зв'язків між природою та антропогенною діяльністю [30].

Запровадження політики раціонального використання виробничих ресурсів. Ресурсозберігаюча політика може здійснюватися із підвищенням науково-технічного рівня і може включати такі заходи:

- створення наукоємної продукції;
- підвищення якості сировини і матеріалів;

- упровадження нової техніки і технології на основі досягнень науково-технічного прогресу;
- впровадження ресурсозберігаючої технології;
- підвищення якості, надійності і довговічності конструкції в рамках її життєвого циклу;
- впровадження нових видів матеріалів, у тому числі сучасних замінників;
- скорочення витрат і відходів виробництва;
- використання сировини і матеріалів економічних сортів, марок, розмірів;
- удосконалення якості оснащення і пристроїв;
- вибір вихідних матеріалів за розмірами, що наближуються до розмірів і форми готових деталей;
- використання раціональних витрат матеріалів на ділянках і вибір найбільш раціональних форм замовлення;
- підвищення рівня спеціалізації виробництва під час виготовлення деталей масового використання;
- підвищення потужності, продуктивності та експлуатаційної надійності;
- зменшення маси і габаритів на одиницю технічного параметра потужності, продуктивності;
- встановлення оптимальних запасів міцності деталей та вузлів за рахунок удосконалення методів інженерних розрахунків під час конструювання;
- підвищення технічних вимог до випробувань і здачі продукції [31].

ВИСНОВКИ ДО РОЗДІЛУ 6

Зведення та первинне оброблення статистичних даних екологічної інформації дають ефективне використання статистичних методів обліку, обробки, аналізу і прогнозування екологічних процесів збільшується при використанні комп'ютерних технологій. Статистичне спостереження, даючи об'ємний і різноманітний матеріал про окремі явища досліджуваної сукупності, ще не дає змоги зробити будь-які

висновки про цю сукупність. Адже в результаті збирання фактів дійсність стає відомою, але ще не пізнаною. Статистичне спостереження збігається з першим ступенем людського пізнання дійсності - емпіричним. Щоб за науково зібраними фактами зробити об'єктивні висновки, глибоко пізнати дійсність, ці фактори необхідно узагальнити, теоретично обміркувати.

Роль матеріало- та ресурсозбереження у вирішенні екологічних проблем вирішуються засобами відтворення і ефективне використання природно-ресурсного потенціалу є одним з основним завдань, які стоять перед усіма господарюючими суб’єктами. Адже з використанням інноваційних ресурсозберігаючих технологій досягається збільшення виробництва продукції при незначному негативному впливові на довкілля, а, відповідно, і зростає конкурентоспроможність підприємств на ринку. Уміле застосування еколого-економічних інструментів в поєднанні з іншим методами управління дозволяє ефективно вирішувати проблеми ресурсозбереження в рамках механізмів саморегулювання ринкової економічної системи. При комплексному поєднанні відповідних заходів можна суттєво знизити рівень навантаження на природні комплекси та запобігти значному антропогенному навантаженню. Використання замінників природних ресурсів у виробництві та вживання відходів та побічної продукції не тільки зменшує експлуатацію природних ресурсів, а й ліквідує проблеми, пов’язані із забрудненням навколишнього середовища.

ВИСНОВКИ

Оскільки Інтернет речей складається з безлічі підключених пристроїв, таких як датчики та мітки RFID, важливо адаптувати ці пристрої для роботи у звичайному Інтернеті. Пристрої IoT часто обмежені в обчислювальній потужності та об'ємі пам'яті. Тому використання криптографічних алгоритмів, яким часто потрібно більше ресурсів, ніж усі крихітні пристрої разом узяті, є складним завданням. Ще одна проблема – оновлення пристроїв у польових умовах. Часто доступне лише ненадійне з'єднання, а важливі для безпеки речі вимагають негайних оновлень, які складно розгорнути на всіх пристроях одночасно. Крім того, завдання зробити безпеку інтуїтивно зрозумілою для користувача є актуальним як ніколи, тому що прийняття користувачами залежить від простоти встановлення та обслуговування.

У роботі було порівняно протоколи захисту WEP та WPA

WPA. У 2003 році Wi-Fi Alliance випустив WPA як тимчасовий стандарт, тоді як комітет зі стандартів IEEE працював над розробкою більш досконалого безпечного протоколу WPA2 як довгострокову заміну WEP. Протокол WPA призначений для подолання відомих недоліків, виявлених WEP. Багато функцій WPA безпосередньо усувають вразливість WEP. WPA виправляє багато недоліків протоколу WEP, використовуючи сильніше шифрування, ключі шифрування більшого розміру та безпечнішу перевірку цілісності.

WPA2. Як розширення протоколу WPA стандарт WPA2 був ратифікований комітетом зі стандартів IEEE у 2004 році як стандарт 802.11i. З моменту свого випуску WPA2 невпинно зростає у використанні. Подібно WEP та WPA, WPA2 також пропонує корпоративну та персональну версії. З тих пір WPA2 вважався найбезпечнішим стандартом бездротової безпеки, доступним для бездротової мережі. Подібність WPA та WPA2 полягає у використанні структури 802.1x/Extensible Authentication Protocol (EAP) як інфраструктури для забезпечення взаємної автентифікації та динамічного управління ключами, призначеної для захисту всіх версій пристроїв 802.11.

Основна відмінність між WPA та WPA2 полягає в тому, що WPA2 використовує Advanced Encryption Standard (AES) для шифрування. AES – це блоковий шифр, тоді як RC4 – потоковий шифр.

У першому розділі роботи було розглянуто ідею IoT. Розгянуто та порівняно між собою основні протоколи (ZigBee, Bluetooth Thread). Розглянуто популярні операційні системи IoT. Розглянуто категорії обладннаня пристроїв IoT за їх потужністю. Порівняно старий та новий підхід до побудови архітекутери IoT та перспективи розвитку.

У другому розділі роботи була розглянута суть проблеми безпеки IoT, основні вимоги до безпеки, криптографічні алгоритми, методи керування ключами, алгоритми маршрутизації, основні вектори атак.

У третьому розділі роботи було розглянуто методи покращення безпеки на різних рівнях: транспортному, прикладному, мережевому. Розглянуто протоколи Constrained Application Protocol, Message Queue Telemetry Transport, SMQTT, IPv6, 6LoWPAN.

На фінальному етапі роботи була зазначена процедура (послідовність) вдосконалення випадкового паролю завдяки використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (використовуючи змінний вибір правила ускладнення *d*), а також урахуванню можливостей співпадіння з паролями системи словників та розширення множини U_z (за рахунок використання набору букв/символів, або слів іншою мовою) дозволяє:

по-перше, створити пароль, ймовірність підбору якого серед певної множини паролів U_k буде мінімальною;

по-друге, збільшити кількість варіантів правила ускладнення *d* та кількість можливих комбінацій підбору, а також рівень невизначеності для зловмисника.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/
2. https://www.link-labs.com/blog/bluetooth-vs-bluetooth-low-energy
3. https://www.threadgroup.org/What-is-Thread
4. https://developer.android.com/things/get-started
5. https://storage.googleapis.com/gweb-Cloudblogpublish/original_images/Cloud2BIoT2BFinal2BV6s64u
6. https://www.wired.com/2016/04/nests-hub-shutdownproves-youre-crazy-buy-internet-things/
7. 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)
8. http://www.csl.sri.com/users/neumann/cacm240.pdf
9. 2012 International Conference on Computer Science and Electronics Engineering,
10. IEEE Internet of Things Journal,
11. https://developer.android.com/things/console/update
12. http://www.sciencedirect.com/science/article/pii/S0167739X18321083
13. IEEE Communications Surveys Tutorials
14. https://www.nxp.com/files-static/32bit/doc/ref_manual/MKW41Z512RM.pdf
15. Shipley AJ (2013) Security in the internet of things, lessons from the past for the connected future. Security Solutions, Wind River, White Paper
16. JingQ,VasilakosAV,WanJ,LuJ,QiuD(2014)Securityoftheinternetofthings:perspectives and challenges. Wireless Netw 20(8):2481–2501
17. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comput Netw 57(10):2266–2279
18. https://www.absolutesecurity.co.uk/
19. http://internetofthingsagenda.techtarget.com/essentialguide/Prevent-enterprise-IoT-security-challenges-with-preparation

20. https://www.postscapes.com/internet-of-things-protocols/
21. http://www.darkreading.com/iot/5-tips-for-protecting-firmware-from-attacks/d/d-id/1325604
22. http://safewayconsultoria.com/wp-content/uploads/2016/05/Beware-of-older-cyber-attacks_2016-1.pdf
23. http://www.rfwireless-world.com/Terminology/MQTT-protocol.html
24. SinghM,RajanMA,ShivrajVL,BalamuralidharP(2015) Securemqttforinternetofthings (iot). In: 2015 fifth international conference on Communication Systems and Network Technologies (CSNT). IEEE, pp 746–751
25. Security and Privacy in Internet of Things - Review Educational modules and research surveys on critical cybersecurity topics
26. Верховна Рада України. Кодекс цивільного захисту України. URL: http://www.rada. gov.ua (дата звернення: 05.09.2019).
27. Про захист людини від впливу іонізуючих випромінювань: Закон України від 14 січня 1998 р. Київ, 1998. 24 с.
28. НПАОП 0.00-7.15-18. Правила охорони праці під час експлуатації електронно-обчислювальних машин, затверджені наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду від 26.03.2010 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» від 14.02.2018 No 207
29. Про охорону атмосферного повітря: Закон України від від 14 січня 1992 р Київ: Відомості Верховної Ради України, 1992. – No 50.– Ст. 678.
30. Бикова О.В. Болієв О.В., Деревинський Д.М., Єлісеєв В.Н., Миронець С.М., Осипенко С.І., Півень Ю.О. та інш. Основи цивільного захисту: Навч. посібник К: 2008. 223 с.
31. Васійчук В.О., Гончарук В.Є., Качан С.І., Мохняк С.М. Основи цивільного захисту: Навч. Посібник. Львів, 2010. 384 с.
32. Гончарук В.Є., Качан С.І., Орел С.М., Пуцило В.І., «Оцінка обстановки у надзвичайних ситуаціях». Навчальний посібник, Видавництво НУ «Львівська політехніка». Львів, 2004р. 136 с.

33. Демиденко Г. П. Безпека життєдіяльності: навч. посібник для студ. вищ. навч. закладів / Національний технічний ун-т України Київський політехнічний ін-т. К.: НТУУ КПІ, 2008. 300 с.
34. Депутат О.П., Коваленко І.В., Мужик І.С., Цивільна оборона. Навчальний посібник. За ред. Кашина П.І. – Львів. 2005. 338 с.
35. Тарасова В.В. Екологічна статистика. Київ.: «Центр учбової літератури», 2008. 392 с.
36. Ковальова О.О., Дегтерева Л.І. Конспект лекцій з дисципліни «Основи екології». Конспект лекцій. Харківська національна академія міського господарства. Харків: ХНАМГ, 2010. 94 с.
37. Всеукраїнська екологічна ліга. Екологія та статистика. URL: http://www.ecoleague.net/index.php (дата звернення 05.19.2019).
38. Екологічні норми промислових приміщень. Державна служба України з надзвичайних ситуацій. URL: http://www.dsns.gov.ua (дата звернення 05.09.2019).
39. Міністерство екології та природних ресурсів України. Екологічні норми. URL: https://menr.gov.ua (дата звернення 05.19.2019).
40. Нормативно правова база у сфері екології. Законодавча база екологічних норм. URL: http://www.rada.kiev.ua (дата звернення 08.010.2019).
41. ДСТУ 3051-95 (ГОСТ 30166-95). Ресурсозбереження. Основні положення. Чинний від 1997.01.01. К.: Держстандарт України, 1996. 15 с.
42. Кондратенко Н.О., Тарадай В.Н. Механізми підвищення ефективності ресурсозбереження у регіональних економічних системах. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Економічна». 2011. No 970. Вип. 81. С. 266–273.