МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційниї технологій
Кафедра кібербезпеки

«До захисту допущено»
Завідувач кафедри
_____ Володимир ЛЮБЧАК
(підпис) (Ім'я та ПРІЗВИЩЕ)
___ _____ 20__р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека, освітньо-професійної програми Кібербезпека
на тему: "Протоколи безпеки пристроїв Інтернету речей"

Здобувача (ки) групи КБ-01 Волошина Володимира Сергійовича
(шифр групи) (прізвище, ім'я, по батькові)

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

_____ Володимир ВОЛОШИН
(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник ст. викладач, к. п. наук, доц. Тетяна ЛАВРИК _____
(посада, науковий ступінь, вчення звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«Затверджую»
Завідувач кафедри

_____ Володимир ЛЮБЧАК
(підпис)

«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»
здобувача групи КБ-01 Волошина Володимира Сергійовича

1. Тема роботи: «Протоколи безпеки пристроїв Інтернету Речей».

затверджено наказом по СумДУ №0212-VI від 04.03.2024 р. зі змінами згідно Наказу №0566-VI від 21.05.2024 р.

2. Термін подання студентом роботи: «____» _____ 20 ___ р.

3. Вихідні дані до роботи: _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити):
1) Огляд та роль технології Інтернету речей. 2) Особливості роботи пристроїв Інтернету речей. 3) Постановка завдання. 4) Аналіз потенційних загроз безпеці в мережі IoT. 5) Ідентифікація типових атак на пристрої IoT. 6) Методи забезпечення захисту для пристроїв IoT. 7) Огляд протоколів безпеки для пристроїв IoT. 8) Проєктування топології мережі IoT. 9) Розгортання захисних механізмів. 10) Моніторинг та аналіз запропонованих заходів безпеки.
_____

5. Перелік графічного матеріалу (із зазначенням плакатів, презентацій тощо) Презентація
6. Консультанти до проекту (роботи), із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____
(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Визначення мети роботи, об’єкту і предмету дослідження		
2	Збір, систематизація й узагальнення матеріалу для використання у кваліфікаційній роботі		
3	Робота над першим та другим розділом		
4	Робота над третім розділом		
5	Оформлення текстової і графічної частини		

Здобувач вищої освіти _____ Керівник _____

(підпис) (підпис)

АНОТАЦІЯ

Кваліфікаційна робота виконана на 62 аркушах та містить 17 рисунків, 1 таблицю, 22 джерела.

Об’єкт дослідження: системи Інтернету речей та їхні компоненти, зокрема пристрої, мережі та протоколи передачі даних.

Мета роботи: аналіз сучасних протоколів безпеки для Інтернету речей, оцінка їх ефективності, а також моделювання можливих захисних механізмів з використанням інструментів Cisco Packet Tracer та протоколу MQTT.

Метод дослідження: аналітичний огляд літератури з теми безпеки IoT; порівняльний аналіз існуючих протоколів безпеки; експериментальне моделювання та тестування мережевих рішень; проєктування та розгортання захисних механізмів у середовищі Cisco Packet Tracer з використанням протоколу MQTT.

Результати роботи: визначено роль та значення IoT у сучасних інформаційних системах, зокрема його вплив на різні галузі; ідентифіковано основні загрози безпеці та типові атаки, що можуть впливати на IoT пристрої, включаючи атаки на конфіденційність, цілісність та доступність даних; проведено класифікацію та оцінку сучасних протоколів безпеки для IoT, таких як CoaP, MQTT, з точки зору їх ефективності у забезпеченні захисту від різних видів загроз; спроєктовано топологію мережі IoT та впроваджено захисні механізми у середовищі Cisco Packet Tracer, що включають використання протоколу MQTT для захисту передачі даних; проведено моніторинг та аналіз запропонованих заходів безпеки, що дозволило оцінити їх вплив на захищеність IoT систем та запропонувати рекомендації щодо їх удосконалення.

Ключові слова: Інтернет речей, IoT, протоколи безпеки, кібербезпека, Cisco Packet Tracer, MQTT, загрози безпеці, моделювання мереж.

ЗМІСТ

ВСТУП

Інтернет речей (IoT) – це технологія, що швидко розвивається і проникає в усі аспекти людського існування в сучасному світі, від промислових систем до побутових застосувань. Розробка інтелектуальних систем, які підвищують продуктивність, автоматизують процедури та покращують зручність використання багатьох гаджетів, стала можливою завдяки Інтернету речей. Але з розвитком Інтернету речей зростають і проблеми безпеки цих пристроїв. Несанкціонований доступ до даних, маніпуляції з пристроями та інші кіберзлочини є прикладами потенційних небезпек. Тема «Протоколи безпеки для Інтернету речей» була обрана тому, що необхідно проводити дослідження і створювати практичні стратегії захисту, щоб гарантувати безпеку систем і пристроїв IoT.

Об'єктом дослідження є системи Інтернету речей та всі їхні складові – пристрої, мережі та протоколи передачі даних. У фокусі дослідження – механізми безпеки, які захищають пристрої та дані в мережах Інтернету речей.

Метою кваліфікаційної роботи є аналіз сучасних протоколів безпеки для Інтернету речей, оцінка їх ефективності, а також моделювання можливих захисних механізмів з використанням інструментів Cisco Packet Tracer та протоколу MQTT.

Для досягнення цієї мети необхідно виконати наступні кроки:

1) визначити потенційні загрози безпеці пристроїв Інтернету речей, які можуть призвести до порушення доступності, конфіденційності та цілісності даних;

2) провести огляд протоколів безпеки для пристроїв IoT;

3) дослідити можливості Cisco Packet Tracer для проєктування топології мережі IoT;

4) здійснити розгортання моделі захисту з використанням протоколу безпеки для конкретних IoT-пристрїв.

У роботі буде використано Cisco Packet Tracer і протокол MQTT для моделювання потенційних механізмів безпеки, вивчення існуючих протоколів безпеки Інтернету речей, а також визначення їх переваг і недоліків.

У дослідженні будуть використані різноманітні методи дослідження, такі як експериментальне моделювання, порівняльний аналіз, аналітичні огляди літератури, а також методи створення та тестування мережевих рішень за допомогою спеціалізованого програмного забезпечення.

Робота складається з трьох розділів. Опис проблеми, атрибути пристроїв і технологічний огляд включені в перший розділ, який присвячений загальним характеристикам пристроїв IoT. Проблеми безпеки мережі IoT, аналіз загроз, стратегії виявлення та пом'якшення наслідків атак, а також короткий опис процедур безпеки розглядаються у другому розділі. У третьому розділі використовуються методи для моделювання потенційної безпеки в мережі Інтернету речей.

Тема «Протоколи безпеки Інтернету речей» є актуальною з кількох причин. Перш за все, через експоненціальне зростання кількості пристроїв Інтернету речей у всьому світі зростає кількість атак. Кожен підключений пристрій може стати точкою входу для хакерів, що загрожує не лише конкретному пристрою, але й мережі в цілому. Крім того, багато конфіденційних даних, таких як особиста інформація користувачів, медичні дані, бізнес-дані тощо, часто збираються та обробляються пристроями Інтернету речей. Щоб зберегти конфіденційність і довіру користувачів до пристроїв Інтернету речей, ці дані повинні бути захищені.

Мережі Інтернету речей стають все більш вразливими зі збільшенням кількості підключених пристроїв. Оскільки багато пристроїв Інтернету речей мають низьку обчислювальну потужність, застосування звичайних методів захисту може бути складним завданням. Це вимагає створення спеціальних методів

безпеки, які можуть ефективно захищати ці гаджети, не створюючи при цьому надмірного навантаження на них.

Неоднорідність і різноманітність пристроїв Інтернету речей - ще один важливий фактор. Їхні функції, можливості та потреби в безпеці відрізняються. Це ускладнює гарантування ефективної та універсальної безпеки в мережах IoT. Створення та впровадження надійних протоколів безпеки для Інтернету речей має важливе значення для захисту окремих пристроїв і мережі в цілому від декількох типів загроз, таких як DDoS-атаки, крадіжка даних, несанкціонований доступ та інші кіберзлочини.

Крім того, для успішного розвитку технології Інтернету речей повинні існувати стандарти і протоколи безпеки, які можна використовувати для захисту пристроїв Інтернету речей. Мережі Інтернету речей можуть стати менш ефективними і безпечними в результаті фрагментації галузі, спричиненої відсутністю таких стандартів. В результаті, щоб гарантувати надійну і безпечну роботу цих мереж в майбутньому, дослідження і розробка протоколів безпеки для IoT є не тільки доречними, але й необхідними.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (Internet of Things, IoT) – це мережа фізичних речей, які мають вбудовані технології, встановлені для того, щоб спілкуватися через Інтернет між собою та зовнішнім світом [1]. Пристрої Інтернету речей охоплюють широкий спектр категорій, від базових побутових приладів, таких як фітнес-трекери та розумні термостати, до складних промислових систем з автоматизованими виробничими лініями, датчиками та механізмами. Основними функціями цих пристроїв є збір, обробка та обмін даними. Завдяки цьому можна оптимізувати низку процесів, підвищити продуктивність і відкрити нові перспективи для бізнесу та користувачів [2].

Рисунок 1.1 - Схематичне зображення екосистеми Інтернету речей

Розвиток бездротового зв'язку, зниження вартості мікроелектроніки та збільшення обчислювальних потужностей спричиняють швидке поширення Інтернету речей. Пристрої Інтернету речей використовуються в багатьох галузях, включаючи охорону здоров'я, енергетику, транспорт, розумні міста та сільське господарство. Але ці переваги також приносять нові труднощі, особливо у сфері кібербезпеки. Ретельна стратегія і застосування сучасних методів інформаційної

безпеки необхідні для забезпечення надійного захисту даних і конфіденційності, що все частіше стає вирішальним компонентом при розробці та розгортанні рішень IoT.

1.1 Огляд та роль технології Інтернету речей

Ідея Інтернету речей полягає у використанні програмного забезпечення, вбудованих датчиків та інших технологій для підключення фізичних об'єктів до Інтернету з метою збору та обміну даними. Інтернет речей зараз розвивається швидкими темпами, дозволяючи створювати інтелектуальні системи, здатні миттєво реагувати на зміни в навколишньому середовищі. Технологія Інтернету речей докорінно змінює наше повсякденне життя та комерційну діяльність. Прикладами цього є розумні будинки, де кожен гаджет контролюється одним додатком, та промислові системи, що оптимізують виробничі процеси.

Важко переоцінити важливість технології Інтернету речей у сучасному світі. Підвищуючи продуктивність та ефективність у різних галузях, вона відкриває нові можливості для економічного зростання. У сфері охорони здоров'я носимі пристрої дають змогу дистанційно спостерігати за пацієнтами, що зменшує навантаження на медичні заклади та підвищує стандарти лікування. В енергетиці IoT допомагає створювати «розумні» електромережі, які оптимізують використання ресурсів і скорочують витрати. Відстежуючи за допомогою датчиків стан ґрунту та клімату, фермери можуть підвищити врожайність, використовуючи при цьому менше води та добрив.

Інтернет речей пропонує багато переваг, але він також створює серйозні проблеми, особливо щодо безпеки даних та конфіденційності. Зростаюча кількість взаємопов'язаних гаджетів розширює можливості для атак, роблячи їх бажаною ціллю для кіберзлочинців. Сучасні рішення для захисту даних, такі як

шифрування, автентифікація та системи виявлення вторгнень, повинні використовуватися для того, щоб оптимізувати переваги Інтернету речей та зменшити його небезпеку. Таким чином, технологія Інтернету речей відіграє подвійну роль, вдосконалюючи існуючі процедури і заохочуючи створення свіжих ідей для гарантування ефективності та безпеки в різних сферах життя.

1.2 Особливості роботи пристроїв Інтернету речей

Корисність та ефективність пристроїв Інтернету речей визначається кількома характерними особливостями. Основною характеристикою цих пристроїв є їхня здатність безперервно збирати, обробляти та надсилати дані через мережу. Це стало можливим завдяки бездротовим комунікаційним модулям, мікропроцесорам і вбудованим датчикам, які забезпечують зв'язок між пристроями та централізованими системами управління в режимі реального часу.

Автономність пристроїв Інтернету речей – одна з їхніх основних характеристик. Багато з цих гаджетів працюють на батареях або навіть мають енергозберігаючі функції, такі як процесори з низьким енергоспоживанням та оптимізовані алгоритми управління живленням. Це дозволяє їм працювати протягом тривалого періоду часу, не потребуючи постійної допомоги людини. Наприклад, розумні датчики ідеально підходять для використання у віддалених або важкодоступних районах, оскільки вони можуть працювати від кількох місяців до кількох років від однієї батареї [3]. Приклади пристроїв інтернету речей наведено в таблиці 1.2.1.

Таблиця 1.2.1 - Приклади пристроїв інтернету речей з їх можливостями.

Пристрій IoT	**Можливості**
Розумний термостат	- Регулювання температури в приміщенні відповідно до заданих параметрів

Пристрій IoT	**Можливості**
	- Можливість дистанційного керування за допомогою мобільного додатку - Взаємодія з іншими інтелектуальними гаджетами (наприклад, розумними вікнами)
Розумна лампа	- Керування світлом за допомогою голосових команд або мобільного додатку - Зміна кольору та яскравості світла - Економія енергії та автоматичне вимкнення за відсутності руху
Розумний замок	- Віддалене керування приміщенням за допомогою мобільного додатку - Можливість аутентифікації користувачів за біометричними даними (розпізнавання обличчя, відбитки пальців) - Можливість записувати та зберігати журнал входу та виходу
Розумний годинник	- Моніторинг здоров'я та фізичної активності (кроки, пульс, сон) - Сповіщення зі смартфона про дзвінки, смс та інші події - Інтегрована функція GPS та моніторингу місцезнаходження
Розумний холодильник	- Моніторинг кількості наявних у вас продуктів та інформування про те, коли потрібно купити більше - Пропозиції рецептів залежно від того, що є в наявності - За допомогою мобільного додатку дистанційний контроль температури та інших факторів
Розумна камера безпеки	- Відеомоніторинг в режимі реального часу за допомогою мобільного додатку - Автоматичні сповіщення про сумнівні дії - Хмарний запис відео для подальшого перегляду та аналізу
Розумні ваги	- Вимірюється вага та інші параметри тіла (ІМТ,

Пристрій IoT	**Можливості**
	жирова маса); - Мобільні додатки синхронізуються для моніторингу змін цих параметрів; - На основі зібраних даних надаються поради щодо здоров'я
Розумний датчик диму	- Виявлення диму та інших небезпечних газів - Інтеграція з мобільними додатками для автоматичного сповіщення про тривоги - Інтеграція з системою безпеки для автоматизованого реагування на загрози
Розумний поливальний пристрій	- Автоматичний полив рослин відповідно до заданих параметрів та метеорологічних умов - Конфігурація та дистанційне керування за допомогою мобільного додатку - Економія води та енергоефективність

Масштабованість та системна інтеграція пристроїв Інтернету речей є ще однією важливою характеристикою. Пристрої можуть легко взаємодіяти з хмарними платформами та один з одним завдяки стандартам і протоколам, таким як MQTT, CoAP і HTTP/HTTPS. Це дозволяє створювати складні екосистеми, де прийняття рішень базується на аналізі та застосуванні даних з різних джерел. Наприклад, у системах «розумного міста» інформація з датчиків стану довкілля, дорожнього руху та освітлення може бути використана для оптимізації міської інфраструктури та підвищення рівня життя мешканців.

Крім того, пристрої Інтернету речей часто підтримують бездротове оновлення програмного забезпечення (OTA). Це дозволяє адміністраторам і виробникам підтримувати безпеку та оновлення пристроїв без фізичного доступу до них. Це особливо важливо, коли йдеться про кібербезпеку, оскільки вразливості можна швидко виправити, знижуючи ймовірність того, що ними скористаються зловмисники.

Пристрої Інтернету речей, як правило, дуже гнучкі, автономні та інтегровані завдяки своїм унікальним характеристикам, що створює безліч можливостей для їх застосування як в домашніх, так і в промислових умовах.

1.3 Постановка завдання

Основна проблема полягає в тому, що пристрої Інтернету речей відкриті для різних видів атак, які можуть призвести до втрати даних, незаконного доступу та інших проблем з безпекою. Оскільки поточні процедури безпеки не завжди забезпечують достатній захист, важливо оцінювати їхню ефективність і шукати шляхи їхнього вдосконалення.

Кваліфікаційна робота має на меті дослідити проблеми безпеки, пов'язані з Інтернетом речей, вивчити поточні недоліки безпеки, дослідити можливості сучасних протоколів безпеки IoT та за допомогою симулятора змоделювати захист мережі, а також проаналізувати рішення безпеки, які були впроваджені. Для досягнення цієї мети передбачається здійснити наступні дії: проаналізувати основні ризики та загрози, пов'язані з використанням пристроїв Інтернету речей; виявити загальні вразливості в апаратному та програмному забезпеченні пристроїв Інтернету речей.

Наступним етапом буде вивчення та оцінка переваг та недоліків основних протоколів безпеки, що використовуються для захисту мереж IoT, включаючи MQTT та CoAP. Практична частина буде присвячена моделюванню безпеки мереж IoT з використанням симулятора Cisco Packet Tracer. Для захисту мережевих комунікацій передбачається створення моделі мережі IoT, налаштування пристроїв та впровадження протоколів безпеки. Щоб оцінити, наскільки добре працюють наявні механізми безпеки, особлива увага буде приділена тестуванню мережі.

Завершальним етапом роботи буде аналіз ефективності заходів безпеки, в ході якого буде проаналізовано результати моделювання, визначено переваги і недоліки впроваджених заходів безпеки, а також сформульовано пропозиції щодо посилення безпеки мереж IoT в світлі отриманих результатів. Ці завдання допоможуть нам підняти рівень безпеки в реальних сценаріях, дозволяючи оцінити сучасні протоколи безпеки, застосувати та оцінити запропоновані заходи безпеки в архітектурі мережі IoT.

2 ПРОБЛЕМИ БЕЗПЕКИ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Можливості підключених пристроїв суттєво розширюються завдяки Інтернету речей, пропонуючи користувачам численні зручності та підвищуючи ефективність низки процедур. Але ці переваги також піднімають важливі питання безпеки. Пристрої Інтернету речей приваблюють кіберзлочинців, оскільки їхня поверхня атаки збільшується паралельно з їхнім швидким зростанням. Багато пристроїв мають недостатній рівень захисту та неадекватні стандарти безпеки, що призводить до низки вразливостей, які можуть бути використані для крадіжки даних, незаконного доступу або навіть повного контролю над обладнанням.

Слабкі системи шифрування та автентифікації, нечасте оновлення програмного забезпечення та низький рівень обізнаності користувачів про можливі ризики є ключовими проблемами безпеки Інтернету речей. Наприклад, паролі за замовчуванням на багатьох пристроях часто залишаються незмінними, що полегшує хакерам завдання зловмисників. Також складно розробити єдиний план безпеки для всієї мережі Інтернету речей, оскільки різні пристрої можуть мати різний ступінь захисту через відсутність стандартних стандартів безпеки. Це особливо важливо в промислових і медичних системах, оскільки компрометування пристроїв може мати катастрофічні наслідки.

2.1 Аналіз потенційних загроз безпеці

Атаки на конфіденційність даних є однією з основних загроз. Багато пристроїв Інтернету речей збирають і обробляють великі обсяги персональної інформації, включаючи дані про місцезнаходження, звички користувачів і навіть медичні дані. Ця інформація може бути предметом крадіжки, вимагання або навіть порушення конфіденційності [4].

Атаки на цілісність пристроїв і мереж становлять значний додатковий ризик. Численні гаджети Інтернету речей використовуються в життєво важливих системах, таких як енергоменеджмент або медичне обладнання. Якщо зловмиснику вдасться порушити цілісність або навіть заволодіти таким обладнанням, це може мати катастрофічні наслідки як для життя, так і для безпеки людей.

Ще однією важливою групою атак є атаки, пов’язані з доступністю пристроїв і мереж. Деякі атаки намагаються перевантажити мережеві ресурси, внаслідок чого пристрої стають недоступними для авторизованих користувачів і спричиняють відмову в обслуговуванні (DDoS). Це може призвести до серйозних проблем у роботі бізнесу, а в критичних ситуаціях для медичного обладнання – навіть до летальних випадків.

Також не слід нехтувати і тим, що існує ризик використання гаджетів та пристроїв Інтернету речей для запуску бот-мереж або інших широкомасштабних кібератак. Потенційні масштаби цих атак зростають із поширенням пристроїв Інтернету речей, і вони здатні завдати серйозної матеріальної шкоди, а також порушувати роботу інтернет-інфраструктури.

Мережа Інтернету речей складається з різноманітних систем і пристроїв, тому вразливості можуть бути пов’язані з різноманітними її елементами. Розглянемо деякі з них.

Слабка авторизація та аутентифікація.

Однією з найпоширеніших слабких сторін мережі Інтернету речей є слабка автентифікація та авторизація, що може призвести до серйозних проблем з безпекою.

Аутентифікація: аутентифікація встановлює достовірність особи користувача або пристрою. Процедури ідентифікації можуть бути недостатньо безпечними або складними у випадку неадекватної автентифікації. Пристрої можуть, наприклад,

використовувати звичайні паролі, які ніколи не змінюються, або паролі за замовчуванням, які легко підібрати. Завдяки цьому зловмисники можуть отримати доступ до пристроїв без авторизації.

Авторизація: після успішної автентифікації авторизація контролює, які операції дозволено виконувати користувачу або пристрою. У разі слабкої авторизації доступ користувача може бути недостатньо обмеженим або взагалі відсутнім. Подібне може виникнути через використання слабких паролів, відсутність механізмів двофакторної автентифікації або вразливості програмного забезпечення, які дозволяють обхідний шлях для несанкціонованого доступу. Пристрої можуть, наприклад, мати права адміністратора за замовчуванням без можливості змінити їх або надати обмежений доступ.

Використання незахищених або застарілих протоколів зв'язку.

Безпеці мережі Інтернету речей серйозно загрожує використання застарілих або слабких протоколів зв'язку. Використання протоколів зв'язку, які не мають достатнього шифрування та захисту або мають відомі недоліки, призводить до цієї проблеми.

Наприклад, щоб гарантувати безпеку і цілісність передачі даних, деякі пристрої Інтернету речей можуть використовувати протокол HTTP без шифрування за допомогою TLS (Transport Layer Security). Це означає, що зловмисники можуть перехоплювати та змінювати дані, що надсилаються між пристроями та іншими вузлами мережі.

Крім того, існує ймовірність, що деякі комунікаційні протоколи містять відомі недоліки, які хакери можуть використати для несанкціонованого входу в систему. Наприклад, у протоколах бездротового зв'язку, таких як Bluetooth або Wi-Fi, можуть бути недоліки, що можна використати для атаки на підключені пристрої або отримання доступу до мережі.

Недостатній захист від атак на переповнення буфера.

Важливим недоліком, який дозволяє зловмисникам здійснювати різноманітні атаки на програмне забезпечення пристроїв Інтернету речей, є недостатній захист від атак на переповнення буфера. Розглянемо цю вразливість детальніше.

Атака на переповнення буфера. Коли програма отримує більше даних, ніж вона може вмістити у відведеній їй пам'яті (буфері), відбувається переповнення. Вводячи додаткові дані в буфер, поки він не переповниться, зловмисник може скористатися цією вразливістю і викликати непередбачувану поведінку програми, яка може включати виконання віддалених інструкцій, відмову в обслуговуванні або витік конфіденційних даних.

Переповнення буфера може статися за різних обставин в мережі IoT. Наприклад, програмне забезпечення, що працює на деяких споживчих пристроях IoT, може бути недостатньо захищеним від переповнення буфера через обмеженість ресурсів. Низькорівневі мови програмування, які часто використовуються в мережах IoT, також можуть бути більш вразливими до такого роду атак.

Наслідки атак на переповнення буфера: Атаки на переповнення буфера можуть мати серйозні наслідки. Вони можуть призвести до використання службових ресурсів, відмови в обслуговуванні, віддаленого виконання коду або розкриття приватної інформації. Це може означати, що зловмисник може отримати доступ до споживчих IoT-пристроїв, виконати на них небажані завдання або навіть заволодіти ними.

Нерегулярні чи неоднозначні виправлення безпеки та оновлення програмного забезпечення.

Одним із основних недоліків, який може загрожувати безпеці мережі Інтернету речей, є відсутність оновлень програмного забезпечення та виправлень

безпеки. Ця вразливість виникає через нездатність виробників пристроїв IoT оперативно пропонувати виправлення та оновлення для свого програмного забезпечення, що, в свою чергу, підвищує ймовірність вторгнень і розкриття приватних даних.

Визнані слабкі місця та потенційні небезпеки: Оскільки технології швидко розвиваються, регулярно з'являються нові вразливості в програмному забезпеченні. Це може бути результатом недостатнього тестування, помилок у програмному забезпеченні або поганої реалізації системи безпеки. Пристрої можуть залишатися відкритими для відомих атак, таких як вірусні атаки, вразливості вебдодатків та атаки мережевих протоколів, якщо виробники не випускають своєчасні оновлення для усунення цих вразливостей.

Відсутність захисту від нових загроз: Методи атак та ризики безпеки постійно розвиваються. Пристрої можуть залишатися відкритими для цих атак, якщо виробники не випускають оновлення для захисту від нових ризиків. Наприклад, щойно пристрій вийшов у вільний продаж, зловмисники можуть знайти нові способи порушити безпеку.

Витік конфіденційної інформації: Витік конфіденційної інформації може статися через вразливість програмного забезпечення. Це можуть бути фінансові дані, комерційна таємниця або особиста інформація користувача. Оновлення, які виправляють вразливості, можуть бути проігноровані постачальниками, що може призвести до серйозних проблем з безпекою та порушенням конфіденційності.

Атаки з використанням гаджетів: Кібератаки можуть здійснюватися з використанням пристроїв Інтернету речей, які залишаються вразливими через відсутність оновлень безпеки. Зловмисники можуть, наприклад, отримати контроль над вразливими пристроями і використовувати їх як частину ботнету для вчинення злочинів, таких як DDoS-атаки.

Недостатній контроль доступу до мережі IoT.

Якщо доступ до пов'язаних пристроїв і ресурсів не контролюється належним чином, існує значний ризик неналежного контролю доступу до мережевих пристроїв в мережах Інтернету речей. Ця вразливість може включати будь-яку з наступних особливостей.

Недостатня автентифікація користувачів і пристроїв. Несанкціонований доступ може статися, якщо доступ до ресурсів мережі IoT можливий без достатньо надійної автентифікації. Наприклад, безпечні паролі можуть бути відсутні або встановлені за замовчуванням, що полегшить хакерам доступ до мережі та будь-яких підключених до неї пристроїв.

Недостатнє управління правами доступу: Цілком можливо, що мережі Інтернету речей неправильно налаштовані або не мають методу управління правами доступу. Це підвищує ймовірність зловживання даними та ресурсами, оскільки користувачі та пристрої можуть мати більше прав доступу, ніж потрібно для їхньої роботи.

Недостатня сегментація мережі: Пристрої з різним ступенем довіри можуть співіснувати в одній мережі в результаті недостатньої сегментації мережі. Якщо один з пристроїв зламаний, це може дати зловмиснику можливість легко перемикатися між пристроями.

Незахищені з'єднання пристроїв: Загальна безпека мережі може бути поставлена під загрозу, якщо можуть використовуватися незахищені пристрої, оскільки можуть бути відсутні будь-які процедури перевірки безпеки для нещодавно підключених пристроїв.

Відсутність моніторингу та аудиту доступу: Менеджерам мережі може бути складно виявити та усунути порушення безпеки, якщо вони не можуть побачити незвичну активність або спроби несанкціонованого доступу до мережі.

Таким чином, вивчення можливих ризиків безпеки в Інтернеті речей дозволяє виявити різноманітні проблеми, з якими стикаються користувачі та фахівці. Для того, щоб гарантувати довгострокову безпеку Інтернету речей, необхідно створювати і впроваджувати ефективні заходи безпеки, спрямовані на протидію різноманітним ризикам і загрозам [5].

2.2 Ідентифікація типових атак на пристрої IoT

Оскільки пристрої Інтернету речей набувають все більшого поширення в багатьох сферах життя, їхня безпека має вирішальне значення. Визначення найпоширеніших атак на ці гаджети допоможе створити ефективні плани захисту та зменшити небезпеку. Нижче перераховані основні типи атак, з якими можуть зіткнутися IoT-пристрої:

1. **Шкідливе програмне забезпечення:** У сфері IoT атаки шкідливого програмного забезпечення, наприклад, з використанням бот-мереж, є одними з найпоширеніших. Використовуючи недоліки програмного забезпечення, шкідливе програмне забезпечення може проникати на пристрої і використовувати їх як частину ботнету для здійснення масованих атак, таких як DDoS (розподілена відмова в обслуговуванні). Ботнет Mirai, який використовував тисячі скомпрометованих пристроїв Інтернету речей для проведення масштабних атак на веб-сайти та сервіси, є яскравим прикладом.
2. **Атаки типу «людина посередині» (MitM):** Вони передбачають перехоплення і можливу модифікацію зловмисником зв'язку між двома пристроями Інтернету речей. Це може призвести до проникнення в систему шкідливих команд або крадіжки приватної інформації. Пристрої, які використовують незахищені або незашифровані канали зв'язку, особливо вразливі до MitM-атак.

3. **Атаки на фізичному рівні:** Ці атаки націлені на пристрої IoT шляхом фізичного втручання в їхню роботу. Прикладами такого фізичного втручання є розбирання пристрою для доступу до внутрішніх частин або впровадження шкідливого програмного забезпечення через апаратні інтерфейси. Зловмисники можуть обійти більшість програмних механізмів захисту і отримати контроль над пристроєм, якщо вони мають до нього фізичний доступ.
4. **Відмова в обслуговуванні (DoS):** Засипаючи підключені пристрої Інтернету речей занадто великою кількістю запитів, атаки на відмову в обслуговуванні намагаються вивести їх з ладу. Це може призвести до неможливості доступу до життєво важливих систем або до переривання регулярних операцій. Особливо ризикують пристрої з обмеженою обчислювальною потужністю, які не можуть ефективно обробляти велику кількість запитів.
5. **Атаки на конфіденційність даних:** Оскільки пристрої Інтернету речей збирають і обробляють величезні обсяги даних, вони є основною мішенню для атак на конфіденційність. Отримавши незаконний доступ до пристроїв або мереж користувачів, зловмисники можуть отримати конфіденційну інформацію, включаючи персональні дані. Серйозні наслідки крадіжки даних можуть включати порушення конфіденційності користувачів і порушення юридичних зобов'язань.
6. **Атаки на цілісність даних:** Зловмисники, використовуючи методи порушення цілісності даних, змінюють або підробляють інформацію, що надсилається або зберігається пристроями Інтернету речей. Це може призвести до неправильного вибору на основі сфабрикованої інформації, що особливо небезпечно для таких важливих систем, як промислові або медичні контролери.

Загалом, першим кроком у розробці надійних систем безпеки є виявлення типових загроз на пристроях Інтернету речей. Знаючи про методи і цілі зловмисників, ви можете зменшити ризики, пов'язані з використанням технології Інтернету речей, і створити більш ефективні рішення для забезпечення безпеки.

2.3 Методи забезпечення захисту для пристроїв IoT

Оскільки пристрої Інтернету речей широко використовуються в багатьох сферах життя, захист їх від потенційних загроз кібербезпеки є важливим питанням. Безпека пристроїв Інтернету речей може бути досягнута кількома фундаментальними способами, які мінімізують ризики та захищають дані.

Шифрування даних: Один з найкращих способів захистити дані - це шифрування. Щоб зробити дані нечитабельними для хакерів, використовуються криптографічні методи для перетворення інформації в зашифровану версію. Шифрування має вирішальне значення для зберігання даних на пристроях, а також для передачі даних (TLS/SSL). У разі перехоплення або фізичного доступу до пристрою це гарантує безпеку приватних даних.

Надійні системи **авторизації** (дозволів на доступ) та **автентифікації** (перевірки особи) мають важливе значення для захисту пристроїв Інтернету речей. Оскільки багатофакторна автентифікація (MFA) змушує користувачів підтверджувати свою особу за допомогою декількох незалежних методів (пароль, одноразовий код і біометричні дані), вона значно підвищує рівень безпеки. Можливість контролювати, хто і що може робити з пристроєм або даними, стає можливою завдяки авторизації.

Оновлення програмного забезпечення: Щоб підтримувати високий рівень безпеки пристроїв Інтернету речей, необхідно регулярно оновлювати програмне забезпечення. Виробники повинні надавати оновлення прошивки по повітрю

(OTA), щоб оперативно усувати знайдені вразливості та покращувати роботу пристроїв. І навпаки, користувачі повинні стежити за тим, щоб оновлення встановлювалися на регулярній основі.

Мережеві засоби захисту: Для запобігання несанкціонованому доступу та атакам на пристрої Інтернету речей використовуються такі методи мережевої безпеки, як брандмауери та системи виявлення вторгнень (IDS). У той час як системи виявлення вторгнень перевіряють дані і виявляють незвичайну активність, брандмауери обмежують доступ пристроїв тільки до дозволених джерел. Віртуальні приватні мережі, або VPN, є ще одним важливим інструментом для безпечного підключення до пристроїв, особливо коли це робиться на відстані.

Сегментація мережі: Розділивши мережу на окремі секції, можна легше стримувати атаки. Це відокремлює важливі системи від пристроїв, які скомпрометовані або менш захищені, тим самим зменшуючи вплив можливих загроз. Пристрої Інтернету речей, наприклад, можна розмістити в іншій VLAN або підмережі з обмеженим доступом до інших сегментів мережі.

Аналіз та моніторинг безпеки: Постійний аналіз та моніторинг безпеки дозволяє побачити можливі ризики та вжити негайних заходів. Виявлення аномалій та сумнівної активності, яка може вказувати на атаку, спрощується завдяки використанню аналітичних інструментів та збору логів. Щоб гарантувати швидке реагування та зменшити шкоду, необхідно створити систему сповіщення про інциденти безпеки.

Освіта та тренінги: Підвищення обізнаності персоналу та користувачів з питань кібербезпеки є важливою частиною забезпечення безпеки пристроїв Інтернету речей. Регулярні освітні та навчальні ініціативи допомагають користувачам зрозуміти основні ризики та дотримуватися найкращих практик безпеки, які включають створення надійних паролів, розумне управління доступом та виявлення фішингових атак.

Загалом, ретельна стратегія захисту пристроїв Інтернету речей може значно знизити ризики і підвищити безпеку в мережах Інтернету речей. Ця стратегія повинна включати оновлення програмного забезпечення, шифрування, автентифікацію, мережеву безпеку, сегментацію, моніторинг і навчання.

2.4 Огляд протоколів безпеки для пристроїв IoT

Для вирішення питань безпеки та зменшення ризиків розроблено кілька протоколів безпеки. Ці стандарти призначені для захисту від кіберзагроз, незаконного доступу та крадіжки даних на пристроях Інтернету речей.

У цьому розділі розглянемо деякі з найпопулярніших протоколів безпеки Інтернету речей, а також їхні переваги та недоліки.

2.4.1 Значення стандартів безпеки Інтернету речей

Процедури безпеки необхідні для захисту пристроїв Інтернету речей від онлайн-атак.

У мережі Інтернету речей існує кілька заходів безпеки для захисту конфіденційності даних. Ці заходи включають шифрування трафіку даних, використання захищених протоколів зв'язку, таких як VPN або TLS/SSL, а також належне управління доступом до пристроїв і даних. Використання захищених протоколів допомагає запобігти підслуховуванню та фальсифікації даних під час передачі, а шифрування захищає від хакерів, які розшифровують і перехоплюють інформацію. Щоб гарантувати, що доступ до конфіденційних даних матимуть лише ті, хто має на це дозвіл, важливо також встановити достатні правила доступу та автентифікації користувачів. Ці заходи допомагають підтримувати високий рівень захисту конфіденційності даних у мережі Інтернету речей і захищають їх від небажаних загроз і незаконного доступу.

Цілісність даних часто підтримується за допомогою різних методів та інструментів. Використання методів хешування, таких як SHA-256 або MD5, для створення окремого «відбитка пальця» (хешу) для кожного набору даних є однією з ключових стратегій. Згодом дані надсилаються мережею разом із цим хешем. Одержувач перевіряє, чи збігається отриманий хеш з тим, який йому надали, коли він отримує матеріал. Якщо хеші не збігаються, одержувач може відхилити дані або повідомити про це, оскільки це може свідчити про те, що дані були змінені під час передачі. Надаючи одержувачу можливість підтвердити, що дані були створені або змінені лише визнаними та схваленими джерелами, цифрові підписи або процеси цифрового підпису також можуть бути використані для гарантування автентичності та цілісності даних.

Щоб запобігти або зменшити вплив атак на відмову в обслуговуванні (DoS), мережа Інтернету речей повинна бути захищена від них за допомогою різних тактик і процедур. Це може включати використання методів виявлення атак для виявлення незвично високих обсягів трафіку або надмірного навантаження, розгортання механізмів резервного копіювання для відновлення роботи мережі в разі відмови в обслуговуванні, а також виявлення і фільтрацію небажаного трафіку на рівні мережевого обладнання. Механізми контролю доступу (ACL) також можуть використовуватися для обмеження доступу до мережевих ресурсів. Щоб запобігти DoS-атакам, які використовують відомі вразливості, також важливо регулярно оновлювати програмне забезпечення пристроїв і дотримуватися найкращих практик безпеки.

2.4.2 Типи протоколів безпеки IoT

Для того, щоб гарантувати конфіденційність, доступність і цілісність даних у мережах Інтернету речей, необхідні протоколи безпеки. *Протокол безпеки* – це

набір інструкцій, практик і стандартів, які визначають заходи захисту даних і гарантують безпечний зв'язок між різними системами або пристроями в мережі.

Методи безпеки Інтернету речей існують у різних формах, кожна з яких має свої переваги та недоліки. Розглянемо найбільш поширені методи, зокрема, протоколи безпеки.

Transport Layer Security (TLS) – криптографічний протокол, який забезпечує безпеку з'єднання. Він використовується для захисту від декількох кібератак, таких як перехоплення даних, підміна та шахрайство з особистими даними, і дозволяє забезпечити конфіденційність, цілісність та автентичність даних, які передаються між двома пристроями або додатками [6].

Нижче наведено основні характеристики та елементи TLS:

TLS захищає конфіденційність даних за допомогою симетричного та асиметричного шифрування. Асиметричне шифрування використовується для обміну ключами для симетричного шифрування, а симетричне шифрування використовується для шифрування самих даних.

Аутентифікація: Використовуючи цифрові сертифікати, TLS дозволяє сторонам підтвердити свою особу. Безпечна передача інформації може бути забезпечена завдяки тому, що клієнт і сервер підтверджують справжність сертифікатів один одного.

Цілісність даних: Завдяки TLS дані, що передаються, можна перевірити на точність. Для цього потрібно зашифрувати повідомлення за допомогою методів перевірки цілісності, таких як хеш-кодування повідомлень (HMAC).

Протоколи ключів: TLS сумісний з симетричними алгоритмами шифрування, такими як AES, RSA і протоколами обміну ключами, наприклад, Diffie-Hellman.

Підтримка версій: TLS доступний в декількох версіях, включаючи TLS 1.0, 1.1, 1.2 і 1.3. Ефективність і безпека протоколу підвищуються з кожною новою ітерацією.

Додаткові заходи безпеки: TLS має кілька функцій безпеки, включаючи захист від атак Heartbleed, обмеження на протоколи і алгоритми, які вважаються небезпечними, та інші методи запобігання вразливостей.

TLS є важливим компонентом безпеки підключених пристроїв Інтернету речей, оскільки він забезпечує зашифровану і безпечну передачу даних між пристроями і серверами, захищаючи від маніпуляцій з даними і небажаного доступу. Цей протокол широко використовується і перетворився на галузевий стандарт інтернет-безпеки.

Message Queuing Telemetry Transport (MQTT) – це розподілений, легкий, кооперативний протокол, який полегшує обмін повідомленнями між мережами пристроїв Інтернету речей. MQTT, який був створений у 1999 році та стандартизований OASIS, полегшує комунікацію між пристроями з обмеженою мережевою та обчислювальною потужністю [7].

MQTT має ряд важливих особливостей і можливостей, які дозволяють класифікувати його як протокол безпеки. По-перше, MQTT полегшує шифрування трафіку за допомогою протоколу TLS/SSL, гарантуючи безпечну передачу даних і знижуючи можливість підробки або перехоплення інформації. Крім того, MQTT поставляється з вбудованими можливостями аутентифікації користувачів, що дозволяє підтвердити особу клієнта до встановлення з'єднання. Ступінь контролю доступу в мережі також можна підвищити за допомогою MQTT, використовуючи ACL (*списки контролю доступу*), щоб обмежити доступ до певних тем або клієнтів. Завдяки всім цим можливостям MQTT є надійним та ефективним протоколом для захисту комунікацій в мережах Інтернету речей.

Нижче наведені основні атрибути та елементи MQTT:

Легкість: MQTT – це протокол з низьким енергоспоживанням, який використовує мало мережевих та комп'ютерних ресурсів. Через це він є ідеальним

варіантом для використання в малопотужних пристроях, таких як мікроконтролери або датчики.

Модель публікації та підписки (Pub/Sub): MQTT використовує модель публікації та підписки, в якій пристрої підписуються на теми і отримують повідомлення, опубліковані в цих темах. Це гарантує ефективне розповсюдження повідомлень по всій мережі.

Для управління якістю обслуговування (QoS) повідомлень, MQTT має три рівні QoS: QoS 0 (при доставці), QoS 1 (забезпечити доставку принаймні один раз) і QoS 2 (гарантувати доставку точно один раз). Це дозволяє налаштувати рівень надійності доставки повідомлень відповідно до потреб програми.

Спрощені дозволи та автентифікація: Щоб гарантувати безпечне з'єднання між пристроями, MQTT може використовувати ряд методів автентифікації, включаючи цифрові сертифікати або імена користувачів і паролі.

Підтримка постійного з'єднання: MQTT забезпечує надійну доставку повідомлень, дозволяючи зв'язатися з брокером навіть у випадку перезавантаження пристрою або зміни стану мережі.

Розширення на рівні протоколу: Власні розширення для MQTT дозволяють впроваджувати нові функції для задоволення конкретних вимог додатків.

Мережі IoT значною мірою покладаються на протокол MQTT, оскільки він робить обмін даними між пристроями надійним та ефективним. Завдяки своїй універсальності, невеликій вазі та підтримці різних рівнів QoS, він є популярним варіантом для різних застосувань, від промислових IoT-рішень до систем домашньої автоматизації [8].

CoAP (Constrained Application Protocol) – це швидкий і ефективний протокол, який дозволяє обмеженим пристроям в мережах Інтернету речей спілкуватися один з одним. CoAP оптимізований для використання в пристроях з обмеженими ресурсами, таких як датчики, мікроконтролери та інші пристрої

Інтернету речей. Він був розроблений як альтернатива HTTP для мереж з обмеженими ресурсами [9].

В контексті його відомих можливостей і корисності, CoAP, незважаючи на те, що в основному використовується для обміну даними в обмежених пристроях і мережах IoT, може розглядатися як протокол безпеки. Протокол DTLS (Datagram Transport Layer Security), який забезпечує шифрування та безпечний зв'язок між пристроями IoT, підтримується CoAP за замовчуванням. Крім того, CoAP постачається з інтегрованими механізмами авторизації та автентифікації, які дозволяють контролювати доступ користувачів до ресурсів і підтверджувати їхні особи. Завдяки цим функціям CoAP є практичним і зручним методом для створення безпечних мереж Інтернету речей.

Нижче наведено важливі елементи та аспекти протоколу CoAP:

Ефективність та портативність: CoAP був створений для зменшення використання мережевих ресурсів та обсягу передачі даних. Для ефективної передачі даних він використовує двійковий формат повідомлень і протокол UDP, який має менші накладні витрати, ніж TCP.

Зручність використання: Базовий REST-подібний інтерфейс CoAP простий у розумінні та використанні. Той факт, що він підтримує HTTP-подібні операції, такі як GET, POST, PUT і DELETE, полегшує взаємодію з мережевими пристроями та ресурсами.

Підтримка безпеки: Для захисту CoAP можна використовувати Datagram Transport Layer Security (DTLS), який пропонує шифрування даних і аутентифікацію через UDP. Це сприяє захисту цілісності та конфіденційності даних в Інтернеті речей.

Підтримка протоколів поверхневого контролю доступу (також відома як підтримка проксі-серверів): CoAP підтримує проксі-сервери, які використовуються

для обробки запитів від пристроїв, заблокованих від мережі брандмауерами або іншими бар'єрами.

Управління ресурсами: Використовуючи простий GET-запит, інші пристрої можуть отримати доступ до ресурсів пристрою, дозволивши йому повідомити про свої ресурси та стан через CoAP.

Підтримка низького енергоспоживання та режиму сну: CoAP пропонує такі функції, як періодичність передачі даних, сплячий режим та ефективний обмін даними, які допомагають пристроям споживати менше енергії.

Оскільки він пропонує прості та ефективні засоби обміну даними між обмеженими пристроями, протокол CoAP є важливим компонентом мереж Інтернету речей. Від промислових мереж до систем домашньої автоматизації - простота використання, портативність і підтримка безпеки роблять його популярним варіантом для використання в широкому спектрі додатків Інтернету речей [10].

Zigbee Security – це важливий компонент мережевої технології Zigbee, який використовується в бездротових мережах Інтернету речей, щоб гарантувати доступність, конфіденційність і цілісність даних. Протокол безпеки Zigbee спеціально розроблений для пристроїв з низьким споживанням ресурсів, таких як комутатори, датчики та інші інтелектуальні пристрої. Він використовує ряд захисних механізмів для захисту від різних типів кібератак [11].

Нижче наведено основні елементи та характеристики протоколу безпеки Zigbee:

Симетричне шифрування використовується протоколом безпеки Zigbee для захисту передачі даних між підключеними пристроями. Дані шифруються і розшифровуються за допомогою унікального ключа шифрування, який надсилається кожному пристрою.

Аутентифікація: Кожному пристрою, підключеному до мережі, надається унікальний ідентифікатор і ключ автентифікації, які дозволяють йому автентифікуватися для інших підключених пристроїв. Це запобігає спробам підміни та незаконному доступу до мережі.

Контроль доступу: Протокол безпеки Zigbee включає в себе методи управління доступом до мережі, такі як можливість використання списків контролю доступу (ACL) для обмеження доступу до певних пристроїв.

Внутрішній брандмауер: Внутрішній брандмауер, який фільтрує мережевий трафік і запобігає спробам несанкціонованих пакетів приєднатися до мережі, може бути частиною протоколу безпеки Zigbee.

Підтримка рівнів безпеки: Залежно від потреб конкретної мережі, протокол безпеки Zigbee забезпечує різні рівні безпеки. Це дозволяє адаптувати рівень безпеки до конкретних вимог вашої програми.

Протокол безпеки Zigbee здатний як виявляти, так і запобігати широкому спектру атак, включаючи атаки перевантаження і перехоплення трафіку.

Протокол безпеки Zigbee забезпечує надійний та ефективний захист від кібератак, що робить його ключовим компонентом бездротових мереж Інтернету речей. Його спеціально створені функції безпеки допомагають гарантувати доступність, конфіденційність і цілісність даних в мережі - все це важливо для безпечної роботи систем Інтернету речей і розумних пристроїв [12].

Безпека Bluetooth Low Energy (BLE) – це важливий компонент безпеки мережі Інтернету речей, оскільки BLE забезпечує бездротовий зв'язок між багатьма типами пристроїв IoT, включаючи датчики, мініатюрні пристрої для відстеження та розумні домашні прилади. Однак підтримка безпеки стає складною через обмежену обчислювальну потужність та енергоефективність пристроїв з підтримкою BLE [13].

Серед основних функцій безпеки протоколу Bluetooth Low Energy (BLE) в контексті Інтернету речей можна виділити наступні:

Шифрування з'єднань: BLE включає функції, які гарантують безпеку даних, що передаються між пристроями. Це захищає від перехоплення критично важливої інформації та гарантує конфіденційність даних.

Аутентифікація: Перед встановленням з'єднання пристрої можуть бути перевірені за допомогою BLE. Таким чином, пристрої мережі перевіряються на автентичність, а нелегальні пристрої не підключаються.

Контроль доступу: BLE може використовувати такі функції, як захищений паролем доступ до пристрою, авторизація на рівні сервісів і функцій, а також обмеження на підключення.

Виявлення та захист від атак: BLE здатний виявляти та запобігати широкому спектру загроз, включаючи атаки з перебором паролів, переповнення буферів, атаки з перехопленням даних тощо.

Заходи безпеки на рівні протоколу: BLE постачається з вбудованими механізмами безпеки на рівні протоколу, які дозволяють керувати та обмежувати доступ до пристроїв і сервісів.

Оновлення програмного забезпечення: Пристрої, які використовують Bluetooth Low Energy (BLE), можуть пропонувати процеси оновлення програмного забезпечення через бездротове з'єднання, щоб зменшити вразливості, пов'язані з програмним забезпеченням [14].

Мережа Інтернету речей, яка використовує протокол BLE, може бути більш надійною і безпечною за допомогою всіх цих заходів безпеки. Оскільки BLE широко використовується в багатьох різних додатках Інтернету речей, вкрай важливо враховувати ці фактори безпеки, щоб переконатися, що пристрої та дані в мережі знаходяться в безпеці [15].

Окрім забезпечення конфіденційності, цілісності та доступності даних, такі протоколи безпеки, як Transport Layer Security (TLS), Message Queuing Telemetry Transport (MQTT), CoAP (Constrained Application Protocol), Zigbee Security та Bluetooth Low Energy (BLE) використовуються для аутентифікації, авторизації та контролю доступу до пристроїв IoT.

Створення надійних і безпечних мереж Інтернету речей вимагає впровадження відповідних протоколів безпеки. Для підтримки безпеки і конфіденційності в мережах Інтернету речей вкрай важливо проводити дослідження і впроваджувати ефективні заходи безпеки, враховуючи швидкий розвиток технологій і загроз кібербезпеки.

3 МОДЕЛЮВАННЯ МОЖЛИВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ В МЕРЕЖІ ІОТ

Для забезпечення надійного захисту мереж Інтернету речей практичне моделювання можливих сценаріїв так само важливе, як і теоретичне розуміння ризиків і методів захисту. За допомогою симуляції можна створити віртуальне середовище, в якому можна протестувати різні заходи безпеки, оцінити їх ефективність і знайти потенційні слабкі місця. З огляду на різноманітність пристроїв Інтернету речей і сфер їх використання, які включають як домашні, так і критично важливі інфраструктурні системи, це має особливо важливе значення.

Для того, щоб побудувати безпечну і непроникну інфраструктуру, необхідно визначити основні цілі та методи моделювання безпеки IoT. При моделюванні аналізуються поточні ризики, створюються потенційні сценарії атак і впроваджуються відповідні рішення для забезпечення безпеки, такі як шифрування даних, аутентифікація користувачів, сегментація мережі та моніторинг безпеки. Використовуючи цей метод, ви можете розробити моделі безпеки, які здатні як захистити пристрої Інтернету речей від відомих небезпек, так і підготувати їх до непередбачуваних атак.

Одним із інструментів, що доречно використати при моделюванні мережі IoT, є кросплатформний інструмент візуального моделювання Cisco Packet Tracer. Почнемо з того, що це безпечний і регульований метод тестування різних ситуацій без загрози для реальних мереж і пристроїв. У симуляторі проблеми з конфігурацією або налаштуванням можна безпечно виявити і виправити, але в реальному світі вони можуть мати катастрофічні наслідки. По-друге, не вимагаючи дорогого обладнання, симулятори забезпечують гнучкість експериментів, дозволяючи швидко змінювати характеристики мережі та випробовувати різні тактики. По-третє, використання симуляторів допомагає краще зрозуміти, як

працюють мережі та пристрої, що має вирішальне значення для створення ефективних систем захисту. Через це симулятори є життєво важливим ресурсом для досліджень та навчання в галузі кібербезпеки.

3.1 Проєктування топології мережі IoT

Щоб гарантувати надійність і безпеку пристроїв і даних в мережі IoT, необхідно створити ефективну і безпечну топологію мережі Інтернету речей. У цьому розділі ми розглянемо як використовувати програмне забезпечення Cisco Packet Tracer, яке пропонує практичні інструменти для моделювання мережі та експериментів з конфігурацією для створення топології мережі Інтернету речей.

Програмне забезпечення для моделювання мереж Cisco Packet Tracer було створено компанією Cisco Systems [16]. Створюючи віртуальні мережеві середовища, воно дозволяє викладачам, інженерам та студентам ефективно вивчати та практикувати мережеві концепції. Не вимагаючи реального обладнання, Packet Tracer дозволяє проектувати, налаштовувати і тестувати широкий спектр мережевих налаштувань.

Зокрема, Packet Tracer дозволяє імітувати мережі Інтернету речей та експериментувати з різними пристроями, протоколами і топологіями. Платформа полегшує конфігурацію віртуальних пристроїв Інтернету речей, включаючи датчики, мікроконтролери, шлюзи та інші, і дозволяє керувати їх мережевими з'єднаннями та взаємодією. Крім того, Packet Tracer пропонує кілька інструментів для моделювання мережевої безпеки, що дозволяє досліджувати і вдосконалювати методи захисту в мережах Інтернету речей.

Крок 1: Визначення, що потрібно

Визначення вимог і потреб для мережі Інтернету речей – це перший етап. Це передбачає прийняття рішення про типи пристроїв, які будуть підключені до

мережі, а також про передачу інформації, швидкість передачі даних, вимоги до безпеки та інші елементи.

Крок 2: Вибір гаджетів і технологій

Пристрої та технології для мережі обираються залежно від потреб. Це можуть бути різні види шлюзів, контролерів, датчиків та інших пристроїв Інтернету речей.

Крок 3: Вибір топології мережі

На цьому етапі обираємо найкращу топологію мережі, щоб задовольнити вимоги проєкту і гарантувати ефективне підключення пристроїв. Мережі IoT зазвичай використовують комірчасту, зіркоподібну або деревоподібну топологію [17].

Крок 4: Налаштування інфраструктури та пристроїв

На цьому етапі відбувається сертифікація фізичного розташування пристроїв та мережевої інфраструктури. Це передбачає розташування комутаторів, маршрутизаторів, шлюзів, датчиків та інших пристроїв відповідно до їхніх функціональних вимог і вимог до зв'язку.

Змоделюємо наступний сценарій для домашньої мережі Інтернету речей: власник хоче створити мережу, яка дозволить йому використовувати різні пристрої Інтернету речей для управління освітленням, температурою і станом безпеки в будинку.

Визначення потреб: Власник хоче мати можливість використовувати термостат для регулювання температури, дистанційно керувати світлом у різних кімнатах та отримувати сповіщення про відчинення дверей чи вікна.

Вибір пристроїв і технологій: Для управління всіма цими пристроями в даній ситуації можна використовувати ноутбук, датчики дверей/вікон, розумні термостати та розумне освітлення.

Вибір топології мережі: Ми налаштовуємо домашню мережу, тому ми обираємо топологію "зірка", в якій кожен розумний пристрій підключений

безпосередньо до центральної точки доступу, яка підключена до роутера, що забезпечує доступ до Інтернету. Для симуляції даної мережі буде використано Cisco Packet Tracer, схема топології зображена на рис. 3.1.1.

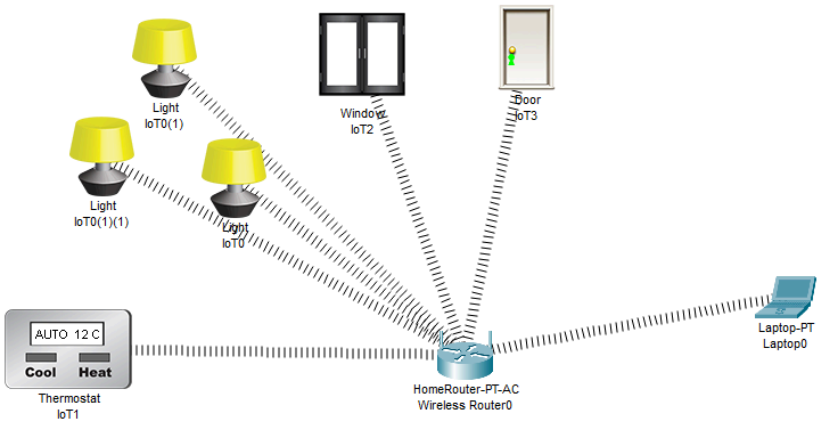

Рисунок 3.1.1 – Топологія домашньої мережі IoT

Інфраструктура та розташування пристроїв: дверні/віконні датчики встановлені на вікнах та дверях, розумні термостати розташовані в основній зоні, панелі управління встановлені на стінах коридору, а розумні лампочки розташовані в кімнатах. Обрані пристрої показані на рис. 3.1.2 - 3.1.5.

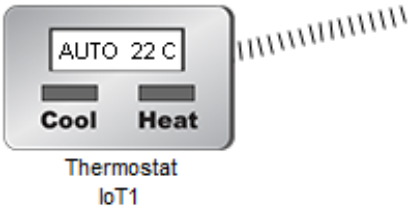

Рисунок 3.1.2 – Термостат

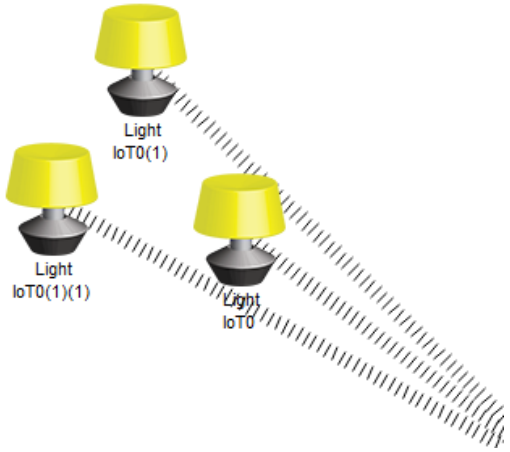

Рисунок 3.1.3 – “Розумні” лампи

Рисунок 3.1.4 – Вікно з дистанційним відкриттям

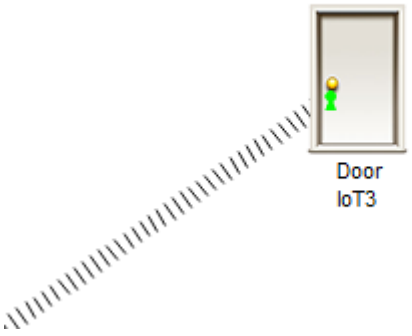

Рисунок 3.1.5 – Двері з дистанційним замком

Для виконання практичної частини роботи, описаної в розділі, було використано програмне забезпечення Cisco Packet Tracer. Спочатку були визначені типи пристроїв, які будуть включені в мережу IoT, а також вимоги до них. Після цього було обрано відповідне обладнання та програмне забезпечення для введення мережі в експлуатацію. Побудовано топологію мережі, обрано розміщення пристроїв та налаштовано параметри зв'язку за допомогою Packet Tracer.

3.2 Розгортання захисних механізмів

Для того, щоб підтримувати безпеку і захищатися від кібератак, мережа Інтернету речей повинна впроваджувати механізми безпеки. У цій частині розглянемо потенційні засоби захисту з використанням протоколу MQTT, застосовуючи програмне середовище Cisco Packet Tracer.

Для Інтернету речей протокол MQTT є одним із кращих варіантів, завдяки цьому ефективному та легкому протоколу, який передає дані між пристроями, споживаючи при цьому мінімально можливу кількість мережевих ресурсів. Його низька вартість використання ресурсів та оптимізація для контекстів з обмеженою пропускною здатністю є особливо важливими для пристроїв з обмеженими можливостями. MQTT є зручним варіантом для багатьох сценаріїв мережевих додатків IoT, оскільки він пропонує надійну доставку повідомлень через механізм QoS (Quality of Service) і дозволяє гнучко вибирати топологію мережі [18].

Протокол MQTT має важливе значення для мережевої архітектури Інтернету речей, оскільки він дозволяє пристроям взаємодіяти один з одним. Клієнти та MQTT-брокер є частиною цієї мережі. Як посередник, брокер MQTT приймає повідомлення від клієнтів і пересилає їх потрібним сторонам. Передача повідомлень і управління підпискою також знаходиться в його компетенції. Клієнтами MQTT можуть бути пристрої Інтернету речей або додатки, які

взаємодіють з цими пристроями. За допомогою певних тем вони встановлюють зв'язок з брокером і обмінюються повідомленнями. Кожен клієнт може бути абонентом, який отримує повідомлення, або видавцем, який їх надсилає.

Протокол MQTT став популярним варіантом для побудови мереж IoT, де необхідна низька затримка і надійна доставка повідомлень, завдяки своїй простій структурі, ефективному транспортуванню даних і можливості забезпечення захисту.

Створення мережі, встановлення брокера MQTT та налаштування з'єднань клієнтів з використанням IP-адрес і портів відповідно до параметрів брокера – це кроки, пов'язані з використанням MQTT в Cisco Packet Tracer. У мережі Інтернету речей клієнти можуть спілкуватися один з одним і з пристроями, надсилаючи та отримуючи повідомлення, які публікуються в темах брокера.

Спершу необхідно розробити механізм аутентифікації. У мережі Інтернету речей автентифікація необхідна для підтвердження особи користувачів і пристроїв. Це дає змогу контролювати, хто має доступ до мережевих ресурсів, а також захищає від потенційних атак і несанкціонованого доступу. Без автентифікації пристрої можуть легко стати мішенню для хакерів, порушити цілісність системи, викрити конфіденційні дані та мати інші серйозні наслідки для безпеки Інтернету речей.

Для імплементації механізму аутентифікації зробимо наступне:

- Використаємо паролі та ідентифікатори для клієнтів MQTT.
- Налаштуємо список дозволених клієнтів MQTT-брокера, щоб обмежити доступ до мережі несанкціонованих користувачів.

За допомогою MQTT Broker, який встановлений на ноутбуці ми маємо можливість додати пристрої до мережі IoT. Через це, підключатись потрібно виключно за допомогою визначеного логіну та паролю, що унеможливить

неавторизоване підключення. Спосіб додавання пристрою для авторизації показано на рис. 3.2.1.

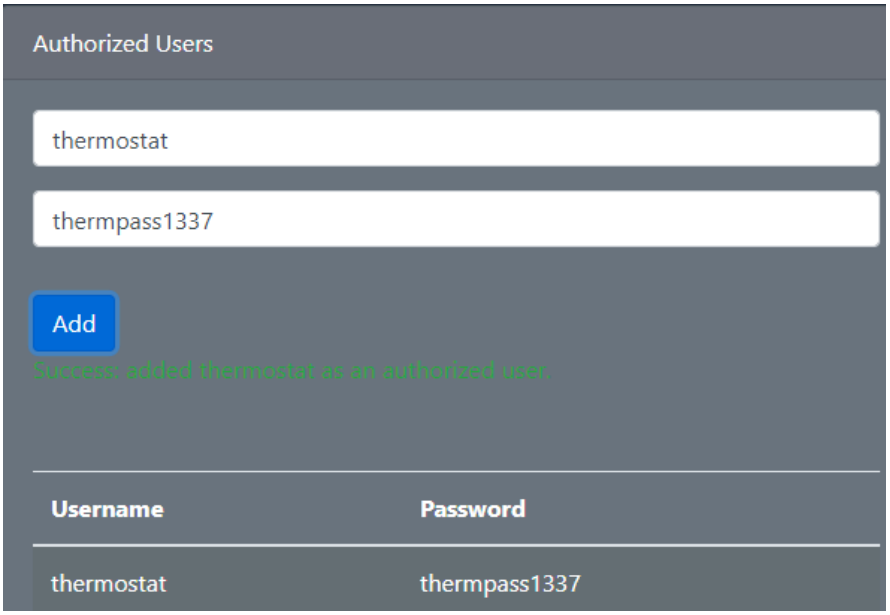

Рисунок 3.2.1 – Додавання пристрою з логіном і паролем для авторизації

Для авторизації пристрою необхідно використати MQTT Client. При підключенні вказуємо раніше визначені логін та пароль, а також адресу MQTT Broker, у нашому випадку – 192.168.0.112 (рис. 3.2.2).

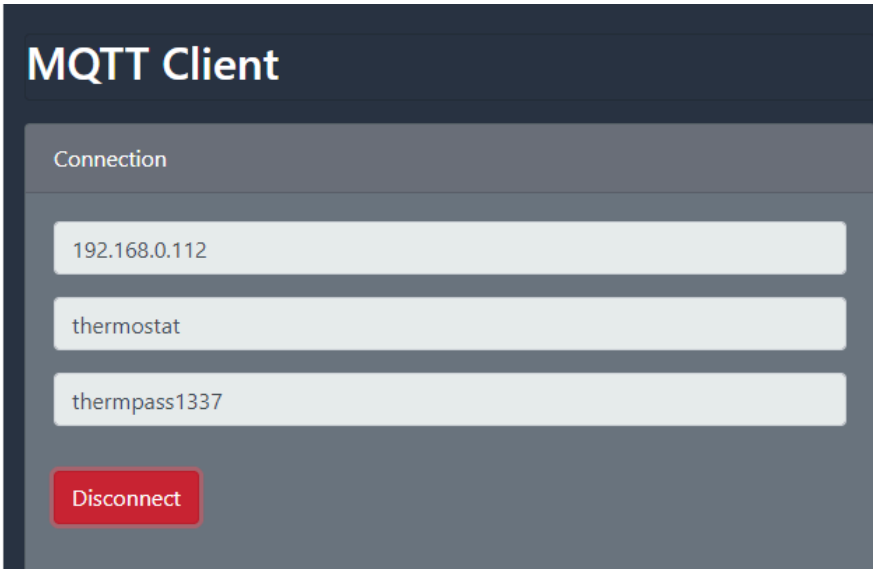

Рисунок 3.2.2 – Авторизація пристрою за допомогою MQTT Client

Після цього ми маємо можливість побачити всі підключення клієнтів в MQTT Broker (рис. 3.2.3).

Рисунок 3.2.3 – Список підключених пристроїв IoT

Логування в MQTT Broker дозволяє контролювати всі події, які відбуваються в мережі IoT. На рис. 3.2.4 показано додавання пристрою, його авторизацію. Ефективність та безпека мережі Інтернету речей значно підвищується завдяки логуванню MQTT. Це дозволяє відстежувати та вивчати повідомлення, події та мережеву активність, що допомагає виявляти аномалії, вторгнення та небезпечні обставини. Журнали можна використовувати для гарантування відповідності нормативним вимогам, проведення аудитів безпеки та відновлення попередніх станів мережі. Вони також можуть бути використані для виявлення та виправлення проблем [19].

Рисунок 3.2.4 – Приклад логування в MQTT Broker

Для гарного забезпечення захисту мережі IoT можна використовувати списки контролю доступу (Access Control List, ACL) та файрволи.

Для обмеження трафіку між клієнтами та брокером MQTT можна налаштувати списки доступу на комутаторах або маршрутизаторах за допомогою Cisco Packet Tracer. Для цього використовується функціонал списку контролю доступу (ACL) [20]. Можна створити список ACL, який фільтрує IP-адреси та порти, які можуть зв'язуватися з брокером MQTT, а потім призначити його вхідному або вихідному інтерфейсу маршрутизатора або комутатора, через який буде проходити трафік, що надходить до брокера MQTT.

На мережевому пристрої, такому як маршрутизатор або комутатор, список контролю доступу (ACL) – це набір правил, які визначають, який трафік є дозволеним або забороненим. Пакети даних, які проходять через мережевий пристрій, фільтруються за допомогою ACL, який потім визначає, як обробляти відфільтровані пакети.

Під час роботи ACL пакети даних перевіряються на відповідність вимогам, викладеним у правилах ACL, щоб переконатися, що вони відповідають вимогам, викладеним у правилах ACL. Пакету надається певна дія, наприклад, можливість пропустити або заблокувати, якщо він задовольняє вимогам одного з правил. Основою для правил ACL можуть слугувати численні характеристики, зокрема IP-адреси джерела та призначення, номери портів, протоколи та інші змінні, які можна використовувати для класифікації трафіку.

До вхідних або вихідних інтерфейсів маршрутизатора або комутатора можуть застосовуватися списки ACL. Наприклад, ACL на вхідному інтерфейсі маршрутизатора може обмежувати доступ до мережевих ресурсів, блокуючи пакети з певних IP-адрес, тоді як ACL на вихідному інтерфейсі може керувати трафіком, що виходить з мережі. Використання правильно встановлених списків

ACL може допомогти максимізувати продуктивність мережі та гарантувати її безпеку. Основою для правил ACL можуть слугувати численні характеристики, зокрема IP-адреси джерела та призначення, номери портів, протоколи та інші змінні, які можна використовувати для класифікації трафіку. Це дозволить обмежити пристрої або сегменти мережі, які мають доступ до брокера.

У Cisco Packet Tracer є можливість омбеження доступу до мережі за допомогою налаштувань роутеру (рис. 3.2.5).

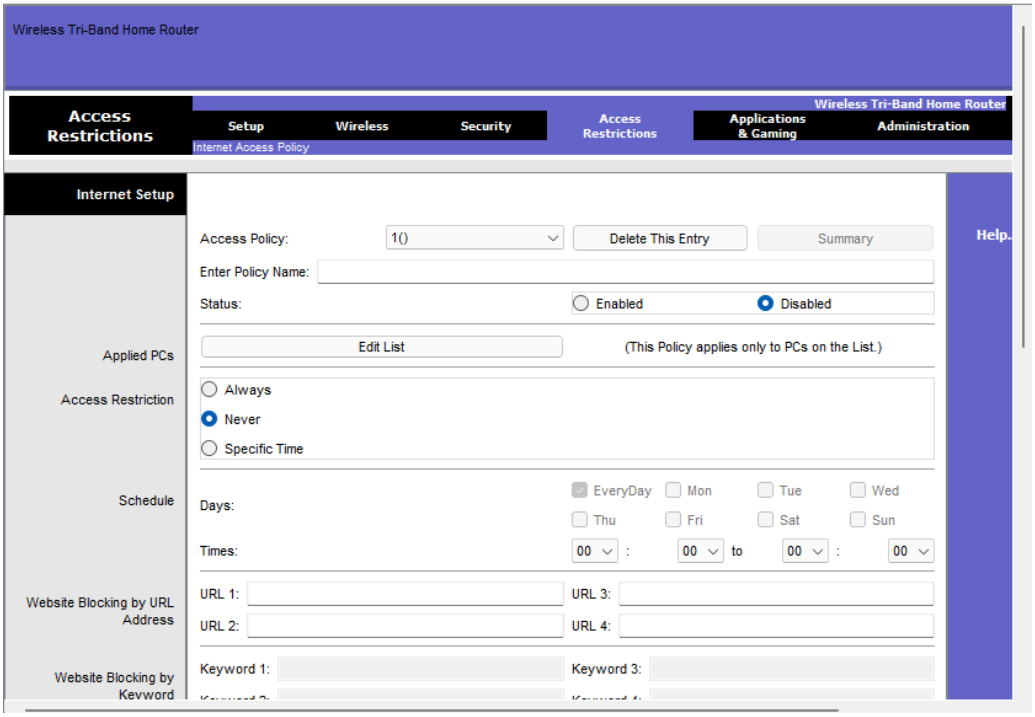

Рисунок 3.2.5 - Внесення обмежень в мережу

Що стосується використання емуляторів мережевих пристроїв у якості брандмауера для фільтрації трафіку та запобігання несанкціонованим з'єднанням, Packet Tracer пропонує кілька емуляторів. Такий пристрій можна додати до мережі і налаштувати правила брандмауера для запобігання трафіку з та на певні IP-адреси або порти, включно з брокером MQTT [21].

У мережі Інтернету речей брандмауери слугують захисним бар'єром, який регулює потік трафіку між підключеними пристроями. Вони використовують

заздалегідь встановлені правила і стандарти безпеки для фільтрації вхідних і вихідних повідомлень. Відстежуючи і запобігаючи трафіку з певних IP-адрес, портів, протоколів або інших критеріїв, брандмауери дозволяють обмежити доступ до мережевих ресурсів і захистити їх від вторгнень і атак.

Брандмауери в мережі Інтернету речей можуть бути встановлені безпосередньо на пристроях або на межі мережі. Вони діють як початкова лінія захисту від онлайн-атак та інших зовнішніх небезпек. Для регулювання зв'язку між різними сегментами мережі брандмауери також можуть використовуватися для поділу мережевих зон і встановлення зон доступу. Для підтримки безпеки і захисту мережевих пристроїв і даних від потенційних загроз і атак розгортання брандмауерів має вирішальне значення в мережах Інтернету речей.

В Cisco Packet Tracer є можливість додавання фаєрволу, за допомогою окремого серверу (рис. 3.2.6). Після його додавання можна створити правила, згідно яких буде працювати брандмауер (рис. 3.2.7).

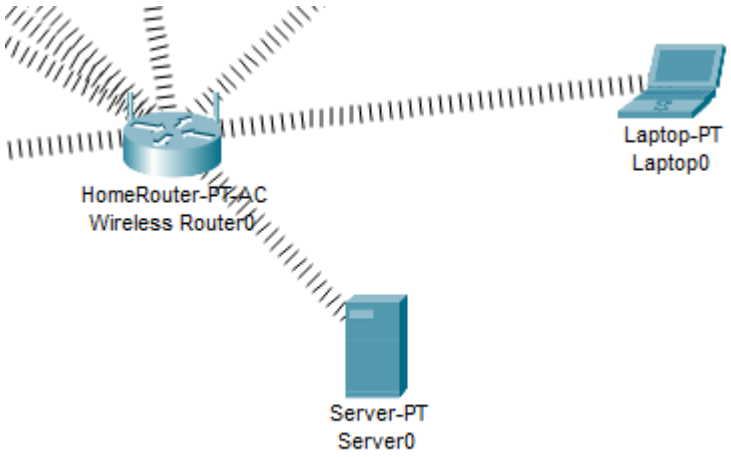

Рисунок 3.2.6 - Додавання окремого серверу для використання фаєрволу

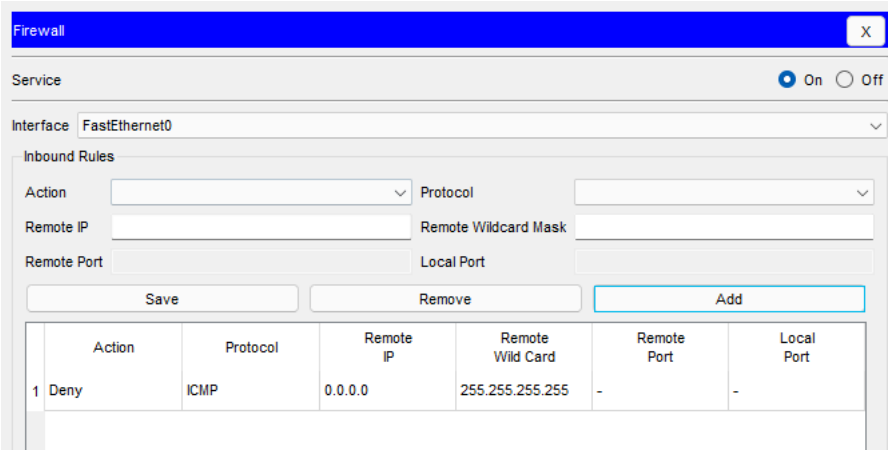

Рисунок 3.2.7 - Налаштування правиль фаєрволу на окремому сервері

Таким чином, можна зменшити ймовірність несанкціонованих підключень або атак на MQTT-брокер і сприяти підтримці мережевої безпеки.

Також можливе покращення захисту повідомлень за допомогою сторонніх алгоритмів шифрування.

Методи шифрування та автентифікації, інтегровані в самі пристрої IoT, можуть бути використані для поєднання протоколу MQTT з алгоритмами шифрування ASCON і Grain128-AEAD. Алгоритми ASCON і Grain128-AEAD спочатку повинні бути застосовані на клієнтських пристроях, які взаємодіють з брокером MQTT. Потім дані повинні бути зашифровані на пристрої-відправнику за допомогою методів шифрування ASCON або Grain128-AEAD, а потім розшифровані за допомогою тієї ж техніки на пристрої-одержувачі, перш ніж відправляти повідомлення через MQTT.

Конфіденційність, цілісність і автентичність даних, що передаються між пристроями і системами, захищаються в мережі Інтернету речей за допомогою методів шифрування. Ці методи ґрунтуються на математичних процесах для перетворення вихідних даних у зашифрований формат, для розшифрування якого потрібен правильний ключ.

У мережі Інтернету речей використовуються численні методи шифрування, включаючи AES, RSA, ECC (*криптографія еліптичних кривих*) та інші. Кожен з цих алгоритмів має унікальні характеристики та налаштування, які впливають на ступінь безпеки та ефективність шифрування.

Дані спочатку шифруються за допомогою обраного алгоритму шифрування та ключа шифрування перед передачею через мережу IoT. Той самий метод і ключ використовуються для дешифрування даних, коли вони потрапляють до одержувача. Шифрування захищає від незаконного доступу та перехоплення інформації, а також допомагає зберегти таємницю даних, що передаються мережею.

Щоб запобігти можливості маніпуляції або зміни повідомлень, алгоритми можуть також використовуватися для перевірки цілісності даних та автентифікації. Також важливо враховувати ключі шифрування та автентифікації, які мають бути надійно збережені та розподілені між пристроями, не будучи заздалегідь відомими хакерам. Таким чином, можна безпечно використовувати протокол MQTT, розмістивши ці алгоритми всередині IoT-пристроїв.

Результати роботи за темою «Analysis of NIST Lightweight Cryptographic Algorithms Performance in IoT Security Environments based on MQTT» автор роботи у співавторстві з професором Університету м. Брандон (Канада) Г. Срівставом висвітлив у науковій публікації [22]. Для того, щоб захистити пристрої Інтернету речей, в ній пропонується ретельний аналіз ефективності легких криптографічних алгоритмів, запропонованих Національним інститутом стандартів і технологій (NIST). Ці алгоритми розроблені для роботи в умовах обмежених ресурсів, які є загальними для багатьох пристроїв Інтернету речей. Враховуючи обмеженість обчислювальних потужностей, пам'яті та енергоспоживання цих гаджетів, вибір ефективних криптографічних методів має важливе значення для гарантування їхньої безпеки без шкоди для функціональності.

По-друге, одним з найпопулярніших протоколів для обміну даними в мережах Інтернету речей є MQTT (Message Queuing Telemetry Transport), який і є предметом цієї статті. MQTT широко використовується завдяки своїй низькій затримці та ефективності, які є критично важливими компонентами для додатків Інтернету речей. Ми можемо оцінити практичну корисність і вплив криптографічних алгоритмів на загальну продуктивність мереж IoT, проаналізувавши їх роботу в рамках цього протоколу. Розробники та дослідники, які прагнуть розгорнути безпечні та ефективні рішення Інтернету речей, підтримуючи при цьому високу якість послуг і надійність системи, знайдуть такий аналіз дуже корисним [22].

3.3 Моніторинг та аналіз заходів безпеки

Стрімкий розвиток технологій Інтернету речей зумовлює потребу в надійних системах моніторингу, які дозволяють швидко виявляти небезпеку та реагувати на неї. Пристрої Інтернету речей вразливі до різноманітних атак, таких як несанкціонований доступ, втрата даних та порушення конфіденційності, оскільки вони часто функціонують у відкритому та динамічному середовищі.

Стеження за протоколами безпеки має важливе значення для забезпечення надійної роботи систем Інтернету речей. Це означає, що потрібно уважно стежити за мережевою активністю, шукати аномалії та вивчати трафік, щоб виявити можливі небезпеки.

Для оцінки ефективності запропонованих механізмів захисту було проведено два тести з використанням протоколу MQTT в мережі Інтернету речей:

1. Спроба аутентифікації з неправильним логіном.
2. Спроба аутентифікації з неправильним паролем.

Спроба аутентифікації з неправильним логіном

Мета тесту – підтвердити, що спроби входу з помилковим логіном належним чином відхиляються системою автентифікації.

Процедура перевірки:

1. На пристрої, який є клієнтом в мережі було введено неправильний логін під час спроби підключення до MQTT-брокера.
2. Відстеження відповідної реакції брокера та запис результату.

Очікуваний результат: Спроба підключення повинна бути відхилена брокером MQTT з повідомленням про помилку автентифікації.

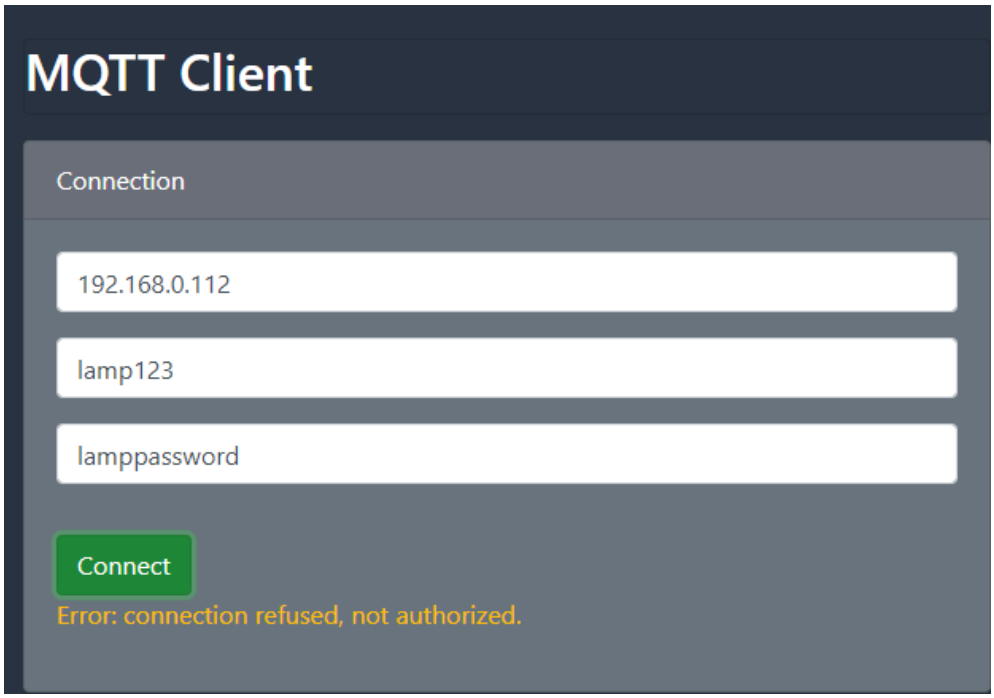

Рисунок 3.3.1 – Повідомлення про помилку при авторизації у клієнта

{"cmd":"ID","ID":"3cf7e4dc652660L"}
{"username":"lamp123","password":"lamppassword","cmd":"CONNEC
T","client":"IoT0 (3cf7e4dc652660L)","protocolId":"MQTT","protoc
olVersion":"3.1.1","clean":1,"clientId":"3cf7e4dc652660L","keepa
live":60,"will":{}}
{"cmd":"CONNACK","client":"IoT0 (3cf7e4dc652660L)","returnCode":
5,"sessionPresent":0}

Рисунок 3.3.2 – Інформація в логах MQTT-брокера про неуспішний вхід

Отриманий результат повністю співпадає з очікуваним. Система аутентифікації відхилила вхід з невірним логіном (рис. 3.3.1). У брокера є інформація про невдалий вхід - вона відображена в логах (рис. 3.3.2).

Спроба автентифікації з використанням неправильного пароля

Мета тесту – підтвердити, що навіть у випадку вводу правильного логіну, система автентифікації буде відхиляти спроби входу з хибним паролем.

Процедура тестування:

1. На клієнтському пристрої IoT було введено правильний логін, але неправильний пароль під час спроби підключення до MQTT-брокера.
2. Відстеження відповідної реакції брокера та запис результату.

Очікуваний результат: Повідомлення про помилку автентифікації має бути надіслано брокером MQTT у відповідь на спробу підключення.

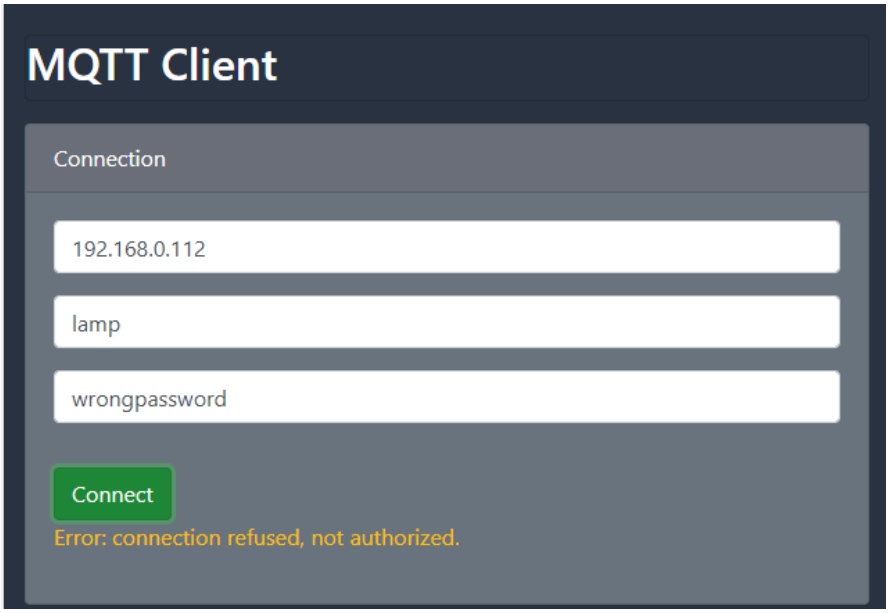

Рисунок 3.3.3 - Повідомлення при авторизації у клієнта

{"cmd":"ID","ID":"3cf7e3b75d47e0L"}
{"username":"lamp","password":"wrongpassword","cmd":"CONNECT","client":"IoT0 (3cf7e3b75d47e0L)","protocolId":"MQTT","protocolVersion":"3.1.1","clean":1,"clientId":"3cf7e3b75d47e0L","keepalive":60,"will":{}}
{"cmd":"CONNACK","client":"IoT0 (3cf7e3b75d47e0L)","returnCode":5,"sessionPresent":0}

Рисунок 3.3.3 - Інформація в логах MQTT-брокера про неуспішний вхід

Отриманий результат повністю відповідає очікуваному – система аутентифікації відхилила вхід з невірним паролем (рис. 3.3.3). У брокера є інформація про невдалий вхід - вона відображена в логах (рис. 3.3.4).

Створення декількох наборів правил доступу було першим кроком у тестуванні ACL. У цьому процесі використовувалися численні параметри, включаючи IP-адреси, порти і протоколи. Після того, як правила були визначені, тестові запити були надіслані як до коректних, так і до помилкових джерел у мережі. Результати тестів були проаналізовані з точки зору застосування ACL, включаючи блокування або дозвіл незаконного трафіку.

Далі ми шукали слабкі місця в ACL. Це включало спроби надсилати пакети через різні порти, змінювати заголовки пакетів або використовувати різні протоколи, намагаючись обійти правила. Ці тести оцінювали ефективність захисту і відстежували, як система реагує на спроби обійти правила.

Були розроблені різні правила фільтрації, щоб визначити, який трафік слід дозволити, а який – заборонити під час тестування брандмауера. Після налаштування правил були запущені тестові запити. Ці запити включали спроби досягти різних мережевих ресурсів, включаючи дозволений і заборонений трафік. Результати тестів були проаналізовані, щоб побачити, як брандмауер обробляє різні типи запитів і як реалізуються правила фільтрації.

Потім брандмауер було перевірено на наявність вразливостей, включаючи спроби надсилання пакетів через альтернативні порти, модифікацію заголовків пакетів або використання інших мережевих протоколів для того, щоб обійти обмеження. Спостерігали, як брандмауер реагував на ці спроби, і оцінювали, наскільки успішно він запобігав потенційним загрозам.

Встановлення безпечного з'єднання за допомогою зашифрованих протоколів зв'язку, таких як TLS, між пристроями Інтернету речей і сервером було першим кроком у процесі тестування шифрування. Для цього використовувалися ключі та сертифікати шифрування. Після встановлення безпечного з'єднання на сервер були надіслані тестові запити, і було помічено, що запити були надіслані в зашифрованому вигляді.

Далі ми спробували перехопити та розшифрувати трафік, що передавався між пристроями та сервером, щоб перевірити ефективність шифрування. Для цього були використані спеціалізовані методи мережевого аналізу. Згідно з результатами тестування, без правильного ключа дані, що передавалися між пристроями та сервером, залишалися нечитабельними та не піддавалися інтерпретації.

В результаті було виявлено, що шифрування успішно забезпечує безпеку комунікації між клієнтами і брокером, а також конфіденційність даних в мережі Інтернету речей.

Для того, щоб підвищити безпеку мереж Інтернету речей, можна запропонувати наступні рекомендації, враховуючи розглянуті теми і проведені експерименти.

Налаштування та застосування ACL

ACL, або списки контролю доступу, є корисним інструментом для контролю доступу до мережевих ресурсів IoT і фільтрації трафіку. Ви повинні правильно налаштувати ACL на основі характеристик вашої мережі та типів трафіку, щоб

підвищити рівень безпеки. Дуже важливо оцінювати правила ACL, в тому числі спроби обійти обмеження доступу, і часто оновлювати їх, щоб забезпечити їх ефективність.

Використання брандмауерів

Завдяки використанню попередньо встановлених правил для фільтрації вхідного та вихідного трафіку, брандмауери забезпечують додатковий рівень безпеки. Брандмауери повинні бути налаштовані таким чином, щоб запобігати всім несанкціонованим з'єднанням і дозволяти тільки ті, які необхідні для функціонування мережі, щоб підвищити безпеку мереж IoT. Оновлення та регулярне сканування брандмауерів на наявність вразливостей сприятиме збереженню високої ефективності захисту.

Використання шифрування

Важливим компонентом гарантування безпеки та цілісності даних є шифрування даних, що передаються між пристроями та серверами Інтернету речей. Завдяки використанню протоколів шифрування, таких як TLS, дані захищені від перехоплення та розшифрування неавторизованими сторонами. Налаштування шифрування вимагає використання актуальних алгоритмів і відповідної довжини ключів.

Впровадження процедур автентифікації

Тільки авторизовані користувачі та пристрої можуть підключатися до мережі Інтернету речей (IoT) завдяки ефективній автентифікації. Слід використовувати багатофакторну автентифікацію (MFA), а також регулярно перевіряти систему на наявність небажаних спроб доступу. Це включає перевірку реакції системи на помилкові облікові дані для входу.

Спостереження та аналіз безпеки

Мережа Інтернету речей знаходиться під постійним наглядом, а аналіз та виявлення загроз допомагають швидко виявляти та усувати ризики. Ви можете відстежувати незвичну поведінку мережі та вживати необхідних заходів за допомогою систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS). Регулярний аналіз журналів і подій допомагає виявити можливі слабкі місця і вдосконалити протоколи безпеки.

Оновлення програмного забезпечення

Щоб захиститися від нових вразливостей та атак, пристрої Інтернету речей повинні регулярно отримувати оновлення програмного забезпечення та прошивки. Виробники часто надають оновлення та патчі для виправлення відомих недоліків безпеки. Переконайтеся, що оновлення ввімкнено автоматично, або часто перевіряйте наявність оновлень.

Крім того, можуть бути створені **правила безпеки**

Ухвалення та введення в дію ретельних правил безпеки, які охоплюють всі аспекти використання пристроїв Інтернету речей, може допомогти гарантувати дотримання найкращих практик безпеки. Правила повинні визначати процедури моніторингу, реагування на інциденти, контролю доступу та конфігурації пристроїв.

ВИСНОВКИ

У рамках кваліфікаційної роботи було проведено ретельний аналіз проблем безпеки в мережах Інтернету речей. В результаті роботи було отримано багато теоретичних та практичних здобутків, які допомагають краще зрозуміти та вирішити проблеми безпеки в цій сфері.

Основні небезпеки та загрози, пов'язані з використанням пристроїв Інтернету речей, були виявлені в результаті аналізу питань безпеки Інтернету речей. Зокрема, було виявлено, що недостатній захист даних та вразливість пристроїв можуть призвести до небажаного доступу, витоку приватних даних та інших проблем безпеки. Слабкі паролі, недостатнє шифрування даних та проблеми з оновленням програмного забезпечення є основними причинами вразливостей програмного та апаратного забезпечення пристроїв Інтернету речей згідно з аналізом поширених недоліків у цих сферах.

У дослідженні розглянуто сучасні протоколи безпеки Інтернету речей, зокрема BLE, MQTT, CoAP та інші. Було ретельно проаналізовано здатність кожного з цих протоколів гарантувати доступність, конфіденційність та цілісність даних. Результати аналізу продемонстрували, що хоча кожен з цих методів має переваги, вони також мають певні недоліки, які слід враховувати, перш ніж застосовувати їх на практиці.

Практична частина роботи включала моделювання безпеки мережі IoT з використанням симулятору Cisco Packet Tracer. Для захисту комунікацій була розроблена модель мережі IoT, налаштовані пристрої та впроваджені процедури безпеки. За допомогою тестування з імітацією різних видів атак ми змогли оцінити, наскільки ефективними є запроваджені заходи безпеки. Результати моделювання показали, що використання відповідних протоколів безпеки значно

покращує безпеку мережі IoT, знижуючи ймовірність незаконного доступу та витоку даних.

Отримані результати свідчать про те, що існує велика потреба в подальших дослідженнях у сфері безпеки Інтернету речей. Подальші дослідження повинні бути зосереджені на розробці нових методів безпеки, які враховують унікальні характеристики пристроїв Інтернету речей та їхні ресурсні обмеження. Вивчення методів автоматизованого виявлення і запобігання атакам в режимі реального часу, а також інтеграція Інтернету речей з іншими технологіями, включаючи блокчейн, мають вирішальне значення для посилення безпеки. Крім того, необхідно створювати і вдосконалювати протоколи безпеки на апаратному рівні пристроїв Інтернету речей.

Отже, отримані в цій роботі результати можуть бути корисними для низки бізнесів, зокрема для інфраструктури та промислових мереж. Наприклад, застосування запропонованих моделей безпеки може значно знизити ризики кібератак, які можуть спричинити перебої у виробництві або втрату життєво важливих даних у промислових організаціях, що використовують Інтернет речей для моніторингу та управління обладнанням. Високий ступінь секретності та цілісності даних, що передаються між пристроями, стає можливим завдяки використанню сучасних протоколів безпеки, таких як BLE, MQTT і CoAP, що знижує ймовірність несанкціонованого доступу.

Крім того, результати цього дослідження мають застосування в системах «розумного будинку», які автоматизують побутові гаджети за допомогою Інтернету речей. Безпека в таких середовищах є надзвичайно важливою, оскільки відкриті отвори можуть призвести до вторгнення в особисте життя або навіть становити фізичну загрозу для мешканців. Впроваджуючи запропоновані практики та стандарти безпеки на практиці, можна захистити приватну інформацію

користувачів та уникнути потенційних атак на розумні пристрої, такі як замки, камери спостереження та термостати.

Цей висновок має значення як для дослідницьких, так і для освітніх установ. Вони можуть створити нові методи навчання і підготовки фахівців з кібербезпеки, які зможуть успішно вирішувати проблеми безпеки IoT, використовуючи результати моделювання та аналізу безпеки. Отже, це допоможе в розробці майбутніх систем Інтернету речей, які будуть більш безпечними.

Застосування результатів дослідження на практиці може значно підвищити рівень безпеки в різних сферах, пов'язаних з Інтернетом речей, знизивши ймовірність зломів і витоку даних. Це підвищить довіру громадськості до технологій Інтернету речей і сприятиме їхньому подальшому розвитку та впровадженню. Результати дослідження можуть бути застосовані для підвищення загальної надійності рішень Інтернету речей та зниження ризиків кіберзлочинності шляхом посилення безпеки систем Інтернету речей у різних галузях бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Madakam S., Ramaswamy R., Tripathi S. Internet of things (iot): a literature review. *Journal of computer and communications*. 2015. Vol. 03, no. 05. P. 164–173. URL: https://doi.org/10.4236/jcc.2015.35021 (date of access: 28.05.2024).

2. Жураковський Б., Зенів І. Технології інтернету речей навчальний посібник. *DSpace :: ELAKPI :: Репозитарій КПІ ім. Ігоря Сікорського*. URL: https://ela.kpi.ua/server/api/core/bitstreams/dcd9e1aa-8bcc-4e76-b1e0-ed133bf616b2/content (дата звернення: 29.04.2024).

3. A Review of Low-End, Middle-End, and High-End Iot Devices / M. O. Ojo et al. *IEEE access*. 2018. Vol. 6. P. 70528–70554. URL: https://doi.org/10.1109/access.2018.2879615 (date of access: 28.05.2024).

4. Shiuhpyng S., Cheng Yi Cho M., Zhi-Kai Z. Emerging security threats and countermeasures in iot. URL: https://dl.acm.org/doi/abs/10.1145/2714576.2737091 (date of access: 02.05.2024).

5. Проблеми та загрози безпеці IoT пристроїв / І. Opirskyy та ін. 2021. 25 берез. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/231.

6. Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. *Wayback Machine*. URL: https://web.archive.org/web/20140508025330/http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf (date of access: 02.05.2024).

7. MQTT - the standard for IoT messaging. *MQTT - The Standard for IoT Messaging*. URL: https://mqtt.org/ (date of access: 02.05.2024).

8. MQTT version 5.0. *docs.oasis-open.org*. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (date of access: 02.05.2024).

9. CoAP – constrained application protocol | overview. *CoAP – Constrained Application Protocol | Overview*. URL: https://coap.space/ (date of access: 02.05.2024).

10. CoAP: an application protocol for billions of tiny internet nodes. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/abstract/document/6159216 (date of access: 02.05.2024).

11. IoT Zigbee device security: a comprehensive review / A. Zohourian et al. URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660523001142 (date of access: 02.05.2024).

12. Zigbee security 101 - architecture and security issues. *Payatu*. URL: https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/ (date of access: 02.05.2024).

13. Bluetooth technology overview | bluetooth® technology website. *Bluetooth® Technology Website*. URL: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/ (date of access: 02.05.2024).

14. Bluetooth low energy | Bluetooth technology website. *Wayback Machine*. URL: https://web.archive.org/web/20170310111443/https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy (date of access: 02.05.2024).

15. Evaluating Bluetooth low energy for IoT / J. Fürst et al. URL: https://ieeexplore.ieee.org/abstract/document/8429494.

16. Cisco packet tracer - networking simulation tool. *Networking Academy*. URL: https://www.netacad.com/courses/packet-tracer (date of access: 02.05.2024).

17. Gangman Y., Jong Hyuk P., Sangil C. Energy-efficient distributed topology control algorithm for low-power IoT communication networks. URL: https://ieeexplore.ieee.org/abstract/document/7752857/authors#authors.

18. Secure MQTT for internet of things (iot) / M. Singh et al. URL: https://ieeexplore.ieee.org/abstract/document/7280018 (date of access: 02.05.2024).

19. Fear and logging in the internet of things / Q. Wang et al. *Network and distributed systems symposium*. URL: https://par.nsf.gov/biblio/10047686 (date of access: 02.05.2024).

20. ACL injury prevention in athletes with iot system and active sensors / Abaranjitha et al. URL: https://ieeexplore.ieee.org/abstract/document/10134406 (date of access: 02.05.2024).

21. Naman G., Vinayak N., Srishti S. A firewall for internet of things. URL: https://ieeexplore.ieee.org/abstract/document/7945418 (date of access: 02.05.2024).

22. Analysis of NIST lightweight cryptographic algorithms performance in IoT security environments based on MQTT / V. Voloshyn et al. *2024 IEEE wireless communications and networking conference (WCNC)*. 2024.