МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПАНІБРАТЮК ОЛЕКСАНДР МИКОЛАЙОВИЧ

Допускається до захисту:
Завідувач кафедри інформаційних технологій, кандидат технічних наук, доцент
_____ Т. В. Нескородєва
«___» _____ 2021 року

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ САМОРОБНИХ ДОМАШНІХ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
Барибін О. І., доцент кафедри інформаційних технологій, кандидат технічних наук

_____
(підпис)

Оцінка: _____ /_____ /_____
(бали за шкалою ЄКТС / за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця – 2021

АНОТАЦІЯ

Панібратюк О.М. Оцінка ризиків інформаційної безпеки саморобних домашніх систем інтернету речей. Спеціальність 125 Кібербезпека. Донецький національний університет імені Василя Стуса, Вінниця, 2021.

Основна увага в цій бакалаврській роботі спрямована на безпеку пристроїв, що входять до екосистеми «Розумного дому», що є частиною концепції домашньої автоматизації. В даному проекті представлено ретельне вивчення ризиків і проблем безпеки в Інтернеті речей та приведено класифікації можливих кібератак на кожен з рівнів архітектури IoT.

Ключові слова: інтернет речей, домашні системи автоматизації, ризики безпеки, контроль доступу, кібератаки.

69 с., 8 табл., 6 рис., 21 джерело.

Panibratiuk O.M. Information security risk assessment of homemade domestic Internet of Things systems. Specialty 125 Cybersecurity. Vasyl' Stus Donetsk National University, Vinnytsia, 2021.

The focus of this bachelor's project is on the safety of devices that are part of the smart home ecosystem, which is part of the concept of home automation. This project presents a thorough study of the risks and security issues of the Internet of Things and provides classifications of possible cyberattacks at each level of the IoT architecture.

Keywords: Internet of Things, Domestic Automation Systems, Security Risks, Access Control, Cyberattacks.

69 p., 8 tab., 6 fig., bibliography: 21 items.

ЗМІСТ

ВСТУП

Останнім часом спостерігається яскраво виражена тенденція зростання уваги до такої області інформаційних технологій, як автоматизація життєдіяльності.

Ідея Інтернету речей (IoT) полягає в об'єднанні між собою речей або пристроїв, підключених до глобальної мережі Інтернет, для виконання будь-яких прикладних завдань. Кількість пристроїв на ринку продовжує зростати відповідно до попиту, а їх функціонал дозволяє значно розширити спектр застосувань. Як приклад, розумний дім, розумні міста, розумна система охорони здоров'я, інтелектуальні ліхтарі, системи керування дорожнім рухом, безпілотні транспортні засоби, інтелектуальний моніторинг навколишнього середовища у разних галузях, інтелектуальне вимірювання, моніторинг водопровідних мереж, розумна логістика та багато іншого. Сфера застосування IoT не обмежується прикладами, зазначеними вище.

Актуальність теми. Володіння даними і кібербезпека є головними проблемами, які викликають заклопотаність щодо майбутнього Інтернету речей. Безпека і контроль всіх фізичних об'єктів, які стали «розумними», вимагають правильного рівня захисту, не ставлячи під загрозу особисті дані споживачів і не допускаючи витоку даних. Марк Гудман, професіонал в правоохоронних органах і технологіях, автор книги «Злочини майбутнього», вважає, що слід прийняти більш ефективні заходи безпеки, щоб запобігти «небезпечного підключення всього». Апаратна безпека важлива як ніколи, оскільки ідентифікація пристроїв, безпечне масштабування мережі і фізична безпека стають вирішальними проблемами для забезпечення того, щоб платформи та операційні системи, які обмінюються даними з пристроями і основними каналами, були зашифровані і безпечні для приватного використання.

Мета роботи: оцінка інформаційних ризиків в саморобних домашніх системах Інтернету речей, пропонування контрзаходів для запобігання або пом’якшення наслідків цих загроз.

Задачі роботи:

1. Визначити особливості інформаційної безпеки стосовно систем Інтернету речей
2. Дослідити архітектуру системи IoT в цілому і розумних пристроїв зокрема
3. Оцінити значення всіх аспектів ІБ для даної архітектури
4. Класифікувати основні вразливості на кожному з рівнів архітектури
5. Розглянути методології управління інформаційними ризиками
6. оцінити найпоширеніші ризики системи Розумного будинку
7. запропонувати заходи протидії визначеним загрозам

Об’єкт дослідження: безпека систем автоматизації Інтернету речей.

Предмет дослідження: інформаційні ризики домашньої системи автоматизації «Розумний будинок».

Структура роботи: Кваліфікаційна (бакалаврська) робота складається зі вступу, чотирьох основних розділів, висновків та списку використаних посилань. Загальний обсяг складає 67 аркушів, 8 таблиць, 6 рисунків. Список використаних посилань складається з 21 найменувань.

РОЗДІЛ 1
ОСНОВНІ ПОЛОЖЕННЯ ТА ХАРАКТЕРИСТИКИ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ. ЖИТТЄВИЙ ЦИКЛ ІНФОРМАЦІЇ

Цей розділ являє собою знайомство з основними принципами технології Інтернету речей, в тому числі домашніх систем автоматизації. Більшість пристроїв домашньої автоматизації в основному базуються на одних і тих же популярних технологіях та протоколах, а платформи є модульними, що дає змогу користувачам комплектувати такі системи самостійно. Отже, доцільно буде зазначити, що будь-яка довільна домашня система Інтернету речей може вважатись саморобною.

1.1 Поняття та історія Інтернету речей

Термін «Інтернет речей» як концепція вперше був згаданий в 1990-х роках. Поточний формат вираження був запропонований Кевіном Ештоном в 1999 році [1]. Тоді використання цього терміну означало взаємозв'язок між радіочастотною ідентифікацією (RFID) та Інтернетом. З тих пір використання цього терміна стало набагато популярнішим, а великі компанії пророкували даній концепції світле майбутнє [12].

IoT може бути визначений як глобальна інфраструктура інформаційного суспільства для з'єднання фізичних і віртуальних активів та речей, яка заснована на каналах зв'язку і технологіях, що розвиваються.

По суті Інтернет речей складається з фізичних пристроїв, здатних контролювати навколишнє середовище і передавати отримані дані на інші пристрої, а також виконувати дії на основі отриманої інформації. Коротше кажучи, термін Інтернет речей стосується пристроїв, підключених один до одного за допомогою різних технологій і каналів зв'язку. Ці пристрої можуть передавати дані і взаємодіяти один з одним.

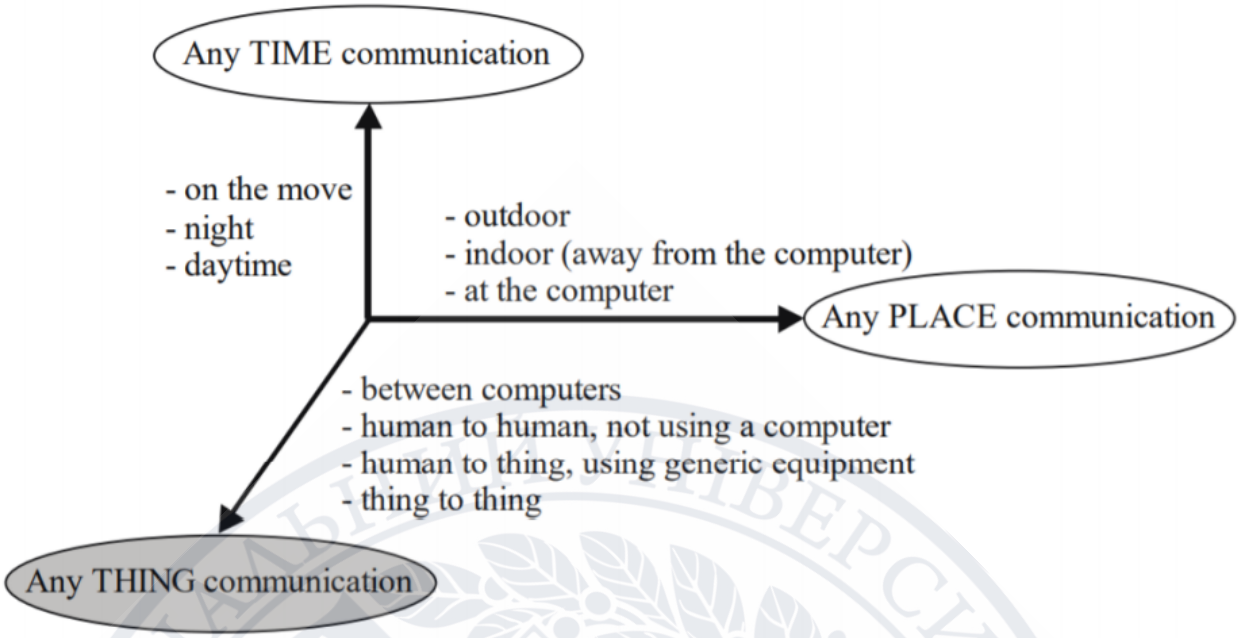

Рисунок 1.1 – Розміри концепції Інтернету речей

Вперше Інтернет речей, як явище, світ побачив у червні 2000 року, коли LG представила перший підключений до Інтернету холодильник, Internet Digital DIOS. Холодильник містив високоякісний екран з низкою функціональних можливостей, таких як відображення температури всередині холодильника, оцінювання збереженості продуктів та використання функції веб-камери для відстеження продуктів, що зберігаються [12].

А першим пристроєм, який, мабуть, привернув найбільшу увагу ЗМІ та споживачів, був термостат Nest Learning у жовтні 2011р. Цей пристрій міг аналізувати розпорядок дня користувача, щоб автоматично регулювати бажану температуру у різний час доби. Придбання новинки компанією Google за 3,2 мільярда доларів стало подією, яка сповістила світ про майбутню революцію в технологіях [12].

Незабаром з’явилися сотні нових стартапів, які намагалися з’єднати між собою різні аспекти навколишнього світу з пристроями, а великі організації запустили спеціалізовані внутрішні команди, щоб розробити власні лінійки IoT пристроїв та якомога швидше випустити їх на ринок.

1.2 Типові приклади пристроїв IoT

Пристрої Інтернету речей можна розділити на споживчі пристрої, такі як побутова техніка та системи домашньої автоматизації, а також пристрої для промислового використання, такі як різні типи датчиків для вимірювання температури, вологості і руху. Типовими побутовими приладами є, наприклад, камери спостереження, мережеві комутатори, маршрутизатори і мережеві сховища, холодильники, інтелектуальні телевізори і автомобілі. Для систем домашньої автоматизації, тобто розумних будинків, типовими приладами є, наприклад, системи опалення та вентиляції, системи управління освітленням і різні датчики для контролю вологості і рівня CO2 всередині будівель.

1.3 Інциденти порушення інформаційної безпеки IoT

Майже кожен розумний пристрій має власні критичні проблеми безпеки та конфіденційності, включаючи розумні системи автоматизації будинку, портативні пристрої, радіоняні та навіть особисті інтимні іграшки.

Серед найбільш яскравих випадків атаки на IoT-пристрої, варто згадати інциденти 2016-2017 років з побутовими приладами. Зокрема, в жовтні 2016 року в США була здійснена серія DdoS-атак на компанію Dyn – головного провайдера DNS-послуг для таких IT-гігантів, як Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal і Verizon. Метою атаки було захоплення системних ресурсів і ускладнення доступу для користувачів. Атака здійснювалася завдяки підключенню до незахищених IoT-пристроїв: роутерів, камер відеоспостереження, які, незважаючи на малу обчислювальну потужність, генерували величезні обсяги інформації. Рівень навантаження на сервери був критичним, враховуючи, що всі заражені пристрої були підключені одночасно. В результаті даного інциденту, соцмережі і онлайн-магазини стали тимчасово недоступні [2].

У 2017 році добре відомий ботнет Mirai провів подібну атаку на інших провайдерів. Перебравши бутфорсом комбінації пар «логін:пароль», встановлених за замовчуванням, було зламано величезну кількість камер і

роутерів. Зламані IoT пристрої були використані для наймогутнішої DdoS-атаки на провайдерські мережі UK Postal Office, Deutsche Telekom, TalkTalk, KCOM і Eircom. Злом IoT-приладів виконувався по протоколу Telnet, а роутерів – за протоколами TR-064 і TR-069 через порт 7547 [2].

Приблизно в той же час була виявлена уразливість в мобільному і хмарному додатках домашніх смарт-пристроїв LG SmartThinkQ, яка дозволяла зловмисникам створити підроблений обліковий запис і віддалено отримати контроль над усіма видами побутової техніки LG: від пилососа з вбудованою відеокамерою до холодильника, електроплити, посудомийної і пральної машин.

Для захисту IoT необхідні очевидні заходи, а саме контроль доступу, автентифікація пристрою та шифрування. Але враховуючи природу таких пристроїв, їх недостатня обчислювальна потужність значно ускладнює цю задачу. Найбільшою проблемою залишається те, що наразі немає єдиної думки щодо того, як впровадити безпеку безпосередньо на IoT-пристрої. Іншою складністю є стандартизація термінів апаратного та програмного забезпечення, що використовується пристроями. Враховуючи те, як IoT обробляє критичні процеси та скільки даних проходить через пристрої, це доволі вигідна мета для зловмисників. Наслідки проблем безпеки стають все більш серйозними, що призводить до загрози здоров'ю людини, непоправної шкоди продукції, тривалого простою на виробництвах та багатьох інших.

1.4 Життєвий цикл інформації

Щоб розуміти, що саме загрожує даним в IoT, потрібно мати уявлення про життєвий цикл інформації в системі IoT в цілому. Довідкова модель, запропонована Cisco, описана в розділі 2 і базується на життєвому циклі інформації, включно зі всіма аспектами середовища IoT.

В системі IoT збір і обробка інформації проводяться у п'ять етапів. Однак у кожен з етапів повинні бути закладені основи безпеки, щоб інформація залишалася стійкою до будь-яких несанкціонованих дій з нею [18].

1. **Етап генерації** – пристрої або датчики збирають інформацію з навколишнього світу.

2. **Етап зв'язку** – згенеровані дані та події надсилаються через мережу зв'язку до місця призначення.

3. **Етап комбінування** – усі зібрані дані об'єднуються централізовано, або ж самими пристроями.

4. **Етап аналізу** – алгоритми використовуються для пошуку серед об'єднаного масиву даних, для контролю та оптимізації процесів.

5. **Етап дії** – здійснюються доцільні дії на основі отриманих даних.

Інформація та процеси на кожному із цих етапів є схильними до атак. Процес генерації чи обробки даних може бути атакований як шляхом модифікації центрального середовища для введення хибної інформації, так і шляхом фізичного втручання в сам пристрій. Канали зв'язку вразливі до перехоплення, сніфінгу та ін'єкції небезпечного коду. Комбінування даних, яке виконується локально на пристрої, може бути змінене безпосередньо зловмисником або за допомогою раніше встановленого шкідливого ПЗ. Віддалене комбінування даних вимагає використання API, який, як правило, є недостатньо захищеним, що забезпечує зловмиснику втручання в обробку даних. Аналіз, як правило, базується на алгоритмах машинного навчання та штучного інтелекту. Вхідні дані алгоритмів можуть бути модифіковані, що призводить до небажаних дій і відповідних наслідків. Отже, забезпечення безпеки на кожному з етапів необхідне для того, щоб підтримувати цілісність інформації протягом усього її життєвого циклу в системах IoT.

1.5 Характеристики IoT

IoT – це складна система з низкою характеристик, які можуть відрізнятися в залежності від пристрою та технології. Основні та загальні ознаки, визначені під час дослідження, містяться в таблиці 1.1 [17].

Характеристика	Опис
Інтелект	Поєднання алгоритмів, обчислень, програмного та апаратного забезпечення для інтелектуальних пристроїв. Розширення можливостей Інтернету речей для розумного реагування на різні ситуації і підтримки виконання конкретних завдань.
Зв'язок	З'єднання пристроїв за допомогою простих взаємодій на рівні об'єктів сприяє колективному розуму в мережі IoT, що забезпечує їх доступність та сумісність. Все може бути пов'язано з комунікаційною та інформаційної інфраструктурою в глобальному масштабі.
Неоднорідність	Можливість взаємодії з іншими пристроями або сервісними платформами. Пристрої в IoT є неоднорідними, оскільки базуються на різних апаратних платформах та мережах.
Безпека	Обсяг конфіденційної інформації, яка збирається речами, повинен бути захищений від неправомірного використання, як і самі пристрої. Захист даних на кінцевих точках, мережах та передачах даних вимагає міцної основи безпеки.
Динамічний характер	Стан пристроїв змінюється динамічно, наприклад спить або активно працює. Кількість підключених пристроїв також залежить від даного контексту.
Масштаб	Кількість пристроїв, що працюють і обмінюються даними, буде більше, ніж пристроїв, підключених до поточного Інтернету. Трафік, що генерується в Інтернеті, буде помітно переходити від комунікації, ініційованої людиною, до трафіку, ініційованого пристроями. Забезпечення сприйнятливості до ефективної обробки даних.
Зондування	Забезпечення засобів для створення можливостей, що відображають справжнє усвідомлення фізичного світу за допомогою сенсорних пристроїв. Зібрана інформація представлена як аналоговий вхід із реального світу для забезпечення складного розуміння.

Таблиця 1.1 – Основні характеристики пристроїв IoT

Кожен пристрій обмежений його апаратною продуктивністю та джерелом живлення, що обмежує його обчислювальну потужність до певного рівня, щоб зробити її досить розумною, незважаючи на виробничі витрати, розмір та ефективність.

Оскільки зв’язок є основною характеристикою IoT, це змінює спосіб розуміння та управління світом. Таким чином можна зв’язати все що завгодно, від примітивного датчика до холодильника задля створення загальної мережі підключених пристроїв.

Диверсифікація не тільки апаратних рішень, але і протоколів, що використовуються пристроями, ускладнює підтримку на різних платформах і мережах. З недавнього зростання у світі IoT закладаються основи стандартизації протоколів, щоб зробити зв'язок між пристроями якомога ближчим. Регулювання технологій, що використовуються в Інтернеті речей, безпосередньо призводить до загрози безпеці, якщо все пов’язане і здатне взаємодіяти між собою.

Підтримка безпеки необхідна в усіх аспектах пристрою, щоб забезпечити стійкість до зовнішніх атак, а рівень конфіденційності інформації користувача відповідав заданим вимогам. Системи повинні підтримувати захист даних під час збору, передачі, зберігання, комбінування та обробки даних. Одним із основних призначень Інтернету речей є збір даних з оточення, що зумовлено динамічними змінами умов навколо пристрою. Вони змінюють контекст на основі конкретних тригерів з навколишнього середовища, таких як температура, місцезнаходження або швидкість. Збір даних здійснюється за допомогою сенсорів та датчиків, які надають інформацію для використання в будь-якій формі обчислень, наприклад, для побудови вищезгаданих тригерів [19].

1.6 Еталонна модель Cisco

Модель, запропонована Cisco, є схожою на семирівневу еталонну модель ISO/OSI і найбільш широко поширена в наукових та промислових публікаціях. У цій моделі розміщений двоспрямований потік даних, основний напрямок якого здебільшого залежить від програми. У системі управління дані та команди рухаються від верхньої частини моделі до нижньої, тоді як у сценарії моніторингу потік змінюється [16].

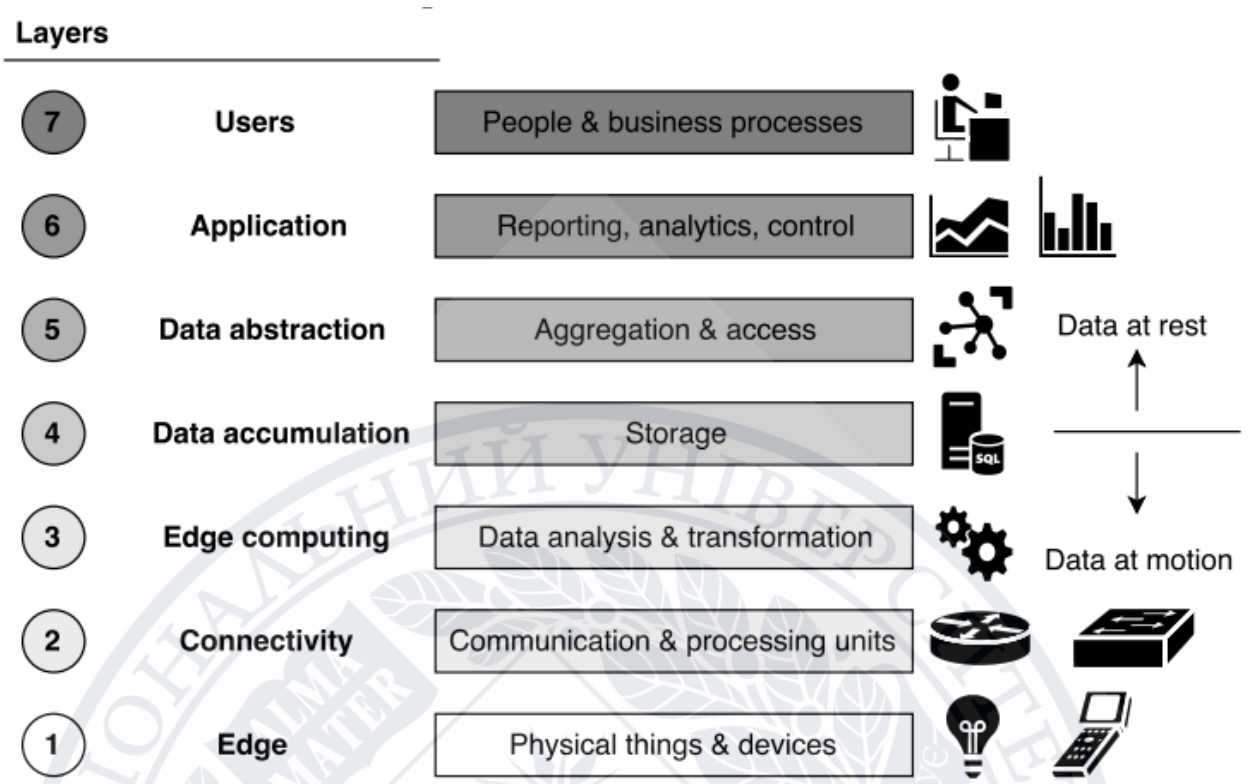

Рисунок 1.2 – Еталонна модель Інтернету речей

Рівень 1 – Прикладний рівень

Перший рівень містить обчислювальні вузли, такі як інтелектуальні контролери і датчики. Пристрої здатні перетворювати аналоговий сигнал в цифрові дані, для генерації даних і запитів на більш високих рівнях. Конфіденційність і цілісність даних повинні прийматися до уваги починаючи з цього рівня.

Рівень 2 – Комунікативність

Комунікація і можливість підключення зосереджені на даному рівні, щоб забезпечити передачу інформації між об'єктами першого та другого рівнів, а також між першим і третім рівнями для виконання периферійних обчислень. Можливості підключення також враховують надійну доставку пакетів даних по мережі, реалізацію різних протоколів і інтерфейсів між ними, а також безпеку на мережевому рівні. З точки зору безпеки цей рівень повинен забезпечувати безпечний доступ до мережі, безпосередньо реалізуючи необхідний захист в протоколах і самому обладнанні.

Рівень 3 – Периферійні обчислення

Функція третього рівня в цій моделі полягає в перетворенні мережевих потоків даних в інформацію, яка підходить для зберігання і обробки більш високого рівня. Це важливо для зниження обчислювального навантаження на вищому рівні, а також для забезпечення швидкого відгуку. Основна увага приділяється комунікації між рівнями, генерації подій і простій обробці за допомогою алгоритмів навчання. У периферійних обчисленнях також необхідно враховувати шифрування для забезпечення безпеки зв'язку.

Рівень 4 – Накопичення даних

Більшість додатків не вимагають миттєвої обробки даних, тому додатки зазвичай припускають, що дані в пам'яті або на диску не змінилися. Цей рівень дозволяє перетворювати динамічні дані для отримання даних в стані спокою, щоб вони могли оброблятись системами, які не працюють у режимі реального часу. Для досягнення цього перетворення мережеві пакети перетворюються в таблиці бази даних, скорочуючи обсяг даних за рахунок фільтрації і вибіркового зберігання. Всі ці дані повинні оброблятися програмним забезпеченням, яке захищене від несанкціонованого доступу і не містить фальшивої інформації.

Рівень 5 – Абстрагування даних

Цей рівень враховує масштабованість систем IoT за рахунок розміщення даних пристрою в декількох системах зберігання. Дані піддаються подальшій обробці, щоб оптимізувати їх для більш високих рівнів, наприклад подавати дані у такому вигляді, як цього вимагають додатки. Простіше кажучи, основна увага приділяється абстрагування інтерфейсу даних для додатків. Системи зберігання повинні мати не тільки безпечне обладнання, а й програмні засоби для запобігання витоку даних.

Рівень 6 – Рівень додатків

На даному рівні відбувається інтерпретація інформації. Програмне забезпечення взаємодіє з даними двох попередніх рівнів, які знаходяться в стані спокою, тому йому не потрібно працювати на мережевих швидкостях. У

домашніх системах це може включати прості взаємодії, засоби управління і аналітику. Використання аутентифікації і авторизації – шлях до захисту додатків від неправомірного використання.

Рівень 7 – Рівень користувача

Найвищий рівень моделі IoT – це місце, де знаходяться користувачі. Додатки виконують логіку на основі своїх даних, щоб дати людям можливість використовувати їх і пов'язані з ними дані для своїх конкретних потреб. Метою цього рівня є не сам додаток, а надання користувачу потрібних даних у необхідний час. Все це виконується і захищається системою управління ідентифікацією та доступом.

РОЗДІЛ 2
ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Що являє собою інформаційна безпека

Безпека в загальному сенсі означає захист інформації від зловмисників, які намагаються отримати доступ до мережі; шкідливого коду, стихійних лих, збоїв живлення, крадіжки або навіть вандалізму. Щоб стандартизувати дану дисципліну, були встановлені основні правила і політики щодо паролів, брандмауера, шифрування, антивірусного програмного забезпечення тощо.

Щоб визначити, що може вважатись безпечним, важливо розуміти три основних параметри, які визначають безпеку: конфіденційність, цілісність і доступність [20].

Конфіденційність гарантує доступ до приватної інформації тільки уповноваженому персоналу із застосуванням набору правил. Оскільки пристрої IoT часто обробляють важливу особисту інформацію, вкрай важливо зберігати їх конфіденційність. Наприклад, якщо зловмисник отримає доступ до таких пристроїв, як розумний замок, ймовірність крадіжки зі зломом зростає в геометричній прогресії.

Цілісність необхідна для надання надійних послуг. Пристрій з використовуваними протоколами має гарантувати, що інформація, яка надходить від і до нього, знаходиться в початковому стані і не піддавалася модифікації. Це реалізується простою хеш-функцією, згенерованою відправником для обчислення контрольної суми, щоб гарантувати справжність переданих даних. Атаки на цілісність можуть сфабрикувати інформацію для запуску певної події в особистих цілях.

Доступність важлива для забезпечення гарантованої функціональності пристроїв. Це гарантує, що пристрої доступні для збору даних і зв'язку, при цьому запобігаючи перебоям в обслуговуванні.

Але вищеперераховані характеристики не враховують нові загрози, які почали виникати внаслідок розвитку систем Інтернету речей. Новий

пропонований список вимог безпеки називається IAS-OCTAVE, де OCTAVE означає «Оперативно критична загроза, оцінка активів і вразливості» (Operationally Critical Threat, Asset and Vulnerability Evaluation). У таблиці 2.1 наведені вимоги безпеки в IAS-OCTAVE [21].

Вимога	Визначення
Конфіденційність	Забезпечення доступу до інформації тільки авторизованим користувачам.
Цілісність	Гарантія того, що дані не були підроблені під час передачі або зберігання.
Доступність	Забезпечення доступності всіх систем за запитом авторизованого користувача.
Підзвітність	Здатність системи залучати користувачів до відповідальності за їхні дії.
Ревізійність	Здатність системи вести постійний моніторинг всіх дій.
Надійність	Здатність системи перевіряти особистість і встановлювати довіру до третьої сторони.
Безвідмовність	Здатність системи забезпечити настання/ненастання дії.
Приватність	Гарантує, що всі системи приховують особисту інформацію про користувача і дотримуються політику конфіденційності.

Таблиця 2.1 – Вимоги безпеки в IoT

2.2 Особливості безпеки в IoT

Швидкий розвиток Інтернету речей являє собою складну задачу для безпеки. Широко розподілена інфраструктура Інтернету речей, використання простих технологій і слабких методів захисту роблять його відмінною метою, яку можуть використовувати зловмисники. Є не тільки програмні загрози, з якими стикаються пристрою, але і фізичні. Пристрої часто знаходяться в незахищених зонах, що робить їх легкодоступними і уразливими для фізичного пошкодження.

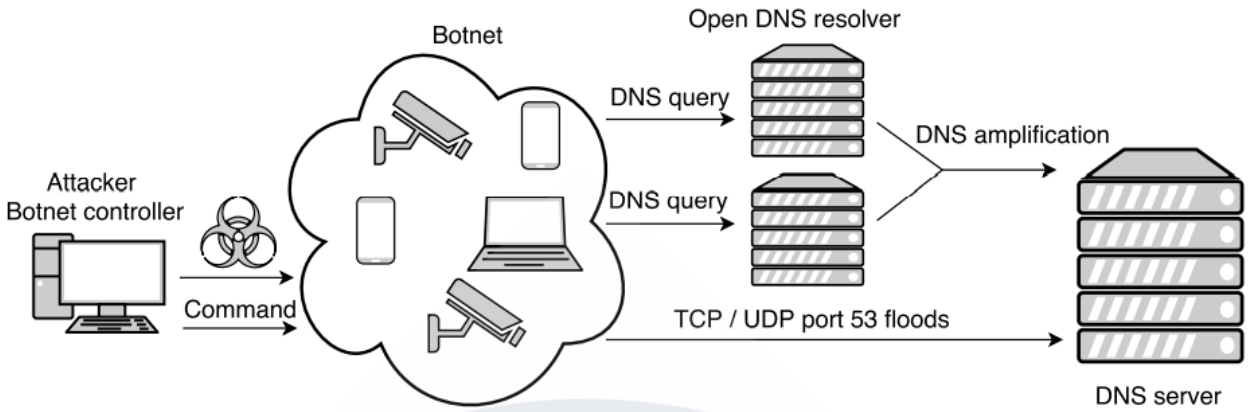

Рисунок 2.1 – Схематичний приклад DNS DDoS-атаки

Після інцидентів 2016-2017 років, з’явилося досить багато питань щодо безпеки Інтернету речей, у тому числі було висвітлено найпоширеніші вразливості пристроїв, які необхідно усунути. Традиційного захисту у вигляді простої криптографії, безпечних протоколів і забезпечення конфіденційності вже недостатньо. Зазвичай безпека навіть не береться до уваги виробником, все заради зниження вартості продукту, який має тільки базові функції, що робить його вразливим для мережевих атак. Щоб уникнути цих загроз, Інтернет речей повинен мати міцну основу безпеки [12].

2.2.1 Протоколи зв’язку

Різноманітність Інтернету речей впливає на можливості захисту інфраструктури. Зв'язок між речами і мережевою інфраструктурою в основному заснований на стандартах бездротового зв'язку. Оскільки бездротовий сигнал може бути перехоплений неавторизованими користувачами, необхідно переконатися, що вони не можуть отримати доступ до системи. Навіть користувачі, які законно отримали доступ до системи, можуть спробувати зламати інші пристрої в межах тієї ж мережі. Протоколи і стандарти, що використовуються в IoT, повинні враховувати такі ситуації, створюючи безпечні канали зв'язку і забезпечувати шифрування передачі в цілому.

Елементарні пристрої в основному використовують стандарти з сімейства протоколів IEEE 802.15, а також варіанти цих протоколів передачі з низьким енергоспоживанням. Група стандартів 802.15 визначає безліч бездротових персональних мереж (WPAN) для різних додатків. Категорія 802.15.4 – один з найпопулярніших стандартів зв'язку з низькою пропускною здатністю, який широко використовується пристроями в IoT. Для забезпечення безпечних каналів зв'язку в мережевий моделі цього протоколу потрібні полегшені криптографічні алгоритми, які підходять для системи управління ключами і безпечні протоколи для об'єднання пристроїв в групи, які пов'язані через глобальну мережу Інтернет.

З іншого боку, пристрої, яким не потрібні полегшені протоколи для економії енергії або яким потрібна вища пропускна здатність, можуть реалізовувати стандарти з сімейства протоколів 802.11. Нещодавно розроблений протокол 802.11ah забезпечує низьке енергоспоживання при збереженні більш високої пропускної здатності по безпечному каналу зв'язку, у порівнянні з групою стандартів 802.15. Згадані протоколи регулюються Wi-Fi Alliance, який враховує всі вимоги для безпечного зв'язку в своїх протоколах [19].

2.2.2 Криптографія / шифрування

Криптографія – один із основних заходів безпеки, необхідних для захисту даних під час передачі. Такі стандарти, як Advanced Encryption Standard (AES), можуть бути реалізовані одночасно на великій кількості пристроїв IoT, від 8-бітних інтегральних схем до високопродуктивних датчиків. З іншого боку, шифрування чіпів RFID за допомогою AES фізично можливе через їх природу. Криптографічні системи повинні бути більш швидкими, умовно компактними і з такими ж заходами безпеки, щоб їх можна було використовувати на пристроях з обмеженою продуктивністю. Система загальних секретних ключів являє собою проблему в динамічному середовищі. Традиційні інфраструктури відкритих ключів не можуть масштабуватися, щоб

пристосуватися до поєднання контекстів і пристроїв Інтернету речей, наприклад, з огляду на необхідність зміни ключів пристроїв для забезпечення безпеки потоку інформації в довгостроковій перспективі [19].

2.2.3 Комунікативність

Інтернет речей працює на рівнях зв'язку і широко використовує стандарти Інтернету для надання послуг. Деяким пристроям не вистачає ресурсів для реалізації заходів безпеки для безпечного використання цих протоколів, щоб забезпечити необхідну функціональність, тому стандарти безпеки вимагають деякої адаптації для постійного росту і розвитку Інтернету речей. Адаптація стандартів повинна не тільки враховувати вимоги до продуктивності Інтернету речей, але й зменшувати відмінності між існуючими протоколами Інтернету речей та Інтернету, зберігаючи при цьому оригінальні властивості безпеки в контексті традиційної архітектури Інтернету [19].

2.2.4 Приватність

Приватність викликає серйозну заклопотаність у сфері захисту Інтернету речей. Дані, що вільно доступні в Інтернеті, дозволяють відстежувати об'єкти, збирати їх і профілювати користувачів без їх дозволу. З недавнім зростанням Інтернету речей практика збору даних може легко призвести до небажаних ситуацій.

Одне з можливих рішень – надати користувачам інструменти для управління своїми даними, що призведе до конфіденційності ще на рівні дизайну. Це приблизно описує поточну ситуацію, коли користувач дає згоду на те, скільки даних необхідно певним службам для правильної роботи або загалом. З іншого боку, пристрої Інтернету речей часто порушують цю концепцію, збираючи інформацію без згоди користувача.

Тому потрібно більш суворе забезпечення приватності, щоб особиста інформація користувачів Інтернету речей залишалася захищеною від сторонніх очей. Механізм делегування – це новий запропонований підхід, що

обмежує спілкування користувача з метою обміну мінімальним обсягом необхідної інформації. Деякі рішення, засновані на цьому механізмі, дозволяють користувачеві знаходити інші, які найкраще відповідають його перевагам, практично не розкриваючи таку інформацію всім.

Ще одна ідея в розробці – це так званий «коуч по конфіденційності». Суть цієї ідеї полягає в пристрої, здатному сканувати теги вбудованих пристроїв і завантажувати їх політику конфіденційності. Якщо політика не відповідає вподобанням користувача, він може запросто відмовитися від користування об’єктом. В іншому сценарії скановані об'єкти можуть безпосередньо транслювати свою політику конфіденційності та запитувати в користувачів їхню згоду. Зрештою, це може слугувати механізмом захисту фізичного простору, щоб сканувати шкідливі чи небажані об'єкти, залишені для спостереження за даним простором без згоди користувача [19].

2.2.5 Прозорість

Важливе значення для конфіденційності має прозорість, оскільки користувачі повинні знати, які організації оперують їх особистими даними та яким чином ця інформація використовується. Подальший розвиток цього підходу може змусити зацікавлені сторони, наприклад, постачальників послуг, відмовитися від ліцензійних угод за принципом «бери або залиш». Компанії змушені адаптувати свої сервіси в залежності від того, яким обсягом даних бажають ділитися з користувачем. В основному існують два типи прозорості:

- **Обмежена прозорість** приховує деталі протоколів, використовуваних між пристроєм і хмарою, а також необроблені дані, що відправляються по каналах зв'язку. Доступні користувачеві прозорі дані попередньо обробляються і фільтруються на основі призначених для користувача переваг, щоб забезпечити відповідний огляд спільно використовуваної інформації.
- **Повна прозорість** вважається шкідливою, оскільки вона не захищає інтелектуальну власність, і всі дані в необробленому вигляді можуть

бути доступні користувачеві. Повна прозорість чимось близька до підходу з відкритим кодом, коли користувачі мають повний контроль над тим, щоб приховати інформацію, якої вони не бажають ділитися.

Однак багато хто вважає, що обмежена прозорість – це правильний підхід стосовно користувачів, щоб не перевантажувати їх інформацією, зберігаючи при цьому контроль над даними, необхідними для правильного функціонування пристроїв [19].

2.2.6 Управління ідентифікацією

Управління ідентифікацією в IoT – це доволі розпливчатий термін, який насправді для об'єктів означає:

- Власний тип ідентифікації, незалежний від використовуваного основного механізму, такого як IP-протоколи, щоб покладатися не лише на IP-адресу як на єдиний спосіб ідентифікації.
- Наявність одного основного ідентифікатора і безлічі тимчасових ідентифікаторів, які можна міняти місцями в залежності від його ролі. Так званий хаб може служити блоком керування для пристроїв Інтернету речей і в той же час надавати користувачам можливість підключення до Інтернету.
- Наявність ідентифікації, заснованої на деяких індивідуальних особливостях. Датчик ідентифікується за показаннями навколишнього середовища.
- Визначення особистості їх власників. Наприклад, пристрій з голосовим управлінням має розрізняти голоси і відповідним чином реагувати на запити.

Підтвердження ідентичності – ключова частина процесу управління ідентичністю, оскільки пристроїв потрібно інфраструктура, що дозволяє виконувати взаємну аутентифікацію об'єктів. Для досягнення цього рівня бази для Інтернету речей необхідний баланс між централізованим управлінням і

розподіленою ієрархічною структурою. У даного підходу є недоліки з авторизацією і аутентифікацією, так як повинен бути централізований орган для визначення та розмежування ролей в системі [19].

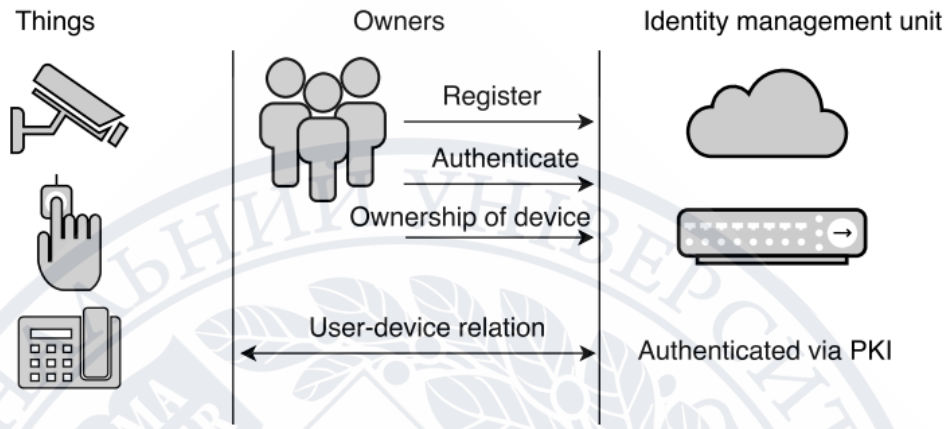

Рисунок 2.2 – Схема управління ідентифікацією

У деякому контексті IoT, може бути корисним підхід «single sign-on», скорочений як SSO, тобто користувачам необхідно пройти аутентифікацію тільки один раз для зв'язку з різними пристроями. Однак цей підхід був розроблений без урахувань вимог Інтернету речей, таких як вибір постачальника посвідчень на ряду з масовим масштабуванням технології. З іншого боку, альтернативні механізми можуть змусити користувачів використовувати певний протокол, що може викликати проблеми в гетерогенному обчислювальному середовищі.

Згадані вище проблеми враховують необхідність адаптувати існуючі механізми SSO для впровадження їх в IoT, або розробити нові механізми для конкретного варіанту використання. В даний час ці проблеми вирішуються шляхом розгортання гібридних архітектур зі спеціальним ПЗ, створеним конкретно для IoT, проте як і раніше, проблема з кількістю розгорнутих пристроїв залишається актуальною.

Новим підходом для перевірки ідентичності користувача є цифрове тіньове копіювання, при якому користувач проектує свою віртуальну

ідентичність на логічні вузли. Ідея концепції цифрового сліду (або Fingerprinting) заснована на тому, що користувач діє від свого імені, не викриваючи свою особистість безпосередньо. Тобто об'єкти в системі працюють лише з віртуальним ідентифікатором користувача, що містить інформацію про його атрибути, сеанси та взаємодію з архітектурою. Таким чином, цифровий слід лише побічно вказує на особу користувача [19].

2.2.7 Відмовостійкість

Відмовостійкість в IoT може бути досягнена за допомогою трьох спільних факторів:

- Безпека за замовчуванням для всіх об'єктів за рахунок розробки безпечних протоколів і механізмів та підвищення якості впровадженого програмного забезпечення, оскільки оновлення кількох мільярдів пристроїв за допомогою програмного виправлення не завжди можливо.
- Визначення стану мережі та її сервісів для зворотного зв'язку з іншими елементами, в кінцевому підсумку створюючи систему підзвітності, яка допомагає відслідковувати стан.
- Можливість захисту від мережевих збоїв і атак. Всі використовувані протоколи повинні враховувати механізм реагування на форс-мажорні ситуації. Наприклад, використання системи виявлення вторгнень для протидії атакам.

Поєднання цих факторів має вирішальне значення для здатності IoT відновлюватися після будь-якої нестандартної ситуації. Наприклад, щоб мати здатність забезпечити вищезгаданий зворотний зв'язок чи відобразити розташування небезпечних зон, визначити рівень безпеки і з'ясувати, де відбувається атака та на які зони вона впливає. Така інформація може бути основою для систем відновлення: які зони отримують доступ в першу чергу, а які необхідно уникати в даний момент. Також важливою є можливість

інформування операторів про проведення технічного обслуговування в зонах з низьким рівнем безпеки [19].

РОЗДІЛ 3
АТАКИ, ПРИЧИНИ ЇХ РЕАЛІЗАЦІЇ І КЛАСИФІКАЦІЯ. МЕТОДИ ПРОТИДІЇ ТА ЗАПОБІГАННЯ АТАКАМ

У даному розділі пояснюються мотиви, що спонукають людей до отримання несанкціонованого доступу, а також типи атак, які здійснюються на пристрої та збитки, які можуть бути завдані як наслідок.

Системи на основі Інтернету речей часто керують величезним обсягом інформації і використовуються службами від управління виробництвом до моніторингу стану здоров'я. Цей факт зробив парадигму Інтернету речей цікавою метою для різних атак, таких як хакери, кіберзлочинці, «хактивісти» тощо. У потенційних зловмисників можуть бути різні мотиви для злому пристроїв Інтернету речей, наприклад фінансові, політичні або ідеологічні.

3.1 Причини реалізації атак

Широке використання мереж і можливостей підключення робить атаки більш легкими для виконання і більш складними для запобігання. Хоча Інтернет речей спрощує людське життя, він також збільшує ризик. Хакеру потрібно знайти тільки одну дірку, щоб потрапити всередину, але розробнику необхідно перекрити їх всі, щоб не допустити хакера до системи.

Отже, чому люди намагаються зламувати [3]:

- Злом як хоббі. Люди часто займаються зломом заради задоволення, щоб довести собі чи іншим, що вони можуть перехитрити механізм безпеки. Оскільки багато систем практично не мають захисту, їх легко зламати і контролювати на свій розсуд. Ці хакери можуть займатися чим завгодно, від вандалізму веб-сайтів до злому домашньої мережі Wi-Fi.
- Злом з метою крадіжки інформації. У міру того, як інформація переміщується в віртуальний світ, хакерам набагато цікавіше отримати доступ до таких систем, як онлайн-банкінг жертви, для отримання фінансової вигоди. Мотив для деяких хакерів може полягати в

поширенні секретної та конфіденційної інформації. Це можна зробити за допомогою соціальної інженерії, установки шкідливих програм, фішингу або злому баз даних за допомогою троянського коня.

- Злом з метою порушення роботи служб. Хакери можуть використовувати системи IoT для створення ботнету, щоб вивести з ладу певну систему або службу. Вони масово заражають мережі шкідливим програмним забезпеченням, використовуваним в різних цілях, при цьому користувачі можуть навіть не підозрювати про це. Найпопулярніша підривна атака – відмова в обслуговуванні, інакше – DDoS.
- Хактивізм або ідеалізм. У сучасному світі кращим засібом звернення до суспільства є мережа Інтернет. Хактивізм – це суміш слів «хакерство» і «активізм», тобто коли людина використовує Інтернет для освітлення деяких політичних або соціальних проблем. Хактивісти прагнуть зробити якусь заяву, зазвичай без будь-якої фінансової вигоди [14].
- Кібертероризм – окремий впадок хактивізму. Злом іноді є інструментом, використовуваним групами зловмисників, які намагаються підвищити обізнаність про політичне питання або створити хаос. Хакери націлені на критично важливі урядові системи, щоб підірвати їх авторитет або довіру шляхом втручання у роботу вищезгаданих систем, крадіжки інформації або здійснення DDoS-атаки.
- Тестування на проникнення – зазвичай метою хакера є не миттєвий прибуток, а надання послуг. Вони зламують системи великих організацій з метою виявлення ризиків, дірок або недоліків безпеки. Потім організації можуть використовувати ці результати для поліпшення безпеки своєї продукції. Такі хакери часто наймаються корпораціями в якості «пентестерів».

Зрештою, вищевказані групи можна умовно розділити три категорії: білих, сірих та чорних хакерів (white-hat/grey-hat/black-hat).

Хакери в «білому капелюсі», так звані етичні хакери, спеціалізуються на тестуванні на проникнення і інших методах забезпечення безпеки систем компанії.

По інший бік діють хакери в «чорному капелюсі», які по суті є кіберзлочинцями. Вони зламують захищені мережі, щоб знищити, змінити або вкрасти дані, або зробити системи непридатними для використання.

Посередині між ними знаходяться хакери в «сірому капелюсі», які іноді можуть порушувати законодавство чи етичні норми, не маючи при цьому злого умислу, типового для хакерів в чорному капелюсі. Вони не підкорюються законам, але намагаються досліджувати і поліпшувати безпеку систем [14].

3.2 Типи атак

Типи різних атак засновані на еталонній моделі Cisco, оскільки вона є універсальною і має багато спільного з еталонною моделлю ISO/OSI. Атаки, описані нижче є атаками, які спрямовані переважно на пристрої домашніх систем IoT і можуть представляти для них реальну загрозу [16].

3.2.1 Атаки першого рівня

Представляє собою поглиблений аналіз різних атак на перший рівень еталонної моделі, який включає самі вузли.

Відмова в обслуговуванні

Атака відмови в обслуговуванні, скорочено DoS, в загальному, є тип атаки, який зазвичай наводнює сервери, системи або мережі трафіком, щоб перевантажити ресурси жертви і утруднити чи зробити неможливим їх використання законними користувачами. DoS може являти собою 3 різних атаки на граничні обчислювальні вузли в світі Інтернету речей:

- **Розряд батареї.** Обмежені розміри пристроїв IoT призводять до того, що невеликі батареї мають дуже обмежену ємність. Цей факт зробив даний

тип атак потужним інструментом, що може призвести до серйозних наслідків, таких як вихід з ладу вузла або взагалі відмова від роботи. Наприклад, якщо зловмисник знайде спосіб розрядити акумулятор розумного датчика задимлення, він зможе відключити ввсю протипожежну систему в цілому. Якщо заміна або підзарядка акумулятора в такому пристрої неможлива, атака може привести до руйнування цілого вузла в мережі. Атака може бути реалізована шляхом відправки великої кількості випадкового трафіку на вузол і примусового запуску механізмів перевірки, таких як аутентифікація і контрольна сума пакетів.

- **Позбавлення сну.** Це особливий тип DoS-атаки, який віддалено схожий на атаку розряду батареї. Пристрої, вразливі для цієї атаки, живляться від акумулятора з обмеженою енергоємністю. Зловмисник відправляє набір запитів через певні проміжки часу, щоб саботувати механізм сну або дрімоти вузла. Виявляється набагато складніше, порівняно з атакою першого типу, оскільки пакети, як правило, сприймаються системою як легітимні і можуть не викликати підозри.
- **Атаки через збій.** Це найбільш загальний тип DoS-атак, призначений для припинення передачі інформації і виникнення системного збою. Він не дає їй змогу виконувати нормальну роботу, а в деяких випадках повністю припиняє роботу. Може бути досягнуто в результаті помилки у процесі розробки, а також внаслідок згаданої вище атаки на акумулятор, несанкціонованого фізичного доступу до пристрою або ін’єкції шкідливого коду. Добре відомим прикладом такої атаки є Stuxnet, коли шкідливий код не дозволив системі управління ядерними процесами Ірану виявити підозрілу поведінку, що призвело до неможливості активації надзвичайного стану [6].

Апаратний троян

Прямі апаратні атаки останнім часом стали серйозною проблемою для безпеки інтегральних схем. Апаратні трояни - це шкідлива модифікація схеми інтегральних схем, яка дозволяє зловмисникові обходити заходи безпеки і призвести до витоку інформації, несправності або руйнування всього пристроою або деяких його компонентів. Його також можна використовувати просто для отримання доступу до даних або програмного забезпечення, що запускається на інтегральній схемі. Ці атаки зазвичай діляться на дві основні категорії в залежності від їх механізмів запуску:

- **Зовнішньо-активований**, запускається деяким віддаленим джерелом, наприклад антеною або датчиком, який взаємодіє з зовнішнім світом.
- **Внутрішньо-активований**, активується після виконання певних умов всередині інтегральної схеми. Наприклад, схема зворотного відліку, яка запускає сценарій для активації атаки.

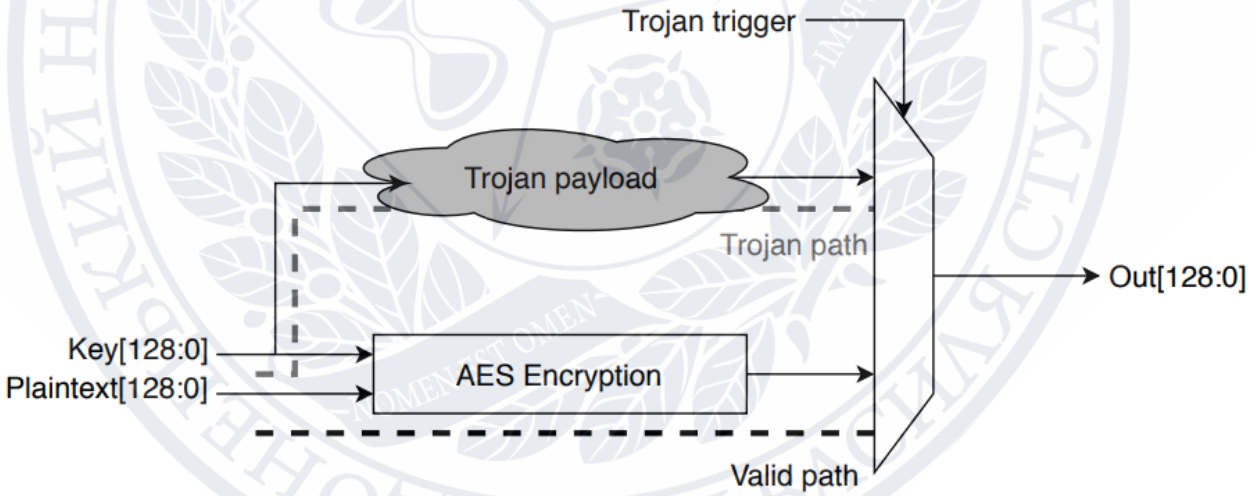

Рисунок 3.1 – Модуль шифрування AES з апаратним трояном [5]

Фізичне втручання

Периферійні пристрої часто працюють у такому середовищі, де зловмисник може отримати фізичний доступ до пристрою, що робить його вразливим як для апаратних, так і для програмних атак. Зловмисник з таким доступом може підмінити важливі компоненти схеми, витягти цінну

зашифровану інформацію, змінити операційну систему або повністю перепрограмувати пристрій. Виробники зазвичай розміщують наліпку на корпусі з інформацією за замовчуванням для доступу до пристрою. Проте більшість користувачів не змінюють дану інформацію, тим самим залишають свої пристрої незахищеними. Фізична атака на такий пристрій може призвести до незворотного знищення даних, але в більшості випадків основна мета зловмисника – витягнути необхідну інформацію для майбутнього використання. Однією з таких атак була нещодавня атака на термостат Nest, в якій зловмиснику вдалось замінити прошивку за замовчуванням на шкідливу. Це дозволило йому зберегти контроль над термостатом, навіть якщо він більше не має фізичного доступу до пристрою [6].

Безпосереднє маніпулювання вузлами

Отримання фізичного доступу до мережі відкриває можливості для нових атак. Атаки прямого маніпулювання вузлами можна розділити на кілька категорій залежно від типу операції, яка виконується з вузлом при такій атаці. Кожна з цих атак може завдати серйозної шкоди і часто призводить до значного зниження загальної продуктивності мережі.

- **Реплікація вузла** – це тип атаки, при якій зловмисник додає нові вузли до існуючого набору шляхом копіювання ідентифікаційного номера одного або декількох з вузлів, що дозволяє зловмисникові легко модифікувати або перенаправляти пакети даних. Така атака дозволяє зловмисникові отримати необхідний доступ для вилучення ключів шифрування або навіть відкликати доступ законних і авторизованих вузлів.
- **Атаки маскування** виконуються для вставки підробленого вузла або для атаки на існуючий авторизований вузол з метою маскування Цей шкідливий вузол може працювати в звичайному режимі для отримання, обробки, відправлення або перенаправлення пакетів, що розпізнається системою як активний режим. З іншого боку, пасивний режим

характеризується функцією вузла тільки для аналізу трафіку і збору даних.

- **Пошкодження вузла** – типова атака з метою отримання несанкціонованого доступу до базової мережі вузлів. Шкідливі вузли, впроваджені в мережу, можуть отримати доступ до інших вузлів, можливо, контролюючи всю систему від імені зловмисника. Вузол, що містить шкідливе ПЗ, також може використовуватися для модифікації даних, які надходять до системи або блокування чи фільтрації оригінальних повідомлень [6].

3.2.2 Атаки на рівень комунікації

Атака на з’єднання – це другий рівень еталонної моделі Cisco 2.3, який представляє собою зв'язок між пристроями.

Сніфінг-атака

Захоплення даних є однією з найвідоміших атак в мережі і відноситься до навмисного прослуховування трафіку по каналах зв'язку. Така атака перехоплює потоки даних, які можуть бути легко інтерпретовані, якщо вони не були зашифровані. Перехоплені пакети часто містять важливу інформацію, наприклад імена користувачів, паролі, конфігурацію вузлів, ідентифікатори вузлів і багато іншого. Оброблені в результаті сніфінга дані можуть бути пізніше використані для реалізації інших спеціалізованих атак. Якщо зловмисник може успішно витягти інформацію, необхідну для додавання нового вузла в набір авторизованих вузлів, він може впровадити в систему шкідливий вузол, заражений шкідливим ПЗ.

Атаки по побічним каналам

Атаки по побічним каналам на рівні зв'язку особливо ефективні проти шифрування. Суть атаки полягає у зломі криптосистеми на основі глибокого аналізу і зібраної інформації. Частина атаки по побічному каналу може

поширюватися на атаки на граничні вузли для збору електромагнітного підпису, інформації про дату, час, енергоспоживання тощо. Кожен вузол може розкривати важливу інформацію при нормальній роботі, навіть без використання бездротового зв'язку для передачі даних.

У порівнянні з рівнем граничного вузла, таку атаку можна вважати неінвазивною, оскільки вона збирає інформацію, яка випадково витекла. Типовими прикладами ненавмисного витоку інформації є діапазон частот зв'язку, модуляція сигналу і час між послідовними пакетами. Виявити такі атаки неможливо, і в результаті від них немає простого захисту, окрім як мінімізації витоку і додавання шуму до інформації [6].

Відмова в обслуговуванні

DoS-атаки також виконуються на рівні зв'язку, щоб заглушити передачу радіосигналів. Є два типи активних приглушуючих атак:

- Безперервне глушіння, яке включає в себе повне придушення всієї передачі, використовуваної для зв'язку між вузлами. Мета цієї атаки – заблокувати всі комунікації, що в результаті призведе до припинення обслуговування системи.
- Переривчасте глушіння, при якому блокування є періодичним і призводить до того, що вузли періодично відправляють і приймають пакети. У цьому сценарії зловмисник має намір знизити продуктивність систем, чутливих до часу, аби зробити систему максимально нестійкою.

У порівнянні з атаками активного глушіння, зловмисник може запустити DoS лише проти зв'язку з використанням шкідливих вузлів або маршрутизаторів. Такий елемент може навмисно порушити протокол зв'язку, який використовується в системі, і спровокувати виникнення колізій або перешкод при передачі даних [6].

Ці типи DoS-атак можуть виконуватися періодично або постійно. Безперервні атаки зазвичай легко виявити, тоді як переривчасті вимагають ефективного і точного моніторингу.

Маршрутні атаки

Маршрутні атаки націлені на те, як і куди пакети направляються на рівні зв'язку. Зловмисник може використовувати таку атаку для підробки, перенаправлення або повного видалення пакета даних з мережі. Це може бути виконано простою зміною маршрутної інформації або генерацією фальшивих повідомлень про помилку [6]. Такі атаки можна розділити на кілька категорій:

- **Атаки «чорної діри»** характеризуються використанням шкідливого вузла, який заманює весь трафік і концентрує його в одній частині мережі, «рекламуючи» йому найкоротший шлях. В результаті цієї атаки всі пакети відправляються на шкідливий вузол, щоб їх можна було обробити або відфільтрувати. Варіант цієї атаки, коли вузли вибірково відкидають деякі пакети, називається **атакою «сірої діри»**.
- **Атаки через «червоточини»** є набагато серйознішими, ніж атаки чорної або сірої діри, оскільки вони можуть бути запущені навіть з гарантією автентичності та конфіденційності всіх повідомлень. Суть цієї атаки полягає в тому, що пакети записуються в одному місці в мережі, а потім тунелюються в інше місце. По суті, вузли-червоточини підроблюють маршрут для даних, в результаті він буде коротшим ніж оригінальний в рамках мережі. Тунель повинен бути швидким шляхом, щоб створити ілюзію, що два вузли червоточини знаходяться дуже близько один до одного.

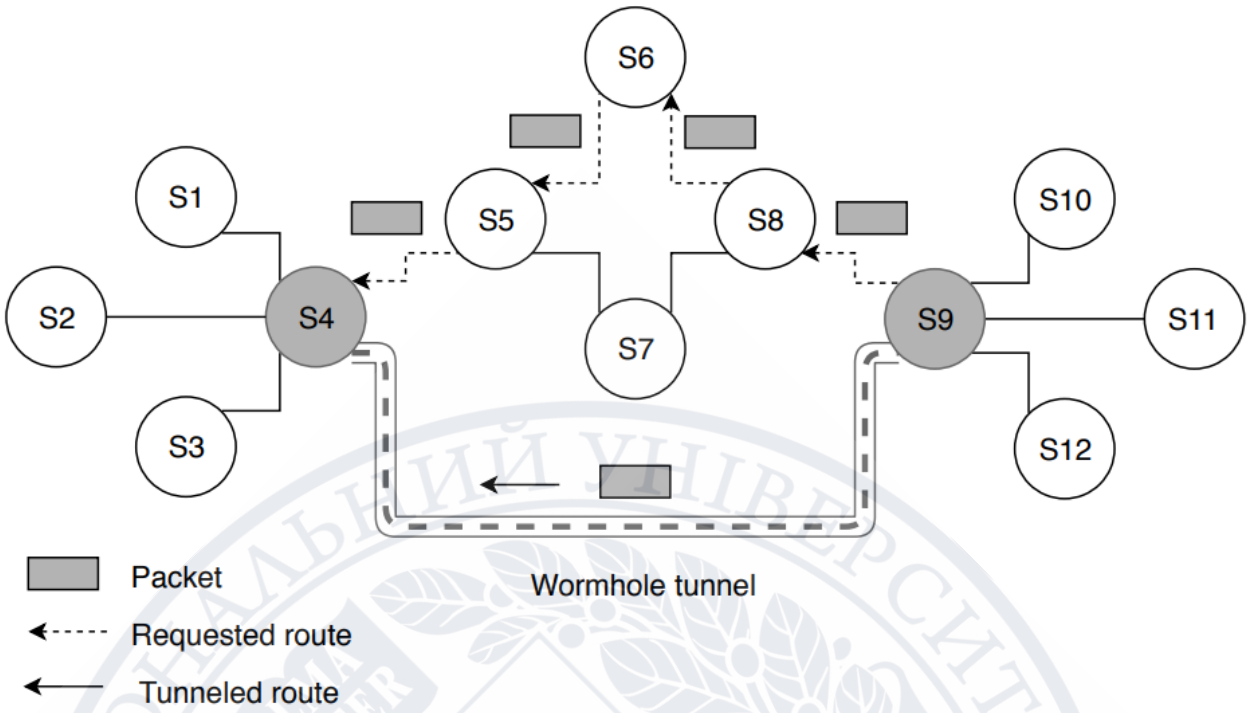

Рисунок 3.2 – Атака маршрутизації через червоточини

Як показано на рис. 3.2, пакети можуть бути тунелюватись від зараженої кінцевої точки S9 до S4. Це дає зловмиснику контроль над маршрутизацією, а також контроль над кожним пакетом, що проходить через тунельний канал червоточини [6].

- Атака **Hello Flood** заснована на тому факті, що вузли повинні постійно транслювати пакети в мережу, щоб показати свою присутність сусіднім вузлам. Якщо легітимний вузол отримує такий пакет, передбачається, що він знаходиться в зоні дії відправника. Зловмисник використовує шкідливий вузол з високою потужністю передачі для відправки пакетів Hello всім іншим вузлам в мережі і стверджує, що є їх сусідом.
- Атака **Sybil** націлена на систему репутації мережі шляхом підробки ідентифікаторів вузлів. Шкідливі вузли використовують підроблені ідентифікатори, щоб повністю виключити оригінальні вузли з системи.

3.2.3 Рівень периферійних обчислень

Периферійне або так зване туманне обчислення – це відносно нова концепція, тому її вразливості ще недостатньо вивчені. Традиційні атаки, призначені для традиційних систем та мереж, також можуть бути застосовані до систем на базі периферійних обчислень.

Ін’єкція шкідливого коду

Ін’єкція можлива, коли мережа не має суворої перевірки введення. Це може призвести до несанкціонованих дій від імені зловмисника не тільки на третьому рівні, наприклад, створення елемента для рівня зв'язку, який може вводити шкідливі вхідні дані на сервери. Такими діями зловмисник може вкрасти дані, обійти аутентифікацію або порушити цілісність бази даних. Тобто, зловмисник може навмисно «заразити» базу даних деякими помилками або виключеннями, щоб отримати відомості про таблиці бази даних та їх вміст.

Атака проти машинного навчання

Ці атаки можна розділити на два основних типи, які використовуються в системах на основі Інтернету речей: **причинні** і **дослідницькі**. При причинних атаках зловмисник маніпулює набором навчальних даних, що призводить до зміни процесу навчання на свій розсуд. У конкретної причинної атаки, так званої **атаки отруєння**, зловмисник додає точно вибрані підроблені дані в набір навчальних даних. Ця атака може бути запущена безпосередньо з сервера або побічним шляхом, додаючи достатню кількості фальшивих вузлів, щоб вплинути на процес навчання. Основна мотивація полягає в тому, щоб змусити алгоритми класифікації відхилитися від вивчення справжньої моделі, маніпулюючи набором підроблених даних.

Дослідницькі атаки не впливають на процес навчання, а скоріше використовують наявні уразливості і недоліки алгоритму машинного навчання у власних цілях.

Атака на побічні канали

Атаки по побічним каналам також здійснюються на рівні периферійних обчислень, де зловмисник може агрегувати та обробляти важливі дані з серверів і провайдерів, які генерують докладні попередження про аварійне завершення роботи внутрішньої структури системи. Зібрана інформація дедалі може бути використана для втручання в роботу системи периферійних обчислень [6].

Нестандартний API та некомпетентне тестування

Нестандартні API-інтерфейси і некомпетентне тестування – це в основному помилки в коді і недбалість виробників, що призводить до загрози конфіденційності та безпеки інформації в цілому. Оскільки системи IoT зазвичай складаються з різнорідних компонентів, API-інтерфейси повинні бути стандартизовані, щоб забезпечити зв'язок між пристроями різних брендів. Крім того, вузли зазвичай вимагають підключення до проміжних серверів, тому інтерфейси повинні бути сумісними між собою, щоб буквально розуміти і сприймати одне одного. Проте багато виробників реалізують власні самостійні протоколи та інтерфейси, тому повна сумісність не може бути гарантована, що також може призводити до витоку інформації [6].

3.3 Аналіз методів протидії атакам

3.3.1 Захист на прикладному рівні

Далі будуть описані механізми захисту, які використовуються для захисту пристроїв від атак на першому рівні еталонної моделі. Впровадження контрзаходів на прикладному рівні вимагає змін у виробничій процедурі, що може привести до збільшення вартості продукції і збільшення розмірів мікросхеми в пристроях.

Аналіз побічних каналів

Цей захід протидії забезпечує ефективний спосіб виявлення як апаратних троянів, так і шкідливого програмного забезпечення, встановленого на пристрої. Аналіз використовує сигнали побічного каналу, в тому числі час, потужність, температуру окремих компонентів і інші, для виявлення підозрілої активності.

Записані сигнали використовуються для порівняння фізичних характеристик і карти розподілу тепла на мікросхемі з еталонною мікросхемою, яка стовідсотково не заражена трояном. Наявність цієї уразливості зазвичай впливає на потужність та розподіл тепла на мікросхемі. Аналіз енергоспоживання пропонує метод моніторингу активності для виявлення підозрілих дій, що виявляються в аномальному споживанні енергії пристроєм. Методи, засновані на аналізі часу, перевіряють схему за допомогою ефективного тестування затримок. Вони чутливі до будь-яких затримок, і можуть відрізнити троян від звичайних змін в робочому процесі.

Аналіз побічних каналів може служити також для виявлення інших видів шкідливого ПЗ, встановленого на пристрої, аналогічно виявленню троянів. Аналіз може використовуватись для порівняння з еталонною поведінкою пристрою, щоб виявити аномалії, які були спричинені роботою шкідливого ПЗ, встановленого на пристрої.

Модифікація схеми

Модифікація інтегральної схеми – зазвичай дорогий і недоступний для реалізації захід протидії, але, тим не менше, він залишається найбільш ефективним проти фізичних, побічних і троянських атак. Існує кілька основних методів, які використовуються залежно від мети, яку необхідно досягти:

- **Захист від несанкціонованого доступу і самознищення** є модифікацією інтегральної схеми вузла для підвищення захисту від

фізичних атак. Посилені методи захисту від несанкціонованого доступу для розробки фізичних пакетів вузлів виявилися успішними для боротьби з більшістю спроб втручання. Крім того, реалізація механізмів самознищення забезпечує альтернативний підхід до боротьби з фізичними атаками [7].

- **Мінімізація витоку інформації** є визнаним підходом до боротьби з атаками по побічним каналам шляхом включення таких методів, як додавання випадкової затримки, навмисне створення шуму, балансування ваг Хеммінга, тим самим створюючи код з постійною вагою, покращуючи архітектуру кеша і екранування [8].
- **Інтеграція PUF-функції** (Physically Unclonable Function), яка, по суті є вбудованою функцією шуму. Коли до вузла відправляється запит, PUF генерує відповідь залежно від запиту і унікальних властивостей пристрою. PUF-файли вважаються фізично непередбачуваними і захищеними від несанкціонованого доступу, що в свою чергу забезпечує унікальну ідентифікацію та аутентифікацію пристрою, а також реалізує механізми виявлення троянів. Будь-яка ненавмисна модифікація схеми змінює її параметри, які можуть бути поміченими методами виявлення троянів [9].

Система виявлення вторгнень

Даний контрзахід, також відомий як **IDS (Intrusion Detection system)**, заснований на механізмі виявлення порушення основних політик і забезпечує непорушність загальних правил системи. Він являє собою надійний захист від атак, пов'язаних з розрядкою акумулятора чи позбавленням сну, шляхом виявлення аномальних запитів до вузлів. IDS в даний час розгортаються для моніторингу прикладних вузлів і виявлення потенційних загроз. На прикладному рівні це може бути в основному реалізовано у вигляді додатку, який відстежує двонаправлений трафік, або у вигляді частини інтегральної схеми самого вузла.

Оновлення прошивки

Оновлення прошивки можна запустити як віддалено, так і безпосередньо. Метод віддаленого оновлення прошивки включає в себе розсилання команди з бази або сервера, щоб оголосити про доступність нової версії прошивки. Виникає ієрархічний підхід, коли вузол з новою прошивкою передає оголошення сусіднім вузлам. Вузли, які також отримали оголошення, порівнюють нову версію зі своєю існуючої прошивкою і надсилають відповідний запит, якщо вони потребують оновлення. Для забезпечення безпеки віддаленого оновлення в цьому процесі, необхідно слідувати базовим вимогам концепції інформаційної безпеки: конфіденційності, цілісності та доступності. Крім того, на кожному з етапів процесу оновлення можливий ризик виникнення DoS-атаки, що обов'язково необхідно брати до уваги.

Пряме оновлення прошивки можна використовувати в критично важливих системах Інтернету речей, де потрібний мінімальний трафік для підтримки максимально можливого рівня безпеки. Фізичний інтерфейс пристрою використовується для перевірки цілісності прошивки аутентифікованим користувачем, щоб зловмисник не мав змоги замінити оригінальну прошивку пристрою на шкідливу. На рисунку 3.3 показано, як оновлення прошивки завантажується в так звану «демілітаризовану зону», скорочено DMZ. Цей процес можна використовувати для забезпечення цілісності оновлення, а також для тестування перед відправкою безпосередньо в пристрої всередині локальної підмережі.

Ізоляція

Ізоляція пристрою – це ефективна апаратна протидія загрозам для захисту конфіденційності в IoT. Такий захід може бути реалізований шляхом часткової ізоляції пристрою від електромагнітних хвиль, або їх повного екранування. В даному підході використовуються кімнати, спеціально побудовані для електромагнітної ізоляції. Існує альтернативний підхід, що

дозволяє блокувати тільки певні частоти за допомогою спеціальної металевої сітки Фарадея. Ще один спосіб – глушіння всіх довколишніх радіоканалів з допомогою активного радіочастотного випромінювача і постійним перериванням певних радіочастотних каналів. Ізоляція самої мережі також може використовуватися на більш високих рівнях еталонної моделі. Тому раціональною є ізоляція всієї підмережі IoT від інших пристроїв, щоб утримувати в захищеній системі тільки ті пристрої, які необхідні для спільної роботи. Цей метод також проілюстрований вище на рис. 3.3, він є тісно пов'язаним з децентралізацією. Навіть якщо зловмисник проникне в мережу і отримає доступ до пристрою всередині ізольованої області, він не матиме змоги отримати контроль над всією мережею. Ізоляція може бути не тільки фізичною шляхом особливості розміщення пристроїв, але і логічною на рівні віртуальної локальної мережі (VLAN).

Персональний брандмауер

Брандмауер використовується для перевірки всіх запитів, що надходять на пристрій, а в особливих випадках і трафіку, що генерується самим пристроєм. Можна припустити, що брандмауер реалізований в пристроях з досить високою обчислювальною потужністю і достатнім обсягом пам'яті для регулювання складних політик. Наприклад, пристрій може не розголошувати особисту інформацію власника, якщо він не перебуває у безпосередній близькості.

Практичне використання персональних міжмережевих екранів дозволяє фільтрувати трафік, що проходить через мережу, що може забезпечити розмежування обміну даними між авторизованими пристроями та користувачами у відповідних розділах мережі. Реалізація брандмауерів також забезпечує існування DMZ, тим самим додає ще один ефективний рівень безпеки в мережу.

Шифрування

Шифрування являє собою основним засобом протидії загрозам безпеки на прикладному рівні. Є кілька основних типів криптографічних схем:

- **Схеми на основі хешування** широко використовуються для захисту пристроїв з жорсткими обмеженнями. Для кожного пристрою з низькою продуктивністю визначено два робочих стани:
  - **Заблокований стан**, коли пристрій відповідає на всі запити своїм хеш-ключем.
  - **Розблокований стан**, при якому пристрої працюють нормально.

Щоб розблокувати пристрій, зчитувач відправляє запит до внутрішньої бази даних і очікує отримання хеш-ключа. Потім зчитувач відправляє ключ заблокованому пристрою, який після перевірки змінює свій стан на розблокований.

- **Полегшені криптографічні протоколи** є найбільш ефективною мірою протидії загрозам на прикладному рівні, але поки що недостатньо стандартизованою для впровадження в пристроях. Найбільша проблема полегшеного шифрування – зробити систему досить стійкою, щоб протистояти зовнішнім загрозам, маючи при цьому мінімально можливі вимоги до потужності обладнання [10].

3.3.2 Захист на рівні зв'язку

Більшість атак, виявлених як в звичних мережах, так і в IoT мережах, спрямовані саме на комунікативний рівень, тому необхідно реалізувати належні механізми захисту для забезпечення безпеки таких систем.

Надійна маршрутизація

Маршрутизація з надійною доставкою в мережі Інтернету речей має складну реалізацію через особливості характеру IoT в цілому. Проміжним вузлам або серверам може знадобитися прямий доступ до вмісту повідомлення перед його пересиланням, що ускладнює реалізацію протоколів безпечної маршрутизації, а також стає вразливим для різних атак маршрутизації. З

іншого боку, протоколи, засновані на симетричному шифруванні не є придатними для використання в мережі IoT через додаткові витрати на обробку пакетів та процеси обчислювання. Ці протоколи призначені для пошуку і встановлення маршрутів між будь-якою парою пристроїв.

Це означає те, що спеціалізовані протоколи надійної маршрутизації для Інтернету речей, які будуть стійкими до всіх атак на основі маршрутизації, все ще знаходяться в розробці. На даний момент використовуються протоколи, які стійкі лише до деякого ряду атак. На основі розгортання і вимог мережі IoT реалізується відповідний протокол маршрутизації [11].

Система виявлення вторгнень

IDS також необхідна і на рівні зв'язку, в якості альтернативної лінії захисту для моніторингу мережевих операцій і попередження будь-якої підозрілої активності. У порівнянні з програмними IDS на прикладному рівні, їх реалізація на рівні зв'язку є повністю апаратною, як фізичний датчик, розміщений в мережі. Цей підхід також відомий як система виявлення вторгнень в мережу (NIDS – Network Intrusion Detection System), в якій пристрій розміщується в стратегічно-важливих точках мережі.

Звичайні IDS в значній мірі адаптовані для бездротових сенсорних мереж, де пристрої не вимагають прямого підключення до Інтернету. Хоча недавні пропозиції IDS спрямовані на вирішення проблем безпеки та конфіденційності в мережах IoT. SVELTE – це недавно розроблена полегшена система IDS, доповнена міні-брандмауером для задоволення вимог IoT пристроїв з використанням IPv6. Його можливості полягають у виявленні атак маршрутизації разом із зараженим трафіком, нехарактерним для систем Інтернету речей [5].

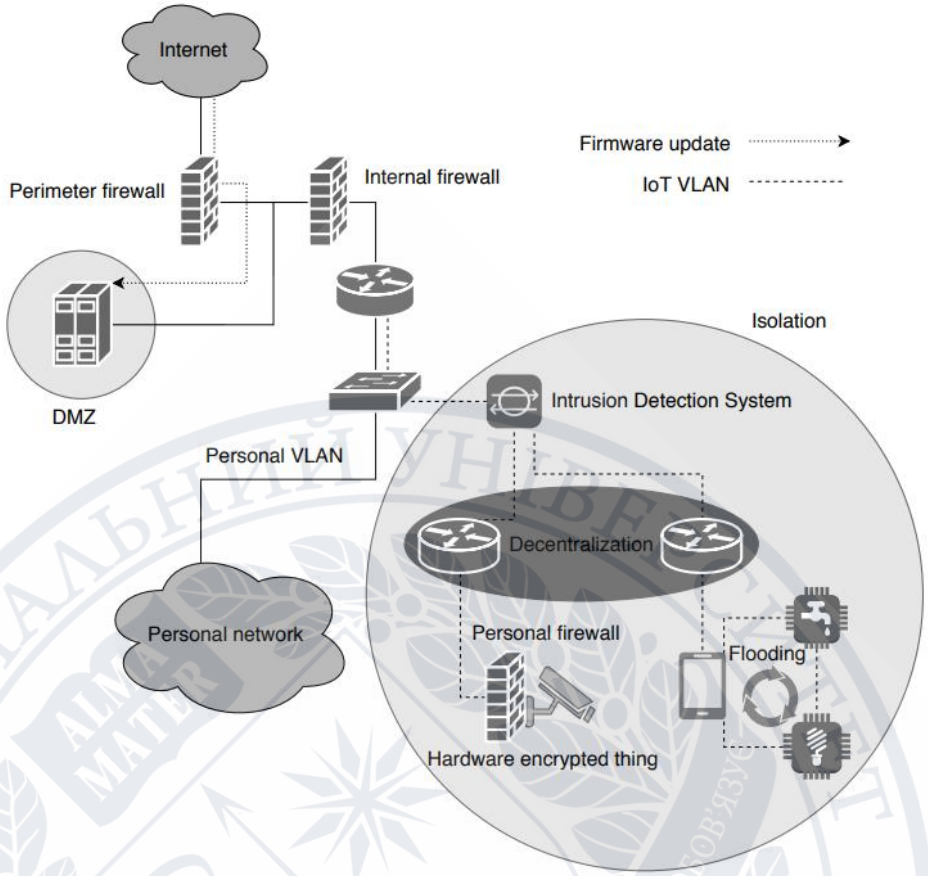

Рисунок 3.3 – Заходи протидії загрозам в Інтернеті речей

Рисунок 3.3 в цілому пояснює організацію контрзаходів для створення безпечної мережі IoT. Дизайн цієї мережі допускає наявність демілітаризованої зони, яка може бути надзвичайно корисним механізмом безпеки для захисту внутрішньої мережі.

Рисунок демонструє співіснування персональної мережі з мережею виключно для пристроїв Інтернету речей. Комутатор використовується для поділу підмереж на окремі віртуальні локальні мережі. Це додає ще один рівень безпеки на випадок втручання.

IDS, присутня в мережі, використовується для відстеження та виявлення будь-яких ознак зловмисної активності або порушень політики безпеки.

Далі, після IDS використовуються два окремих маршрутизатора, виділених для підмереж IoT, які служать для децентралізації. Така фрагментація мережі IoT зменшує розмір домена, схильного до атаки.

І, нарешті, в системі є наявний персональний брандмауер, який використовується з метою забезпечення зв'язку між потрібними кінцевими точками або адресами. Апаратне шифрування розширює концепцію вищезгаданих схем криптографії. Використання апаратного шифрування, а також передача шифрування виділеним захищеним апаратним схемам зводить до мінімуму ймовірність використання вразливостей програмного шифрування. Такий тип контрзаходів вирішує майже всі проблеми. Навіть якщо зловмисник отримає доступ до підмережі, яка містить виключно IoT пристрої, він зіткнеться з потоком даних, який протидіятиме атакам, заснованих на маршрутизації або перехопленні інформації.

Криптографічні схеми

Криптографічні схеми забезпечують надійне шифрування для захисту протоколів зв'язку в якості механізму захисту від атак маршрутизації, перехоплення, підслуховування та інших. Однак більшість методів шифрування і дешифрування неспроможні виконуватись безпосередньо на рівні зв’язку в IoT через достатньо високі вимоги, що призводить до більш високого енергоспоживання, використання пам'яті, затримки і можливої втрати пакетів. Полегшені методи шифрування з відкритим ключем, які б задовольняли всі вимоги систем Інтернету речей, все ще знаходяться в розробці [6].

Депаттернізація і децентралізація

Ці контрзаходи в основному використовуються в якості розширеного захисту від атак на побічні канали і забезпечують анонімність мережі. Однак завжди існує компроміс між анонімністю і необхідністю взаємозв'язку для спілкування. Депаттернізація передачі даних може захистити систему від атак по побічним каналам, таких як аналіз трафіку, шляхом вставки підроблених пакетів в потік даних, що призводить до значної зміни структури трафіку. З іншого боку, децентралізація забезпечує анонімність за рахунок розподілу

конфіденційних даних в такій області, при якій жоден вузол не має повного уявлення про вихідні дані.

На рисунку 3.3 децентралізація відбувається за рахунок використання декількох маршрутизаторів для пристроїв IoT, що призводить до створення відокремлених мереж.

Управління доступом на основі ролей

Авторизація на основі ролей використовується для запобігання відповіді на запит зловмисників або шкідливих вузлів в системі, вимагаючи перевірки кожного компонента в мережі. Різні компоненти, що взаємодіють в мережі, мають різні ролі і права, наприклад, постачальник послуг або маршрутизатор можуть отримувати доступ, спільно використовувати або змінювати інформацію на основі їх повноважень. У схемі з авторизацією на основі ролей кожне повідомлення перевіряється системою авторизації, а саме чи перевірені всі учасники комунікації і чи мають вони необхідні повноваження [4].

Флуд

Механізм аналізу трафіку на основі флуду використовується для запобігання відстеження зовнішнього зловмисника розташування джерела даних, оскільки пакети можуть містити місце розташування вузлів. Флуд можна розділити на три систематичних підходу.

- **Базова техніка флуду** заснована на тому, що кожен вузол в мережі пересилає кожен пакет тільки один раз, повторна передача одного і того ж пакету неможлива. Якщо вузол отримує пакет вперше, він передає його всім своїм сусідам, в іншому випадку пакет ігнорується. Це забезпечує захист конфіденційності, оскільки майже кожен вузол в мережі приймає участь у пересиланні даних, і зловмисник може потрапити не в те джерело. Однак це доволі енерговитратний метод обміну даними.

- **Імовірнісний флуд** включає в себе практично той самий механізм, лише з однією різницею, що тільки деяка кількість вузлів у всій мережі бере участь у пересиланні даних, решта учасників ігнорує отримані пакети. Це покращує загальну енергоефективність за рахунок скорочення шляху проходження пакету, але деякі пакети можуть бути втрачені.
- **Фантомний флуд** розширює імовірнісний метод, приводячи зловмисника до підробленого джерела, зберігаючи при цьому короткий реальний шлях. Він складається з двох етапів:
    - **Фаза «блукання»**, також називається фазою випадкового блукання.
    - **Фаза флуду** призначена для подальшої доставки повідомлення адресату.

  Коли джерело надсилає пакет даних, він розсилається випадковим чином в межах кількох перших переходів у першій фазі. Після чого повідомлення передається з використанням базової техніки з перемиканням на другу фазу. Кількість переходів є змінною, що безпосередньо впливає на характеристики алгоритму, такі як конфіденційність та затримка всередині мережі.

Практичне використання технік флуду можна побачити на рисунку 4.3. У такій невеликій мережі зловмисник, скоріше за все, перехопить повідомлення, які можуть привести його до реального джерела трафіку, тому флуд може банально заплутати зловмисника. Система намагається направити пакети в різні місця в мережі, щоб зловмисник не мав можливості отримувати постійний потік пакетів для відстеження джерела [6].

3.3.3 Захист на рівні периферійних обчислень

У цьому розділі наведено рішення щодо усунення загроз безпеки на рівні периферійних обчислень. Однак, оскільки це нова технологія, її уразливості все ще досліджуються.

Попереднє тестування

Перш ніж їх впроваджувати заходи в критично важливу систему, вкрай важливо протестувати дизайн та оновлення. Попереднє тестування слід використовувати для ретельного вивчення поведінки всієї системи і її компонентів (маршрутизаторів, сервера тощо.) шляхом надання різних вхідних даних в систему і моніторингу вихідних даних. Його також можна використовувати для моделювання можливих сценаріїв атаки, щоб оцінити поведінку системи. Крім того, на етапі тестування необхідно задати рівень ведення журналу, а вхідні файли повинні бути перевірені на предмет можливості ін’єкції шкідливого коду, щоб не допустити виконання будь-яких неавторизованих команд [6].

РОЗДІЛ 4
ОЦІНКА РИЗИКІВ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей привів до відсутності гармонізації та спільного бачення, коли справа доходить до питань безпеки, які створює ця технологія. На даний момент ISO опублікувала стандарти взаємодії і архітектури IoT, але опублікованих міжнародних стандартів безпеки та конфіденційності щодо IoT немає. На міжнародному рівні існує тільки один стандарт безпеки та конфіденційності IoT, що входить в сімейство ISO27k – це ISO/IEC 27030, але він все ще знаходиться на ранній стадії розробки. Але навіть ISO/IEC 27030 – це стандарт, який пропонує керівні принципи, а не вимоги, і тому не є стандартом, за яким організації, що займаються IoT, можуть пройти сертифікацію.

Ця невідповідність перешкоджає стандартизації та впровадження ефективних правил безпеки і конфіденційності IoT, таких як **«Privacy By Design»**. Кіберзлочинці з кожним днем стають все більш витонченими і відкривають для себе різні методи атак на системи безпеки. Це викликає побоювання, що відсутність узгодженості може привести до того, що аналіз ризиків безпеки, оцінка ризиків і контрзаходи стануть важкими завданнями. З цієї причини важливо створювати безпечні рішення, які були б націлені на захист постійно зростаючого числа «речей», які пов'язані між собою через глобальну мережу Інтернет.

В даному розділі наведено огляд найпоширеніших методологій управління ризиками, а також проілюстровано управління ризиками безпеки Інтернету речей для розумної кімнати / розумного будинку.

4.1 Поширені методології оцінки ризиків

З огляду на унікальний характер кіберзагроз та вразливостей систем IoT, система управління ризиками IoT вимагає розуміння як технологій кібербезпеки IoT, так і існуючих структур управління ризиками. Існує безліч

конкуруючих і доповнюючих одне одного систем управління ризиками, проте, як зазначено вище, жодна з них не здатна цілком відповідати вимогам архітектури Інтернету речей.

Однією з найпопулярніших структур кібербезпеки є **NIST** – «Система кібербезпеки Національного інституту стандартів і технологій». Фреймворк складається з ядра, рівнів реалізації і профілю структури. Ядро фреймворка описує п'ять функцій програми кібербезпеки. Рівні реалізації описують ступінь, в якій методи управління кібербезпекою організації демонструють конкретні можливості кібербезпеки, певні на рівнях. Організація може використовувати профіль структури для визначення можливостей розвитку свого стану кібербезпеки, шляхом порівняння «поточного» профілю з «еталонним» профілем.

ISO/IEC 27005 – набір стандартів, розроблений Міжнародною організацією зі стандартизації **(ISO)** і Міжнародної електротехнічної комісією **(IEC).** Стандарт пропонує основні принципи і методи для реалізації і управління ризиками інформаційної безпеки. Хоча ISO/IEC 27005 забезпечує структуровану послідовність дій, він не використовує безпосередньо якийсь конкретний метод управління ризиками. Тобто очікується, що організація визначить свій власний підхід до управління ризиками, в залежності від типу системи управління інформаційною безпекою, стану ризику, стану управління і / або галузеві проблеми безпеки.

Сім етапів **Cyber Kill Chain® (CKC)** – це система управління ризиками, розроблена Lockheed Martin. Модель аналізує, як діє кіберзловмисник для досягнення своїх цілей, і пропонує заходи протидії, які повинен зробити спеціаліст, щоб розірвати ланцюжок як на ранній, так і на більш пізніх стадіях. Основна увага в цій структурі приділяється технологічній стороні кібербезпеки за участю зловмисників і спеціалістів з ІБ, але не повністю вирішуються людські та організаційні проблеми ризиків, такі як людський фактор чи внутрішні загрози.

Оцінка критичних загроз, активів і вразливостей **(OCTAVE)** – це структура оцінки безпеки, розроблена в Координаційному центрі CERT (R) (Піттсбург, Пенсільванія, США). OCTAVE допомагає організації ідентифікувати і ранжувати ключові IT-активи, зважувати загрози для цих активів, аналізувати їх уразливості і вплив, а також визначати пріоритети безпеки для зниження ризику для IT-активів. В основі OCTAVE лежить концепція самоврядування, за допомогою якої невелика міждисциплінарна команда, що складається з власних відділів організації, керує процесом оцінки організації. Вихідна версія OCTAVE пізніше була оновлена до **OCTAVE Allegro**, щоб спростити реалізацію інфраструктури в організації. OCTAVE Allegro дозволяє проводити широку оцінку середовища операційних ризиків організації в умовах спільної роботи в стилі семінарів без необхідності в великих знаннях з оцінки ризиків.

Нижче наведено список деяких вузьконаправлених стандартів, так чи інакше пов'язаних з безпекою Інтернету речей:

- **X.1362** (Процедура шифрування для середовищ IoT)
- **Y.4102 / Y.2074** (Вимоги до пристроїв IoT і програми, які працюють IoT під час лих)
- **Y.4455** (Еталонна архітектура для розкриття можливостей мережевих послуг IoT)
- **Y.4118** (Вимоги та технічні можливості IoT для підтримки обліку та нарахування плати)
- **Q.3952** (Архітектура і можливості модельної мережі для тестування IoT)
- **Y.4702** (Загальні вимоги та можливості керування пристроями в IoT)
- **Q.3913** (Набір параметрів для моніторингу пристроїв IoT)
- **Агентство Європейського Союзу з мережевої та інформаційної безпеки (ENISA)**: «Базові рекомендації з безпеки для IoT в контексті критично важливих інформаційних інфраструктур»
- **ISO/IEC 27030** (Рекомендації з безпеки і конфіденційності в IoT)

- **Офіційний документ NIST (White Paper)** з кібербезпеки (питання довіри до Інтернету речей)

4.2 NIST IR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

В даному стандарті визначено три загальних фактора, які можуть вплинути на управління ризиками кібербезпеки і конфіденційності для пристроїв IoT, в порівнянні зі звичайними IT-пристроями:

1. ***Більшість пристроїв IoT взаємодіють з фізичним світом так, як зазвичай не роблять звичайні IT-пристрої.*** Потенційний вплив деяких пристроїв IoT, що вносять зміни в фізичні системи і, таким чином, впливають на фізичний світ, необхідно чітко усвідомлювати і вирішувати з точки зору кібербезпеки і конфіденційності. Крім того, експлуатаційні вимоги до продуктивності, надійності, відмовостійкості та безпеки можуть суперечити загальноприйнятим практикам кібербезпеки і конфіденційності для звичайних IT-пристроїв.
2. ***Більшість пристроїв IoT недоступні для управління або моніторингу так само, як звичайні IT-пристрої.*** Це може вимагати виконання завдань вручну для великої кількості пристроїв IoT, розширення знань персоналу та інструментів для включення набагато більш широкої різноманітності програмного забезпечення пристроїв IoT і усунення ризиків, пов'язаних з виробниками та іншими третіми особами, які мають віддалений доступ або контроль над пристроями IoT.
3. ***Доступність, ефективність та дієвість можливостей кібербезпеки і конфіденційності для пристроїв IoT часто відрізняється від звичайних IT-пристроїв.*** Це означає, що організаціям, можливо, доведеться обирати, впроваджувати і керувати додатковими засобами контролю, а також визначати, як реагувати на ризик, коли засоби контролю для зниження ризику відсутні.

4.2.1 Взаємодія пристрою з фізичним світом

Багато пристроїв IoT взаємодіють з фізичним світом так, як зазвичай не роблять звичайні IT-пристрої.

Взаємодія з фізичним світом, яку забезпечують пристрої IoT, може вплинути на ризики кібербезпеки і конфіденційності декількома способами:

- Дані датчиків, що представляють вимірювання фізичного світу, завжди пов'язані з невизначеністю. Ефективне управління даними з датчиків, включаючи розуміння невизначеностей, необхідно для оцінки якості і значення даних, щоб організації могли приймати рішення щодо використання даних і уникати появи нових ризиків. Без цього частота помилок може бути невідома для різних контекстів, в яких може використовуватися пристрій IoT. Ефективне управління даними датчиків IoT важливо при пом'якшенні фізичних атак на сенсорні технології, таких як атаки, що здійснюються за допомогою бездротових сигналів, які можуть викликати спрацьовування датчиків і призводять до помилкових результатів.
- Повсюдне поширення датчиків Інтернету речей в громадських і приватних місцях можуть сприяти збору та аналізу величезних обсягів даних про людей. Ці дії можуть використовуватися, щоб впливати на поведінку або прийняття рішень людей, або приводити до розкриття інформації, яку люди не бажають розкривати, включаючи повторну ідентифікацію раніше знеособлених персональних даних і можуть виходити за рамки передбачуваного обсягу роботи пристрою IoT.
- Пристрої Інтернету речей з виконавчими механізмами можуть вносити зміни в фізичні системи і, таким чином, впливати на фізичний світ. Потенційний вплив цього необхідно чітко усвідомлювати і розглядати з точки зору кібербезпеки і конфіденційності. У гіршому випадку компрометація може дозволити зловмиснику використовувати пристрої IoT, щоб поставити під загрозу безпеку людей, пошкодити або знищити обладнання та об'єкти або викликати серйозні збої в роботі.

- Мережеві інтерфейси IoT часто забезпечують віддалений доступ до фізичних систем, до яких раніше можна було отримати доступ тільки локально. Виробники, постачальники та інші треті сторони можуть використовувати віддалений доступ до пристроїв Інтернету речей для управління, моніторингу, обслуговування та усунення неполадок. Це може збільшити схильність фізичних систем до набагато більшого ризику злому через пристрої IoT.

4.2.2 Функції доступу до пристрою, управління і моніторингу

Більшість пристроїв IoT недоступні для управління або моніторингу так само, як звичайні IT-пристрої.

Звичайні пристрої зазвичай надають уповноваженим людям, процесам та іншим пристроям доступ до апаратного та програмного забезпечення, а також функції управління і моніторингу. Іншими словами, авторизований адміністратор, процес або пристрій можуть безпосередньо звертатися до вбудованого ПО, ОС і додатків звичайного IT-пристрою, повністю керувати пристроєм і його програмним забезпеченням протягом усього життєвого циклу пристрою в міру необхідності, а також контролювати внутрішні характеристики і стан пристрою в будь-який час. Авторизовані користувачі також можуть отримати доступ до обмеженого набору функцій доступу, управління і моніторингу.

Уповноважені люди, процеси та пристрої можуть зіткнутися з однією або декількома з наступних проблем при доступі, управлінні та моніторингу пристроїв IoT, які впливають на кібербезпеку та ризики конфіденційності:

- Відсутність функцій управління.
- Відсутність інтерфейсів.
- Труднощі з масштабним управлінням.
- Широкий вибір програмного забезпечення для управління.
- Різна тривалість життя пристроїв.

- Несправне обладнання.
- Відсутність інвентарних можливостей.
- Гетерогенна власність.

4.2.3 Доступність, ефективність та дієвість можливостей кібербезпеки і конфіденційності

Доступність, ефективність та дієвість можливостей кібербезпеки і конфіденційності для пристроїв IoT часто відрізняється від звичайних IT-пристроїв.

Передпродажні можливості інтегруються в пристрої Інтернету речей виробником або постачальником до того, як вони будуть відправлені клієнтам. Пост-ринкові можливості – це ті можливості, які організації вибирають, набувають і розгортають самі на ряду з передпродажними можливостями. Можливості кібербезпеки і конфіденційності до і після виходу на ринок для пристроїв IoT часто відрізняються від звичайних IT-пристроїв. Основними причинами цього є:

- Багато пристроїв IoT не підтримують або не можуть підтримувати ряд функцій кібербезпеки і конфіденційності, які зазвичай вбудовані в звичайні IT-пристрої. Якщо для пристроїв IoT доступні передпродажні можливості, вони можуть бути недостатніми з точки зору надійності або продуктивності, наприклад, використання надійного шифрування і взаємної аутентифікації для захисту зв'язку може викликати неприпустимі затримки.
- Рівень зусиль, необхідних для управління, моніторингу та підтримки передпродажних можливостей кожного пристрою IoT, може бути надмірним. Особливо, коли пристрої IoT не підтримують централізоване управління, може бути більш ефективним реалізувати і використовувати централізовані пост-ринкові можливості, які допомагають захистити

численні пристрої IoT, замість того, щоб намагатися досягти еквівалентного рівня захисту на кожному окремому пристрої IoT.

- Деякі пост-ринкові можливості традиційних IT-пристроїв, такі як мережеві системи запобігання вторгнень, сервери захисту від шкідливих програм і брандмауери, можуть виявитися не настільки ефективними для захисту пристроїв IoT. Пристрої Інтернету речей часто використовують протоколи, які звичайні IT-служби не можуть зрозуміти і проаналізувати за допомогою засобів управління кібербезпекою і конфіденційністю. Крім того, пристрої IoT можуть безпосередньо зв'язуватися один з одним, наприклад, за допомогою бездротового зв'язку типу «точка-точка», замість використання контрольованої мережі інфраструктури.

Пристрої IoT можуть не використовувати деякі з можливостей кібербезпеки і конфіденційності, які використовують звичайні IT-пристрої – прикладом є пристрій IoT без функції зберігання даних, якому не потрібно захищати свої дані в стані спокою. Пристрою IoT також можуть знадобитися додаткові можливості, які не використовуються в більшості звичайних IT-пристроїв, особливо якщо пристрій IoT забезпечує взаємодію з фізичним світом.

4.2.4 Ризики кібербезпеки і конфіденційності

NIST поставив три основні цілі для оцінки ризиків Інтернету речей: захист пристрою, захист даних і конфіденційність користувачів. Вони описані нижче в Таблиці 4.1:

Захист пристроїв	Запобігання використання пристрою для проведення атак, включаючи участь в розподілених атаках типу «відмова в обслуговуванні» (DdoS) проти інших організацій, а також перехоплення мережевого трафіку або компрометацію інших

	пристроїв в тому ж сегменті мережі. Дана мета може бути застосована до всіх пристроїв Інтернету речей.
Захист даних	Захист конфіденційності, цілісності і / або доступності даних (включаючи особисту інформацію), що збираються, зберігаються, обробляються чи передаються на пристрій IoT або з нього. Дана мета застосовується до всіх пристроїв Інтернету речей, крім тих, які не містять даних, що підлягають захисту.
Конфіденц. користувачів	Мета застосовується до всіх пристроїв IoT, які прямо чи опосередковано впливають на життєдіяльність людини.

Таблиця 4.1 – Категорії оцінки ризиків Інтернету речей за NIST

Кожна мета грунтується на попередній, не замінює її і не скасовує необхідність в ній. Досягнення кожної з цілей зниження ризику включає розгляд набору областей зниження ризику. Кожна область визначає аспект кібербезпеки або зниження ризику конфіденційності. Для кожної області зниження ризиків існує одне або кілька очікувань щодо того, як звичайні IT-пристрої допомагають знизити ризики кібербезпеки і конфіденційності в цій області. Області зниження ризиків для кожної з цілей вказано в таблиці 4.2:

Мета 1. Захист пристрою	
Управління активами	Точна інвентаризація всіх пристроїв IoT і їх відповідних характеристик протягом усього життєвого циклу пристроїв, щоб використовувати цю інформацію в цілях кібербезпеки і управління ризиками конфіденційності.
Управління вразливостями	Виявлення та усунення відомих вразливостей в програмному забезпеченні і прошивці пристроїв IoT, щоб знизити ймовірність несанкціонованого втручання.
Управління доступом	Запобігання несанкціонованому та неналежному фізичному чи логічному доступу, використанню і

	адмініструванню пристроїв IoT людьми, процесами та іншими обчислювальними пристроями.
Виявлення інцидентів безпеки пристроїв	Відстеження та аналіз активності пристроїв IoT на предмет ознак інцидентів, пов'язаних з безпекою пристроїв.
Мета 2. Захист даних	
Захист даних	Запобігання несанкціонованого доступу до даних, що знаходяться в стані спокою або при передачі, які можуть розкрити конфіденційну інформацію або дозволяють маніпулювати чи порушувати операції при роботі пристроїв.
Виявлення інцидентів безпеки даних	Відстеження і аналіз активності пристроїв IoT для виявлення ознак інцидентів, пов'язаних з безпекою даних.
Мета 3. Конфіденційність користувачів	
Управління інформаційними потоками	Підтримка поточного відображення інформаційного життєвого циклу персональної інформації, включаючи тип дії з даними, елементи, оброблювані дією даних, суб’єкт, що виконує обробку, і будь-які додаткові відповідні контекстуальні фактори, пов'язані з обробкою. для використання в цілях управління ризиками конфіденційності.
Управління дозволами на обробку ПД	Підтримка дозволів на обробку персональних даних для запобігання несанкціонованої обробки інформації.
Ухвалення поінформованих рішень	Дозволяє людям розуміти наслідки обробки ПД і взаємодії з пристроєм, брати участь у прийнятті рішень

	щодо взаємодії і обробки даних, а також вирішувати проблеми.
Управління непов'язаними даними	Визначення дозволу обробки ПД і визначення того, як ПД можуть бути мінімізовані чи відокремлені від окремих осіб і пристроїв IoT.
Виявлення порушень конфіденційності	Відстеження і аналіз активності пристроїв Інтернету речей на предмет порушень конфіденційності окремих осіб.

Таблиця 4.2 – Області зниження ризиків IoT

4.2.5 Шкала оцінки ризиків та ранжування

Першим кроком в оцінці ризику є виявлення загроз для розглянутого активу IoT з подальшим визначенням невід'ємного ризику і його впливу. Вплив ризику має такі рейтинги, як високий, середній і низький. Наприклад, «високий» рейтинг впливу означає, що вплив може бути досить значним. Середній означає, що удар буде руйнівним, але відновити події і / або незручним. Низький означає, що вплив буде мінімальним або відсутній. Наступним кроком є визначення ймовірності даного експлойта з урахуванням контрольного середовища. Приклади рейтингів ризику:

- **Високий** – джерело загрози високо мотивоване і доволі дієздатне, а заходи щодо запобігання використання уразливості є неефективними.
- **Середній** – джерело загрози мотивоване і дієздатне, але існують засоби контролю, які можуть перешкодити успішному використанню уразливості.
- **Низький** – джерелу загрози бракує мотивації або можливостей, або існують засоби контролю для запобігання або, принаймні, значної перешкоди для реалізації уразливості.

Рейтинг ризику може бути розрахований за формулою:

рейтинг ризику (rr) = вплив × ймовірність

Приклади ранжування:

- **Серйозний** – існує значна і невідкладна загроза для об’єкту, і усунення ризиків має здійснюватися негайно.
- **Підвищений** – існує реальна загроза для об’єкту, і усунення ризиків має бути завершено в розумні терміни.
- **Низький** – загрози в цілому прийнятні, але все ж можуть мати деякий вплив на об’єкт. Впровадження додаткових рішень з безпеки може забезпечити додатковий захист від потенційних або непередбачених загроз.

Розрахунок рангу ризику виконується на основі вагомості ризику (це відноситься до впливу ризику) і оцінки ризику (це відноситься до ймовірності ризику).

Якісний рівень	**Вагомість (W)**	**Оцінка ризику (RS)**	**Ранг ризику (RR) = W * RS (приклад)**	**Діапазон RR**	**Опис**
Дуже високий	*96-100*	*1.0*	*97 × 1,0 = 97*	*81–100*	*надзвичайно сильний вплив*
Високий	*80-95*	*0.8*	*90 × 0,8 = 72*	*51–80*	*велике занепокоєння*
Середній	*31–79*	*0.5*	*50 × 0,5 = 25*	*21–50*	*помірне занепокоєння*
Низький	*11-30*	*0.2*	*25 × 0,2 = 5*	*5-20*	*не викликає занепокоєння*
Дуже низький	*1-10*	*0.1*	*10 × 0,1 = 1*	*0-4*	*не викликає занепокоєння*

Таблиця 4.3 – Приклад ранжування ризиків

4.3 Результати дослідження загроз

Результати дослідження, представлені в Таблицях 4.4 і 4.5, дають кращий огляд виявлених загроз безпеки і потенційних ризиків в середовищі розумного будинку на основі Інтернету речей. У двох таблицях показані інформаційні активи, які були ідентифіковані і використані в процесі оцінки ризиків, пов'язані з ними загрози, а також наслідки чи потенційний вплив у формі конкретних ризиків і їх оцінки.

У таблиці 4.4 наведено загрози, виявлені в результаті вивчення всієї системи розумного будинку на основі Інтернету речей, з точки зору інформаційної і фізичної перспективи, у відповідності з різними активами. В таблиці 4.5 визначено можливі дії або потенційні ризики, пов'язані з активами і загрозами, згаданими в таблиці 4.4.

ID	Інформаційний актив	Можливі загрози безпеки
1	Облікові дані користувача	Видача себе за користувача; Крадіжка персональних і облікових даних
2	Мобільні особисті дані і додатки	Шкідливий код, впроваджений в мобільні додатки, що встановлені на телефоні
3	Інформація, що збирається пристроями та інформація про стан розумного будинку	Модифікація інформації; Атаки типу «відмова в обслуговуванні»; Злом пристрою або датчика; Розкриття інформації; Переривання важливих функцій
4	Пристрої розумного будинку / інвентарна інформація	Отримання доступу до інвентарної інформації для пошуку певного пристрою з відомими вразливостями для атаки на розумний будинок
5	Інформація з журналу	Отримання доступу до даних журналу і отримання корисну інформацію, що

		дозволяє атакувати систему розумного будинку
6	Інформація, передана через шлюз	Викрадення інформації з пакетів, що передаються через шлюз
7	Інформація про налаштування розумного будинку	Модифікація інформації
8	Відео з камер спостереження	Дистанційне керування камерами, з метою стеження за користувачами і шпигування за ними
9	Інформація про місцеположення	Спостереження за трафіком даних про місцезнаходження
10	Інформаційні ресурси (наприклад, зображення, документи та мультимедіа)	Викрадення особистої інформації; Недоступність носіїв через збій в обладнанні

Таблиця 4.4 – Основні інформаційні загрози активів для Розумного будинку

ID	**Можливі наслідки вказаного ризику**	**RR**
1	Несанкціонований доступ до основної системи розумного будинку; Несанкціоноване виконання операцій; Втрата контролю над системою розумного будинку	41
2	Зловмисник може робити фотографії, записувати розмови і відстежувати місцеположення; Зловмисник може керувати смартфоном віддалено; Зловмисник може здійснювати дзвінки і отримувати доступ до мікрофона та камери телефону	41
3	Маніпуляція роботою датчиків, щоб проникнути в домашню систему; Відстеження відсутності людей веде до вторгнення в будинок; Фінансові втрати	39

4	Визначення найслабшого пристрою системи з відомими вразливостями; Отримання контролю над системами розумного будинку в цілому; Фінансові втрати	39
5	Знаходження способу доступу до основної системи; Зловмисник змінює конфігурацію системи і додає лазівки (backdoor); Фінансові втрати	39
6	Системні ресурси виснажуються через постійний перезапуск; Можливість вивести систему з ладу, зробивши її повністю непридатною для використання; Можливість впровадження нових вразливостей безпеки в систему;	39
7	Складність правильного налаштування системи розумного будинку; Неправильне використання систем розумного дому з можливістю виведення його з ладу;; Фінансові втрати	36
8	Порушення конфіденційності користувача Фінансові втрати	34
9	Порушення конфіденційності користувача; Проникнення в розумний будинок за відсутності власника; Фінансові втрати	34
10	Порушення конфіденційності користувача Втрата інформації Збиток репутації	23

Таблиця 4.5 – Ризики безпеки, виявлені при виконанні оцінки з точки зору можливих впливів на безпеку

4.4 Контрзаходи

Можливі контрзаходи з метою захисту інформаційних активів і, отже, підвищення безпеки розумного будинку, представлені в таблиці 4.6. Ключовими концепціями пропонованих підходів до пом'якшення наслідків є

правильні технічні конфігурації, сувора аутентифікація користувачів і обізнаність мешканців будинку про безпеку. Запропоновані контрзаходи відповідають загрозам та ризикам безпеки.

ID	Можливі заходи протидії чи пом’якшення загроз
1	Контроль доступу до системи за допомогою ефективних біометричних ідентифікаторів; Впровадження програми підвищення обізнаності користувачів для ознайомлення користувачів з соціальною інженерією; Використання багатофакторної аутентифікації
2	Уникнення використання незахищеного Wi-Fi; Налаштування безпечної мережі перед використанням програми для домашньої автоматизації; Сповіщення про викрадення або загублення пристроїв
3	Використання безпечного каналу зв'язку; Обмеження мережевого трафіку, щоб він був доступний тільки авторизованим користувачам; Розробка програми навчання з питань безпеки для жителів розумного будинку
4	Використання системи виявлення вторгнень (IDS) / системи запобігання вторгнень (IPS); Використання механізму шифрування для передачі даних безпеки; Регулярні резервні копії даних, для збереження копій конфіденційних даних.
5	Забезпечення фізичного розташування встановлених пристроїв; Забезпечення безпечного доступу до інтерфейсів конфігурації пристрою; Редагування конфігурації зручності використання за замовчуванням для встановлених пристроїв
6	Використання стандартного обладнання та програмного забезпечення для збору та аналізу мережевого трафіку;

	Створення резервних копій конфігурації робочої системи; Постійне стеження за продуктивністю системи, виявляючи випадки неналежної поведінки
7	Застосування надійного механізму аутентифікації, наприклад аутентифікації по відбитку пальця; Ознайомчі та навчальні програми з питань безпеки системи; Конфігурації системи на безпечність і автентичність.
8	Обмеження фізичного доступу до пристроїв тільки автентичним людям; Уникання передачі інфраструктури на аутсорсинг сторонньому постачальнику послуг; Зміна конфігурації пристрою, з метою підвищення рівню безпеки.
9	Вимкнення непотрібних служб відстежування місцеположення на мобільних пристроях; Розвивання розуміння проблем конфіденційності користувачів; Відстеження поведінки системи для виявлення будь-яких підозрілих витоків конфіденційності.
10	Використання надійних і автентичних мереж (дротові або бездротові); Використання перевірених постачальників для отримання технічної підтримки при збоях обладнання в розумному будинку.

Таблиця 4.6 – Можливі заходи протидії загрозам для розумного дому

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було ознайомлено з концепцією Інтернету речей, її архітектурою, а також визначено, в чому полягають її особливості і недоліки. Для опису проблем безпеки IoT використано єдину еталонну модель, запропоновану Cisco, на окремих рівнях якої вказуються основні вимоги і потреби безпеки, внаслідок чого було охарактеризовано і пояснено кожен з типів вразливостей і атак, поряд з необхідними контрзаходами для запобігання можливим наслідкам цих атак.

На основі отриманої інформації та знань, в даній кваліфікаційній роботі було наведено детальний аналіз основних загроз інформаційної безпеки, розглянуто декілька поширених методологій оцінки вразливостей, а також виконано оцінку ризиків інформаційної безпеки для саморобної системи Інтернету речей «розумний будинок» з використанням методології NIST IR 8228 «Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks».

Внаслідок оцінки інформаційних ризиків для системи автоматизації було знайдено 10 найважливіших вразливостей. Проаналізовано основні вектори інформаційних загроз та вияснено, що окрім технічних недоліків пристроїв Інтернету речей, причинами системних збоїв або отримання несанкціонованого доступу до ресурсів користувача може бути людський чи техногенний фактор. Для кожного з інформаційних ризиків запропоновано контрзаходи, які можуть значно зміцнити безпеку таких систем і запобігти виникненню потенційних загроз в майбутньому.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. A. Gupta: The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, 2019. С. 1.
2. S. Hilton: Dyn Analysis Summary of Friday October 21 Attack, 2017,
3. P. Leeson., C. Coyne: The economics of computer hacking, 2005. С. 511.
4. S. Misra, A. Vaish: Reputation-based role assignment for role-based access control in wireless sensor networks. Computer Communications, 2011. С 281-294.
5. A. Nahiyan, M. Sadi, R. Vittal: Hardware Trojan Detection through Information Flow Security Verification, 2017. С. 1-10.
6. A. Mosenia, N. Jha: A Comprehensive Study of Security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 2017. С. 586-602.
7. A. Wood, J. Stankovic: Denial of service in sensor networks. Computer, 2002. С. 54-62.
8. V. Sundaresan, S. Rammohan, R. Vemuri: Defense against Side-Channel Power Analysis Attacks on Microelectronic Systems, 2008. С. 144-150.
9. K. Rosenfeld, E. Gavas, R. Karri: Sensor physical unclonable functions, 2010. С. 112-117.
10. P. Peris-Lopez, J. Hernandez-Castro: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags, 2006. С. 912-923.
11. C. Karlof, D. Wagner: Secure routing in wireless sensor networks: attacks and countermeasures, 2003. С. 113-127.
12. Стаття «INTERNET OF THINGS: CONNECTED DEVICES TO TRIPLE BY 2021, REACHING OVER 46 BILLION UNITS», URL: https://www.juniperresearch.com/press/internet-of-things-connected-devices-triple-2021
13. S. Raza, L. Wallgren, T. Voigt: SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 2013. С. 2661-2674.

14. Стаття «What is Hacktivism?». URL: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html
15. A. Gupta: The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, 2019. С. 2.
16. Журнал «Cisco – The Internet of Things Reference Model», URL: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf
17. Стаття «Internet of Things (IoT) Characteristics». URL: https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c
18. Стаття «The more things change: Value creation, value capture, and the Internet of Things». URL: https://www2.deloitte.com/us/en/insights/deloitte-review/issue-17/value-creation-value-capture-internet-of-things.html
19. R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things", 2011. С. 51-58.
20. Стаття «INFOSEC – CIA Triad». URL: https://resources.infosecinstitute.com/topic/cia-triad/
21. Ю. Черданцева, O. Rana, J. Hilton: Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success, 2011. С. 546-555.