ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Аналіз методів захисту інформації IoT пристроїв»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

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

_____ Єлизавета ГАВРИЛЕЦЬ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД- 42
Єлизавета ГАВРИЛЕЦЬ
Ім'я, ПРІЗВИЩЕ

Керівник: PhD Віра МИКОЛАЙЧУК
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти бакалавр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Гаврилець Єлизаветі Григорівні
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Аналіз методів захисту інформації IoT пристроїв

керівник кваліфікаційної роботи Віра МИКОЛАЙЧУК к.т.н, доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Науково-технічна література з теми бакалаврської роботи.
2.Інтегроване середовище розробки.
3. Науково-технічна література.
4.Спеціальне програмне забезпечення.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.Дослідження необхідності впровадження систем захисту для пристроїв IoT;
2. Аналіз методів захисту IoT пристроїв;
3. Висновки та результати виконаної роботи

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання: «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	27.02-05.03.2024	
2	Ознайомлення та вивчення інформації з даної літератури	06.03-11.03.2024	
3	Дослідження існуючих методів для захисту інформації IoT пристроїв	12.03-27.03.2024	
4	Оцінка можливостей захисту інформації IoT пристроїв	28.03-10.04.2024	
5	Впровадження рішення, що підвищить захист інформації на пристроях IoT	11.04-15.05.2024	
7	Оформлення роботи: вступ, висновки, реферат	16.05-22.05.2024	
8	Розробка демонстраційних матеріалів	23.05-24.05.2024	

Здобувач(ка) вищої освіти _____ Єлизавета ГАВРИЛЕЦЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віра МИКОЛАЙЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавр: 56 стор., 1 табл., 22 рис., 20 джерел.

Мета роботи – розробка програми на основі мови програмування Python для IoT пристроїв.

Об'єкт дослідження- методи захисту інформації IoT пристроїв.

Предмет дослідження – пристрої Інтернету речей, методи їх захисту.

Короткий зміст роботи: в роботі реалізовано вирішення задачі, яка спрямована на те, щоб покращити рівень безпеки роботи пристроїв IoT, завдяки здобутим знанням та навичкам у процесі навчання. Дана робота базується на основних поняттях про пристрої інтернет речей, аналізу загроз, що можуть спричинити витік даних, та методів забезпечення безпеки для цих пристроїв.

КЛЮЧОВІ СЛОВА: ІОТ, МЕТОДИ ЗАХИСТУ, БЕЗПЕКА ЗАХИСТУ ПРИСТРОЇВ, ЗАГРОЗА БЕЗПЕКИ, ЕТАЛОННА АРХІТЕКТУРА, ЗАГРОЗИ РІВНІВ БЕЗПЕКИ, КІБЕРБЕЗПЕКА, ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ВРАЗЛИВОСТІ СИСТЕМИ БЕЗПЕКИ, ІОТ СИСТЕМА, ВБУДОВАНА СИСТЕМА БЕЗПЕКИ

ABSTRACT

Text part of the bachelor level qualification work: 56 pages, 22 pictures, 1 table, 20 sources.

The purpose of the work - development of a program based on the Python programming language for IoT devices..

Object of research is the methods of protecting the information of IoT devices..

Subject of research - Internet of Things devices, methods of their protection.

Summary of the work: the work implements a solution to the problem, which is aimed at improving the level of security of IoT devices, thanks to the acquired knowledge and skills in the learning process. This work is based on the basic concepts of Internet of Things devices, analysis of threats that can cause data leakage, and security methods for these devices.

KEYWORDS: IOT, PROTECTION METHODS, DEVICE PROTECTION SECURITY, SECURITY THREAT, REFERENCE ARCHITECTURE, SECURITY LEVEL THREATS, CYBER SECURITY, INFORMATION SECURITY ISSUES, SECURITY SYSTEM VULNERABILITIES, IoT SYSTEM, EMBEDDED SECURITY SYSTEM

ЗМІСТ

ВСТУП

Актуальність теми: пристрої інтернет речей – це комплекс системно взаємопов'язаних пристроїв, що мають свій власний унікальний ідентифікатор, та здійснюють обмін та передачу інформації між собою завдяки мережі Інтернет без прямого втручання людини безпосередньо в процес обміну інформації. Такі пристрої значно можуть полегшити життя людини, та спростити його у декілька разів. Великої популярності у нашому житті набирає проект, що включає в себе безліч пристроїв IoT, і має назву «Розумний будинок». Суть цього проекту полягає в тому, щоб автоматизувати якомога більше систем будинку, наприклад: система безпеки, система опалення, клімат-контроль, система керування медіа. Найбільш основною та базовою системою в усьому домі є саме система безпеки. Ця система є найбільш актуальною, оскільки забезпечує низку проблем, яких можна уникнути. Перше - це захист від крадіжок. Завдяки системі відеоспостереження та системі сигналізації можна завчасно побачити та зреагувати на випадок можливої крадіжки, а отже і уникнути його. Друге- це моніторинг ситуації на відстані. Пристрої IoT дають можливість спостерігати за ситуацією дистанційно. Людина може спокійно кудись поїхати, і бачити що відбувається у неї вдома. При виникненні екстренної ситуації система безпеки зможе надіслати повідомлення користувачу, або навіть викликати поліцію. Третє- це використання технологій розпізнавання у пристроях IoT задля власної безпеки та зручності у керуванні доступом. До пристроїв розпізнавання відносять різноманітні технології розпізнавання обличчя, сканери відбитку пальців, датчик вдиху та видиху. Завдяки цим технологіям у будинок не зможуть проникнути сторонні люди без відому власника, та людей, які мають доступ до системи безпеки будинку. Четверте- моніторинг стану систем усього будинку. Система безпеки в IoT включає в себе пристрої, що мають спеціальні сенсори, що реагують на різноманітні специфічні запахи. Вони здатні вловлювати та виявляти витоки газу, реагують на наявність диму, а також сповіщають про витоки води. Усі ці можливості дають змогу вчасно реагувати та діяти, щоб запобігти серйозних проблем. Усе це можуть контролювати

пристрої IoT, та надавати людині відчуття безпеки. Аналіз та розробка методів захисту інформації IoT є найбільш актуальною та основною для пристроїв IoT, оскільки пристрої можуть піддаватися хакерським атакам, а тому вони мають коректно працювати та зберігати інформацію, щоб мати можливість уникати збою в системі.

Об'єкт дослідження: аналіз методів захисту інформації, призначених для IoT пристроїв.

Предмет дослідження: основні методи аналізу для захисту інформації для IoT пристроїв.

Мета і завдання дослідження: аналіз, розробка та удосконалення методів для захисту інформації IoT пристроїв на основі мови програмування C++. У даній роботі буде здійснено огляд та аналіз основних методів захисту інформації пристроїв IoT, виконати розбір проблем, які можуть здійснювати загрозу у збереженні інформації, проведення аналізу та порівняння існуючих методів захисту інформації пристроїв IoT, а також реалізацію різноманітних кроків , що забезпечать якісне та правильне застосування методів захисту інформації на пристроях IoT.

Методика дослідження: у роботі застосовано описові дослідження, що надають можливість чітко та якісно описати дану мету роботи, методика аналізу, завдяки якій здійснено розбір та розгляд даних та їх концепцій, для кращого розуміння та взаємодії цих даних.

Наукова новизна: програма що забезпечить надійний захист системи, самостійно буде здійснювати моніторинг безпеки всіх підключених до неї систем.

Практична значущість результатів: розроблена програма зможе здійснювати аналіз ситуації усіх підключених до неї підсистем, сканувати стан своєї безпеки, та оповіщати користувача коли хтось буде намагатися здійснити хакерську атаку.

Апробація результатів бакалаврської роботи:

Гаврилець Є.Г. «Аналіз методів захисту IoT пристроїв». Тези доповіді на Всеукраїнській науково-технічній конференції «Технологічні горизонти:

дослідження та застосування інформаційних технологій для технологічного прогресу України і світу». – Київ 16.листопада 2023 р.

Гаврилець Є.Г. «Безпека в IoT мережах». Тези доповіді на п’яту міжнародну науково-технічну конференцію «Сучасний стан та перспективи розвитку IoT».

1 РОЗВИТОК ІНФОРМАЦІЇ.ВИДИ ТА ВЛАСТИВОСТІ ІНФОРМАЦІЇ

1.1 Розвиток захисту інформації

Захист інформації- це сукупність певних засобів та методів, які сприяють забезпеченню доступності, цілісності, повноти, коректності та конфіденційності інформації за умов розповсюдження впливу загроз природного (наприклад фізичне пошкодження електромережі під час поганої погоди, що призведе до збою в системі) та штучного (наприклад хакерська атака на систему) характерів. Завдяки стрімкому розвитку технологій виникло широке застосування комп'ютерних технологій в автоматизованих системах та мережах, та з цим людство зіткнулось з загострення проблеми захисту інформації. Уся діяльність що пов'язана з роботою та збереженням інформації повинна базуватися на свідомому контролі загальної безпеки шляхом нагляду за безпекою інформації, яку ми збираємо, використовуємо та ділимося одне з одним, а також з навколишнім середовищем. Саме тому виникає потреба у розробці інформаційної безпеки. Інформаційна безпека — це, насамперед, здатність аналізувати середовище з точки зору збору та використання багатьох доступних даних для поточних проблем, пов'язаних безпосередньо з безпекою цих даних, що можуть застосовуватись у певних закладах, організаціях та інших установах.

Проблема у забезпеченні захисту інформації для людства існувала завжди, оскільки інформація завжди підлягала впливу людей, та цей вплив неодноразово мав негативний помисел. Під час воєнних років інформацію неодноразово намагались приховати, змінити, або навіть знищити. Саме тому завжди виникала потреба у її захисті. В процесі розвитку, людство винаходило та змінювало вже існуючі види інформації, а тому існувала необхідність у розвитку нових методів захисту інформації. В загальному можна виділити три основні етапи становлення методів захисту інформації.

Рис.1.1 Етапи становлення методів захисту інформації

Під час розвитку першого періоду виникає таке поняття , як «криптографія». Ціллю криптографії тоді було забезпечення конфіденційності повідомлень, тобто їх шифруванням. Воно представляло собою перетворення повідомлень із зрозумілої форми подання на незрозумілу, роблячи це повідомлення зашифрованим (незрозумілим) для тих, хто не знав як його розшифрувати, або не мав спеціального ключа доступу до нього. Останнім часом сфера криптографії значно розширилась, і її завданням являється не тільки шифрування інформації повідомлень, а також і методи перевірки цілісності повідомлень, з'явились цифрові підписи, було запроваджено можливість ідентифікації відправника та отримувача, і насамперед у криптографії було введено технології безпечного спілкування. Одним з найперших приладів шифрування вважають Циліндр Джефферсона, що був винайдений у 1795 році. Цей прилад являє собою набір дисків, кожен з яких розміщає на собі 26 букв алфавіту, розташованих по краях приладу. У кожному диску циліндра був свій порядок букв, і кожен диск мав свій унікальний номер. У центрі дисків розміщувались отвори, за допомогою яких вони нанизувались на циліндр. Диски можна було знімати і встановлювати в будь-якому порядку, що давало безліч варіацій для шифрування. Ключем даного шифру був саме порядок

встановлення дисків у правильній послідовності. Всього у пристрої Джефферсона налічувалося 36 дисків.

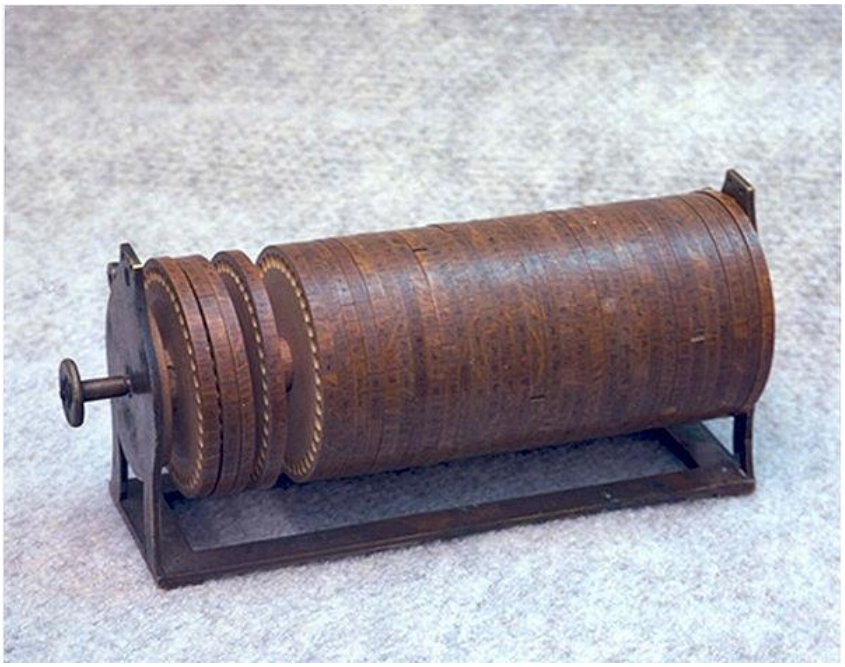

Рис.1.2 Циліндр Джефферсона

Другий період розвитку методів захисту інформації розпочався приблизно з середини XIX століття. Для періоду цього століття характерною рисою був стрімкий розвиток технічних засобів обробки інформації, а також з’являється передача повідомлень за допомогою електромагнітних полів (наприклад використання телеграфу), та електричних сигналів. Технічний засіб обробки інформації - це технічний засіб, за допомогою якого здійснюють пошук інформації, її обробку, передавання інформації, зберігання та накопичення, а також для її відображення та перетворення. У зв’язку з розвитком різноманітних технічних засобів обробки інформації виникла необхідність у шифруванні даних, які передавались по засобам обробки інформації. Найвідомішим апаратом для шифрування тоді являлась «Енігма». Цей апарат використовувався для шифрування та дешифрування повідомлень. Він складався з комбінації механічних і електричних систем, у механічній частині апарату був набір обертових дисків, які розташовувалися вздовж валу що обертався, та була присутня клавіатура. При натисканнях на кнопки клавіатури ступінчатий механізм рухав обертові вали, і

таким чином шифрувалось повідомлення. Рух роторів призводив до різних криптографічних перетворень, які здійснювались при кожному наступному натисненні клавіші на клавіатурі.

Третій період триває з 60х років XX століття і до наших днів. Це сучасний період у розвитку засобів для захисту інформації. Стрімкий розвиток технологій також спричинив різноманітні методи та способи, що дають змогу кіберзлочинцям змогу у доступі до викраденні та отриманні інформації. Різко зросла необхідність у тому щоб захищати дані, щоб вони не підлягали кібератакам та різним витокам. Інформація що міститься на пристроях, які мають доступ до мережі Інтернет, дуже сильно підлягає таким атакам. Виникає така галузь у сфері IT як кібербезпека. Кібербезпека це безпека IT систем, що включає в себе певну сукупність методів захисту , що пов’язані з контролюванням та оцінкою ризиків, які виникають чи можуть виникнути при користуванні комп’ютерами та комп’ютерними мережами. Ця галузь IT забезпечує їх надійний захист, надійне збереження інформації та її цілісності, унеможливлює злам систем.

1.2 Види інформації та її властивості

Види інформації можуть бути за способом сприйняття або за формою подання.

За способом сприйняття інформація буває :

- аудіальна(сприйняття інформації у звуках);
- візуальна(сприйняття інформації органами зору);
- тактильна(сприйняття шляхом дотиків);
- смакова;
- нюхова.

За формою подання:

- образно-знакова(числова, текстова, графічна);
- сигнальна.

Людина в житті сприймає інформацію, що надається у вигляді певних знаків та образів, а технічні системи сприймають та опрацьовують інформацію, що надається у вигляді сигналів.

Характерні ознаки, що притаманні інформації:

- суб’єктивність;
- актуальність – інформація має завжди оновлюватись;
- своєчасність – інформація має бути вчасно надана відповідно до певних подій, які вже відбулися;
- достовірність – властивість, що відповідає за те, щоб інформація об’єктивно описувала явища та події які відбуваються, та не містила помилок чи хибних тверджень;
- релевантність – відсутність в інформації зайвих небажаних відомостей, які зможуть заплутати тих, хто працює з цією інформацією;
- повнота – інформація має містити у собі повний опис наданих свідчень, щоб її легко та зрозуміло було сприймати;
- коректність подання – зображення інформації у правильному форматі;
- доступність;
- надійність.

Значний вплив на інформацію у сфері ІТ мають інформаційні технології. Інформаційні технології це система методів та процесів, що забезпечують використання систем зв’язку та способів застосування обчислювальної техніки з ціллю створення, пошуку, передачі, обробки та поширення інформації для того, щоб ефективно організовувати та налагоджувати людську діяльність. Переваги комп’ютерних технологій засновані на досягненнях телекомунікаційних технологій, та розподіленої обробки інформації. Також інформаційні системи мають на меті створення високоефективного власного інформаційного середовища, що може бути розроблене для різноманітних галузей, та мати широке та ефективне застосовування.

1.3 Історія виникнення Інтернету Речей

Поняття Інтернету речей вперше виникло в 90ті роки. Вперше саму концепцію Інтернету речей запровадив дослідник технологій, якого звали Кевін Ештон у 1999 році. Під цим терміном він мав на увазі систему, в якій об'єкти оснащені спеціальними датчиками , та спілкуються і обмінюються даними між собою та комп'ютером. На той час всі розробки, обговорення та теорії, що стосувались поняття Інтернету речей, були лише теоретичного характеру. На практиці ця уся концепція почала реалізовуватись в 2008 – 2009 роках. Саме цей момент вважається початком застосування концепції IoT, оскільки вже в ті часи кількість пристроїв, підключених до Інтернету, перевищувала населення планети в декілька разів. Основним завданням набору технологічних рішень в області Інтернету речей являється підвищення ефективності управління простором людини, її часом та власною безпекою. Крім того вони надають змогу у дистанційному керуванні об'єктами, що може бути легко здійсненим за допомогою смартфону у відповідному застосунку. Розвиток та доопрацювання Інтернету речей також вплинуло на сфери використання, в яких його застосовують. Основними сферами використання та застосування IoT є Industrial Internet of Thing та Consumer Internet of Thing. Consumer Internet of Thing або CIoT – це Інтернет речей, основною ідеєю якого є кінцевий користувач, а Industrial Internet of Thing або IIoT- це Інтернет речей, основними напрямками якого являються різноманітні галузі виробництва, життєдіяльність людини та корпоративне використання. Споживчий Інтернет речей(CIoT) стосується інтеграції технології IoT у споживчі програми та пристрої. Він включає мільйони фізичних пристроїв, які мають доступ для підключення до Інтернету, і використовує датчики для збору, обробки та обміну даними і інформації. На відмінну від промислового Інтернету речей (IIoT), споживчий Інтернет речей спрямований на надання рішень і зручності на індивідуальному рівні. Ці рішення включають ефективне відстеження, покращені з'єднання, кращу статистику, кращий контроль і підвищений комфорт. Усі ці якості можна застосувати до різних аспектів повсякденного життя, включаючи розваги,

безпеку вдома, охорону здоров'я. Споживчий Інтернет речей найкращим чином підбирає бажане для людини саме на персональному рівні. На основі цих сфер Інтернету речей також виокремили таке поняття, як Internet of Everything (IoE). Internet of Everything (Інтернет всього)- це загальна сфера Інтернету речей, технології і послуги якої підключаються до Інтернету. Така технологія Інтернету речей надає можливість користувачам легко взаємодіяти одне з одним, а також збирає персональні дані, завдяки чому компанії зможуть використовувати дані для адаптації та вдосконалення у виробництві своїх продуктів. Наприклад у найближчому часі з'явиться розумний шолом, який зможе отримати доступ до медичної карти пацієнта, та у разі необхідності надати необхідну інформацію лікарю, а також швидко знайде найближчу лікарню, що буде дуже зручно та ефективно, якщо людина буде у критичному стані. Також такий шолом може заздалегідь надати лікарю інформацію про поточний стан пацієнта, що значно зекономить час на його обстеження, та дозволить найшвидшим чином почати лікування. Такий розумний шолом є гарним прикладом використання сфери Internet of Everything. Тут яскраво видно як концепція Інтернету всього поєднує у собі концепцію Інтернету споживача та промислового Інтернету речей.

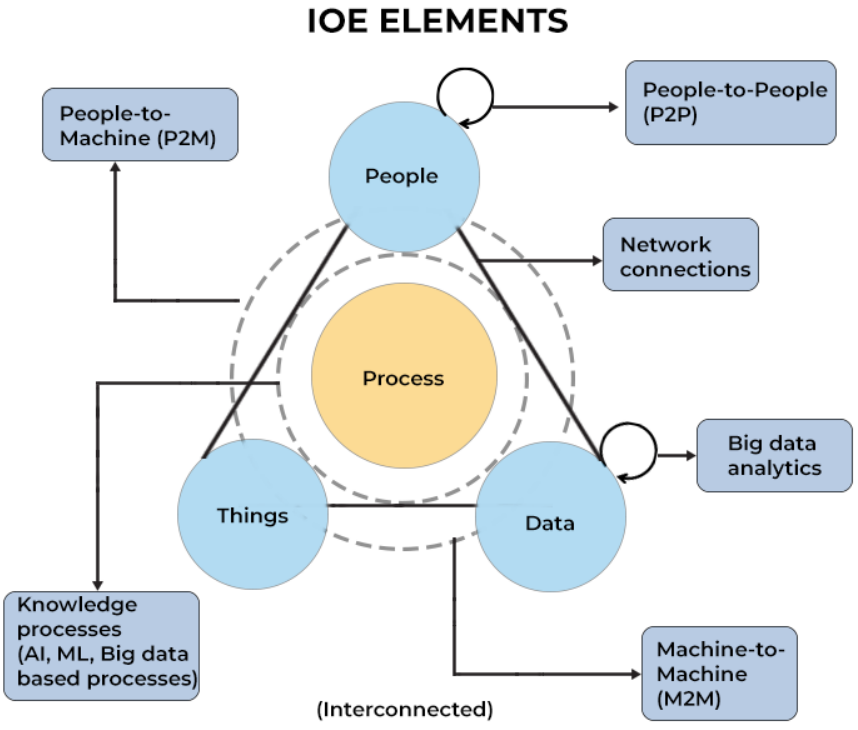

Рис.1.3 Елементи Інтернету всього

1.4 Особливості роботи Інтернету речей

Одними з базових та основних елементів Інтернету речей, які існують вже багато років, можна вважати дистанційний виклик служб екстреного реагування, різноманітні комунікаційні мережі, використання різних сенсорних пристроїв та обробку подій, з можливістю урахування контексту події. Система IoT має на меті представити собою єдину та цілісну мережу розумних об'єктів, що взаємодіють з людьми, та обмінюються інформацією один з одним. Архітектура IoT являє собою цілісну систему, і гарантує швидку та бездоганну роботу своїх пристроїв та компонентів, при цьому пов'язуючи у собі віртуальну та фізичну сфери.

Основні переваги роботи Інтернету речей:

1.Швидкий аналіз даних. Система IoT забезпечує легкий доступ до даних, необхідних для прийняття подальших рішень і спостереження за вибраними областями ринку.

2.Підвищення безпеки. Безпека у роботі є ключовим елементом, тому у системах IoT забезпечено контроль небезпечних і недоступних місць та процесів, що дозволить ізолювати співробітників від загроз. Здатність інтерпретувати історичні дані допоможе мінімізувати майбутні ризики.

3.Підвищення ефективності роботи. IoT збільшить можливість роботи в команді та усуне різницю між поколіннями, оскільки сприятиме передачі знань та досвіду від людей, які завершують професійну кар'єру, до новачків.

4.Найбільш ефективне прийняття рішень. Система IoT здатна за лічені секунди приймати найбільш оптимальні рішення, що в рази може збільшити показник ефективності у роботі, та мінімізує негативні наслідки, які могли бути спричинені неправильним та необдуманим рішенням.

Оптимізація процесів та ресурсів. Однією з найбільших переваг систем Інтернету речей є швидкий та обширний аналіз великих даних. Завдяки Інтернету речей усі операції адаптуються до структури поведінки

клієнтів і постачальників, а окрім того, він дає змогу опціонально прогнозувати рівень виробництва.

6.Виявлення проблем у роботі на ранніх стадіях. Завдяки тому що системи IoT здійснюють великий аналіз усіх даних з якими вони працюють, це дає змогу одразу швидко та точно визначити проблему, можливі причини її виникнення, та варіанти того, як швидко та максимально ефективно можна вирішити цю проблему.

Головним аспектом для того, щоб досягти усіх цих переваг у роботі, та отримати цілісність системи, є детальний та ретельний розгляд під час проектування системи таких моментів, які нададуть змогу системі швидко оновитися, та почати свою роботу знову. Уся система IoT реалізована на такому рівні, завдяки якому є можливість приховувати деякі деталі у реалізаціях системи, та її обмеженнях, що безсумнівно вважається перевагою серед наявних еталонних архітектур та моделей систем.

Еталонна архітектура IoT речей це структура, що забезпечує загальне розуміння ключових компонентів в системі IoT, та їх взаємодію між собою. Така архітектура дозволяє забезпечення в системі високої надійності та масштабованості. Еталонна архітектура складається з декількох рівнів:

1.Рівень проміжного програмного забезпечення- він надає різноманітні служби та функції, які будуть забезпечувати обробку, аналіз та зберігання даних. Цей рівень включає в себе платформи, які надають послуги у аналітиці даних, їх обробці та зберіганні.

2.Рівень сприйняття- складається з різноманітних приводів, пристроїв та датчиків, які збирають та генерують дані, отримані з навколишнього середовища. Дані пристрої відповідають за визначення та вимірювання різних фізичних параметрів, наприклад температура повітря, або його вологість.

3.Мережевий рівень. Цей рівень складається з різних видів мережевих технологій, таких як Wi-Fi та Bluetooth з’єднання, які у свою чергу дозволяють пристроям обмінюватись інформацією між собою та з хмарними

серверами. Даний рівень включає в себе мережеві протоколи, які оптимізовані для міжмашинного зв'язку.

4.Рівень безпеки- забезпечує різні механізми безпеки, такі як: шифрування, автентифікація та авторизація, для забезпечення цілісність, конфіденційність та доступність даних у системі IoT.

5.Рівень додатків- складається з служб та додатків, які використовують дані, зібрані та згенеровані пристроями IoT, з метою надання цінності кінцевому користувачу. Дані програми та послуги застосовуються у широкому діапазоні сфер та областей. Найпопулярнішими сферами такого застосування є промислова автоматизація, управління транспортом та енергетикою, охорона здоров'я та розумні будинки.

Ключові особливості еталонної архітектури IoT:

- стандартизує взаємодію між різними службами та пристроями IoT;
- визначає функціональні компоненти, які є необхідними для ефективної роботи IoT систем;
- гарантує, що системи Інтернету речей розроблені та впроваджені сумісно між собою та безпечно;
- підтримує розробку масштабованих та гнучких рішень в системах IoT;
- надає структуру для керування даними та аналітикою у системі.

Еталонна архітектура може бути використана у проектуванні розумних міст, вона може допомогти забезпечити ефективну та безпечну взаємодію різних компонентів системи розумного міста , таких як датчики, аналітика даних та інтерфейси користувача, у системі промислової автоматизації та управління- еталонна архітектура IoT може допомогти гарантувати що промислові системи розроблені та впроваджені у спосіб, який є безпечним, надійним та сумісним з іншими компонентами промислової екосистеми, а також одним з успішних варіантів використання еталонної архітектури IoT може бути у її запровадженні до системи охорони здоров'я - така система здатна підтримувати розробку підключених медичних пристроїв і систем віддаленого моніторингу пацієнтів , надаючи гарантію, що вони розроблені та реалізовані таким чином, щоб

захищати конфіденційність і безпеку пацієнтів. Загалом еталонна архітектура IoT надає план для проектування та впровадження систем Інтернету речей, які є сумісними, масштабованими та безпечними. Це дозволяє розробникам проектувати та впроваджувати системи IoT, які можуть спілкуватися одна з одною та з існуючими системами, а також буде забезпечено спільну мову та структуру для обговорення та аналізу систем IoT.

2 АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ.ОСОБЛИВОСТІ РІВНЕЙ АРХІТЕКТУРИ БЕЗПЕКИ

2.1.Проблеми інформаційної безпеки

Вхід до системи інтернету речей та отримання доступу до персональних даних користувачів можна здійснити маючи доступ до будь-якого пристрою IoT. Через автономне прийняття рішень та іншу специфіку у роботі Інтернету речей, у зловмисників з’являється різні лазівки для того, щоб отримати доступ до персональних даних користувача або організації, а також у системі зростає її потенційна вразливість. Завдяки цим аспектам питання захисту конфіденційності та безпеки системи є актуальним.

Рис.2.1 Основні проблеми у безпеці IoT

Поняття «інформаційна безпека» це не лише захист інформації від несанкціонованого доступу. Певним чином це також частина управління інформаційними ризиками, яка включає захист від несанкціонованого доступу до інформації, її використання, розкриття, порушення, модифікації, контролю, запису або повного її знищення. Безпека на усіх архітектурних рівнях має прямий вплив

на успіх у роботі IoT систем, оскільки саме вона має вплив на забезпечення надійності, сумісності та бездоганної роботи в системі. Зараз система Інтернету речей на такому рівні, який дає змогу у поєднанні в собі цифровий(різноманітні датчики, які обробляють отриману інформацію) та фізичний простір, які між собою обмінюються інформацією. Такі датчики дуже використовувані та розповсюджені, їх застосовують починаючи з використання у дитячих іграшках, і закінчуючи у їх використанні на великих промислових підприємствах та масштабних організаціях. Зважаючи на ці аспекти можна дійти висновку, що інформаційна безпека підлягає до ризику у витіканні даних, їх модифікації, а також зростає вразливість цифрового світу. Швидкий розвиток пристроїв IoT призвів до збільшення атак на підключені пристрої та мережі.

Види загроз які впливають на безпеку у роботі систем Інтернету речей:

- ботнет: ботнети- мережі заражених пристроїв, створюють загрозу безпеці Інтернету речей, уможливлюючи скоординовані кібератаки, витік даних і несанкціонований доступ до них;
- програми-вимагачі: загрози програм-вимагачів для пристроїв Інтернету речей полягають в тому, що вони шифрують дані, вимагаючи викупу, що призводить до втрати даних або несанкціонованого доступу, якщо їх не подолати
- -Shadow IoT: Shadow IoT включає некеровані пристрої IoT, які становлять загрозу безпеці без належного нагляду та інтеграції з протоколами безпеки.

Переважна більшість загроз Інтернету речей є низькоризиковими, але є й більш серйозні, які можуть призвести до значної шкоди, зокрема до паралічу публічних служб. Пристрої IoT вразливі до атак головним чином тому, що вони не мають ефективних засобів захисту від загроз. Хакери можуть захотіти отримати доступ до конфіденційної інформації, що зберігається в системах, до яких підключені пристрої IoT. Ця інформація включає особисту інформацію (таку як імена, адреси та паролі), фінансову інформацію (таку як номери банківських рахунків і номери кредитних карток) і навіть військову інформацію (таку як рух

військ і стратегічні плани). Іншим поширеним способом використання хакерами пристроїв IoT є маніпуляції з прошивкою, що може спричинити непоправне пошкодження пристроїв і, як наслідок, повну втрату даних. Досвідчені викрадачі даних можуть завдати значної шкоди, просто знаючи адресу Інтернет-протоколу (IP) пристроїв IoT. Ці адреси можуть використовуватися для визначення точного місцезнаходження та домашньої адреси користувача. Захист Інтернету речей не є простим завданням. Деякі параметри у специфіці роботи IoT, які ускладнюють це завдання:

1.Багато різних типів пристроїв. IoT охоплює все: від розумних холодильників і термостатів до автомобілів і заводського обладнання. Ці пристрої виробляються різними компаніями, і всі вони працюють по-різному, тому для кожного з типів пристроїв треба застосовувати різний підхід для захисту даних.

2.Величезний масштаб. З мільярдами пристроїв IoT по всьому світу стежити за всіма ними — це величезна робота, з якою не легко впоратись. Постійний моніторинг потребує багато часу та ресурсів, але незважаючи на це, все одно можна пропустити якісь деталі, що у подальшому зможуть призвести до витоку інформації.

3.Складне оновлення. Іноді достатньо просто оновити пристрій, щоб вирішити певні проблеми у його роботі. У випадку з IoT зробити ці оновлення не завжди легко та доцільно.

4.Закріплення крайових пристроїв. Деякі пристрої IoT збирають і надсилають дані саме там, де вони знаходяться, наприклад, світлофор, який контролює рух, ймовірно, знаходиться на загальнодоступному перехресті. Захистити ці пристрої може бути складно, оскільки вони часто знаходяться під відкритим небом і доступні для багатьох людей..

5.Важко контролювати. Відстежувати все, що відбувається з такою кількістю різних пристроїв, важко. Фізично це потребує багато часу та ресурсів.

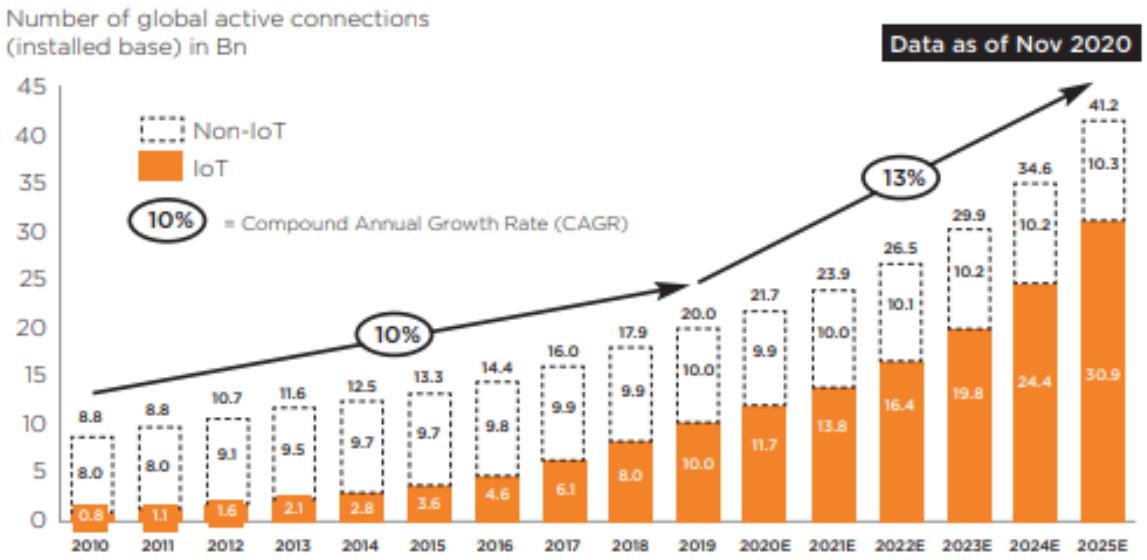

Рис.2.2 Діаграма використання IoT пристроїв

Низька безпека багатьох пристроїв Інтернету речей, особливо тих, які не інтегровані з ПК, робить їх легкою мішенню. Через слабку структуру операційних систем і низьку обчислювальну потужність вони рідко оснащені програмами безпеки. Зловмисне програмне забезпечення використовує як ці вразливості, так і саме підключення цих пристроїв до Інтернету. Також ризики виникають у звязку з тим, що більшість служб IoT використовують персональні дані користувачів, такі як дата народження, місце проживання і тд. Через це виникають нові ризики у витоку даних, та являють собою один з великих аспектів у шахрайстві. Захоплюючи пристрої IoT, хакери можуть запускати DDoS-атаки з кількох платформ IoT одночасно, що раніше було рідкістю. Очікується, що подібні ситуації будуть частішими, оскільки кількість пристроїв, підключених до мережі з кожним днем продовжує зростати. Також зростає кількість шкідливих програм, здатних передаватись між платформами, оскільки хакери легко створюють шкідливі віруси для різних архітектур. Згідно з даними компанії Symantec, на пристрої IoT таких країн здійснювали атаки, а саме: Китай- 34%, США- 28%, Німеччина- 15%, Нідерланди- 5%, Україна- 5%, В’єтнам- 4%, Франція- 3%, Великобританія- 3%, Південна Корея- 3%. Провідна світова дослідницька компанія у сфері IT Gartner

прогнозує, що до 25% атак буде здійснюватись на пристрої IoT, та понад 527 мільйонів доларів США буде витрачено на потреби безпеки у цьому секторі. Дослідження даної компанії показують, що протягом останніх років практично п'ята частина організацій по всьому світу зіткнулася щонайменше з однією кіберзагрозою, яка в свою чергу була пов'язаною з Інтернетом речей. Експерти вважають, що найближчому майбутньому кількість атак на IoT-пристрої буде тільки зростати. Фахівці виділяють кілька основних проблем Інтернету речей-зокрема це застарілі прошивки пристроїв, а також стандартні паролі, які встановлюють виробники. IoT-атаки можуть здійснюватися з використанням найрізноманітніших пристроїв, таких як маршрутизатори, IP-камери, Wi-Fi-повторювачі, обладнання для розумного будинку, та навіть принтери.

2.2 Безпека IoT систем

Інтернет речей став ключовою частиною бізнес-операцій у всьому світі. Однак зростання та підвищення складності глобальної мережі інтелектуальних пристроїв породило нові проблеми безпеки. Захист пристроїв Інтернету речей є життєво важливим компонентом безпеки сучасної мережі . Люди можуть покладатися на розгалужені сенсорні мережі або використовувати кілька інтелектуальних камер безпеки, щоб допомогти у роботі своїм локальним пристроям. Системи роботи пристроїв IoT потребують належних практик безпеки Інтернету речей, щоб уникнути потенційно небезпечних нових ризиків, які мають тенденцію до розширення поверхні атаки через кожен підключений пристрій. Наприклад, зловмисники, націлені на інтелектуальні пристрої, можуть отримати віддалений доступ до ресурсів далеко за межі їх початкової точки входу в мережу, потенційно збираючи конфіденційні дані для створення атак на пристрій. Використовуючи метод збирання та аналізу інформації, можна виокремити основні загрози та ризики, для пристроїв Інтернету речей:

1.Відсутність вбудованої безпеки

Багато пристроїв IoT часто не мають вбудованих заходів безпеки для боротьби із загрозами, зосереджуючись головним чином на своїх основних функціях. Віддалений доступ до пристроїв Інтернету речей може спричинити проблеми з безпекою. Прогалини в безпеці виникають через те, що постачальники мало інвестують в оновлення прошивки або довгострокову підтримку , а деякі пристрої IoT перестають підтримуватися незабаром після випуску. Крім того, невиправлені бекдори(методи обходу стандартної процедури автентифікації) та недоліки веб-додатків можуть створити проблеми з доступом. Отже, користувачі повинні розробити надійні плани безпеки для всіх пристроїв IoT і програмного забезпечення для їхнього керування, заповнивши порожнечу, залишену виробниками.

2.Атаки шкідливих програм

Вразливості IoT загрожують окремим пристроям і можуть перерости до повномасштабних мережевих криз, таких як DDoS-атака, яка перевантажує та виводить з ладу критичні системи. Зловмисники часто використовують слабкі паролі, щоб залучати пристрої до ботнетів для створення масштабних атак. Хоча деякі зловмисні програми можуть спричиняти лише незначні неприємності, як-от перетворювати пристрої на спам-ботів або криптомайнери, інші мають серйозні наслідки. Наприклад, ботнети можуть забезпечувати DDoS-атаки, які вимикають мережі, або зловмисне програмне забезпечення може «блокувати» пристрої, роблячи їх повністю непрацездатними.

3.Втрата даних

Витоки даних очолюють список корпоративних кіберзагроз, причому незахищені пристрої IoT часто вважаються винуватцями критичного доступу до даних. Спільне дослідження компаній Viettel і Kaspersky Labs у 2021 році показало, яку роль у 16 значних зломах зіграли несправні посилання IoT, що вплинуло на близько 100 000 фінансових рахунків. Подібним чином одна з компаній зіткнулась з проблемами, через які вразливі місця їхніх фітнес-пристроїв могли призвести до витоку даних про здоров’я, стать і вік користувачів

4.Фізична охорона

Багато компаній покладаються на технологію IoT у своїх налаштуваннях фізичної безпеки. Наприклад, вони можуть використовувати інноваційні системи доступу до дверей або замки для своїх серверних центрів. Ці пристрої так само вразливі до атак, як і будь-який інший продукт IoT. Якщо шкідливе програмне забезпечення потрапить на один з таких пристроїв, то уся система безпеки буде під загрозою. В такому випадку зловмисники дуже легко зможуть контролювати усю ситуацію, пов’язану з системою безпеки. Тому захист пристроїв Інтернету речей, таких як замки та камери, має вирішальне значення, оскільки вони так само вразливі до атак, як і будь-який продукт Інтернету речей, і є важливими для захисту від крадіжки та пошкодження. Отже, під час захисту цілісності мереж даних і критично важливих активів також необхідно враховувати фізичний аспект технології IoT.

5.Неправильна конфігурація IoT.

Якщо пристрої IoT неправильно налаштовані, вони можуть обійти заходи безпеки, особливо якщо використовуються паролі за замовчуванням, такі як "123456", як це часто буває у користувачів. . Крім того, старіші пристрої IoT можуть використовувати застаріле мікропрограмне забезпечення з невиправленими вразливостями. Без цілеспрямованих зусиль із захисту пристроїв IoT застаріле мікропрограмне забезпечення та слабкі паролі можуть зробити мережі вразливими до тривалого впливу та атак.

Для наглядної демонстрації вимог безпеки в Інтернеті речей, варто змоделювати архітектуру IoT, яка складається з чотирьох рівнів: рівень служб, рівень інтерфейсів, сенсорний та мережевий рівень. Усі ці рівні мають забезпечувати якісний та надійний захист інформації, контроль даної інформації, інструменти для автентифікації у системі, цілісність даних та інструменти, які в подальшому зможуть надавати та забезпечувати захист системи IoT від атак на систему, вірусів та несанкціонованого доступу до неї. Повсякденно багато пристроїв IoT стикаються з декількома терміновими вразливими місцями безпеки, та становлять значний ризик для компаній, які їх використовують. Однак все це не є приводом для того, щоб відмовлятися від технологій IoT. У будь-якому випадку

багато сфер та компаній в даний період розвитку IoT систем залежать від них у повсякденній роботі та житті.

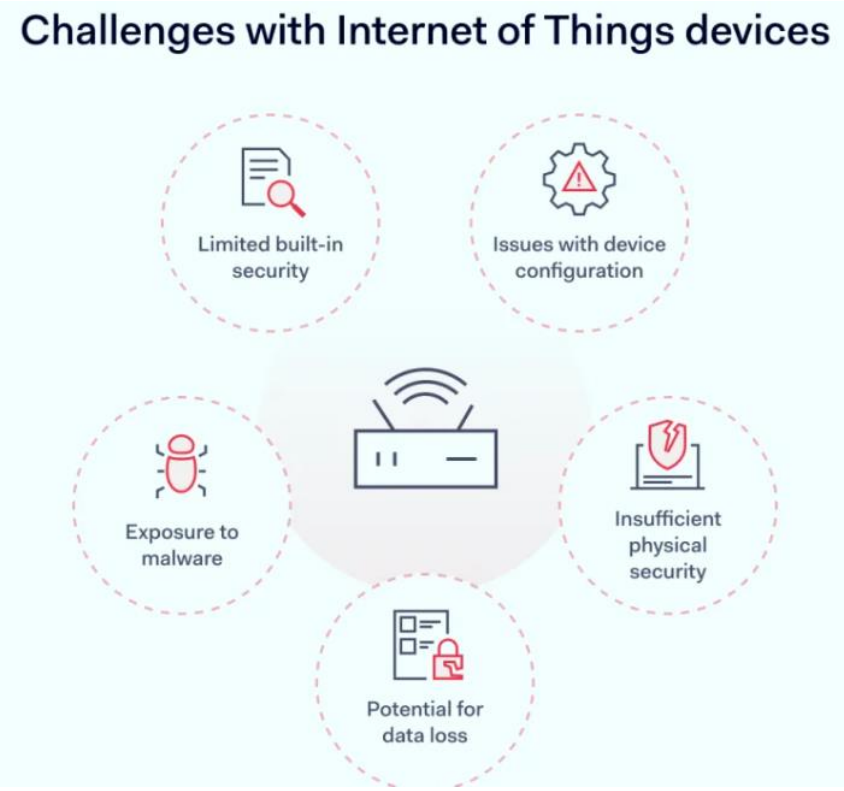

Рис. 2.3 Основні загрози для пристроїв IoT

	Сенсорний рівень	Мережевий рівень		Рівень служб	Рівень інтерфейсів
Відсутність шифрування		X		X	
Недостатній рівень автентифікації	X	X	X	X	X
Проблеми конфіденційності	X	X		X	
Погана фізична безпека	X	X			

Рис. 2.4 Проблеми у безпеці системи IoT на різних рівнях

2.3 Питання безпеки IoT на різних рівнях його архітектури

2.3.1 Безпека мережевого рівня

Даний рівень надає обмін та зв'язок даних користувачів IoT та хмарних технологій. З’єднання з мережею Інтернет містить у собі поєднання приватних мереж, громадських, а також спеціальних великих мереж(таких як великі компанії та установи), тому питання безпеки на цьому рівні є дуже важливим. Безпека на мережевому рівні являє собою мережеву безпеку, яка захищає саму мережу та її дані від злому, вторгнень та атак.. Це обширний і загальний термін, який описує апаратні та програмні рішення, а також процеси або правила та конфігурації, пов’язані з використанням мережі, її доступністю та загальним захистом від загроз. Безпека мережі передбачає контроль доступу, антивірусне та антивірусне програмне забезпечення, безпеку додатків, мережеву аналітику, типи безпеки, які є пов’язані з мережею. Безпека мережі має життєво важливе значення для захисту клієнтських даних та інформації, забезпечення безпеки спільних даних і забезпечення надійного доступу та продуктивності мережі, а також захисту від кіберзагроз, що також має значний вплив на систему IoT речей, оскільки мережевий рівень для IoT є одним з основних. Добре спроектоване рішення для безпеки та безпечної роботи мережі зменшує наявні витрати та захищає організації та користувачів від дорогих витрат, які можуть виникнути через порушення даних або інший інцидент, який буде пов'язаний з питанням безпеки роботи мережі. Основні види захисту для мережевого рівня:

1.Брандмауери. Брандмауери контролюють вхідний і вихідний трафік у мережах із заздалегідь визначеними правилами безпеки. Брандмауери запобігають небажаному трафіку, та є необхідною частиною щоденної роботи. Безпека мережі на даному мережевому рівні значною мірою покладається на брандмауери,

особливо брандмауери наступного покоління , які зосереджені на блокуванні шкідливих програм і атак на рівні додатків.

2.Сегментація мережі. Сегментація мережі визначає межі між сегментами мережі, де активи всередині групи мають спільну функцію, ризик або роль в організації. Наприклад, шлюз сегментує мережу компанії від Інтернету. Потенційні загрози за межами мережі запобігаються, гарантуючи, що конфіденційні дані організації залишаються всередині. Організації також можуть піти далі, визначивши додаткові внутрішні межі в межах своєї мережі, що потім зможе забезпечити покращену безпеку та контроль доступу.

3.Контроль доступу до мережі. Контроль доступу визначає людей або групи та пристрої, які мають доступ до мережевих програм і систем. Таким чином забороняється несанкціонований доступ і, можливо деякі специфічні загрози. Інтеграція з продуктами ідентифікації та керування доступом (IAM) може чітко ідентифікувати користувача, а політика керування доступом на основі ролей (RBAC) гарантує авторизований доступ особи та пристрою до активу.

4. VPN віддаленого доступу. Віддалений доступ VPN надає віддалений та безпечний доступ до корпоративної мережі окремим хостам або клієнтам, таким як дистанційні користувачі, мобільні користувачі. Кожен хост зазвичай має завантажене програмне забезпечення клієнта VPN або використовує веб-клієнт. Конфіденційність і цілісність конфіденційної інформації забезпечується багатофакторною автентифікацією, скануванням відповідності кінцевих точок і шифруванням усіх переданих даних.

5. Доступ до мережі з нульовою довірою (ZTNA). Модель безпеки з нульовою довірою стверджує, що користувач повинен мати лише доступ і дозволи, які є необхідними для виконання своєї ролі. Це зовсім інший підхід, ніж традиційні рішення безпеки, які надають користувачеві повний доступ до цільової мережі. Доступ до мережі з нульовою довірою (ZTNA) дозволяє деталізувати доступ до програм організації від користувачів, яким цей доступ потрібен для виконання своїх обов’язків.

6. Запобігання втраті даних (DLP). Запобігання втраті даних (DLP) поєднує технології та найкращі практики для запобігання розкриттю конфіденційної інформації за межами організації, особливо регульованих даних, таких як інформація, що ідентифікує особу, і дані.\

7. Безпека хмарної мережі. Захист сучасного центру обробки даних вимагає більшої гнучкості та інновацій, щоб не відставати від міграції робочих навантажень додатків у хмару, тому існують рішення програмно-визначеної мережі (SDN) і програмно-визначеної глобальної мережі (SD-WAN), які забезпечують рішення мережевої безпеки в приватних, публічних та гібридних хмарних технологіях.

Моніторинг безпеки IoT має важливе значення для захисту підключених пристроїв від цих ризиків безпеки. Моніторинг безпеки IoT включає постійний моніторинг усіх пристроїв і мереж IoT на наявність загроз в безпеці, а також вразливостей. Відстежуючи пристрої IoT, можна в реальному часі виявляти потенційні інциденти безпеки та вживати відповідних заходів для їх усунення. Ось деякі з ключових переваг моніторингу безпеки IoT:

1.Виявлення загроз у реальному часі. Моніторинг безпеки IoT дає змогу виявляти загрози безпеці та вразливості, коли вони виникають. Відстежуючи пристрої IoT у режимі реального часу є змога виявляти підозрілу активність і швидко реагувати на неї, щоб зменшити потенційні інциденти безпеки.

2.Покращене реагування на інциденти: за допомогою моніторингу безпеки IoT є можливість швидко й ефективно реагувати на інциденти безпеки. Надається можливість надавати сповіщення в режимі реального часу, виконувати криміналістичний аналіз і вживати заходів для виправлення, щоб мінімізувати вплив інциденту безпеки.

3.Вимоги відповідності: у багатьох галузях є нормативні вимоги щодо моніторингу безпеки Інтернету речей, наприклад Загальний регламент захисту даних (GDPR). Моніторинг безпеки IoT може допомогти організаціям виконати ці вимоги відносно безпеки мережі та уникнути додаткових потенційних юридичних зобов’язань.

4.Захист критично важливих активів: організації повинні захищати свої критично важливі активи, зокрема інтелектуальну власність, дані клієнтів і фінансову інформацію.

2.3.2 Безпека на сенсорному(прикладному рівні)

Прикладний рівень це рівень, який надає користувачам розумні послуги IoT. Основними функціональними компонентами цього рівня є різноманітні додатки, які можна класифікувати, наприклад, як «розумний дім», «розумне місто», «розумний транспорт», «розумна комерція» та «розумне здоров'я» та інші. Прикладний рівень відповідає за надання різноманітних послуг і одночасно визначає набір протоколів проходження повідомлень на прикладному рівні. Пристрої є частиною мережі на даному рівні, які здійснюють збір та обробку інформації між собою та мережами на сенсорному рівні. Цей рівень також відповідає за представлення даних, технічне обслуговування додатків, контроль доступу до додатків і оновлення програмного забезпечення та виправлень безпеки для цих додатків. Пристрої на даному рівні мають обмежені можливості підключення та низьке енергоспоживання, що спричиняє більше ризиків для порушення безпеки на цьому рівні.

Таблиця 2.1

Основні види загроз на сенсорному рівні

Загрози безпеки	Опис
Несанкціонований доступ	Через фізичне захоплення або логічної атаки, конфіденційна інформація на кінцевих вузлах захоплюється зловмисником.
Доступність	Кінцевий вузол перестає працювати, оскільки фізично захоплений або логічно атакований
Spoofing атака	За допомогою вузла шкідливого ПО зловмисник успішно маскується під кінцеве пристрій IoT, кінцевий вузол або кінцевий шлюз шляхом фальсифікації даних.
Selfish загроза	Деякі кінцеві вузли Інтернету речей перестають працювати, щоб заощадити ресурси або пропускну здатність, щоб викликати збій мережі.
Шкідливий код	Вірус, троян і небажані повідомлення, які можуть викликати збій програмного забезпечення

2.3.3 Безпека на рівні інтерфейсів

Рівень інтерфейсів це точка взаємодії між користувачами та системами. Даний рівень може наражати конфіденційні дані, функції чи ресурси на потенційні загрози. Вимоги безпеки для вхідних сеансів до інтерфейсів застосовуються до облікових записів і вихідного пристрою, незалежно від того, чи це пряме з’єднання з фізичних пристроїв , або віддалене, і для коректної роботи даного рівня мають виконуватись такі основні вимоги:

-наявність можливості автентифікації, авторизації;

-завантаження та вчасне оновлення програмного забезпечення з метою уникнення помилок в роботі системи, наявність патчей, необхідних для підтримки рівня безпеки.

Основні види загроз, які можуть бути на даному рівні:

-віддалена конфігурація: не вдалося провести налаштування на рівні інтерфейсів;

-управління безпекою: можливий витік логінів, ключів доступу, та іншої конфіденційної інформації, необхідної для безпечної роботи;

-система управління: збій в системі, що може призвести до порушення цілісності інформації, витоку даних, та надати зловмисникам несанкціонований доступ до системи.

Даний рівень є «мостом» між IoT системою та додатками, що є важливим критерієм для того, щоб забезпечити надійний рівень безпеки на даному рівні. У інакшому випадку зловмисники зможуть отримати доступ до усієї персональної інформації, яку зберігають застосунки та пристрої IoT.

2.3.4 Безпека на рівні служб

Службовий рівень являє собою сукупність програмних засобів, які надають користувачеві можливість у додаткових послугах в роботі з комп'ютером, та розширюють можливості операційних систем. Програми службового рівня

надають користувачам вибір у використанні зручного інструментарію для перевірки та налаштування комп’ютерної системи.

Таблиця 2.2

Подання видів загроз безпеки на рівні інтерфейсів

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

В системі IoT даний рівень архітектури може вказувати на рівень доступності, надійності та ефективності послуг, які надаються за допомогою підключених до Інтернету пристроїв. Також службовий рівень може визначати, наскільки швидко реагує ваша система на команди користувача, наскільки надійно вона працює, а також як часто вона вимагає обслуговування чи виправлення помилок у її роботі. У роботі Інтернету речей існують деякі загрози на службовому рівні, які можуть вплинути на доступність, надійність та ефективність послуг, наданих за допомогою підключених пристроїв. Основними видами загроз даного рівня є:

1.Доступність мережі. Однією з основних загроз на службовому рівні являється відсутність доступу до мережі, через що може виникнути перебої у зв'язку, відмову маршрутизаторів або інших мережевих пристроїв.

2. (DDoS) атаки. Такі типи атак спрямовані на переповнення ресурсів мережі чи системи, що призводить до перебоїв у роботі пристроїв IoT та недоступності наявних послуг для користувачів.

3. Відсутність оновлень програмного забезпечення. Якщо виробник не надає регулярні оновлення програмного забезпечення для пристроїв IoT, то це може залишати їх вразливими до нових загроз і атак.

Таблиця 2.3

Основні загрози на рівні служб

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

Протоколи відноситься до набору правил і стандартів, які дозволяють пристроям і системам спілкуватися та обмінюватися даними в мережі IoT. Розглянемо основні протоколи, які задіяні при роботі IoT пристроїв. Ці протоколи визначають методи та формати для передачі даних, виявлення пристроїв, а також підключення та безпеки в середовищі IoT.

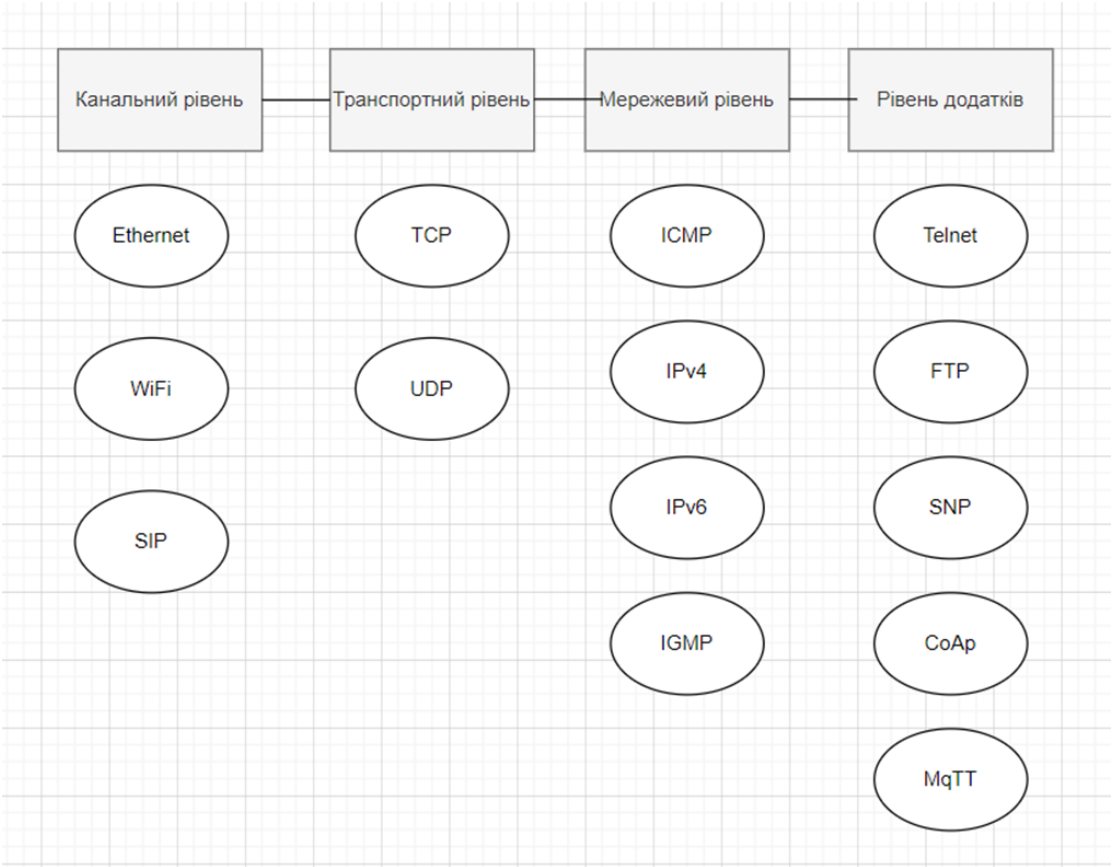

Рис.2.5 Основні протоколи що задіяні під час роботи IoT пристроїв

Зв'язок між пристроями відбувається через протоколи IoT, які гарантують, що дані, надіслані з кінцевих пристроїв, (наприклад датчиків) приймаються та розуміються, в підключеному середовищі, незалежно від того, куди та де здійснюється обмін інформацією між цими даними пристроїв.

Протоколи рівня додатків:

1.Telnet. Це протокол, який дозволяє підключатися до віддалених комп'ютерів (хостів) через мережу TCP/IP (наприклад, Інтернет). Використовуючи клієнтське програмне забезпечення на комп'ютері, можна встановити з'єднання з сервером. Коли клієнт telnet встановлює з'єднання з віддаленим хостом, клієнт стає віртуальним терміналом, що дозволяє вам спілкуватися з віддаленим хостом зі свого комп'ютера.

2.FTP(File Transfer Protocol). Даний протокол є стандартним мережевим протоколом, який використовується для передачі файлів з одного хоста на інший через мережу. FTP працює, забезпечуючи два типи з'єднань, які з'єднують

комп’ютери, що намагаються спілкуватися один з одним. Одне з’єднання призначене для команд і відповідей, які надсилаються між двома клієнтами, а інший канал обробляє передачу даних. Під час передачі по FTP комп’ютери, сервери або проксі-сервери, які спілкуються, використовують чотири команди. Це «надіслати», «отримати», «змінити каталог» і «перенести».

3.SNMP. Протокол SNMP використовується для обміну інформацією про керування між мережевими пристроями, для моніторингу та керування пристроями в локальній (LAN) або глобальній (WAN) мережах.

4.CoAP. Протокол надає набір методів для виявлення ресурсів, маніпулювання ними та спостереження, а також підтримку асинхронного зв'язку та кешування. Завдяки низьким накладних витрат і простоті CoAP є найбільш популярним в додатках IoT.

5.MQTT. Цей протокол надає послугу обміну повідомленнями, який забезпечує зв’язок між пристроями. MQTT працює за моделлю публікації-підписки , яка дозволяє пристроям надсилати повідомлення на певні теми, тоді як інші пристрої можуть підписуватися на ці теми, щоб отримувати повідомлення. Тип підключення по даному протоколу можна описати як «машина до машини».

Протоколи мережевого рівня:

1.ICMP. Цей протокол слугує для звітування про помилки та діагностики мережі. Зворотній зв'язок у мережі повідомляється призначеному хосту. Тим часом, якщо виникає будь-яка помилка, про це повідомляється в ICMP, даний протокол складається з багатьох повідомлень про помилки та діагностичних повідомлень.

2. IPv4. Даний протокол забезпечує 32-розрядну схему адреси; адресація IPv4 складається з чотирьох числових полів, розділених крапкою. Такий протокол можна налаштувати за допомогою DHCP або вручну. IPv4 не надає додаткових функцій безпеки, оскільки не підтримує автентифікацію чи методи шифрування.

3. IPv6. IPv6 є найновішою версією IP. Він забезпечує більше функцій безпеки, таких як автентифікація та шифрування, а також підтримує цілісність наскрізного з’єднання.

4. IGMP це протокол багатоадресної передачі даних. Він ефективно використовує ресурси під час трансляції повідомлень і пакетів даних. Також він є протоколом, який використовується в TCP/IP. Інші хости, підключені до мережі, і маршрутизатори використовують ICMP для багатоадресного зв'язку, які мають IP-мережі.

Протоколи транспортного рівня:

1.UDP. Це транспортний протокол без з'єднання. Протокол UDP використовується в програмах, де швидкість і розмір даних, що передаються, важливіші за безпеку та надійність. Даний протокол забезпечує контроль помилок контрольної суми, адреси транспортного рівня та інформацію про довжину до даних, отриманих із рівня над ним.

2. TCP. Протокол TCP є протоколом, що орієнтується на підключення. Між відправником і одержувачем встановлюється безпечне з'єднання, а для створення захищеного з'єднання між відправником і одержувачем створюється віртуальний канал. Дані що передаються за протоколом TCP мають форму безперервних потоків байтів.

Протоколи канального рівня:

1.Ethernet. Цей протокол він частіше використовується в середовищах локальної мережі, які використовуються майже в усіх мережах, таких як офіси, будинки, громадські місця, підприємства та університети. Ethernet набув величезної популярності завдяки максимальним швидкостям на великих відстанях за допомогою оптичних носіїв.

2. WI-Fi. IEEE 802.11 відноситься до набору стандартів, які визначають зв'язок для бездротових локальних мереж. Технологія, що лежить в основі 802.11 - це набір технічних інструкцій щодо впровадження Wi-Fi.

3.SIP. Протокол ініціації сеансу — це протокол сигналізації, який умикає протокол Voice Over Internet Protocol (VoIP), визначаючи повідомлення, що надсилаються між кінцевими точками, і керуючи фактичними елементами виклику. SIP підтримує голосові виклики, відеоконференції, обмін миттєвими повідомленнями та розповсюдження медіа.

2.4 Архітектура SOA та міжрівневі загрози

Сервісно-орієнтована архітектура (SOA) це архітектура системи, що надає можливість у використанні інформаціїї на усіх чотирьох рівнях даної системи. Така якість архітектури SOA значним чином підвищує рівень сумісності пристроїв у системі та забезпечує більш якісну роботу між службами наявних у системі пристроїв. У цій архітектурі надаються послуги для формування додатків через мережевий виклик завдяки мережі Інтернет. Він використовує загальні стандарти зв'язку для прискорення та оптимізації інтеграції послуг у додатки. Можна зауважити, що SOA відрізняється від архітектури мікро-сервісів. Ця архітектура дозволяє користувачам комбінувати велику кількість можливостей із наявних існуючих служб для формування додатків, охоплює набір принципів проектування, які структурують розробку системи та забезпечують засоби для інтеграції компонентів в узгоджену та децентралізовану систему, а також обчислення на основі SOA об'єднують функціональні можливості в набір сумісних служб, які потім можна буде інтегрувати в різні програмні системи. SOA дозволяє службам спілкуватися за допомогою системи слабкого зв'язку для передачі даних або координації діяльності. Слабкий зв'язок означає, що клієнт служби залишається незалежним від послуги, яка йому потрібна, а крім того клієнт, який також може бути службою, зможе спілкуватися з іншими службами, навіть якщо вони не пов'язані між собою. Завдяки цьому процесу можна поєднувати різні служби для створення складнішого програмного забезпечення, яке інші програми можуть використовувати як єдине ціле. Споживач або власник програми надсилає вхідні дані для запиту інформації або завдання від служби, а служба обробляє дані або виконує потрібне завдання та надсилає відповідь. У цьому архітектурному стилі бізнес-функції та процеси реалізуються як програмні сервіси, доступ до яких здійснюється через набір суворо визначених інтерфейсів прикладного програмування.

Основні характеристики архітектури SOA:

- забезпечує взаємодію між службами;

-полегшує якість послуг через контракт на обслуговування на основі угоди про рівень обслуговування;

- надає методи для інкапсуляції, виявлення, композиції, можливості повторного використання та інтеграції служб.

Сервісно-орієнтована архітектура має чотири основні ролі- це постачальник послуг, споживач служби, сервіс та реєстр послуг.

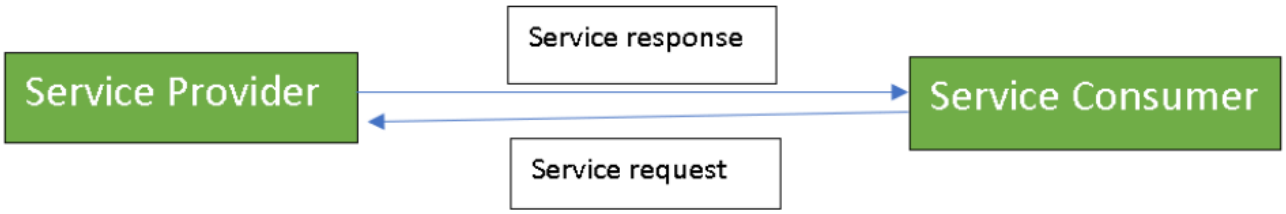

Рис. 2.6 Зображення взаємодії постачальника та споживача архітектури SOA

Постачальник послуг являє собою супроводжувача послуги та організацію, яка надає доступ до однієї чи кількох послуг іншим. Щоб рекламувати послуги, постачальник може опублікувати їх у реєстрі разом із контрактом на надання послуг, у якому вказується характер послуги, спосіб її використання, вимоги до послуги та розмір плати. Споживач служби може знайти метадані служби в реєстрі та розробити необхідні клієнтські компоненти для зв’язування та використання служби. Сервіси можуть бути приватними та доступними лише для авторизованих користувачів або відкритими та загальнодоступними. Кожна служба містить реалізацію служби, яка є кодом, відповідальним за виконання послуги; договір про надання послуг, в якому описуються параметри послуги, її вартість і якість. Реєстр послуг (також відомий як репозиторій сервісів) являє собою каталог доступних сервісів. Його завданням є зберігання описів послуг та іншої відповідної інформації про те, як користуватися послугами постачальника послуг.

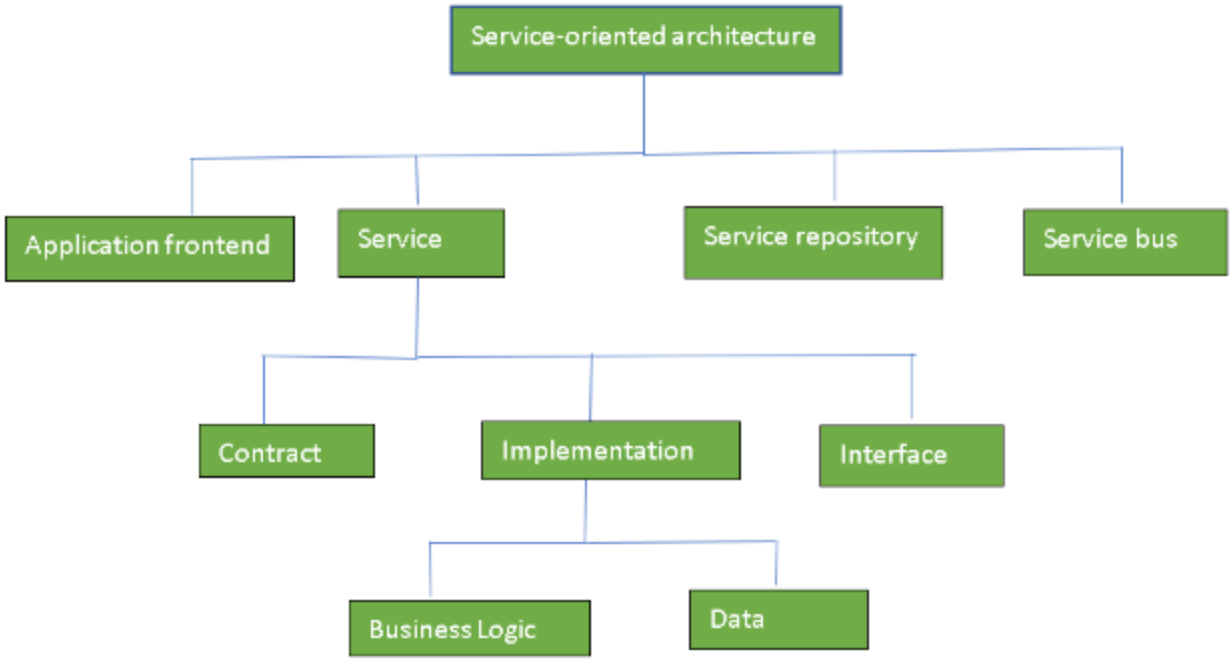

Рис. 2.7 Компоненти архітектури SOA

Основні якості, що надає архітектура:

1. Абстракція. Послуги повністю визначаються договорами про надання послуг і документами з описом, і вони приховують свою логіку, яка закладена в їх реалізації.

2. Можливість повторного використання. Розроблені сервіси можна повторно використовувати більш ефективно, таким чином скорочуючи час розробки та пов’язані з цим витрати.

3.Здатність виявляти. Послуги визначаються документами з описом, які становлять додаткові метадані, за допомогою яких їх можна ефективно виявляти служби що закладені в архітектуру системи. Виявлення служб забезпечує ефективний засіб для використання сторонніх ресурсів.

4. Автономність. Служби контролюють логіку, яку вони інкапсулюють, що дає змогу покращити ефективність їх роботи.

5.Сервіс. Ця мета архітектури спрямована на структурування процедур або програмних компонентів як послуг. Послуги створено для слабкого зв’язку з програмами, тому вони використовуються лише за потреби. Вони також розроблені

для того, щоб розробники програмного забезпечення могли легко використовувати їх для узгодженого створення програм.

6.Видавництво. SOA також має на меті забезпечити механізм для публікації доступних послуг, що включає їх функціональні можливості та вимоги до введення та виведення. Послуги публікуються таким чином, щоб розробники могли легко включати їх у програми.

Перевагою цієї архітектури є найпростіший і найшвидший спосіб реалізації з'єднань між службами, а з цього витікає один найбільш серйозний недолік- оскільки служби тісно пов'язані між собою у даному типі архітектури та покладаються на синхронний зв'язок, вони стають повністю залежними одна від одної, і навіть тимчасова недоступність однієї служби може заблокувати роботу усіх інших служб, що призведе до масштабного збою в системі, на відновлення якого може потребуватись не менше доби.

У даному розділі було наглядним чином розглянуто основні питання, що стосуються загрози безпеки IoT пристроїв, розглянуто види загроз з їх детальним описом. З усього цього можна зробити висновок, що питання захисту інформації IoT пристроїв наразі є одним з найактуальніших питань у сфері IT, яке потребує нагальних рішень. Сфера застосування IoT пристроїв розширюється з кожним днем, а запровадження безпеки у зберіганні інформації на пристроях IoT досі не вирішено. Аналізуючи велику кількість інформації з цього приводу, можна дійти висновку, що з кожним днем атаки на пристрої IoT збільшуються, а система захисту на пристроях слабка, та потребує невідкладного вдосконалення та модернізації. У наступному розділі буде запропоноване рішення, що дасть змогу покращити рівень безпеки у використанні пристроїв IoT. Завдяки ньому буде забезпечено мінімальний базовий захист пристроїв, який буде надавати захист від несанкціонованого доступу до пристроїв.

3 РОЗРОБКА ПРОГРАМИ ДЛЯ ЗАХИСТУ ПРИСТРОЇВ ІОТ

3.1 Основна інформація про обрану мову програмування

Дана програма була розроблена на основі мови програмування Python. Я зробила свій вибір на цій мові програмування, оскільки ми вивчали її на другому та третьому курсі, та ця мова програмування здалась мені найбільш оптимальною для використання у поставленій мною задачі.

Мова програмування Python являє собою інтерпретовану об’єктно-орієнтовану мова програмування високого рівня (мова програмування, що розроблена для швидкого та зручного програмування для програміста) з динамічною семантикою (або ще семантика виконання,- визначає як і коли різні конструкції мови повинні задавати поведінку програми). Дана мова програмування є однією з найлегших, та іноді її вважають навіть легшою за мову програмування Java, оскільки вона справляється з більшою частиною складності для користувача, дозволяючи початківцям зосередитися на повному розумінні концепцій програмування, а не на найменших деталях та нюансах. Python використовується для веб-розробки на стороні сервера, розробки програмного забезпечення, математики та системних сценаріїв, і популярний для швидкої розробки додатків, а також як мова сценаріїв або з’єднувальна мова для зв’язування існуючих компонентів завдяки своїм високорівневим вбудованим структурам даних, динамічний тип і динамічне зв'язування.

Рис. 3.1 Логотип мови програмування Python

Python широко поширений у використанні завдяки його чіткому синтаксису та зручності читання. Основною перевагою є те, що код, написаний на даній мові програмування, легше сприймається, та є більш читабельним, завдяки широкій підтримці спільноти та синтаксису, який наголошує на зручності читання, тому Python порівняно легко можна вивчити. Python також пропонує динамічні типи даних, готові класи та інтерфейси для багатьох системних викликів і бібліотек. Високорівневі структури даних, що застосовуються у цій мові програмування, динамічне зв'язування та динамічна типізація роблять її однією з основних мов програмування для швидкої та комфортної розробки програм.

Популярні бібліотеки Python:

1.NumPy – бібліотека для наукових обчислень на Python

2.Pandas – бібліотека для обробки та аналізу даних

3.SciPy – бібліотека для наукових обчислень

4.Matplotlib – бібліотека для побудови графіків для Python

5.Scikit-learn - бібліотека для машинного навчання

6.Запити - бібліотека для створення HTTP-запитів

7.TensorFlow – бібліотека для глибокого навчання

8.Keras - Бібліотека для створення та навчання нейронних мереж

9.Flask – мікровеб-фреймворк для Python

10.NLTK – бібліотека обробки природної мови для Python

Переваги використання бібліотек Python

-простота у використанні: бібліотеки Python легко використовувати та підтримувати, що робить їх неймовірним вибором для початківців та досвідчених інженерів. Вони надають безліч корисних функцій і стратегій, які можна швидко скоординувати у ваші підприємства з незначними зусиллями;

-підтримка спільноти: Python охоплює велику та динамічну онлайн-спільноту, яка може запропонувати допомогу з будь-яких проблем, які у вас виникають. Величезний обсяг доступних бібліотек також передбачає щедрість ресурсів і навчальних вправ, які вам допоможуть;

-рентабельність: бібліотеки Python, як правило, безкоштовні та з відкритим кодом, що робить їх економічно ефективними для дизайнерів;

-висока продуктивність: бібліотеки Python розроблені як швидкі та продуктивні, що покращує виконання ваших завдань;

-гнучкість: бібліотеки Python можна використовувати для багатьох завдань і додатків, від вдосконалення Інтернету до аналізу даних і машинного навчання. Це робить їх чудовим вибором для будь-якого розширення чи доручення.

Бібліотеки Python являють собою це набори модулів і пакетів, які надають певні необхідні можливості та функції для використання в програмуванні. Бібліотеки Python використовуються для різних доручень, таких як перевірка інформації, машинне навчання, графічний інтерфейс клієнта та багато іншого. Як і в багатьох мовах програмування, у Python необхідно встановити потрібні бібліотеки на комп’ютер для їх подальшого використання. Перед використанням бібліотек необхідно читати документацію бібліотеки, оскільки документація є важливою для розуміння того, як правильно та ефективно використовувати бібліотеку. Ознайомлення з документацією також допоможе ознайомитися з функціями та обмеженнями необхідної бібліотеки. При роботі також необхідно звертати увагу на версію бібліотеки. Якщо версія є застарілою, то в подальшій роботі з такою бібліотекою можуть виникнути проблеми через несумісність.

3.2 Кібербезпека в IoT

Розроблена мною програма певним чином пов’язана з таким поняттям як кібербезпека. Якщо узагальнити, то кібербезпека означає будь-яку технологію, захід або практику для запобігання кібератакам або пом’якшення їхнього впливу. Ефективна стратегія кібербезпеки може забезпечити надійний захист від зловмисних атак, спрямованих на доступ, зміну, видалення, знищення або вимагання систем і конфіденційних даних організації або користувача. Кібербезпека також відіграє важливу роль у запобіганні атакам, призначеним для вимкнення або порушення роботи системи чи пристрою. Ідеальний підхід до

кібербезпеки повинен мати кілька рівнів захисту для будь-якої потенційної точки доступу або поверхні атаки . Це включає захисний шар для даних, програмного забезпечення, обладнання та підключених мереж. Важливість кібербезпеки полягає в тому, що зі збільшенням кількості користувачів, пристроїв і програм на сучасному підприємстві разом із збільшенням обсягу даних, значна частина яких є конфіденційною або конфіденційною, кібербезпека стає більш важливою, ніж будь-коли. Але кількість і складність кібератак і технік атак ще більше ускладнюють проблему. Без відповідної стратегії кібербезпеки — і персоналу, належним чином навченого найкращим практикам безпеки — зловмисники можуть призвести до повної зупинки діяльності організації.

Термін «кібербезпека» застосовується в різних контекстах, від бізнесу до мобільних комп'ютерів, і його можна розділити на кілька загальних категорій.

1.Мережева безпека — це практика захисту комп'ютерної мережі від зловмисників, чи то цільових зловмисників, чи то зловмисне програмне забезпечення.

2.Безпека додатків зосереджена на захисті програмного забезпечення та пристроїв від загроз. Зламана програма може надати доступ до даних, які вона призначена для захисту. Успішна безпека починається на етапі проектування, задовго до розгортання програми чи пристрою.

3.Інформаційна безпека захищає цілісність і конфіденційність даних як у зберіганні, так і під час передачі.

4.Операційна безпека включає процеси та рішення щодо обробки та захисту активів даних. Дозволи, які користувачі мають під час доступу до мережі, а також процедури, які визначають, як і де дані можуть зберігатися або ділитися, підпадають під цю парасольку.

5.Аварійне відновлення та безперервність бізнесу визначають, як організація реагує на інцидент кібербезпеки або будь-яку іншу подію, яка спричиняє втрату операцій або даних. Політика аварійного відновлення диктує, як організація відновлює свої операції та інформацію, щоб повернутися до тієї ж робочої

здатності, що й до події. Безперервність бізнесу — це план, до якого організація повертається, намагаючись працювати без певних ресурсів.

6.Навчання кінцевих користувачів стосується найбільш непередбачуваного фактора кібербезпеки: людей. Будь-хто може випадково занести вірус у безпечну систему, не дотримуючись правил безпеки. Навчання користувачів видаляти підозрілі вкладення електронної пошти, не підключати неідентифіковані USB-накопичувачі та інші важливі уроки є життєво важливими для безпеки будь-якої організації.

Інтернет речей з'єднує різні об'єкти та пристрої через Інтернет для зв'язку з подібними пристроями чи машинами, тому зважаючи на фактор росту використання пристроїв IoT також збільшується площа атаки, якою можуть скористатися хакери. Питання з кібербезпеки у пристроях IoT є досі актуальним, оскільки захистити пристрої IoT важко з різних причин. Оскільки виробники та інноватори змушені випускати нові продукти, безпеці часто надається менший пріоритет, ніж показникам часу виходу на ринок. Багато компаній також не знають про вразливі місця, які представляє IoT, і часто більше стурбовані економією коштів і зручністю, які забезпечують пристрої Інтернету речей.

Нижче наведено основні приклади того, як можуть бути здійснені атаки на пристрої Інтернету речей:

-Пристрої. Вони можуть бути основним засобом для запуску атак. Пам'ять, вбудоване програмне забезпечення, фізичний інтерфейс, веб-інтерфейс і мережеві служби – це області, де можуть виникнути вразливості. Зловмисники також можуть використовувати незахищені параметри за замовчуванням, застарілі компоненти та незахищені механізми оновлення, серед іншого.

-Канали зв'язку. Атаки на пристрої IoT можуть виникати в каналах зв'язку, які з'єднують компоненти IoT. Протоколи, що використовуються в системах Інтернету речей, можуть мати недоліки безпеки, які впливають на всю систему. Системи IoT також уразливі до добре відомих мережевих атак, таких як DoS і спуфінг(вид атаки, коли одна програма маскує себе під іншу, і таким чином збирає інформацію про користувачів).

-Програмне забезпечення та додатки. Уразливості у веб-додатках і пов’язаному програмному забезпеченні для пристроїв Інтернету речей можуть зламати системи. Веб-програми, наприклад, можна використовувати для викрадення облікових даних користувача або розповсюдження шкідливих оновлень мікропрограми.

3.3 Важливість захисту пристроїв IoT

Як було сказано мною у першому та другому розділах даної роботи, популярність та застосування пристроїв IoT росте з кожним днем, і кваліфіковані фахівці у цій сфері роблять прогнози, що кількість таких пристроїв зростає з кожним днем. З огляду на те, що Інтернет речей може створювати величезні обсяги даних, та якщо урахувати ріст їх популярності, можна сказати, що питання безпеки на цих пристроях є серйозною проблемою, оскільки раніше пристрої IoT не були такими популярними та широко застосовуваними, тому питанню з їх безпеки надавалось дуже мало уваги. Окрім початкового створення даних на окремому пристрої, дані надсилаються до централізованих систем, які збирають і зберігають їх для подальшого використання, тому користувачі повинні знати та розуміти які данні вони хочуть передавати, як вони зберігаються та ким можуть бути оброблені. Існують штрафи за недотримання правил персональних даних, які можуть становити дуже великі суми, тому важливо, щоб виробники пристроїв IoT, а також ті, хто їх використовує, розуміли та дотримувались цих правил, а також, для особистої впевненості, мали змогу проконсультуватись з юристами, щодо підходу до використання, передачі та зберігання персональних даних на пристроях IoT. Конфіденційність даних IoT має бути вбудована в ці пристрої з нуля, щоб особиста інформація залишалася в безпеці, але поки що у більшості випадків конфіденційність дуже мало забезпечена на даних пристроях.

Для підтвердження вразливості IoT пристроїв можу привести приклад досліду компанії Consumer Records. Компанія Consumer Records провела низку тестів, за допомогою яких було виявлено недоліки у безпеці даних та

конфіденційності у дверних відеодзвінках. У цілому можна сказати, що дверні відеодзвінки були розроблені для того, щоб людина мала змогу бачити всіх, хто до неї приходить, при цьому не виходячи зі свого помешкання. Це б мало надавати людині відчуття захищеності та безпеки, але будь-які камери, що підключені до мережі Інтернет, завжди підлягають до злому. Цифрова лабораторія Consumer Reports займається оцінкою цифрових продуктів та послуг, на предмет того, наскільки добре чи погано вони захищають конфіденційність і безпеку споживачів. Під час тестування найбільш критичні результати були виявлені у дверних відеодзвінках п’яти брендів, а саме:

- Eufy;
- GoControl;
- LaView;
- Netvue.

Під час тестування камери відеодзвінків компанії Eufy експертами було виявлено вразливість, яка розкриває інформацію облікового запису користувача-адресу та пароль електронної пошти, а також паролі від WiFi. Дверні відеокамери компаній GoControl та LaView теж мають вразливість, що дозволяє отримати адресу та паролі від електронної пошти користувача, а також паролі WiFi. Тестуючи камери для відеодзвінків бренду Netvue було виявлено недолік у роботі, завдяки якому хакери можуть отримати доступ до паролів користувачів і знайти адреси електронної пошти, пов’язані з обліковими записами. Пристрої проходили тестування у лабораторії, використовуючи The Digital Standard. The Digital Standard являє собою набір критеріїв із відкритим кодом для оцінки цифрових продуктів і послуг, створених CR спільно з іншими організаціями, для того, щоб проводити тести пристроїв у наявності їх безпеки, та надання конфіденційності, або ж її можливої відсутності. Маючи доступ до такої інформації, зловмисники легко та без будь-яких проблем можуть використати усю інформацію та дані з облікових записів користувачів у своїх цілях.

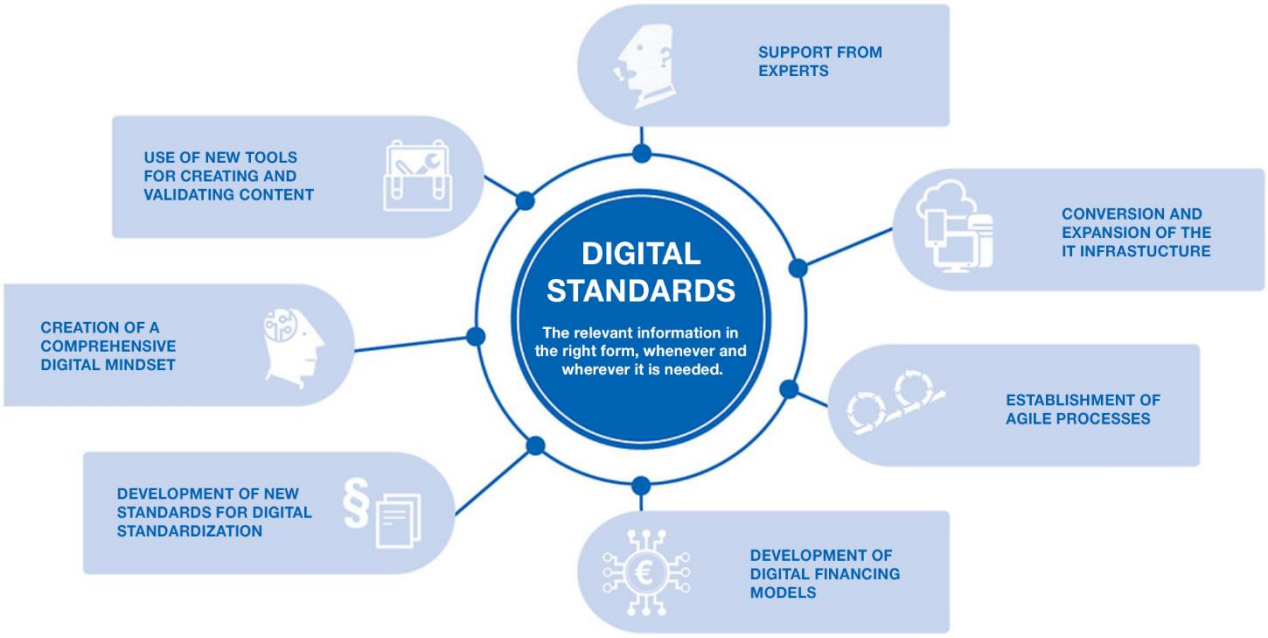

Рис. 3.2 Основні критерії The Digital Standard

Окрім цього, більшість виробників не мінімізують кількість інформації, на яку створюють запит у користувачів, а збільшують її, і при цьому не дають змогу користувачам змогу до створення копії своїх даних, або ж можливість видалити їх. Усе це дає великі можливості хакерам у викраденні та використанні даної інформації у своїх цілях. Такі недоліки у системі безпеки пристроїв можуть становити велику загрозу для користувачів, а також для великих компаній, які теж застосовують дані пристрої у своїй роботі.

Підсумовуючи усе вище сказане, хочу сказати, що аналізуючи усю надану інформацію з приводу безпеки IoT пристроїв, я вирішила розробити програму, яка надасть можливість підвищити рівень безпеки пристроїв IoT. На основі глибокого аналізу, що стосується методів захисту пристроїв IoT, можу сказати, що із зростанням впливу пристроїв Інтернету речей зростає і потенціал до отримання та здійснення неавторизованого доступу до мережі. Інші дослідження з приводу безпеки у цій сфері показують, що 98% усього трафіку пристроїв IoT є незашифрованим, що розкриває особисті та конфіденційні дані в мережі, а також дає зловмисникам можливість прослуховувати незашифрований мережевий трафік, збирати особисту чи конфіденційну інформацію, для того, щоб потім

використовувати ці дані для отримання прибутку в DarkNet (темній мережі), 51% становлять загрози для організацій охорони здоров'я, і стосуються пристроїв візуалізації, що порушує якість медичної допомоги та дозволяє зловмисникам отримати дані пацієнтів, що зберігаються на цих пристроях, 72% VLAN для охорони здоров'я поєднують IoT та IT-активи, дозволяючи зловмисному програмному забезпеченню поширюватися з комп'ютерів користувачів на вразливі пристрої IoT у тій же мережі.

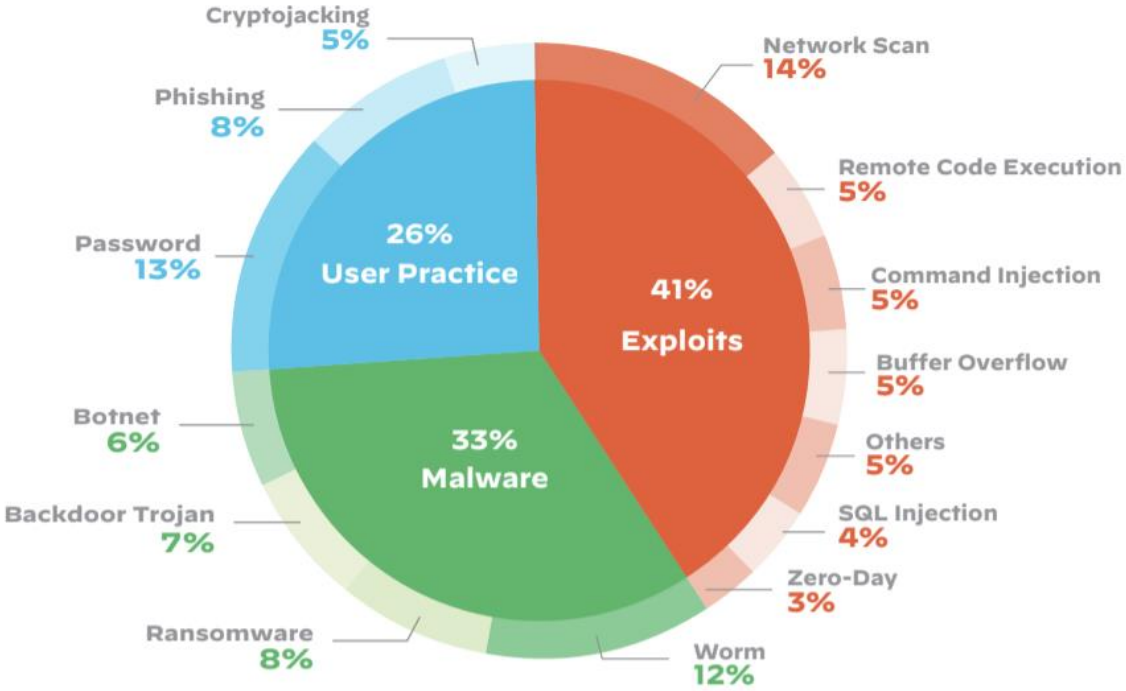

Рис 3.3. Розподіл основних загроз IoT у відсотках

Для покращення даної ситуації, я розробила програму, яка допоможе підвищити рівень безпеки пристроїв IoT. Для її реалізації я обрала мову програмування Python, оскільки ця мова є однією з нескладних мов програмування. Також я зробила вибір саме на цій мові програмування, оскільки на третьому курсі навчання ми пройшли курс з програмування мовою Python, завдяки якому я почала більше розуміти суть програмування та те, як реалізовуються програми. Python має чистий та лаконічний синтаксис, який робить його легким для вивчення, особливо для початківців, і це дозволяє швидше розвиватися в області програмування, також

ця мова програмування має великий обсяг доступність бібліотек, одна з яких була використана мною у створенні програми для IoT пристроїв.

3.4 Розробка програми мовою програмування Python

Аналізуючи усі проблеми у захисті інформації IoT пристроїв, що були детально розписані у другому розділі, я дійшла висновку що хоча б для мінімального захисту даних пристроїв необхідно розробити невеличку програмку, яка буде сканувати пристрій з метою забезпечення його коректної та безпечної роботи. Дана програма є аналогом антивірусу, але являється не такою обширною у своїй роботі. Як було сказано вище, дана програма розроблена мовою програмування Python.

```python
from bluepy.btle import Scanner, DefaultDelegate

class ScanDelegate(DefaultDelegate):
    def __init__(self):
        DefaultDelegate.__init__(self)

    def handleDiscovery(self, dev, isNewDev, isNewData):
        if isNewDev:
            print(f"Знайдено новий пристрій: {dev.addr}")
        elif isNewData:
            print(f"Нові дані від: {dev.addr}")

scanner = Scanner().withDelegate(ScanDelegate())

print("Сканування пристроїв IoT...")

devices = scanner.scan(10.0) # Сканувати протягом 10 секунд

print("Список знайдених пристроїв:")
for dev in devices:
    print(f"Пристрій {dev.addr} ({dev.addrType}), сигнал: {dev.rssi} dB")
```

Рис 3.4. Код програми

Пояснення до коду

```python
from bluepy.btle import Scanner, DefaultDelegate
```

Даний рядок імпортує певні класи та функції з модулю bluepy.btle. У цьому випадку ми імпортуємо класи Scanner та DefaultDelegate.

```
class ScanDelegate(DefaultDelegate):
    def __init__(self):
        DefaultDelegate.__init__(self)

    def handleDiscovery(self, dev, isNewDev, isNewData):
        if isNewDev:
            print(f"Знайдено новий пристрій: {dev.addr}")
        elif isNewData:
            print(f"Нові дані від: {dev.addr}")
```

Уданій частині визначається підклас ScanDelegate, який наслідується від класу DefaultDelegate. ScanDelegate містить метод handleDiscovery, який викликається при знаходженні нового пристрою або при отриманні нових даних від існуючого пристрою; у цьому методі виводиться інформація про пристрій.

scanner = Scanner().withDelegate(ScanDelegate()) - тут створюється об'єкт Scanner, який використовується для сканування пристроїв. withDelegate() встановлює метод для обробки результатів сканування.

```
print("Сканування пристроїв IoT...")
```

Даний рядок слугує для того, щоб при запуску користувач розумів що відбувається, а саме що проходить сканування його пристрою.

```
devices = scanner.scan(10.0)
```

Встановлюємо обмеження на час сканування пристрою. Десяти секунд буде достатньо для того, щоб повністю просканувати пристрій на наявність загроз.

```
print("Список знайдених пристроїв:")
for dev in devices:
    print(f"Пристрій {dev.addr} ({dev.addrType}), сигнал: {dev.rssi} dB")
```

На цьому етапі виводяться результати сканування. Проходить ітерація(повторення виконання дії для забезпечення правильного результату) по знайдених пристроях, і для кожного пристрою виводиться його MAC-адреса, тип адреси та сигнал.

Код програми:

```
from bluepy.btle import Scanner, DefaultDelegate
class ScanDelegate(DefaultDelegate):
    def __init__(self):
        DefaultDelegate.__init__(self)
  def handleDiscovery(self, dev, isNewDev, isNewData):
        if isNewDev:
            print(f"Знайдено новий пристрій: {dev.addr}")
        elif isNewData:
            print(f"Нові дані від: {dev.addr}")
scanner = Scanner().withDelegate(ScanDelegate())
print("Сканування пристроїв IoT...")
devices = scanner.scan(10.0) # Сканувати протягом 10 секунд
print("Список знайдених пристроїв:")
for dev in devices:
    print(f"Пристрій {dev.addr} ({dev.addrType}), сигнал: {dev.rssi} dB")
```

У написанні даного коду була застосована бібліотека bluepy. Дана бібліотека використовується для роботи з Bluetooth Low Energy (BLE) в середовищі Python. BLE (Bluetooth Low Energy) - це бездротова технологія зв'язку, яка призначена для низькоспоживаної енергії і розроблена спеціально для взаємодії між різними пристроями, такими як смартфони, датчики, розумні годинники, медичні пристрої та інші пристрої Інтернету речей. Вона дозволяє взаємодіяти з BLE-пристроями на різних рівнях, включаючи сканування, підключення до пристроїв, читання/запис даних, а також роботу з рекламними пакетами та характеристиками. Основні можливості bluepy включають в себе:

1.Сканування пристроїв: Ви можете сканувати навколишні пристрої BLE для виявлення доступних пристроїв.

2.Підключення до пристроїв: bluepy дозволяє здійснювати підключення до BLE-пристроїв для взаємодії з ними.

3.Читання/запис даних: Після успішного підключення до пристрою ви можете читати та записувати дані з/на характеристики пристрою.

4.Робота з рекламними пакетами: Ви можете отримувати доступ до рекламних пакетів, які передаються пристроями, і використовувати їх для ідентифікації та взаємодії.

5.Робота з характеристиками: bluepy надає інтерфейс для роботи з характеристиками пристроїв, дозволяючи зчитувати та записувати дані.

Ця бібліотека досить потужна та широко використовується в розробці програмного забезпечення для IoT-пристроїв, датчиків та інших пристроїв, які використовують BLE для бездротового зв'язку.

ВИСНОВКИ

Підсумовуючи перший розділ дипломної роботи, можна дійти до висновку, що інформація, її види та носії починала розвиватися ще дуже давно, задовго до появи перших комп'ютерів, однак методи захисту інформації з'явились набагато пізніше після розвитку самої інформації, та були дуже примітивні, або у більшості випадків їх взагалі не було. У підсумку до другого розділу можу сказати, що мною були розглянуті сучасні проблеми у сфері безпеки IoT пристроїв, які своїм прикладом підкреслюють нагальну необхідність у прийнятті заходів, спрямованих на вирішення даної проблеми. У третьому розділі мною було запропоноване рішення, що дасть змогу у певній мірі підвищити рівень безпеки пристроїв.

У цілому під час виконання даної дипломної роботи, мною було проведено дослідження на тему безпеки IoT пристроїв. З впевненістю можна сказати, що з кожним днем популярність таких пристроїв стрімко зростає. Їх широко застосовують у різних сферах бізнесу, промисловості та в повсякденному житті, оскільки пристрої IoT значно полегшують життя. Завдяки IoT людина без проблем може керувати підсистемами свого дому, лікарі можуть ефективніше проводити складні операції, навіть процес виробництва значним чином стає легшим та ефективнішим для людей, і це все завдяки IoT пристроям.

Нажаль, на відмінну від плюсів є і мінуси. Основним недоліком сфери IoT є те, що до пристроїв IoT дуже легко отримати несанкціонований доступ. Зловмисники можуть отримати доступ майже до більшості таких пристроїв, не прикладаючи до цього великих зусиль. Саме тому можна підкреслити велику необхідність у тому, що сфера IoT в цілому потребує нагальних дій, спрямованих на врегулювання та запровадження надійної системи безпеки. Ця потреба є необхідністю, та являється актуальною і зараз. IoT пристрої збирають та обробляють великі обсяги даних, і захист цих даних є критично важливим для того, щоб запобігти та унеможливити несанкціонований доступ та порушення

конфіденційності користувачів. Якщо не робити нічого з цим, то у майбутньому наслідки можуть стати фатальними.

ПЕРЕЛІК ПОСИЛАНЬ

1.Хронологія розвитку засобів і методів захисту інформації – Вікі ЦДУ. *Вікі ЦДУ*. URL: https://wiki.cusu.edu.ua/index.php/Хронологія_розвитку_засобів_і_методів_захисту_інформації (дата звернення: 30.04.2024).
2. Gartner прогнозує, що витрати на безпеку в області інтернету речей (iot) будуть стійко зростати в найближчі роки. - ITPRO.UA. *ITPRO*. URL: https://itpro.ua/post/gartner_prognoziruet_chto_raskhody_na_obespechenie_bezopasnosti_v_oblasti_interneta_veshchei_iot_budut_ustoichivo_rasti_v_blizhaishie_gody (дата звернення: 30.04.2024).
3. How to secure IoT devices in business. *Network Access & Security Solutions | NordLayer*. URL: https://nordlayer.com/blog/how-to-secure-iot-devices-in-business/?gad_source=1&gclid=Cj0KCQjwncWvBhD_ARIsAEb2HW9aCda1JZ02B- (date of access: 30.04.2024).
4. The Importance of IoT Security in a Connected World - IEEE Innovation at Work. *IEEE Innovation at Work*. URL: https://innovationatwork.ieee.org/the-importance-of-iot-security-in-a-connected-world/ (date of access: 15.05.2024).
5. The importance of iot security in a connected world - IEEE innovation at work. *IEEE Innovation at Work*. URL: https://innovationatwork.ieee.org/the-importance-of-iot-security-in-a-connected-world/ (date of access: 15.05.2024).
6. IoT security: what it is and why it's important | built in. *Built In*. URL: https://builtin.com/articles/iot-security (date of access: 15.05.2024).
7. Unit 42. 2020 unit 42 iot threat report. *Unit 42*. URL: https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (date of access: 15.05.2024).
8. Internet of Things (IoT) - Internet Society. *Internet Society*. URL: https://www.internetsociety.org/iot/?gad_source=1&gclid=CjwKCAjwupGyBhBBEiwA0UcqaD6ixToPfq0jiGwUgsKukE2OBz2-N1c3Ha6NsnI9GqHcwKDR_m_pNBoCBb4QAvD_BwE (date of access: 15.05.2024).
9. Unit 42. 2020 unit 42 iot threat report. *Unit 42*. URL: https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (date of access: 15.05.2024).
10. Kanade V. Internet of Everything: Meaning, Examples, and Uses. *Spiceworks Inc*. URL: https://www.spiceworks.com/tech/iot/articles/what-is-internet-of-everthing/ (date of access: 15.05.2024)

11. IoT Security: What It Is and Why It's Important | Built In. *Built In*. URL: https://builtin.com/articles/iot-security (date of access: 15.05.2024).
12. IoT Protocols vs IoT Standards. *Symmetry Electronics*. URL: https://www.symmetryelectronics.com/blog/iot-protocols-vs-iot-standards/ (date of access: 15.05.2024).
13. A Complete Guide to IoT Protocols & Standards In 2023. *Nabto*. URL: https://www.nabto.com/guide-iot-protocols-standards/ (date of access: 15.05.2024).
14. URL: https://www.mojix.com/internet-of-things-everyday-lives/ (дата звернення: 15.05.2024).
15. URL: https://www.ness.com/iot-is-everywhere-how-iot-is-changing-our-daily-lives (дата звернення: 15.05.2024).
16. Industrial Internet of Things Raises New Security Implications. *JPT*. URL: https://jpt.spe.org/industrial-internet-of-things-raises-new-security-implications?gad_source=1&gclid=CjwKCAjwupGyBhBBEiwA0UcqaHDQ2L9LxYe1OXyOejLN5zUs8s9frB7oq6RvLjoPACr5SW-IYPlFMBoCHYkQAvD_BwE (date of access: 15.05.2024).
17. Henke C. IoT Security: Risks, Examples, and Solutions | IoT Glossary. *emnify | IoT Solution Provider*. URL: https://www.emnify.com/iot-glossary/iot-security (date of access: 15.05.2024).
18. IoT Technologies Explained: History, Examples, Risks & Future. *Vision of Humanity*. URL: https://www.visionofhumanity.org/what-is-the-internet-of-things/ (date of access: 15.05.2024).
19. The History of IoT: How This Technology Is Evolving. *Software Development Company | Cogniteq*. URL: https://www.cogniteq.com/blog/history-iot-how-technology-evolving (date of access: 15.05.2024).
20. Technology – BOLD. *BOLD*. URL: https://bold.expert/technology/?filter-category[]=education-technology-technology&gad_source=1&gclid=CjwKCAjwupGyBhBBEiwA0UcqaKLZeawniyLJk8fsbB_FiJ0Gqh_n6DXXoLQ2P5QE62acrlCFv24DWhoC7ZEQAvD_BwE (date of access: 15.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ(ПРЕЗЕНТАЦІЯ)