ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ МЕРЕЖ ІОТ ВІД КІБЕРАТАК»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Косенко В.В.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2020

РЕФЕРАТ

Текстова частина магістерської роботи: 89 сторінок, 15 рисунків, 8 таблиць, 26 джерел.

Об'єкт дослідження – процес захисту мережі Інтернет речей від кібератак.

Предмет дослідження – засоби захисту мережі IoT від кібер загроз.

Мета роботи –розробити шляхи і рекомендації щодо захисту мереж IoT від кібератак.

Методи дослідження – теорія складних систем, теорія масового обслуговування, теорія інформації, практичне тестування програмного забезпечення.

В роботі проаналізовано сучасний стан та росповсюдження пристроїв мережі IoT. Проведено глибинний аналіз архітектури мереж IoT та розглянуто кожну її складову. Досліджено принципи роботи IoT такі як зчитування інформації, передача та обромка данних.

Виокремлено основні протоколи, технології зв'язку та обміну інформації пристроїв мережі IoT. Зазначено перелік найбільш поширених та актуальних взразливостей, які притаманні пристроям мереж Інтернету Речей. Проаналізовано основні вектори атак та статистику використяних уразливостей та експлойтів.

Досліджено засоби забезпечення безпеки мережі IoT, а також принцип роботи блокчейну та хмарних платформ для забезпечення безпеки Інтернету Речей.

Надано детальні рекомендацій щодо захисту пристроїв мережі IoT.

Галузь використання – телекомунікаційні мережі.

ІНТЕРНЕТ РЕЧЕЙ, СЕНСОРНА СИСТЕМА, БЕЗПРОВОДОВА МЕРЕЖА, СИСТЕМА, КІБЕРАТАКА, ЕКСПЛОЙТ, ВІРУС, АТАКА, БЛОКЧЕЙН, ХМАРА, ПЕРЕДАЧА ДАННИХ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Автоматизований – пристрій, який працює.

Атака – загальна назва спроби заподіяти шкоду інформаційному носію.

Розумний дім – будинок з мікроконтроллерами, що керують всіма або більшою частиною пристроїв всередині.

BLE – Bluetooth Low Energy

DDoS-атака (Distributed Denial of Service attack) - комплекс дій, здатний повністю або частково вивести з ладу інтернет-ресурс.

Ethernet - це сімейство комп'ютерних мережних технологій, які зазвичай використовуються в локальних мережах.

Firewall- це система мережевої безпеки, яка контролює та контролює вхідний та вихідний мережевий трафік на основі заздалегідь визначених правил безпеки.

IoT - Internet of Things

PenTest - це авторизована імітаційна кібератака на комп'ютерну систему, яка виконується для оцінки безпеки системи.

PIN - Personal identification number

UART - Universal Asynchronous Receiver/Transmitter

Web сервер - це сервер, що приймає HTTP-запити зазвичай веббраузерів, видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою,
зображенням, файлом, медіа-потоком або іншими даними.

NFC - Near field communication

IP – інтернет речей

ВСТУП

Актуальність дослідження. Концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку. Окрім давачів, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів. Основною концепцією IP є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки. Всі ці об'єкти (речі) повинні бути оснащені вбудованими давачами або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, а в разі спекотної погоди будинок має механізми відкривання і закривання вікон, завдяки чому провітрюється будинок, і все це відбувається без втручання людини. Передбачається, що Інтернет речей (IoT) буде швидко рости завдяки поширенню комунікаційних технологій, доступності пристроїв і обчислювальних систем. Безпека IoT - це область, яка потребує уваги для захисту обладнання і мереж в системі IoT. Інтернет речей може викликати величезні зміни у повсякденному житті, надавши звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, за допомогою

надійного криптографічного алгоритму, замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки. Оскільки речі із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, зокрема можуть знати його точне місцезнаходження, доступ до такої інформації може допомогти зловмисникам вчинити злочин. Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження інтернету речей у повсякденне життя. В останні роки було відмічено, що академічні дослідження, присвячені питанням конфіденційності та безпеки для систем IoT, отримав позитивні зрушення. В даний час запропоновані методи і способи захисту по суті засновані на традиційних методах захисту мережі. Однак застосування механізмів безпеки в системі IoT є більш складним завданням.

Об'єкт дослідження – процес захисту мережі Інтернет речей від кібератак.

Предмет дослідження – засоби захисту мережі IoT від кібер загроз.

Мета роботи –розробити шляхи і рекомендації щодо захисту мереж IoT від кібератак

Наукові завдання:

- Аналіз аспектів роботи мережі IoT
- Дослідження правових аспектів безпеки та розвинутості мережі IoT
- Аналіз наявності проблеми захисту мережі IoT
- Розробка рекомендацій захисту IoT

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання топології системи захисту корпоративних комп'ютерів.

Практичне значення одержаних результатів полягає в розробці план захисту від кібер атак у мережі IoT для кінцевого користувача.

Апробація результатів: Косенко В.В. Використання технології блокчейн для захисту пристроїв мережі Інтернету речей. /В.В. Косенко // Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Тези доповідей. 22 жовтня 2020 року, м. Київ – с. 49-51.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ТА ОСОБЛИВОСТЕЙ РОБОТИ МЕРЕЖІ IOT

1.1 Базові визначення мережі IoT

Інтернет речей (IoT) - це широкий термін для підключених пристроїв, які обмінюються даними з іншими підключеними пристроями через вбудовані датчики і бездротові мережі, в основному стільниковий зв'язок і Wi-Fi. Ці пристрої спрощують виконання звичайних і не дуже поширених завдань. В даний час ми живемо в світі, який щодня використовує пристрої IoT, проте з приходом ери 5G ми очікуємо, що ці пристрої стануть більш звичайним явищем.

Інтернет речей впливає на те, як ми відстежуємо навколишнє середовище і взаємодіємо з нею, автоматизуємо і формуємо наші купівельні звички, і навіть впливає на те, як ми підтримуємо наше фізичне здоров'я. Приклади пристроїв IoT включають автономні автомобілі, інтелектуальну техніку і носяться пристрої.

Інтернет-речей грунтується на трьох базових принципах. По-перше, повсюдно поширену комунікаційну інфраструктуру, по-друге, глобальну ідентифікацію кожного об'єкта і, по-третє, можливість кожного об'єкта відправляти і отримувати дані за допомогою персональної мережі або мережі Інтернет, до якої він підключений [1].

В IoT кожна річ має свій ідентифікатор, які спільно утворюють континуум речей, здатних взаємодіяти один з одним, створюючи тимчасові або постійні мережі. Так речі можуть брати участь в процесі їх переміщення, ділячись інформацією про поточну геопозіції, що дозволяє повністю автоматизувати процес логістики, а маючи вбудований інтелект, речі можуть змінювати свої властивості і адаптуватися до навколишнього середовища.

Інтернет-речі мають єдиний протокол взаємодії, згідно з яким будь-який вузол мережі рівноправний в наданні своїх сервісів. Кожен вузол мережі інтернет-речей надає свій сервіс, надаючи якусь послугу поставки даних. У той же час вузол

такої мережі може приймати команди від будь-якого іншого вузла. Це означає, що всі інтернет-речі можуть взаємодіяти один з одним і вирішувати спільні обчислювальні завдання. Інтернет-речі можуть утворювати локальні мережі, об'єднані якоюсь однією зоною обслуговування.

1.2 Правові аспекти технологій IoT

Передусім, необхідно сформулювати правові та етичні норми щодо IP-пристроїв. Для галузі IP варто розробити комплексні рішення, які забезпечуватимуть захист усього ланцюга вразливостей від кінцевих точок до «хмари», куди стікаються всі дані. Не можна перекладати відповідальність за безпеку на користувача. Людина схильна до помилок, неправильного застосування паролів та інших хибних дій. Проблеми мають вирішуватися на зовсім іншому рівні, тобто виробниками пристроїв, яких до цього має спонукати законодавча база.

Законодавці та особи, причетні до розробки нових правил кібербезпеки, повинні розглядати питання безпеки не тільки на рівні програмного забезпечення, але й на рівні кінцевої точки (пристрою, що підключений до інтернету). Йдеться про брандмауери, які вбудовуються в маршрутизатори (роутери), засоби безпеки та системи блокування атак безпосередньо у процесорах, інструменти автентифікації доступу, застосування безпечного завантаження тощо.

Необхідно усвідомлювати, що певні ризики стосовно кібербезпеки не можуть зупинити процес невпинного поширення IP. Адже це відкриває занадто вагомі перспективи для покращення життя у різних сферах. Зокрема, це Smart City («розумне місто»), оптимізація транспортного трафіку в мегаполісах, великі позитивні зрушення в галузі охорони здоров'я, збільшення врожайності, зменшення витрат на логістику, раціональне використання енергії, запобігання злочинності. Інтернет речей допомагатиме суспільству ставати більш ефективним, безпечним, інноваційним, стабільним, інклюзивним [2].

28 вересня 2018 року Каліфорнія схвалила законопроект, який врегульовує питання конфіденційності та безпеки в одному з провідних секторів технічної

індустрії – інтернеті речей (Internet of Things, IoT). У той час як прогресивні виробники побутової техніки говорять про чарівні переваги розумного холодильника, Каліфорнійський закон буде регулювати їх «темну» сторону – використання і захист даних, зібраних пристроями IoT.

З швидким зростанням (згідно з прогнозами, загальний ринок інтернету речей подвоїться до 2021 року і досягне 520 мільярдів доларів по всьому світу) виникають нові виклики для цієї індустрії. Велике питання полягає в тому, чи слід приймати окреме законодавство з регулювання розумних девайсів як, наприклад, в Каліфорнії, або застосовувати вже існуючі положення законодавства про кібербезпеку і захист персональних даних. Так чи інакше, для виробництва і надання розумних пристроїв необхідно враховувати специфіку інформаційної безпеки.

В законі викладені вимоги до виробників пристроїв, які напряму чи опосередковано підключаються до інтернету. Такі пристрої повинні передбачати «розумні» функції безпеки для запобігання несанкціонованого доступу, знищення, зміни чи крадіжки інформації. Положення закону спрямовані на захист звичайних користувачів. Законодавчі ініціативи щодо більш масштабних корпоративних рішень ще попереду.

Уряд Великобританії в минулому році випустив Звід практичних правил для забезпечення безпеки IP. В цьому нормативному акті акцент робиться на тому, що потрібно забезпечити кібербезпеку пристроїв, а не працювати над оновленням програмного забезпечення для посилення безпеки.

Значну увагу питанню кібербезпеки IP-пристроїв приділяє уряд Японії. В лютому 2019 р. японські чиновники з Національного інституту інформаційних та комунікаційних технологій оголосили про перевірку ефективності безпеки 200 млн IP-адрес у країні. Мета цього масштабного дослідження — виявити пристрої з низьким рівнем безпеки. Ця програма допоможе інтернет-провайдерам і телекомунікаційним компаніям краще зрозуміти вразливості в мережах та пристроях.

В ЄС закон про кібербезпеку набрав чинності 27.06.2019 р. Його положення закріплюють індивідуальні схеми сертифікації для певних категорій продуктів, процесів та послуг з IP-сфери. У сертифікатах має позначатися рівень гарантії безпеки та довіри до продукту, процесу чи послуги. Передбачається три рівні довіри. Найвищий відзначає успішне проходження всіх тестувань щодо кібербезпеки та повну гарантію для користувачів від виробника. Поки що застосування схем сертифікації не є обов'язковою вимогою для виробників IP-пристроїв. Це лише перші ініціативи, які намічають подальший напрямок законотворчості в цій сфері.

У серпні 2017 Конгрес представив Закон про вдосконалення кібербезпеки Інтернету речей, який вимагає від будь-якого пристрою Інтернету речей, проданого уряду США, не використовувати паролі за замовчуванням, не мати відомих вразливостей і пропонувати механізм виправлення пристроїв. Незважаючи на те, що він націлений на виробників, що створюють пристрої, що продаються державі, він встановлює базові заходи безпеки, які повинні прийняти всі виробники.

Також в серпні 2017 Сенат прийняв Закон про розвиток інновацій та розширення Інтернету речей (DIGIT), але все ще очікує затвердження Палатою представників. Цей закон вимагає від Міністерства торгівлі скликати робочу групу і підготувати звіт по IoT, включаючи безпеку та конфіденційність [3].

Загальний регламент захисту даних (GDPR), випущений в травні 2018 року, не відноситься до IoT, але уніфікує закони про конфіденційність даних у всьому Європейському союзі. Ці заходи захисту поширюються на пристрої Інтернету речей і їх мережі, і виробники пристроїв Інтернету речей повинні враховувати їх.

У червні 2018 Конгрес представив Закон про сучасних додатках, дослідженнях і тенденції в області Інтернету речей або Закон про SMART IoT, щоб запропонувати Міністерству торгівлі провести дослідження галузі Інтернету речей та надати рекомендації щодо безпечного розвитку пристроїв Інтернету речей.

У вересні 2018 Законодавчий орган штату Каліфорнія ухвалив закон SB-327 «Конфіденційність інформації: підключення пристрою», який ввів вимоги безпеки для пристроїв IoT, що продаються в країні [4].

1.3 Архітектура мережі IoT

Інтернет-речей концептуально належить до мереж наступного покоління, тому його архітектура багато в чому схожа з архітектурою NGN. IoT складається з набору різних інфокомунікаційних технологій, що забезпечують функціонування Інтернет-речей, і його архітектура показує, як ці технології пов'язані один з одного. Архітектура IoT включає чотири функціональних рівня (рис.1.1), описаних нижче [5].

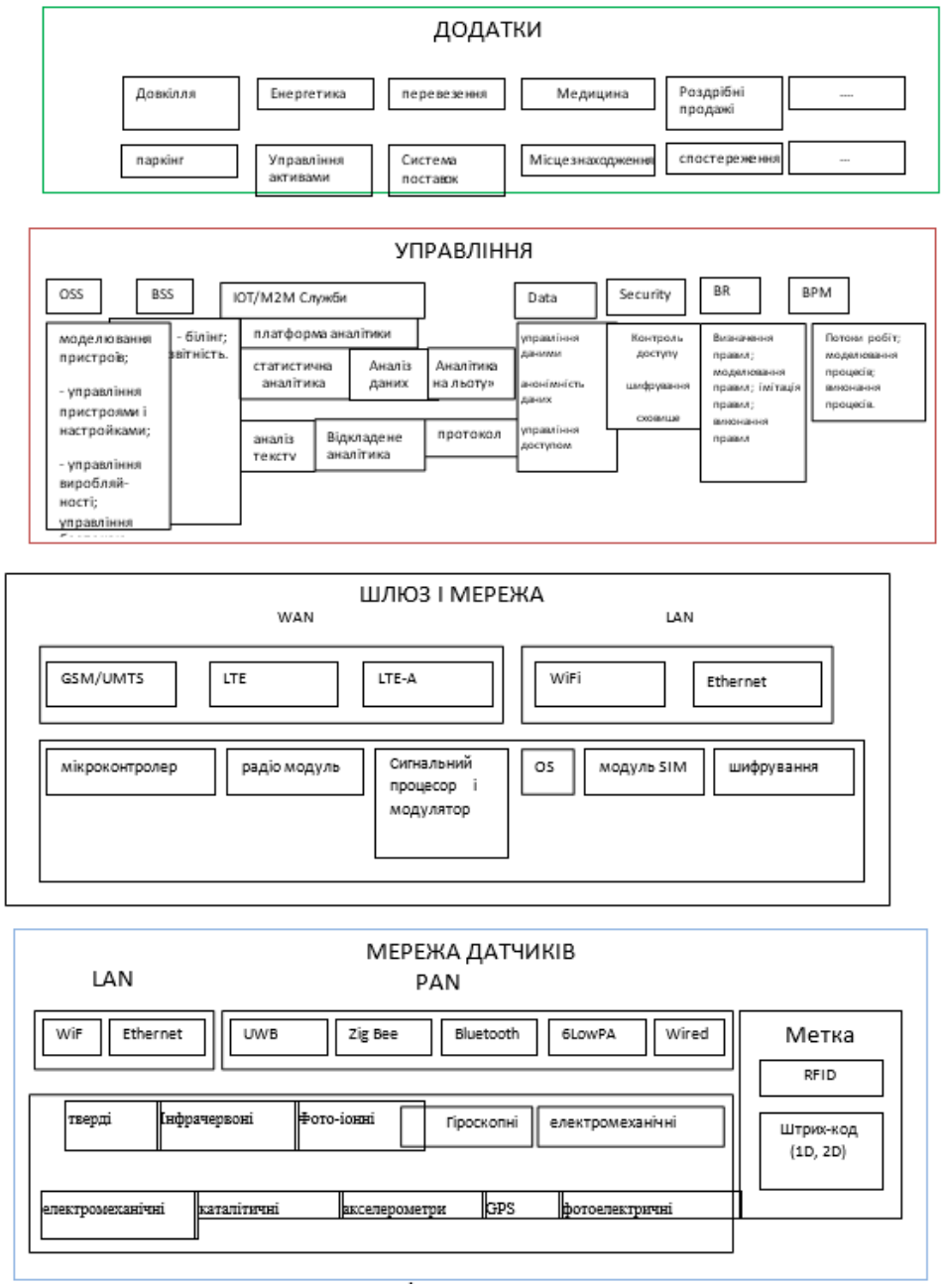

Рис. 1.1. Архітектура Інтернет речей

1.3.1 Аналіз рівня датчиків

Можливості рівня пристроїв можна логічно розділити на два види можливостей: можливості пристрою та можливості шлюзу.

Можливості пристрою діляться в свою чергу на:

а) Пряму взаємодію з мережею зв'язку: пристрої здатні збирати та закачувати інформацію безпосередньо (тобто без використання можливостей шлюзу) в мережі зв'язку та можуть безпосередньо отримувати інформацію (наприклад, команди) із мережі зв'язку.

б) Непряму взаємодію мережі зв'язку: пристрої здатні отримувати та закачувати інформацію в мережі зв'язку непрямим чином, тобто за допомогою можливості шлюзу. На іншій стороні пристрою можуть не прямим чином отримувати інформацію (наприклад, команди) з мережі зв'язку. Організація спеціальних мереж в ряді сценаріїв вимагає підвищену масштабованість та швидкого розгортання, пристрої можуть мати можливість будувати мережі довільним чином.

в) Сплячий режим та пробудження: можливості пристроїв можуть підтримувати механізми «сну» і «пробудження» для економії енергії.

Можливості шлюзу включають:

а) Підтримку декількох інтерфейсів: на рівні пристроїв можливості шлюзу підтримують пристрої, сполучені з використанням різних дротових і бездротових технологій, таких як шина локальних мереж контролерів (CAN), Bluetooth, або Wi-Fi. На рівні мережевих можливостей шлюзу можуть обмінюватися даними з використанням різних технологій, таких як комутована телефонна мережа загального користування, мережі другого або третього покоління (2G або 3G), мережі на базі технології довгострокового розвитку (LTE), Ethernet або цифрові абонентські лінії (DSL).

б) Перетворення протоколу: існує дві ситуації в яких потрібні можливості шлюзу. Перша ситуація виникає тоді, коли для зв'язку на рівні пристроїв використовуються різні протоколи рівня пристроїв, наприклад, протоколу

технологій Z-Wave, Bluetooth; друга ситуація виникає тоді, коли для зв'язку потребується і рівень пристроїв і мережевий рівень, використовуються різні технології, наприклад, протокол технології Z-Wave на рівні пристроїв і протокол технології 3G на мережевому рівні.

Головна мета рівня датчиків – ідентифікація різних явищ навколишнього середовища за допомогою периферійних пристроїв та отримання даних з реального світу. Цей рівень складається з декількох видів датчиків. Використання великої кількості датчиків є однією з найважливіших функцій IoT пристроїв. Датчики в IoT пристроях зазвичай інтегруються за допомогою концентратора датчиків. Концентратор датчиків є головною точкою з'єднання для кількох датчиків. Він акумулює та передає дані з датчиків до блоку обробки даних в пристрої. Концентратор датчиків використовує декілька транспортних механізмів таких, як (Inter-Integrated Circuit (I2C) чи Serial Peripheral Interface (SPI)) для передачі даних між датчиками та додатками. Ці транспортні механізми залежать від IoT пристроїв. Вони створюють канал зв'язку між датчиками та додатками збору даних з датчиків.

Датчики в IoT пристроях можуть бути класифіковані на 3 широкі категорії:

- Датчики руху, які вимірюють зміни в русі, а також орієнтацію пристроїв. Є два типи рухів, які можна спостерігати за допомогою датчику цього пристрою: лінійний та кутовий рух. Лінійний рух відноситься до лінійного переміщення пристрою IoT, в той час як кутовий рух відноситься до обертального переміщення пристрою.

- Датчики навколишнього середовища до них відносяться такі пристрої, як датчики світла, датчики тиску та інші, які вбудовані в IoT пристрої реагують на зміни в параметрах навколишнього середовища за допомогою периферійних пристроїв. Основною метою використання цих датчиків в IoT пристроях є допомога пристроям приймати автономні рішення відповідно до змін в периферійних пристроях. Наприклад, датчики навколишнього середовища використовуються в більшості додатків для спрощення життя користувачів (розумні замки, система домашньої автоматизації, розумне освітлення та ін.).

- Датчики місцеперебування пристроїв IoT взаємодіють з фізичним

місцеперебуванням та розташуванням самого пристрою. Найбільш поширеними датчиками місцеперебування, що використовуються в IoT є магнітні датчики та Global Position System (GPS) датчики. Магнітні датчики використовуються, як цифрові компаси та допомагають фіксувати орієнтацію дисплею пристрою. GPS датчики використовується для навігаційних цілей в IoT пристроях.

1.3.2 Аналіз мережевого рівеня

Мережевий рівень використовується, як комунікаційний канал для передачі даних, зібраних на рівні датчиків, до інших підключених пристроїв. В IoT пристроях, мережевий рівень реалізований для використання різноманітних комунікаційних технологій (наприклад, Z-Wave, LoRa, Wi-Fi, Bluetooth та ін.), що дозволяють передавати дані між різними пристроями всередині самої мережі.

Великий обсяг даних, воздававшому на першому рівні IoT численними сенсорами, вимагає надійної та високопродуктивної дротовогї або бездротовогї інфраструктури, як транспортне середовище даний рівень складається з конвергентної мережевої інфраструктури, яка створюється шляхом інтеграції різнорідних мереж в єдину мережеву платформу.

Сервісний рівень містить набір інформаційних послуг, які автоматизують технологічні бізнес операції в IoT: підтримки операційної і бізнес діяльності (OSS/BSS Operation Support System/Business Support System), різної аналітичної обробки інформації, зберігання даних, забезпечення інформаційної безпеки, управління бізнес.

- Можливості організації мереж: надає відповідні функції управління мережевим з'єднанням, такі як функції управління доступом та ресурсами транспортування, управління мобільністю або автентифікація, авторизація та облік (AAA).

- Можливості транспортування: призначені для надання з'єднання для транспортування інформації у вигляді даних, що відносяться до послуг і додатків IoT, а також транспортування інформації контролю та управління, що відносяться

до IoT.

1.3.3 Аналіз рівень обробки даних

Рівень обробки даних складається з головного блоку обробки даних IoT пристрою. Рівень обробки даних отримує зібрані дані на рівні датчиків та аналізує їх. Потім приймає рішення, що базуються на результаті аналізу. В деяких IoT пристроях (наприклад, смарт-годинник, розумний домашній концентратор та ін.), цей рівень також зберігає результати попередніх аналізованих даних для подальшої можливості використання цих даних. Також цей рівень може передавати результати обробки даних з одного підключеного пристрою на інший пристрій через мережевий рівень.

1.3.4 Аналіз рівеня додатків

Рівень підтримки послуг та додатків складається з наступних двох груп можливостей, таких як загальні можливості підтримки та спеціалізовані можливості підтримки:

- Загальні можливості підтримки - це можливості, які можуть використовуватися різними додатками такими як обробка та зберігання даних. Ці можливості можуть бути активовані за допомогою спеціалізованих можливостей підтримки, наприклад, для створення інших спеціалізованих можливостей підтримки;
- Спеціалізовані можливості підтримки - це конкретні можливості, які призначені для задоволення вимог різноманітних додатків. Насправді вони можуть складатися з ряду груп чітко визначених можливостей, для того щоб надавати різні функції підтримки різних програм IoT.

Рівень додатків презентує результати роботи рівню обробки даних за допомогою різного роду додатків IoT пристроїв. Рівень додатків є рівнем орієнтованим на користувачів, який виконує різні завдання для користувача.

Існують різні IoT додатки, які включають розумний будинок, розумний транспорт тощо.

На даному рівні існують різні типи додатків для відповідних промислових секторів і сфер діяльності (енергетика, транспорт, торгівля, медицина, освіта та ін.). Додатки можуть бути:

«Вертикальними», коли вони є «специфічними» для конкретної галузі промисловості, а також «горизонтальними», які можуть використовуватися в різних секторах економіки.

Складовою частиною інтернету речей є Веб речей (WEB of Things, WoT), який забезпечує взаємодію різних інтелектуальних об'єктів («речей») з використанням стандартів і механізмів Інтернет, таких як уніфікований однаковий ідентифікатор ресурсу URI (Uniform Resource Identifier), протокол передачі гіпертексту HTTP (HypperText Transfer Protocol), стиль побудови архітектури розподіленого додатка REST (Representational State Transfer) та ін. Фактично WoT передбачає реалізацію концепції IoT на прикладному рівні з використанням вже існуючих архітектурних рішень, орієнтованих на розробку web- додатків.

1.4 Аналіз принципу роботи IoT

Принцип роботи IoT об'єднує чотири різні етапи:

- Зчитування інформації за допомогою датчиків;
- Передача даних від датчиків до хмарних сховищ;
- Обробка даних отриманих за допомогою датчиків;
- Передача інформації на інтерфейс користувача.

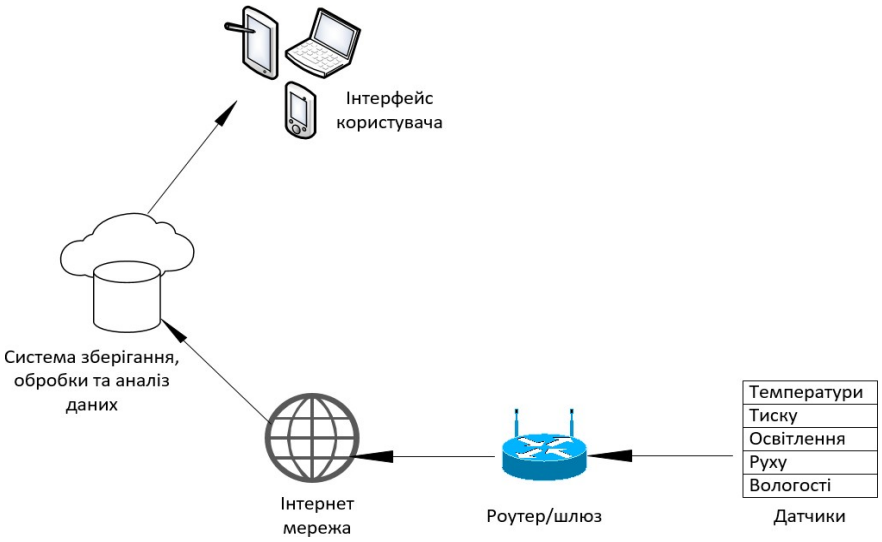

Рис. 1.2. Принцип роботи IoT

1.4.1 Зчитування інформації за допомогою датчиків

Датчики або пристрої збирають дані зі свого оточення. Це може бути як простим процесом, таким як зчитування температури, або складним, як запис відео на камеру відеоспостереження.

Використовується на даному етапі також й пристрої, оскільки декілька датчиків можуть бути об'єднані разом або датчики можуть бути частиною пристрою, що робить більше, ніж просто аналіз даних. Наприклад, ваш телефон - це пристрій з кількома датчиками (камера, акселерометр, GPS тощо), але телефон не є лише датчиком. На цьому кроці дані збираються з нашого оточення [6].

1.4.2 Передача даних від датчиків до хмарних сховищ

Датчики можуть бути підключені до хмари за допомогою різних методів, включаючи: стільникову мережу, супутникову мережу, Wi-Fi, Bluetooth, малопотужні широкосмугові мережі (LPWAN), або з’єднатися безпосередньо до Інтернету через Ethernet технологію.

Кожна опція має компроміс між споживанням енергії, діапазоном та пропускною здатністю. Вибір того чи іншого варіанту підключення зводиться до вибору конкретної області, де буде використовуватися Інтернет речей, але всі вони

виконують одне і те ж завдання - передачу даних до хмари.

1.4.3 Обробка даних отриманих за допомогою датчиків

Після того, як дані потраплять до хмари, програмне забезпечення виконує певну обробку даних.

Це може бути, наприклад, перевірка того, що зчитувана температура знаходиться в межах допустимого діапазону. Чи це може бути процесом обробки інформації, наприклад, використання комп'ютерного програмного забезпечення, яке здійснює ідентифікацію об'єктів, що знаходяться на відео (наприклад, зловмисників у вашому домі).

1.4.4 Передача інформації на інтерфейс користувача

На даному етапі відбувається передача корисної інформації кінцевому користувачу певним чином. Це може бути через сповіщення користувача (електронна пошта, текст, сповіщення тощо). Наприклад, текстове сповіщення, коли температура занадто висока в холодному сховищі компанії. Крім того, користувач може мати інтерфейс, який дозволяє йому активно перевіряти систему. Наприклад, користувач може захотіти перевірити камери відеоспостереження в їхньому будинку через телефонну програму, або веб-сторінку.

Однак це не єдиний шлях. Залежно від програми IoT, користувач може також виконувати дії на відстані та впливати на систему. Наприклад, користувач може дистанційно регулювати температуру в холодному сховищі за допомогою програми на своєму телефоні.

А деякі дії виконуються автоматично. Замість того, щоб чекати, коли користувач налаштує температуру, система може зробити це автоматично за допомогою попередньо визначених правил. І замість того, щоб просто викликати вас, щоб попередити вас про зловмисника, система IoT також може автоматично повідомляти відповідні органи.

Система IoT складається з датчиків, які розмовляють з хмарою через певний тип зв'язку. Після того, як дані потрапляють у хмару, програмне забезпечення обробляє його, а потім може вирішити виконати певну дію, наприклад, надіслати попередження, або автоматично регулювати роботу датчика без потреби користувача [7].

1.5 Огляд та порівняльний аналіз протоколів та технологій мережі IoT

В найближчому майбутньому до Інтернету речей будуть підключені велика кількість пристроїв. Більша доля цих пристроїв буде мати живлення від батарейок. У зв’язку з цим, однією з основних характеристик є тривалість роботи обладнання без втручання людини.

1.5.1 Технології та протоколи передачі даних на довгі відстані в IoT мережах

Для того щоб розв’язати цю проблему були створені нові мережі спеціально для IoT. Ці мережі називаються LPWAN (Long Power Wide Area Network). Основними технологіями цих мереж є NB-IoT, Weightless, LoRa, SIGFOX та інші. Ці технології з’явилися через те, що необхідно буде підключати велику кількість датчиків та приладів для централізованого збору інформації на хмарних серверах. Надалі буде наведено основні технології мережі LPWAN.

LoRaWAN. Мережева архітектура LoRaWAN розгорнута в зіркоподібною топології, в якій шлюзи ретранслюють повідомлення між кінцевими пристроями і центральним сервером. Шлюзи підключаються до мережевого сервера через стандартні IP-з'єднання і діють як прозорий міст, просто перетворюючи RF-пакети в IP-пакети і навпаки. Бездротовий зв'язок використовує переваги великого радіусу дії фізичного рівня LoRaÒ, дозволяючи встановити односкачковое з'єднання між кінцевим пристроєм і одним або декількома шлюзами. Всі режими підтримують двосторонню зв'язок, і є підтримка груп многоадресной адресації для ефективного

використання спектра під час таких завдань, як оновлення мікропрограм по бездротовій мережі (FOTA) або інші повідомлення масового поширення.

LoRaWAN має три різних класи кінцевих пристроїв для задоволення різних потреб, відображених в широкому спектрі додатків.

Клас А - двонаправлені кінцеві пристрої з найменшою потужністю: клас за замовчуванням, який повинен підтримуватися всіма кінцевими пристроями LoRaWAN, зв'язок класу А завжди ініціюється кінцевим пристроєм і є повністю асинхронної. Кожна передача по висхідній лінії зв'язку може бути відправлена в будь-який час і супроводжується двома короткими вікнами по низхідній лінії зв'язку, що дає можливість для двобічної зв'язку або команд управління мережею, якщо це необхідно. Це протокол типу ALOHA. Кінцеве пристрій може переходити в сплячий режим з низьким енергоспоживанням до тих пір, поки це визначено його власним додатком: немає необхідності в мережі для періодичних пробуджень. Це робить клас А режимом роботи з найменшим енергоспоживанням, при цьому забезпечуючи зв'язок по висхідній лінії зв'язку в будь-який час. Оскільки зв'язок по низхідній лінії зв'язку завжди повинна слідувати за передачею по висхідній лінії за розкладом, визначеним додатком кінцевого пристрою, зв'язок по низхідній лінії зв'язку повинна буферизованного на мережевому сервері до наступної події висхідній лінії зв'язку.

Клас В - двонаправлені кінцеві пристрої з детермінованою затримкою спадного каналу: на додаток до вікон прийому, ініційованим класом А, пристрої класу В синхронізуються з мережею за допомогою періодичних маяків і відкривають «слоти перевірки зв'язку» низхідній лінії зв'язку в запланований час. Це дає мережі можливість відправляти дані по низхідній лінії зв'язку з детермінованою затримкою, але за рахунок деякого додаткового енергоспоживання на кінцевому пристрої. Затримку можна запрограмувати до 128 секунд для різних додатків, а додаткове енергоспоживання досить низька, щоб працювати з додатками на батарейках.

Клас С - найнижча затримка, двонаправлені кінцеві пристрої: на додаток до структури класу А висхідній лінії зв'язку, за якою слідують два вікна низхідній лінії

зв'язку, клас С додатково знижує затримку в низхідній лінії зв'язку, залишаючи приймач кінцевого пристрій відкрите весь час, коли пристрій не передати (полудуплекс). На основі цього мережевий сервер може в будь-який момент ініціювати передачу по низхідній лінії зв'язку за умови, що приймач кінцевого пристрою відкритий, тому немає затримки. Компромісом є споживана потужність приймача (до ~ 50 мВт), тому клас С підходить для додатків, де доступна постійна потужність. Для пристроїв з батарейним харчуванням можливе тимчасове перемикання режимів між класами А і С, що корисно для періодичних завдань, таких як оновлення прошивки по бездротовій мережі.

Безпека - це основна проблема будь-якого масового розгортання Інтернету речей, і специфікація LoRaWAN визначає два рівня криптографії:

- Унікальний 128-бітний мережевий сеансовий ключ, яким користуються кінцевим пристроєм та сервером.
- Унікальний 128-бітний ключ сеансу додатка (AppSKey), загальний наскрізний на рівні додатку.

Алгоритми AES використовуються для забезпечення аутентифікації і цілісності пакетів на мережевому сервері і для наскрізного шифрування на сервері додатків. Надаючи ці два рівня, стає можливим реалізувати «мультітенантние» спільно використовувані мережі без того, щоб оператор мережі мав видимість даних корисного навантаження користувачів.

Ключі можуть бути активовані за допомогою персоналізації (ABP) на виробничій лінії або під час введення в експлуатацію, або можуть бути активовані по бездротовому зв'язку (OTAA) в польових умовах. OTAA дозволяє при необхідності змінювати ключі пристроїв.

Специфікація визначає параметри фізичного рівня «пристрій-інфраструктура» (LoRa) і протокол (LoRaWAN) і, таким чином, забезпечує безшовне взаємодію між виробниками, що демонструється за допомогою програми сертифікації.

Хоча специфікація визначає технічну реалізацію, вона не визначає будь-яку комерційну модель або тип розгортання (загальнодоступне, спільне, приватне,

корпоративне) і, таким чином, пропонує галузі свободу для інновацій і диференціації того, як вони використовуються. Специфікація LoRaWAN® розроблена і підтримується LoRa Alliance: відкритої асоціацією співпрацюють членів.

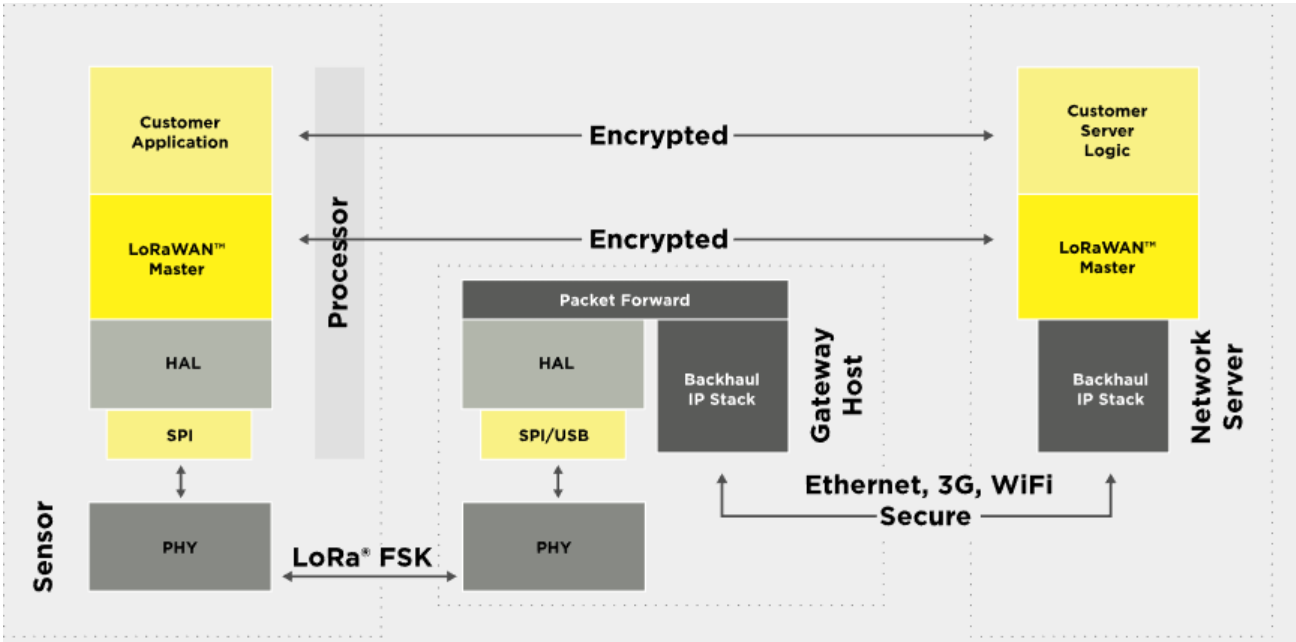

Рис. 1.3. Архітектура мережі LoRaWAN

SigFox. Французький глобальний мережевий оператор, заснований у 2010 році , який будує бездротові мережі для підключення малопотужних об'єктів, таких як лічильники електроенергії та розумні годинник, які повинні бути постійно включені і передавати невеликі обсяги даних.

Sigfox використовує диференціальну двійкову фазову маніпуляцію (DBPSK) і гауссову частотну маніпуляцію (GFSK), що забезпечує зв'язок з використанням промислового, наукового та медичного радіодіапазону ISM, який використовує 868 МГц в Європі і 902 МГц в США. Він використовує широко поширюється сигнал, який вільно проходить через тверді об'єкти, званий «Ультра вузькосмуговий» і вимагає невеликої кількості енергії, званий «глобальною мережею з низьким енергоспоживанням» (LPWAN). Мережа заснована на зіркоподібній топології з одним переходом і вимагає, щоб оператор мобільного зв'язку передавав генерований трафік. Сигнал також можна використовувати для легкого охоплення

великих територій і досягнення підземних об'єктів. Станом на жовтень 2018 року мережа Sigfox IoT покрила в цілому 4,2 мільйона квадратних кілометрів в 50 країнах і до кінця 2018 року має досягти 60 країн.

Sigfox співпрацює з низкою фірм, що працюють в галузі LPWAN, такими як Texas Instruments, Silicon Labs і ON Semiconductor. Радіодіапазоні ISM підтримують обмежену двосторонню зв'язок. Існуючий стандарт зв'язку Sigfox підтримує до 140 повідомлень висхідній лінії зв'язку в день, кожне з яких може нести корисне навантаження в 12 октетів при швидкості передачі даних до 100 біт в секунду. Зона, яку покриває SigFox складає близько 30-50 км в міський та сільський місцевості. В містах де дуже багато шумів, діапазон роботи 3-10 км.

На рис. 1.4 представлена архітектура мережі технології SigFox. Загальна топологія мережі була розроблена для забезпечення масштабованої, високопродуктивної мережі, з дуже низькою витратою енергії.

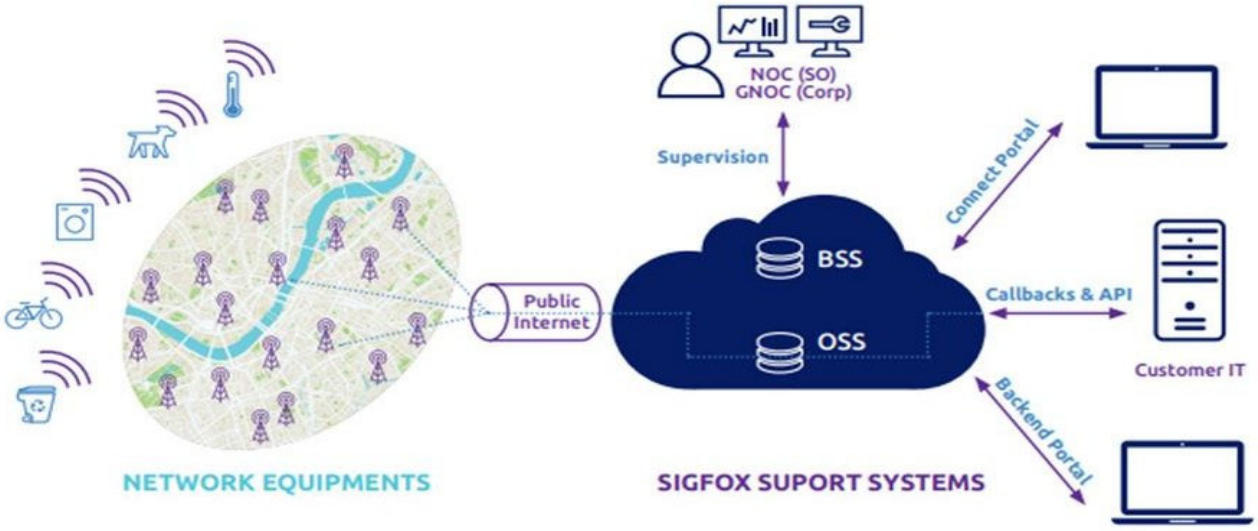

Рис. 1.4. Архітектура мережі SigFox

SigFox використовує надвузьку смугу частот UNB (Ultra Narrow Band), на основі радіо технології для підключення пристроїв до глобальної мережі. Використання UNB - ключовий фактор у забезпечені дуже низького рівня потужності передавача, який буде використовуватися під час стану підтримки надійного з'єднання для передачі даних. У Європі широко використовується діапазон 868,8 МГц (як визначено в ETSI і CEPT), а у США 915 МГц (як визначено

FCC).

Пристрої передають свої повідомлення до базової станції SigFox. За допомогою point-to-point (P2P) протоколу на базову станцію Sigfox підключають до своєї Інтернет бази даних, після отримання і декодування повідомлення, дані надсилаються до її Інтернет бази даних. Нарешті, хмарний сервер SigFox посилає повідомлення на клієнтські сервери та IT платформи через інтерфейси прикладного програмування (APIs).

NB-IoT (Narrow Band Internet of Things). Технологія стільникового зв'язку на основі LTE, призначена для стаціонарних пристроїв з низькими обсягами переданих даних і малим споживанням. Асоціація GSM обіцяє, що пристрої NB-IoT будуть дешевими і (за певних умов) зможуть працювати від звичайних батарейок до 10 років. Цікаво, що асоціація також описує NB-IoT як технологію, створену в стислі терміни у відповідь на запити користувачів і конкуренцію з боку аналогічних пропрієтарних рішень:

NB-IoT відноситься з так званого CIoT, Cellular IoT (за термінологією 3GPP) або MIoT, Mobile IoT (за термінологією GSMA) і просувається операторами стільникового зв'язку і виробниками відповідного обладнання. Вузькосмуговим (Narrow Band) цей вид зв'язку назвали в порівнянні з «традиційним» LTE, де використовуються істотно ширші смуги частот (3, 5, 10, 15, 20 МГц). Ширина частотного каналу NB-IoT становить 200 кГц. На даний момент CIoT (MIoT) розгалужується на 2 напрямки: NB-IoT і LTE-M (також званий eMTC або LTE Cat.M).

NB-IoT орієнтований швидше на нерухомі (стаціонарні) пристрої, так як в цьому режимі не підтримується автоматичне перемикання між сотами (handover). При переміщенні в іншу соту пристрою NB-IoT доведеться знову реєструватися в мережі. Таким чином, NB-IoT призначається в першу чергу для таких додатків, як автоматичний збір показань із лічильників, датчиків, дистанційне керування вуличним освітленням і т.п. На відміну від NB-IoT, інша «гілка» CIoT - LTE-M - підтримує як перемикання між сотами, так і забезпечує в кілька разів більші швидкості прийому/передачі.

Якщо в специфікаціях 3GPP Release 13 було визначено тільки один варіант NB-IoT - Category NB1, то в специфікаціях 3GPP Release 14 з'явилося 2 варіанти: Category NB1 і NB2. Варіант Category NB2 є більш швидкісним. Для порівняння можливостей NB1 і NB2 в таблиці 1.1 наведені максимальні розміри транспортних блоків на прийом і передачу згідно специфікації 3GPP 36.306 Release 14.

Таблиця 1.1.

Розміри транспортних блоків Cat. NB1, NB2 (Release 14)

Категорія обладнання	Максимальний розмір транспортного блоку на прийом (DL), біт	Максимальний розмір транспортного блоку на передачу (UL), біт
Category NB1	680	1000
Category NB2	2536	2536

Qualcomm в специфікації чіпа MDM9206 (використовується в модулі N20) наводить такі швидкості передачі в режимі Cat. NB1: прийом (DL) - 20 кбіт / с, передача (UL) - 60 кбіт/с. Аналогічні результати для NB1 призводять колеги з MTC, згадуючи, що для категорії NB2 максимальна швидкість прийому / передачі складе більше 100 кбіт/с.

Weightless. Це стандарт бездротового зв'язку з низьким енергоспоживанням в загальнодоступних або приватних мережах з кінцевими пристроями до вимог «Інтернету речей» (IoT), такими як обмежена пропускна здатність і мінімальна затримка. Хоча він може працювати в будь-якому частотному діапазоні, в даний час він визначений для роботи в не вимагає ліцензії смугах частот нижче ГГц (наприклад, 138 МГц, 433 МГц, 470 МГц, 780 МГц, 868 МГц, 915 МГц, 923 МГц).

Визначальні характеристики Weightless-P наступні:

- 100% двунаправленная, повністю підтверджена зв'язок для надійності.

- оптимізований для великої кількості кінцевих пристроїв низької складності з переважаючою асинхронної зв'язком по висхідній лінії зв'язку з невеликими розмірами корисного навантаження (зазвичай <48 байтів).

- оптимізований для наднизького енергоспоживання (по рахунок затримки і пропускної здатності по порівняння з стільниковим технологіями).

- стандартні швидкості передачі даних від 0,625 кбіт/с до 100 кбіт/с.

- типова потужність передачі кінцевого пристрою 14 дБм (до 30 дБм).

- типова потужність передачі базової станції 27 дБм (до 30 дБм). Мережі Weightless-P складаються з наступних елементів:

- кінцеві пристрої (ED): кінцевий вузол в мережі, низька складність, низька вартість, зазвичай низький робочий цикл.

- базові станції (BS): центральний вузол в кожному осередку, з Яким все ED взаємодіють через зіркоподібну топологію.

- мережа базових станцій (BSN): об'єднує всі базові станції в єдиній мережі для управління розподілом радіоресурсів і планування в мережі, а також для обробки аутентифікації, роумінгу та планування.

Таблиця 1.2.

Порівняння основних технічних характеристик мереж з високою дальністю дії LPWAN

Характеристики	LoRaWAN	SigFox	NB-IoT
Метод модуляції	CSS	DBPSK/GFSK	GFSK/BPSK/QPSK
Діапазон	ISM	ISM	Ліцензований
Швидкість	0,3-50 кбіт/с	100 кбіт/с	UL: 1-144 кбіт/с
Швидкість	Широкосмуг	Вузькосмуг	DL: 1-200 кбіт/с
	До 500 кГц	100 кГц	200 кГц
Максимальний час автономної роботи пристроїв	> 10 років	До 20 років	До 10 років
Частота	868.8 МГц (Европа)	868.8 МГц (Европа)	800/900/1800 МГц
	915 МГц (США)	915 МГц (США)	

	433 МГц (Азія)		
Безпека	AES-64/128	AES з HMACs	AES-256
Дальність	До 2б5 км у місті	До 10 км у місті	До 2 км
	До 45 км за містом	До 50 км за містом	

1.5.2 Технології та протоколи передачі даних на короткі відстані в IoT мережах

Z-Wave. Z-Wave є запатентованим бездротовим протоколом зв'язку, розробленим для домашньої автоматизації, зокрема для контролю і управління на житлових і комерційних об'єктах. Технологія використовує малопотужні і мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку і різні пристрої, такі як освітлення, опалення, контроль доступу, розважальні системи і побутову техніку. Це бездротова радіо технологія, розроблена спеціально для дистанційного керування. На відміну від Wi-Fi і інших IEEE 802.11 стандартів передачі даних, призначених в основному для великих потоків інформації, Z-Wave працює в діапазоні частот до 1 ГГц і оптимізована для передачі простих керуючих команд (наприклад, включити/виключити, змінити гучність, яскравість і т.д.). Вибір низького радіочастотного діапазону для Z-Wave обумовлюється малою кількістю можливих джерел електромагнітних полів. Також іншими перевагами Z-Wave можна відзначити мале споживання енергії, низьку вартість виробництва і вбудовування Z-Wave в різні побутові пристрої.

У світі налічується понад 200 виробників, що пропонують товари з Z-Wave чіпами або модулями. Відмінною особливістю Z-Wave є те, що всі ці продукти сумісні між собою.

В основі рішення Z-Wave лежить ячеистая мережева технологія mesh, в якій кожен вузол або пристрій може приймати і передавати сигнали інших пристроїв мережі, використовуючи проміжні сусідні вузли. Mesh це самоорганізована мережу з маршрутизацією, залежною від зовнішніх факторів - наприклад, при виникненні перешкоди між двома найближчими вузлами мережі, сигнал піде через інші вузли

мережі, що знаходяться в радіусі дії.

Ще однією перевагою є той факт, що Z-Wave використовує інший бездротової діапазон, ніж Wi-Fi і Bluetooth. Це забезпечує дуже хороше відстань в будинках - навіть крізь стіни. Це також гарантує, що Z-Wave і інші сигнали не заважають один одному.

NFC. Near field communication, NFC («комунікація ближнього поля», «ближня безконтактна зв'язок») - технологія бездротового високочастотного зв'язку малого радіусу дії, яка дає можливість обміну даними між пристроями, що знаходяться на відстані близько 10 сантиметрів.

Ця технологія - просте розширення стандарту безконтактних карт (ISO 14443), яке об'єднує інтерфейс смарт-карти і зчитувача в єдиний пристрій. Пристрій NFC може підтримувати зв'язок і з існуючими смарт-картами, і зі зчитувачами стандарту ISO 14443, і з іншими пристроями NFC, і, таким чином, - сумісно з існуючою інфраструктурою безконтактних карт, вже використовується в громадському транспорті і платіжних системах. NFC націлена перш за все на використання в цифрових мобільних пристроях.

NFC є спільною розробкою компаній NXP і Semiconductor і Sony - являє собою комбінацію декількох існуючих безконтактних технологій радіочастотної ідентифікації та зв'язку. Ця технологія - просте розширення стандарту безконтактних карт, яка об'єднує інтерфейс смарт-карти і зчитувача в єдиний пристрій.

Модель надання послуг з використанням технології безпосередньо пов'язана з розвитком технологій мереж зв'язку. Сьогодні орієнтиром розвитку може служити концепція мереж наступного покоління NGN/IMS/4G/5G, вона передбачає рівневу архітектуру з поділ на шари (Stratum) - транспортний, послуг зв'язку та додатків. Перші два шари реалізуються засобами мереж зв'язку, шар додатків являє собою сукупність всіх прикладних послуг, які формуються і надаються різними постачальниками.

Додатки, що формують контент для послуг на основі NFC, знаходяться в шарі додатків і взаємодіють з функцією підтримки специфіки цих додатків в шарі

послуг. Остання додає до базової функціональності послуги свою функціональність, необхідну для доставки послуги мережевого користувачеві. У терміналі користувача повинна бути встановлена програма, яка з одного боку здійснює взаємодію по інтерфейсу NFC, а з іншого боку - використовує функцію підтримки додатків в мережевому обладнанні.

Частота роботи системи NFC - 13,56 Мгц, швидкість передачі 106 кбіт/с (можливі 212 кбіт/с і 424 кбіт/с) на відстані приблизно 10 см. На відміну від існуючих технологій безконтактної зв'язку на даному діапазоні частот, які дозволяють передавати інформацію тільки від активного пристрою пасивного, NFC забезпечує обмін між двома активними (рівноправними) пристроями. Таким чином, NFC можна використовувати для доступу до пристроїв радіочастотної ідентифікації.

Технологія NFC назад сумісна з широко використовуваним стандартом Smart Card на основі ISO/IEC 14443 A і ISO/IEC 14443 B, а також JIS X6319-4 (FeliCa). Для обміну між двома пристроями використовується протокол ECMA- 340 і ISO, IEC 18092. Стандарт ISO, IEC 18092 визначає схеми модуляції, кодування швидкості передачі і радіочастотну структур інтерфейсу пристрою NFC, а також схеми ініціалізації і умови, необхідні для контролю за конфліктними ситуаціями під час ініціалізації. Крім того, він визначає протокол передачі, включаючи протокол активації і спосіб обміну даними.

В основі технології лежить індуктивний зв'язок. Сигнал піддається амплітудної маніпуляції OOK (On-Off Keyinng) с глибиною 100% або 10% і фазової маніпуляції BPSK. При передачі інформації пасивного пристрою використовується амплітудна маніпуляція ASK (Amplitude Shift Keying). При обміні обидва пристрої виступають в ролі полінгових. Кожен пристрій має власне джерело живлення, тому сигнал відключається відразу після закінчення передачі.

За рахунок індуктивного зв'язку між опитуваних і прослуховуючих пристроїв пасивне пристрій впливає на активну. Зміна імпедансу прослуховувального пристрою викликає зміни амплітуди і фази на антені опитувального пристрою, яке воно виявляє. Цей механізм називається модуляцією навантаження. Вона

виконується в режимі прослуховування із застосуванням допоміжної несучої 848 кГц. Залежно від стандарту застосуються амплітудна (ASK для 14443 A) або фазова маніпуляція (BPSK для 14443). Ще один пасивний режим, сумісний з FeliCa, здійснюється без допоміжної піднесе з маніпуляцією ASK на частоті 13,56 МГц.

RFID. RFID є абревіатурою від «радіочастотної ідентифікації» і відноситься до технології, за допомогою якої цифрові дані, закодовані в RFID-мітках або смарт-етикетках (певних нижче), захоплюються зчитувачем за допомогою радіохвиль. RFID схожий на штрих-кодування в тому, що дані з тега або етикетки захоплюються пристроєм, який зберігає дані в базі даних. Однак RFID має ряд переваг перед системами, в яких використовується програмне забезпечення для відстеження активів зі штрих-кодом. Найбільш примітним є те, що дані RFID-міток можна зчитувати за межами прямої видимості, тоді як штрих-коди повинні бути суміщені з допомогою оптичного сканера. Якщо ви роздумуєте про впровадження рішення RFID, зробіть наступний крок і зверніться до фахівців з RFID в AB & R® (американський штрих-код і RFID).

RFID належить до групи технологій, званих автоматичною ідентифікацією та збором даних (AIDC). Методи AIDC автоматично ідентифікують об'єкти, збирають дані про них і вводять ці дані безпосередньо в комп'ютерні системи з мінімальним втручанням людини або без нього. Для цього в методах RFID використовуються радіохвилі. На простому рівні системи RFID складаються з трьох компонентів: RFID-Мітки смарт-мітки, зчитувача RFID і антени. RFID-мітки містять інтегральну схему і антену, які використовуються для передачі даних в зчитувач RFID (також званий запитувачем). Потім зчитувач перетворить радіохвилі в більш зручну форму даних. Інформація, зібрана з тегів, потім передається через інтерфейс зв'язку в систему головного комп'ютера, де дані можуть бути збережені в базі даних і проаналізовані пізніше.

Як зазначено вище, RFID-мітка складається з інтегральної схеми та антени. Бирка також складається з захисного матеріалу, який скріплює деталі і захищає їх від різних умов навколишнього середовища. Захисний матеріал залежить від області застосування. Наприклад, бейджи співробітників, що містять мітки RFID,

зазвичай виготовляються з міцного пластику, а мітка вбудовується між шарами пластику. RFID-мітки бувають різних форм і розмірів і можуть бути пасивними або активними. Найбільш широко використовуються пасивні теги, так як вони менше за розміром і дешевше в реалізації. Пасивні мітки повинні бути активовані зчитувачем RFID, перш ніж вони зможуть передавати дані. На відміну від пасивних міток, активні RFID-мітки мають вбудований джерело живлення (наприклад, акумулятор), що дозволяє їм передавати дані в будь-який час. Для більш детального обговорення зверніться до цієї статті: Пасивні мітки RFID проти активних міток RFID.

Смарт-мітки відрізняються від міток RFID тим, що в них використовуються технології RFID і штрих-коду. Вони зроблені з самоклеючої етикетки з вставкою RFID-мітки, а також можуть містити штрих-код і / або іншу друковану інформацію. Смарт-етикетки можна кодувати і роздруковувати за запитом за допомогою настільних принтерів етикеток, тоді як програмування RFID-міток займає більше часу і вимагає більш сучасного обладнання.

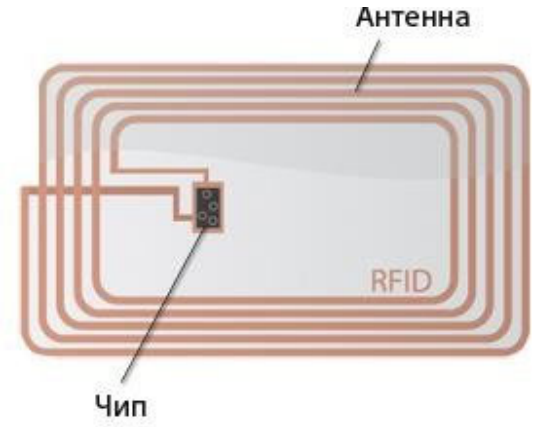

Рис. 1.5. Будова RFID-мітки

Bluetooth Low Energy. Безпроводова технологія з низьким енергоспоживанням Bluetooth (BLE) – це частина специфікації Bluetooth, яка починається з покоління Bluetooth 4.0 і на даний момент закінчується Bluetooth 5.0.

Пристрої, що використовують BLE, споживають менше енергії, ніж інші версії Bluetooth - пристрої попередніх поколінь. У багатьох випадках пристрої зможуть працювати більше року на одній невеличкій батарейці типу таблетка без

підзарядки. Завдяки цьому, можна буде використовувати датчики невеликих розмірів, які будуть постійно працювати та взаємодіяти з іншими пристроями.

Основними рівнями BLE є:

- Додаток – реалізує корисну для кінцевого користувача логіку роботи.
- Основний пристрій, або хост – надає верхні рівні стеку протоколів Bluetooth.
- Контролер – займається нижніми рівнями стеку протоколів Bluetooth.

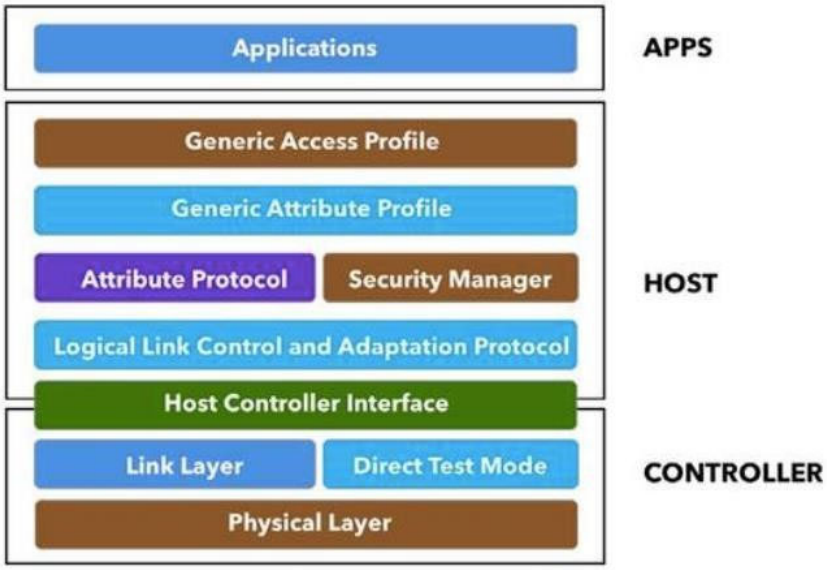

Рис. 1.6. Архітектура BLE

Рівень додатків – найвищий рівень стеку протоколів. Рівень хосту містить такі підрівні:

- GAP (Generic Access Profile) – профіль загального доступу;
- GATT (Generic Attribute Profile) – профіль загальних атрибуті;
- ATT (Attribute Protocol) – протокол атрибутів;
- SM (Security Manager) – менеджер безпеки;
- L2CAP (Logical Link Control and Adaptation Protocol) – протокол логічного з'єднання та адаптації;
- HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні хосту.

Рівень контролеру зв'язан за допомогою протоколу HCI та має такі рівні:

- HCI (Host Controller Interface) – інтерфейс хост-контролеру,на стороні контролеру;
- LL (Link Layer) – канальний рівень;
- PHY – фізичний рівень.

BLE призначений для тих пристроїв, які мають невеликі розміри, тобто для пристроїв, у яких важлива компактність і куди не можна встановити повноцінний акумулятор, або батарею великого об'єму. Bluetooth LE споживає в 10-20 разів менше енергії і цілком здатний передавати дані в 50 і більше разів швидше та на відстані більше 100 метрів, ніж класичні Bluetooth рішення.

Крім перерахованих вище переваг, BLE має високу безпечність, надійність, низьку затримку при підключенні та низьку споживчу потужність. Є ще одна важлива особливість даного стандарту, вона полягає в адаптивності переналаштування частоти, тобто відбувається захист від помилок при передачі сигналу, BLE швидко змінює свою робочу частоту, вибираючи найбільш оптимальну для усунення перешкод, проблем переповнення і для зниження інтерференції. Специфікація Bluetooth 5.0 була створена, з орієнтацією на Інтернет речей. Це остаточно показало, що стандарт прагне «захопити» ринок пристроїв.

В порівнянні з попередньою версією 4.0 була підвищена швидкість передачі даних майже до швидкостей HSPA і LTE ранніх версій, при цьому енергоспоживання залишилося в колишніх показниках. Важливим показником для побудови мереж Інтернету речей як раз є енергоефективність. В даний момент дана специфікація є мало поширеною через те що вона з'явилася нещодавно. Bluetooth 5 як і всі попередні версії має зворотну сумісність. Цілком можливо, через декілька років кожний мобільний пристрій буде підтримувати 5 версію цього стандарту, що є найважливішою перевагою цієї технології над іншими.

Wi-Fi HaLow. Wi-Fi HaLow — це протокол бездротової мережі, опублікований у 2017 році, як доповнення до стандарту бездротової мережі IEEE_802.11. Цей протокол працює на непотребуючій ліцензування частоті 900 МГц, для забезпечення розширеного діапазону Wi-Fi мереж, порівняно зі

звичайними мережами Wi-Fi, працюючими в діапазонах 2,4 ГГц і 5 ГГц. Його низьке енергоспоживання також є перевагою, таким, що дозволяє створювати великі групи станцій або датчиків, які взаємодіють щоб поширювати сигнали, підтримуючи концепцію інтернет-речей (Internet of Things, IoT). Низьке енергоспоживання протоколу конкурує з Bluetooth і має додаткову перевагу - вищі швидкості передачі даних і більш широкий діапазон покриття. Wi-Fi HaLow дозволить розширити можливості енергоефективного сценарію використання розумного будинку, автомобілів, а також в торгівлі, промисловості, сільському господарстві тощо.

Wi-Fi HaLow розширює Wi-Fi в діапазоні 900 МГц, даючи можливість з'єднання пристроїв малої потужності, таких як датчики та портативні комп'ютери. Wi-Fi HaLow успадкує позитивні якості попередніх протоколів, такі як надійний захист інформації, широку сумістність обладнання та простоту встановки.

Пристрої з підтримкою Wi-Fi HaLow будуть також працювати у діапазонах 2,4 та 5 ГГц, що дасть можливість інтегрування в екосистему, яка на даний момент налічує більше 7 млрд пристроїв. Також Wi-Fi HaLow буде мати підтримку підключення по IP, це дозволить працювати з хмарами, що дуже важливо для IoT. Також буде можливість підключатися до одієї точки доступу близько 1000 пристроїв.

Висновки до розділу 1

Проаналізовано сучасний стан та особливості росповсюдження пристроїв мережі IoT на європейському та українському ринках.

Досліджено архітектуру мережі IoT та розглянуто кожну її частину окремо. Виокремлено головні принципи роботи IoT такі як зчитування інформації, передача та обробка даних. Було здійснено огляд та порівняльний аналіз протоколів та технологій IoT.

Описано технології та протоколи передачі даних на довгі та кородкі відстані.

Підкреслено особливості функціонування основних протоколів та технологій

зв’язку та обміну інформації між пристроями в мережах IoT. Після аналізу IoT можна зробити висновок - це мережа, що складається з взаємозв'язаних фізичних об'єктів або пристроїв, які мають елементи збору інформації (датчики), а також програмне забезпечення. Поєднання цих елементів дозволяє здійснювати передачу, збір і обмін даними між фізичним світом і комп'ютерними системами.

2 ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІОТ ПРИСТРОЇВ

2.1 Дослідження вразливостей іот пристроїв

Кібербезпека, кіберзагрози, кібератака – всі ці категорії існують в невидимій області повсякденному житті людей. Однак це робить кібербезпеку не менш важливою. Оскільки всі сьогодні пов’язані з інтернетом, сама природа злочинів змінюється. Шахраям більше не потрібен фізичний доступ до активів – вони можуть їх просто вкрасти, отримавши несанкціонований доступ через онлайн-з’єднання. Як кажуть фахівці з кібербезпеки, жодна система не безпечна. Це можна легко довести, переглянувши останні новини кібербезпеки – щодня відбувається безліч витоків даних – від сумнозвісних витоків в Facebook до витоку даних співробітників Пентагону.

Оскільки розумні пристрої підключені до інтернету, вони не є винятком для зломів. Більш того, користувачі розцінюють розумний пристрій як звичайний домашній прилад, забуваючи про прості заходи комп’ютерної безпеки, тому ситуація навіть погіршується. Те саме можна сказати і до виробників IoT-пристроїв – через обмеженої функціональності вони зазвичай вирішують не дотримуватися відповідних стандартів безпеки.

В результаті, поріг безпеки для доступу до таких пристроїв є низьким, що дає можливість втручатися в їх роботу будь-кому, хто має базові знання в області мережевої безпеки. Згідно з опитуваннями, більшість професіоналів (понад три чверті респондентів), що працюють в галузі IoT, вважають, що їх пристрої будуть зламані в найближчі два роки. Число може бути навіть збільшено тими, хто не знає ризиків або не хоче зізнаватися в витоках даних [8].

Наслідки несанкціонованого доступу можна розділити на дві категорії. Перша категорія пов’язана з можливістю дистанційного керування підключеними пристроями. Через простоту паролів (наприклад, «pass1234» або «12345678»), їх

відсутність або низький рівень кібербезпеки, контроль над пристроєм IoT отримати відносно легко. Подальші дії повністю залишаються на розсуд хакерів. Наприклад, в 2016 році кіберзлочинці відключили всю систему регулювання температури і тиску в житловому будинку в Фінляндії. В результаті цього, жителі залишилися без водопостачання протягом цілого тижня, просто через відсутність базового захисту у вигляді брандмауера.

Приклад ризиків слабких паролів за замовчуванням був представлений атакою BrickerBot в 2017 році. Шкідлива програма BrickerBot могла підключитися до будь-якого пристрою IoT з ім'ям і паролем за замовчуванням – що в основному легко знайти через інтернет і просто "знищити" пристрій. Шкідлива програма наносила настільки серйозної шкоди пристрою, що після цього була потрібна повна заміна обладнання [9].

Друга категорія ризиків пов'язана зі збором даних за допомогою смарт-пристроїв у великих масштабах. Ці дані можуть бути виключно цінними для кіберзлочинців – принципи роботи системи безпеки, дані геолокації або повсякденні звички користувача часто є ключовою інформацією для планування високоякісного шахрайства. Немає необхідності збирати її на законних підставах, оскільки ви можете просто підключитися до пристрою IoT і взяти все, що вам потрібно. Наприклад, навесні минулого року хакери вкрали базу даних за ставками в казино, використовуючи з'єднання з термометром в лобі казино. Чим більше вразливостей в системі IoT, тим доступніше її дані.

Як результат, сьогодні можна спостерігати прогалину в регулюванні виробництва IoT. Існуючі закони про кібербезпеку стосуються тільки певних питань використання розумних пристроїв, таких як захист персональних даних або надання ключових суспільних послуг (наприклад, енергетичного або телекомунікаційного сектора). Поки що, окремого регулювання по IoT, як Каліфорнійський закон, не так багато. Однак, як доведено численними кібератаками на розумні пристрої, необхідно встановити мінімальний рівень для їх безпеки, включаючи вимоги до паролів, брандмауерів і інших методів захисту.

Говорячи про дані, використання розумних пристроїв в повсякденному житті людей значно розширює збір наших персональних даних. Фітнес-трекери, розумні іграшки, автоматичні транспортні засоби і всі інші речі в нашому особистому користуванні збирають великі обсяги інформації про нас. Фактично, підключені пристрої можуть збирати дані про нас 24/7, часто без нашого відома і згоди. Більш того, такий великий збір даних не потрібно для надання функціоналу пристрою, в більшості випадків.

Відповідно до сучасних правил захисту даних, такими як Європейський Загальний Регламент щодо захисту персональних даних (GDPR), на збір персональних даних та їх подальше використання накладаються суворі вимоги. Щоб отримати дані на законних підставах, постачальник IoT повинен забезпечити відповідний рівень конфіденційності користувачів. Це включає зобов'язання інформувати користувачів про збір їх персональної інформації, отримувати згоду на це в певних випадках, зобов'язання мінімізації даних, ті ж заходи кібербезпеки, про які говорилося вище, і багато іншого. Конфіденційність користувачів повинна буквально бути реалізована «в дизайні», з огляду на захист даних на самих ранніх стадіях розробки. На жаль, в дизайн розумних пристроїв рідко закладається захист персональних даних.

Велика частина пристроїв IoT влаштовані так, що вони можуть тільки отримувати інформацію, а не надавати її. Через це провайдери IoT (не) навмисно не інформують користувачів про збір їх даних. Отже, користувачі не знають, хто саме обробляє дані, яким чином вони використовуються, які треті сторони мають доступ до даних і як користувачі можуть здійснювати свої інформаційні права. Крім того, провайдери IoT не замислюються про отримання згоди на використання даних, що стосуються нашого здоров'я або, наприклад, з точки зору. Однак в таких випадках згода на використання даних є основним і часто єдиною законною підставою для обробки [10].

Відповідно, наші персональні дані збираються без нашого відома, за замовчуванням, без гарантій їх безпеки. Така ситуація дозволяє контролерам даних використовувати зібрану інформацію в будь-який спосіб. Випадки зловживання

даними великі: від створення і продажу соціальних профілів електорату політичних партій до продажу фінансових даних брокерам даних. Незважаючи на те, що згадані випадки не стосуються збору даних саме через IoT, до них застосовується та сама схема.

Ще одна важлива проблема, яку слід розглянути, – відсутність мінімізації даних, які збираються пристроями IoT. Принцип «мінімізації даних» означає, що компанія може збирати тільки дані, необхідні для забезпечення функціональності пристрою. Будь-який збір даних, який не пов’язаний з наданням функцій девайса, забороняється.

Як приклад, принцип «мінімізації» публічно застосував Французький орган із захисту даних – The Commission nationale de l’informatique et des libertés (CNIL). 20 листопада 2017 року CNIL вислав офіційне попередження компанії, що використовує технологію розпізнавання мови в іграшках. Розумні іграшки були оснащені мікрофоном і динаміком і були підключені до мобільного додатку. Для розпізнавання мовлення дитини, іграшка направляла записи розмов на сервери в Китай, де вони оброблялися спеціальною програмою, без будь-яких гарантій безпеки. Такі великі обсяги збору даних в дитячій іграшці не відповідали принципу «мінімізації», особливо в зв’язку з відсутністю заходів безпеки. Не було ніякої необхідності відправляти дані в Китай для надання функціоналу іграшки.

Більш того, будь-яка людина з Bluetooth на своєму пристрої, могла підключитися до іграшки, прослухати і записати розмови між дитиною і іграшкою або будь-яку розмову, яка відбувається поблизу. Ця функція іграшки суперечить згаданим вище практикам кіберзахисту пристроїв.

Отримавши офіційне попередження, компанія впровадила відповідні заходи. Іграшки, імпортовані до Франції, більш не оснащуються технологіями розпізнавання мови, і дані не надсилаються на сервер. Отже, компанія більше не «Обробляє дані» в розумінні законодавства про захист персональних даних.

В результаті CNIL завершив розслідування 20 липня 2018 року. Незважаючи на це, компанія так і не вирішила проблему незахищеного доступу до іграшки через

Bluetooth. Подальший розгляд питання було направлено в Французький регуляторний орган із захисту прав споживачів.

Як не дивно, один з перших штрафів за порушення Європейської GDPR також був накладений у зв'язку з принципом мінімізації даних. Австрійський підприємець встановив перед своїм офісом камеру відеоспостереження. Камера також записала більшу частину тротуару. На жаль, для підприємця, австрійський наглядовий орган порахував, що навіть запис вулиці перед офісом є масштабним моніторингом громадських місць. У поєднанні з відсутністю публічного повідомлення про зйомку вулиці за допомогою CCTV, таке використання камер не відповідає Австрійському закону захисту персональних даних. Тому австрійський орган видав штраф в розмірі 4800 євро. Щоб відповідати вимогам захисту даних, компанія може збирати тільки мінімум інформації, необхідний для її цілей, ясним і прозорим способом.

Як уже згадувалося вище, ми не звикли до розуміння побутової техніки як об'єкту загроз кібербезпеки. Отже, постачальники IoT зазвичай не включають в себе належні технічні та організаційні гарантії проти кіберзагроз та особливо порушень конфіденційності. Більш того, навмисне чи ні, вони також порушують приватність користувачів.

Однак з появою специфічного регулювання виробництва IoT і суворих правил захисту персональних даних, ситуація навряд чи залишиться без змін. Щоб забезпечити безпеку розумних пристроїв, основними кроками є:

Прозорість – повідомлення про збір даних і його подальша обробка повинні надаватися кожному кінцевому користувачеві до (або в той час) пристрої почали збирати дані;

Згода – при необхідності, наприклад, обробляючи конфіденційні дані або використовуючи дані для рекламних цілей, постачальник IoT повинен спочатку отримати конкретну згоду від користувача;

Мінімізація – хоча іноді важко підтримувати, власник пристрою / провайдер може збирати і обробляти дані, необхідні тільки для функціональності пристрою;

Безпека і обмежений доступ – last but not least – пристрої IoT повинні бути захищені технічними заходами від стороннього доступу, такими як безпечні з'єднання, брандмауери і паролі. Доступ до зібраних даних повинен обмежуватися тільки тими співробітниками, які підтримують роботу пристрою.

2.1.1 Вразливості IoT пристроїв

До кінця 2018 роки кількість підключених IoT-пристроїв перевищила 22 мільярди. З 7,6 мільярда чоловік на Землі у 4 мільярдів є доступ до інтернету. Виходить, що на кожну людину припадає по 5,5 пристроїв інтернету речей.

В середньому між часом підключення пристрою IoT до мережі і часом першої атаки проходить близько 5 хвилин. Причому більша частина атак на «розумні» пристрої відбувається автоматизовано.

Зрозуміло, така сумна статистика не могла залишити байдужими фахівців в області кібербезпеки. Міжнародна некомерційна організація OWASP (Open Web Application Security Project) перейнялася безпекою інтернету речей ще в 2014 році, випустивши першу версію «OWASP Top 10 IoT» [11].

1. Недостатня фізична безпека. Відсутність заходів з фізичного захисту, що дозволяє потенційним зловмисникам отримати конфіденційну інформацію, яка в майбутньому може допомогти реалізувати вилучену атаку або отримати локальний контроль над пристроєм. Одна з проблем безпеки екосистеми IoT полягає в тому, що її компоненти розподілені в просторі і часто встановлюються в публічних або незахищених місцях. Це дає можливість зловмисникам отримати доступ до пристрою і взяти його під контроль локально або використовувати для доступу до іншої мережі.

Атакуючий може скопіювати налаштування (IP-мережу, MAC-адресу і т.д.) і поставити свій пристрій замість вихідного для прослуховування або зниження продуктивності мережі. Він може зламати RFID-зчитувач, встановити апаратну ятати, заразити шкідливим ПЗ, вкрасти потрібні дані або просто фізично вивести пристрій IoT з ладу. Рішення даної проблеми одне - ускладнити фізичний доступ

до пристроїв. Їх можна встановлювати на захищених майданчиках, на висоті або використовувати антивандальні захищені шафи.

2. Небезпечні настройки за замовчуванням**.** Пристрої або системи поставляються з небезпечними настройками за замовчуванням або не мають можливості зробити систему більш безпечною, обмежуючи користувачів в зміні конфігурації. Будь-який виробник хоче заробити більше і витратити менше. У пристрої може бути реалізовано багато розумних функцій, але при цьому не забезпечена можливість зміни безпеки.

Наприклад, не підтримується перевірка паролів на надійність, відсутня можливість створювати облікові записи з різними правами - адміністратора і користувачів, немає настройки параметрів шифрування, логування та оповіщення користувачів про події безпеки.

3. Відсутність можливості управляти пристроєм. Відсутність підтримки безпеки на пристроях, розгорнутих у виробництві, включаючи управління активами, управління оновленнями, безпечний виведення з експлуатації, моніторинг систем і реагування. Пристрої IoT найчастіше представляють собою «чорний ящик». У них не реалізована можливість стежити за станом роботи, ідентифікувати, які служби запущені і з чим взаємодіють.

Не всі виробники дають користувачам IoT-пристроїв повністю управляти операційною системою і запущеними додатками, а також перевіряти цілісність і легітимність завантаженого ПО або встановлювати патчі поновлення на ОС.

Під час атак прошивка пристрою може бути переконфігурувати так, що починають його можна буде, тільки повністю перепрошити пристрій. Подібним недоліком скористалося, наприклад, шкідливе ПЗ Silex.

Рішенням цих проблем може стати використання спеціалізованого ПЗ для управління пристроями інтернету речей, наприклад, хмарних рішень AWS, Google, IBM і т.д.

4. Небезпечна передача і зберігання даних. Відсутність шифрування або контролю доступу до конфіденційних даних в будь-якому місці екосистеми, в тому числі при зберіганні, при передачі або під час обробки. Пристрої інтернету речей

збирають і зберігають дані про навколишнє середовище, в тому числі різну персональну інформацію. Скомпрометований пароль можна замінити, а вкрадені дані з біометричного пристрою - відбиток пальців, сітківка ока, біометрія особи - немає.

У той же час IoT-пристрої можуть не тільки зберігати у себе дані в незашифрованому вигляді, але також передавати їх по мережі. Якщо передачу даних у відкритому вигляді по локальній мережі можна хоч якось пояснити, то в разі бездротової мережі або передачі через інтернет вони можуть стати надбанням кого завгодно.

Сам користувач може використовувати безпечні канали зв'язку для передачі даних, але шифруванням збережених паролів, біометричних та інших важливих даних повинен потурбуватися виробник пристроїв.

5. Недостатній захист конфіденційності. Особиста інформація користувача, що зберігається на пристрої або в екосистемі, яка використовується небезпечно, неналежним чином або без дозволу.

Цей пункт ТОП-10 перегукується з попереднім: всі особисті дані повинні зберігатися і передаватися в захищеному вигляді. Але цей пункт розглядає приватність в більш глибокому розумінні, а саме з точки зору захисту таємниці приватного життя.

IoT-пристрої збирають інформацію про те, що і хто їх оточує, в тому числі це стосується і нічого не підозрюють людей. Вкрадені або неправильно оброблені дані про користувача можуть як ненавмисно дискредитувати людину (наприклад, коли неправильно налаштовані дорожні камери викривали невірного подружжя), так і використовуватися при шантажі.

Для вирішення проблеми необхідно точно знати, які дані збираються пристроєм IoT, мобільним додатком і хмарними інтерфейсами.

Потрібно переконатися, що збираються тільки необхідні для функціонування пристрою дані, перевірити, чи є дозвіл на зберігання персональних даних і захищені вони, а також прописані політики зберігання даних. Інакше, при недотриманні цих умов, у користувача можуть виникнути проблеми з законодавством.

6. Використання небезпечних або застарілих компонентів. Використання застарілих або небезпечних програмних компонентів або бібліотек, які можуть дозволити скомпрометувати пристрій. Це включає небезпечну настройку платформ операційної системи і використання сторонніх програмних або апаратних компонентів з скомпрометованої ланцюжка поставок. Один уразливий компонент може звести нанівець всю налагоджену безпеку.

7. Відсутність безпечних механізмів поновлення. Відсутність можливості безпечного оновлення пристрою. Це включає в себе відсутність валідації прошивки на пристрої, відсутність безпечної доставки (без шифрування при передачі), відсутність механізмів запобігання відкату і відсутність повідомлень про зміни безпеки через оновлень.

Відсутність можливості оновлення пристрою саме по собі є слабким місцем безпеки. Неможливість встановити оновлення означає, що пристрої протягом невизначеного часу залишаються уразливими. Але крім того, саме оновлення і прошивка також можуть бути небезпечними. Наприклад, якщо для отримання ПЗ не використовуються зашифровані канали, файл оновлення не зашифрований або не підтверджена на цілісність перед установкою, відсутня антіоткатная захист (захист від повернення до попередньої, більш вразливою версії) або відсутні повідомлення про зміни безпеки через оновлень.

Рішення даної проблеми також на стороні виробника. Але ви можете перевірити, чи здатне ваш пристрій взагалі оновлюватися. Переконайтеся, що файли оновлення завантажуються з перевіреного сервера по зашифрованому каналу, і що ваш пристрій використовує безпечну архітектуру установки оновлення.

8. Небезпечні інтерфейси екосистеми. Небезпечний веб-інтерфейс, API, хмарні або мобільні інтерфейси в екосистемі поза пристрої, що дозволяє компрометувати пристрій або пов'язані з ним компоненти. Загальні проблеми включають в себе відсутність аутентифікації або авторизації, відсутність або слабкий шифрування, а також відсутність фільтрації введення та виведення.

Використання небезпечних веб-інтерфейсів, API, хмарних і мобільних інтерфейсів дозволяє скомпрометувати пристрій або пов'язані з ним компоненти навіть без підключення до нього.

Наприклад, Barracuda Labs провела аналіз мобільного застосування та веб-інтерфейсу однієї з «розумних» камер і знайшла уразливості, що дозволяють отримати пароль до пристрою інтернету речей: мобільний додаток ігнорувало дійсність сертифіката сервера; веб-додаток було вразливе до Міжсайтовий Скриптінг; був можливий обхід файлів на хмарному сервері; оновлення пристрою не були захищені; пристрій ігнорувало дійсність сертифіката сервера.

Для захисту необхідно міняти користувача і пароль за замовчуванням, переконатися, що веб-інтерфейс не схильний до Міжсайтовий Скриптінг, SQL-ін'єкцій або CSRF-атак. Також повинна бути реалізована захист від атаки на паролі методом перебору. Наприклад, після трьох спроб неправильного введення пароля аккаунт повинен блокуватися і дозволяти відновити пароль тільки через апаратний скидання.

9. Небезпечні мережеві сервіси. Непотрібні або небезпечні мережеві служби, запущені на самому пристрої, особливо відкриті для зовнішньої мережі, що ставлять під загрозу конфіденційність, цілісність, справжність, доступність інформації або допускають несанкціоноване віддалене управління. Непотрібні або небезпечні мережеві служби ставлять під загрозу безпеку пристрою, особливо якщо вони мають доступ до інтернету.

Небезпечні мережеві служби можуть бути схильні до атак переповнення буфера і DDoS-атакам. Відкриті мережеві порти можуть бути просканувати на наявність вразливостей і небезпечних служб для підключення.

Одними з найпопулярніших векторів атак і зараження пристроїв IoT досі є перебір паролів на НЕ відключених службах Telnet і на SSH. Після отримання доступу до цих служб зловмисники можуть завантажити на пристрій шкідливі програми та отримати доступ до цінної інформації.

10. Слабкий, вгадуваний або жорстко заданий пароль. Використання легко зламував, загальнодоступних або незмінних облікових даних, включаючи бекдори

у вбудованому програмному забезпеченні або клієнтському програмному забезпеченні, яке надає несанкціонований доступ до розгорнутим системам. Дивно, але до їх пір найбільшою вразливістю є використання слабких паролів, паролів за замовчуванням або паролів, злитих в мережу [12].

Незважаючи на очевидність необхідності використання сильного пароля, деякі користувачі досі не змінюють паролі за замовчуванням. Цим в червні 2019 року скористалися шкідливе ПО Silex, яке протягом однієї години перетворило в «цеглина» близько 2000 пристроїв інтернету речей. А до цього відомий всім ботнет і черв'як Mirai встиг заразити 600 тисяч пристроїв інтернету речей, використовуючи базу з 61 стандартних зв'язок логін-пароль.

2.1.2 Основні вектори атак

Інтерес до різних IoT-пристроїв з боку зловмисників продовжує зростати: за першу половину 2019 року було отримано в три рази більше зразків шкідливого ПО, атакуючого «розумні» пристрої, ніж за весь 2018 рік.

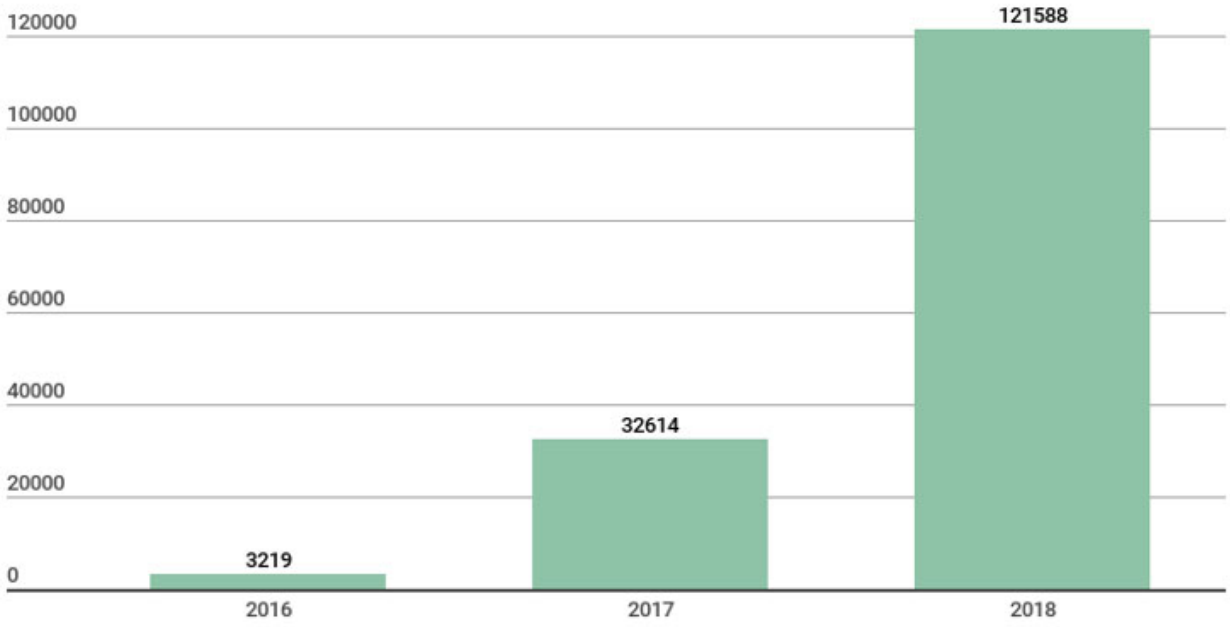

Рис. 2.1. Порівняння кількісті зразків шкідливого ПО для IoT-пристроїв

До слова, в 2018 їх було в 10 разів більше, ніж в 2017 році. Було проаналізувано, які вектори атак використовуються зловмисниками для зараження «розумних» пристроїв, які зловредів завантажуються в систему в результаті успішної атаки, а також чим все це може обернутися для власника пристрою і просто жертв свежеорганізованного ботнету.

Таблиця 2.1.

Найпопулярніщі вектори атак на пристро IP

Сервіс	% атак
Telnet	75,40%
SSH	11,59%
другое	13,01%

Отже, у другому кварталі 2019 року лідером за кількістю унікальних IP-адрес, з яких виходили атаки через перебір пароля Telnet стала Бразилія (23%). Друге місце, з невеликим відривом, зайняв Китай (17%). Росія ж у списку зайняла 4-е місце (7%). Всього за період з 1 січня по липень 2019 року на наших Telnet-ханіпотах було зафіксовано понад 12 мільйонів атак з 86 560 унікальних IP-адрес, а шкідливе ПО скачували з 27 693 унікальних IP-адрес.

Таблиця 2.2.

Статистика популярних зловредів для пристроїв IoT

#	завантажений зловред	% атак
1	Backdoor.Linux.Mirai.c	15,97%
2	Trojan-Downloader.Linux.Hajime.a	5,89%
3	Trojan-Downloader.Linux.NyaDrop.b	3,34%
4	Backdoor.Linux.Mirai.b	2,72%
5	Backdoor.Linux.Mirai.ba	1,94%
6	Trojan-Downloader.Shell.Agent.p	0,38%
7	Trojan-Downloader.Shell.Agent.as	0,27%
8	Backdoor.Linux.Mirai.n	0,27%

9	Backdoor.Linux.Gafgyt.ba	0,24%
10	Backdoor.Linux.Gafgyt.af	0,20%

Оскільки частина власників «розумних» пристроїв змінює штатний пароль Telnet на більш складний, а багато гаджети і зовсім не підтримують цей протокол, зловмисники знаходяться в постійному пошуку нових шляхів зараження. Цьому сприяє і висока конкуренція між вірусописателями, яка призвела до зниження ефективності атак з перебором пароля: в разі успішного злому пристрою його пароль змінюється, а доступ до Telnet блокується.

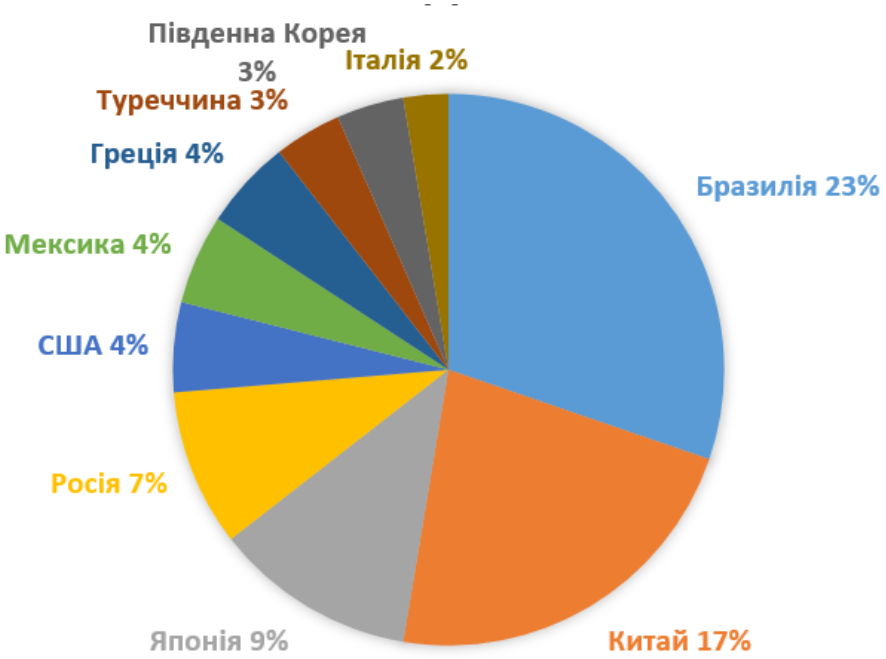

Рис. 2.2. Географічний розподіл кількості заражених пристроїв, другий квартал 2019 р

Як приклад використання «альтернативної техніки» можна привести ботнет Reaper, в його активі станом на кінець 2017 року налічувалося близько 2 мільйонів IoT-пристроїв. Замість перебору паролів до Telnet цей ботнет експлуатував відомі уразливості в ПЗ: вразливості в прошивці роутера D-Link 850L, вразливості в IP-камерах GoAhead, вразливості в CCTV камерах MVPower, вразливість в Netgear ReadyNAS Surveillance, вразливість в Vacron NVR, вразливість в пристроях Netgear DGN, вразливості в роутерах Linksys E1500/E2500, вразливості в роутерах D-Link

DIR-600 і DIR 300 - HW rev B1, вразливості в пристроях AVTech, переваги такого способу поширення в порівнянні з перебором пароля, зараження відбувається значно швидше, закрити вразливість в ПО значно складніше, ніж змінити пароль або відключити/заблокувати сервіс.

Таблиця 2.3.

Аналіз статистики атак різних зловредів

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 23	82.26%	Брутфорс	Mirai, Gafgyt
SSH	22	11.51%	Брутфорс	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	—
tr-069	7547	0.77%	RCE в реалізації протоколу TR-069	Mirai, Hajime
HTTP	80	0.76%	Спроби проексплуатувати уразливості в веб-сервері або підібрати пароль від панелі адміністрування	—
winbox (RouterOS)	8291	0.71%	Використовується для ідентифікації RouterOS (MikroTik) і для атак через сервіс winbox	Hajime
Mikrotik http	8080	0.23%	RCE в MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Виконання довільного коду для певних версій (2000, 2005, and 2008) або зміна пароля адміністратора, крадіжка даних	—
GoAhead httpd	81	0.16%	RCE в IP-камерах GoAhead	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Обхід авторизації (CVE-2017-12113)	—
RDP	3389	0.12%	Брутфорс	—

XionMai uc-httpd	8000	0.09%	Переповнення буферу (CVE-2018-10088) в XionMai uc-httpd 1.0.0 (деякі пристрої китайських виробників)	Satori
MySQL	3306	0.08%	Виконання довільного коду для певних версій (2000, 2005, and 2008) або зміна пароля адміністратора, крадіжка даних	—

Незважаючи на те, що цей спосіб складніший в реалізації, він припав до смаку багатьом вірусописьменниками і нові троянці, що використовують відомі уразливості в ПЗ «розумних» пристроїв, не змусили себе довго чекати. Щоб подивитися, які уразливості намагаються експлуатувати зловредів, було проаналізувано дані про спроби підключень до різних портів на пастках

Поки переважна більшість атак - це все ще перебір паролів Telnet і SSH. На третьому місці за популярністю знаходяться атаки на сервіс SMB, що надає віддалений доступ до файлів. Ми поки не бачили IoT-зловредів, що атакують цей сервіс. Однак деякі його версії містять серйозні відомі уразливості - EternalBlue (Windows) і EternalRed (Linux) -за яких, наприклад, поширювався сумнозвісний троянець-шифрувальник WannaCry і шкідливий майнер криптовалюта Monero EternalMiner. А ось так розподілилися заражені IoT-пристрої, з IP-адрес яких були атаковані ханіпоти в другому кварталі 2019 року:

Таблиця 2.4.

Розподілення заражених IoT-пристрої, з IP-адрес яких були атаковані ханіпоти

Пристрій	% заражених пристроїв
MikroTik	37,23%
TP-Link	9,07%
SonicWall	3,74%
AV tech	3,17%
Vigor	3,15%
Ubiquiti	2,80%
D-Link	2,49%
Cisco	1,40%
AirTies	1,25%

Cyberoam	1,13%
HikVision	1,11%
ZTE	0,88%
Unspecified device	0,68%
Unknown DVR	31.91%

Як можна помітити, з великим відривом лідирують пристрої компанії MikroTik, що працюють під управлінням RouterOS. Причина, по всій видимості, в уразливості Chimay-Red.

Порт 7547. Досить популярні атаки на сервіс віддаленого адміністрування пристроїв (специфікація TR-069), який працює на порту 7547. За даними Shodan, в світі налічується більше 40 мільйонів пристроїв, у яких цей порт відкритий. І це незважаючи на те, що ще не так давно вразливість стала причиною зараження мільйона роутерів Deutsche Telekom, а також «допомогла» поширенню шкідників родин Mirai і Hajime. Ще один тип атак експлуатує уразливість Chimay-Red в роутерах MikroTik під керуванням RouterOS версії нижче 6.38.4. У березні 2018 року за її допомогою активно поширювався Hajime [13].

IP-камери. Зловмисники не обійшли стороною і IP-камери: в березні 2017 року ПО пристроїв GoAhead було виявлено кілька серйозних вразливостей, а через місяць після публікації інформації про це з'явилися нові модифікації троянців Gafgyt і Persirai, що експлуатують ці уразливості. Уже через тиждень після початку активного поширення цих шкідників число заражених пристроїв зросла до 57 тисяч. 8 червня 2018 року було опубліковано proof-of-concept до уразливості CVE-2018-10088 веб-сервера XionMai uc-httpd, який використовується в деяких «розумних» пристроях китайських виробників (наприклад, відеореєстратор KKMoon DVR). Вже на наступний день зареєстрована кількість спроб виявити пристрої, що використовують даний веб-сервер, зросла більш ніж в 3 рази. Винуватцем такого сплеску активності став троянець Satori, раніше атакував роутери GPON.

DDoS-атаки. Головним завданням, яке зловмисники вирішують за допомогою IoT-зловредів, була і залишається організація DDoS-атак. Заражені

«розумні» пристрої стають частиною ботнету, який по команді починає атакувати вказану адресу, позбавляючи хост можливості нормально обробляти запити реальних користувачів. Такими атаками, наприклад, продовжують займатися троянці сімейства Mirai і його клони, зокрема, зловредів Hajime. Це, мабуть, найбільш безневинний сценарій для кінцевого користувача. Максимум, що загрожує власникові зараженого пристрою (і це дуже малоймовірний сценарій) - блокування з боку інтернет-провайдера. А «вилікувати» пристрій найчастіше можна за допомогою простої перезавантаження.

Криптовалюта. Інший тип корисного навантаження пов'язаний з криптовалюта. Наприклад, IoT-зловредів можуть встановлювати майнер на заражене пристрій. Але з огляду на невелику обчислювальної потужності «розумних» пристроїв, доцільність такої атаки залишається під питанням, навіть незважаючи на їх потенційно велика кількість. Більш хитрий і дієвий спосіб збагатитися придумали автори троянця Satori. IoT-пристрій виступає в їх сценарії в ролі своєрідного «ключа», що відкриває доступ до високопродуктивної ПК [14].

На першому етапі зловмисники намагаються заразити якомога більше роутерів, використовуючи відомі уразливості, а саме:

- CVE-2014-8361 - RCE в miniigd SOAP service в Realtek SDK;
- CVE 2017-17215 - RCE в прошивці роутерів Huawei HG532;
- CVE-2018-10561, CVE-2018-10562 - обхід авторизації і можливість виконати довільні команди на роутерах Dasan GPON
- CVE-2018-10088 - переповнення буфера в XiongMai uc-httpd 1.0.0, який використовується в прошивках деяких роутерів та інших «розумних» пристроїв деяких китайських виробників.
- Використовуючи скомпрометовані роутери і вразливість CVE-2018-1000049 в механізмі віддаленого адміністрування ПО для Майнінг криптовалюта Etherium - Claymore, замінити адресу гаманця на свій [15].

Крадіжка даних. Виявлений в травні 2018 року троянець VPNFilter переслідує інші цілі. Головна серед них - перехоплення трафіку зараженого пристрою, витяг з

нього важливих даних (логіни, паролі тощо) і відправка їх на сервер зловмисників. Ось основні особливості VPNFilter:

- Модульна архітектура. Автори зловреда можуть «обладнувати» його новими функціями «на льоту». Так, на початку червня 2018 був виявлений новий модуль, який умів Інжект javascript-код в перехоплені веб-сторінки.
- Стійкість до перезавантаженням пристрою. Троянець прописує себе в стандартний для Linux-систем планувальник crontab, а також може змінювати конфігураційні параметри в незалежній пам'яті (NVRAM) пристрою.
- Використання TOR для комунікації зі своїм сервером управління.
- Можливість самознищення і виведення пристрою з ладу. Отримавши відповідну команду, троянець видаляє себе, а також перезаписує сміттєвими даними критичну частину прошивки після чого перезавантажує пристрій.

Спосіб поширення троянця досі залишається невідомим: його код не містить жодних механізмів самораспространения. Однак ми схильні вважати, що для зараження використовуються відомі уразливості в ПЗ пристроїв. У найпершому звіті про VPNFilter говорилося про 500 тисяч заражених пристроїв. З тих пір їх стало більше, а список виробників вразливих гаджетів значно збільшився. На середину червня він включав такі бренди: ASUS, D-Link, Huawei, Linksys, MikroTik, Netgear, QNAP, TP-Link, Ubiquiti, Upvel, ZTE.

Ускладнює ситуацію ще й те, що пристрої цих виробників використовуються не тільки в корпоративних мережах, але часто і в якості домашніх роутерів звичайних користувачів.

2.2 Приклади здійснених кібер атак мережі IoT

Давно відомо про проблеми кібербезпеки, коли мова йде про пристрої Інтернету речей, і про неминуче ризик, який виникає при підключенні все більшої кількості пристроїв до Інтернету і один до одного. Шкідливі хакери можуть запускати атаки і проникати в тисячі або мільйони незахищених пристроїв, завдаючи шкоди інфраструктурі, відключаючи мережі або отримуючи доступ до

приватної інформації. І оскільки ми все більше і більше покладаємося на IoT в нашому повсякденному житті, ці атаки можуть стати більш руйнівними або навіть небезпечними. У цій статті ми зосередимося на деяких з найбільш серйозних зломів і вразливостей, які ми бачили раніше. Сподіваюся, ця стаття може надихнути вас, коли мова йде про те, щоб ставити безпеку на перше місце в вашому шляху розробки Інтернету речей.

Те, що колись було сюжетом науково-фантастичного фільму, наприклад, злом побутової техніки, спрямоване проти людства, тепер стало реальністю. Злом Інтернету речей може бути надзвичайно ефективним, викликаючи DDoS-атаки, які можуть завдати шкоди нашій інфраструктурі, системам і способу життя », - каже Деніел Маркусон, експерт по цифровій конфіденційності NordVPN. «Якщо у вас є кілька пристроїв, підключених до однієї мережі в вашому будинку або офісі, і хакер отримує доступ до одного пристрою, він може зламати всі з них».

За словами експерта NordVPN в області цифрової конфіденційності, навіть незважаючи на те, що важко повірити, що радіоняня або, здавалося б, проста іграшка може заподіяти значної шкоди, більше не тільки комп'ютери або смартфони піддаються ризику кібератак. Погляньте на ці божевільні приклади злому Інтернету речей і вразливостей, зафіксованих в історії:

1) Ботнет Mirai (також відомий як Dyn Attack). Ще в жовтні 2016 року найбільша в історії DDoS-атака була запущена на постачальника послуг Dyn, що використовує ботнет Інтернету речей. Це призвело до виходу з ладу величезної частини Інтернету, включаючи Twitter, Guardian, Netflix, Reddit і CNN. Цей ботнет IoT став можливий завдяки шкідливому ПО Mirai. Після зараження Mirai комп'ютери постійно шукають в Інтернеті вразливі пристрої IoT, а потім використовують відомі імена користувачів і паролі за замовчуванням для входу в систему, заражаючи їх шкідливим ПЗ. Цими пристроями були цифрові камери і відеореєстратори.

2) Атака на серцеві пристрої з Сент-Джуда. На початку минулого року CNN писала: «FDA підтвердило, що імплантуються кардіологічні пристрої St. Jude Medical мають уразливості, які можуть дозволити хакеру отримати доступ до

пристрою. Увійшовши всередину, вони можуть розрядити батарею або призначити неправильну кардиостимуляцию або розряди розряду. Такі пристрої, як кардіостимулятори та дефібрилятори, використовуються для моніторингу і контролю серцевих функцій пацієнтів і запобігання серцевих нападів».

3) Вразливості монітора серцевого ритму Wi-Fi Owlet. Відразу за кардіологічними пристроями St. Jude знаходиться кардіомонітор Owlet WiFi. За словами Чезаре Гарлаті, головного стратега безпеки фонду prpl: «Цей останній випадок - ще один приклад того, як пристрої з найкращими намірами, такі як оповіщення батьків про те, що у їхніх дітей проблеми з серцем, можуть стати небезпечними, якщо ними скористатися зловісна сторона На жаль, найчастіше це відбувається з вбудованими обчисленнями в так званих інтелектуальних пристроях. Елемент зв'язку робить їх доступними для використання, і якщо виробники і розробники не врахують це і не вживатиме додаткових заходів для захисту пристроїв на апаратному рівні, ці історії, на жаль, ми будемо чути».

4) Злом Jeep. Веб-сайт служби безпеки IBM повідомив про злом Jeep кілька років тому: «Це був всього один раз, але цього було достатньо. У липні 2015 року група дослідників змогла взяти під повний контроль позашляховик Jeep за допомогою шини CAN. Використовуючи уразливість в оновленні прошивки, вони викрали автомобіль через стільникову мережу Sprint і виявили, що можуть змусити його прискорюватися, сповільнюватися і навіть відхилятися від дороги. Це доказ концепції з'являються зломів Інтернету речей (IoT): хоча компанії часто ігнорують безпеку периферійних пристроїв або мереж, наслідки можуть бути катастрофічними».

5) Атака через темпиратурний датчик. Здається, що казино - одні з найбезпечніших організацій в світі, але вони також можуть бути зламані. Кілька років тому група хакерів використовувала досить нетрадиційний метод злому казино. Їм вдалося отримати доступ до його мережі через підключений до Інтернету термометр в акваріумі і витягти з його бази даних хайроллеров всі важливі деталі.

6) Атака на системи отоплювання будинку. У 2016 році хакери залишили жителів двох багатоквартирних будинків в Лаппеенранта, Фінляндія, на морозі майже на тиждень, запустивши DDoS-атаку на їх системи контролю навколишнього середовища за допомогою термостатів. Оскільки атака була атакована як системою центрального опалення, так і системою гарячого водопостачання, екологічні системи перезавантажувались в спробі відбити атаку і застрягли в нескінченному циклі.

2.3 Основні положеня безпеки IoT

Безпека Інтернету речей - це технологічна область, пов'язана із захистом підключених пристроїв і мереж в Інтернеті речей (IoT).

Безпека Інтернету речей стала предметом пильної уваги після низки гучних інцидентів, коли звичайний пристрій Інтернету речей використовувалося для проникнення і атаки в більш велику мережу. Реалізація заходів безпеки має вирішальне значення для забезпечення безпеки мереж з підключеними до них пристроями IoT.

Ряд проблем перешкоджає захисту пристроїв Інтернету речей та забезпечення наскрізної безпеки в середовищі Інтернету речей. Оскільки ідея мережевих пристроїв та інших об'єктів відносно нова, безпека не завжди вважалася вищим пріоритетом на етапі розробки продукту. Крім того, оскільки IoT - це зароджується ринок, багато розробники і виробники продуктів більше зацікавлені в швидкому виведенні своїх продуктів на ринок, а не в прийнятті необхідних заходів щодо забезпечення безпеки з самого початку.

Основною проблемою, пов'язаною з безпекою Інтернету речей, є використання жорстко заданих паролів або паролів за замовчуванням, що може привести до порушень безпеки. Навіть якщо паролі змінюються, вони часто недостатньо надійні для запобігання проникнення [16].

Інша поширена проблема, з якою стикаються пристрої IoT, полягає в тому, що вони часто обмежені в ресурсах і не містять обчислювальних потужностей,

необхідних для реалізації надійного захисту. Таким чином, багато пристроїв не мають або не можуть пропонувати розширені функції безпеки. Наприклад, датчики, контролюючі вологість або температуру, не можуть підтримувати розширене шифрування або інші заходи безпеки. Крім того, оскільки багато пристроїв Інтернету речей «набудували і забули» - помістили в поле або на машину і залишили до кінця терміну служби - вони майже ніколи не отримують оновлення безпеки або виправлення. З точки зору виробника, забезпечення безпеки з самого початку може бути дорогим, уповільнити розробку і привести до того, що пристрій не працюватиме належним чином.

Ще одна проблема безпеки - підключення застарілих активів, які спочатку не призначені для підключення до Інтернету речей. Заміна успадкованої інфраструктури підключеної технологією непомірно висока, тому багато активів будуть оснащені інтелектуальними датчиками. Однак, оскільки застарілі активи, ймовірно, не оновлювалися або ніколи не мали захисту від сучасних загроз, поверхня атаки розширюється.

Що стосується оновлень, багато систем включають підтримку тільки у встановлені терміни. Для застарілих і нових активів безпеку може бути порушена, якщо не буде додана додаткова підтримка. А оскільки багато пристроїв Інтернету речей залишаються в мережі протягом багатьох років, забезпечення безпеки може бути складним завданням.

Безпека Інтернету речей також страждає від відсутності загальноприйнятих стандартів. Хоча існує безліч структур безпеки IoT, єдиної узгодженої структури не існує. Великі компанії та галузеві організації можуть мати свої власні специфічні стандарти, в той час як певні сегменти, такі як промисловий Інтернет речей, мають пропрієтарні несумісні стандарти від лідерів галузі. Різноманітність цих стандартів ускладнює не тільки захист систем, а й забезпечення взаємодії між ними.

Конвергенція мереж IT і операційних технологій (OT) створила ряд проблем для груп безпеки, особливо тих, яким доручена захист систем і забезпечення наскрізної безпеки в областях, що виходять за рамки їхньої компетенції. Потрібно

крива навчання, і IT-команди з належним набором навичок повинні відповідати за безпеку Інтернету речей [17].

Ще один важливий фактор, який слід враховувати, - це те, що багатьма пристроями IoT не можна централізовано керувати і налаштовувати. Деякі пристрої розглядаються як чорні ящики і не надають інформацію про статус свого програмного забезпечення або вбудованого ПЗ, тому було б важко слідувати звичайним методам управління уразливими.

Пристрої IoT мають набагато менші обсяги пам'яті і обчислювальні можливості в порівнянні зі звичайними IT-системами. Отже, було б важко використовувати стандартні рішення безпеки IT, які зазвичай вимагають високої обчислювальної потужності, такі як служби шифрування.

Організації повинні навчитися розглядати безпеку як загальну проблему, від виробника до постачальника послуг для отримання кінцевого користувача. Виробники та постачальники послуг повинні приділяти пріоритетну увагу безпеки і конфіденційності своїх продуктів, а також забезпечувати, наприклад, шифрування і авторизацію за замовчуванням. Але на цьому тягар відповідальності не закінчується; кінцеві користувачі повинні обов'язково прийняти власні запобіжні заходи, включаючи зміну паролів, установку виправлень, коли вони доступні, і використання програмного забезпечення безпеки.

Експерти з безпеки давно попереджають про потенційний ризик великої кількості незахищених пристроїв, підключених до Інтернету, з тих пір, як концепція IoT вперше виникла в кінці 1990-х років. У заголовках газет згодом потрапив ряд атак: холодильники і телевізори використовуються для розсилки спаму хакерам, проникаючим в няньки і розмовляє з дітьми. Важливо відзначити, що багато зломи Інтернету речей не націлені на самі пристрої, а скоріше використовують пристрої Інтернету речей в якості точки входу в більш велику мережу.

У грудні 2013 року дослідник з компанії Proofpoint Inc., що займається корпоративної безпекою, виявив перший ботнет IoT. За словами дослідника,

більше 25% ботнету складалося не з комп'ютерів, а з інших пристроїв, включаючи смарт-телевізори, радіоняні і побутову техніку.

Існує безліч структур безпеки IoT, але на сьогоднішній день немає єдиного загальноприйнятого стандарту. Однак може допомогти просте впровадження системи безпеки IoT; вони надають інструменти та контрольні списки, щоб допомогти компаніям створювати і розгортати пристрої IoT. Такі структури були випущені Асоціацією GSM, Фондом безпеки Інтернету речей, Консорціумом промислового Інтернету та іншими.

У вересні 2015 Федеральне бюро розслідувань випустило офіційне оголошення FBI Alert Number I-091015-PSA, в якому містилося попередження про потенційні вразливості пристроїв Інтернету речей та рекомендації щодо захисту прав споживачів і захисту прав споживачів [18].

2.4 Дослідження відомих засобів забезпечення безпеки мережі IoT

2.4.1 Обгрунтування технології блокчейну у мережах IoT

Блокчейн - це нова ефективна технологія, яка зробила революцію в світі криптовалюта. Він в основному з безпечної розподіленої бази даних (також публічний реєстр), включаючи всі транзакції, вчинені усіма що організаціями. У рішеннях на основі блокчейнов криптовалюта, такі як біткойн і ефіріум, транзакції виконуються і перевіряються в розподіленої тимчасової інфраструктури. По суті, коли об'єкт відправляє запит транзакції з іншим об'єктом B, він відправляє запит транзакції всім партнерам в мережі блокчейна. Потім кожен вузол періодично (10 хвилин у разі біткойнов) збирає набір транзакцій і групує їх в один блок. Нарешті, процес перевірки кожного блоку виконується розподіленим чином з використанням алгоритму консенсусу, який виконується через вузлами в мережі, званими Майнер.

Система безпечного і конфіденційного обміну повідомленнями про транзакції, децентралізація комунікацій, конфіденційність за задумом - все це дуже

важливі функції промислового та Інтернету в цілому. Інтернет-послуги продовжують зростати. Ці дані необхідно використовувати спільно між різними об'єктами і використовувати для аналізу великих даних, а також для цілей моніторингу деяких критично важливих додатків. Блокчейн може допомогти створити захищену від несанкціонованого доступу запис, яка дозволяє усім учасникам інтелектуальним об'єктів отримувати доступ до одних і тих же даних більш узгодженим і безпечним способом. Блокчейн є ефективний спосіб роботи з інтелектуальними пристроями без звернення до центральних об'єктів. Під смарт-контрактами ми розуміємо всілякі цифрові правила, що формують умови контакту. Зокрема, смарт-контракт складається з комп'ютерної програми, яка автоматично виконується смарт-об'єктами і визначає набір правил і умов, заснованих на умовах контракту. Блокчейн може допомогти забезпечити безперебійну роботу контрактів розподіленим чином.

Завдяки децентралізованої мережі IoT блокчейн найбільш підходить в якості рішення безпеки в IoT. Децентралізована архітектура блокчейна робить рішення безпеки найбільш масштабованими і може вирішити проблему єдиної точки відмови, а також стає більш стійкою до DoS-атак.

Вузли в ланцюжку блоків ідентифікуються своїми відкритими ключами (або хешем відкритих ключів). Ці псевдоніми не пов'язують ніякої інформації про особу беруть участь вузлів.

Транзакція перед відправкою в мережу блокчейн підписується вузлом і повинна бути перевірена та підтверджена Майнер. Після перевірки практично неможливо підробити ланцюжок транзакцій, вже збережені в ланцюжку блоків. Це доказ що відслідковуються подій в системі [19].

Перше блокчейн-рішення на основі платформи IoT було розроблено IBM в 2013 році. Ця платформа називається ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry), яка являє собою доказ концепції децентралізованої і безпечної платформи IoT на основі протоколу Ethereum, являє собою безшовне для роботи з пристроями і транзакціями найбільш масштабованим чином. Таким чином, пристрій IoT може самостійно визначати і встановлювати свої власні ролі,

обов'язки і дозвіл у всій екосистемі IoT, а також виконувати транзакції і складні переговори. між собою.

В був предложілен протокол HTTPS для пристроїв IoT, усунувши проміжні пристрої (наприклад, мобільні телефони) для створення безпечного каналу HTTPS (класичне рішення). Ключ сеансу генерується за допомогою алгоритму PBKDF2 (Password-Based Key Derivation Function 2), а транзакції IoT зберігаються в ланцюжку блоків, підтримуваної між кількома пристроями. Це рішення може бути посилена шляхом встановлення пріоритету серед транзакцій.

Нещодавно Kamanashis et al. запропонували багаторівневу архітектуру безпеки для розумних міст, яка інтегрує блокчейн як рівня розподіленої бази даних для обміну та зберігання різнорідних даних Інтернету речей, пов'язаних з навколишнім середовищем розумного міста, таких як трафік, температура, місце розташування, вологість і т. д зберігання даних направлено на безпечний обмін цими даними між різними розумними містами.

На даний момент вже запущено кілька проектів з розвитку блокчейна для корпоративного середовища. Так, корпорація Intel надає необхідне апаратне забезпечення з підтримкою технології блокчейн, а також співпрацює з десятками інших компаній, включаючи JP Morgan і Microsoft, в складі альянсу Enterprise Ethereum Alliance (EEA). Мета діяльності цього альянсу полягає в розробці стандартів і технологій, які спростять компаніям розгортання Ethereum - платформи на базі блокчейна, що дозволяє використовувати розумні контракти. Крім того, в 2016 році корпорація Intel створила платформу розподіленого реєстру Sawtooth Lake для проекту Hyperledger. Цей спільний проект, запущений консорціумом The Linux Foundation, спрямований на вдосконалення технології блокчейн для корпоративного середовища. Одним з компонентів проекту є нова модульна платформа на базі технологій Intel під назвою Hyperledger Sawtooth, призначена для проектування, розгортання і запуску розподілених реєстрів на базі блокчейна. У той час як технології Intel допомагають організаціям підготуватися до повсюдного впровадження технології блокчейн, ймовірно, в найближчому майбутньому з'являться і інші компанії, що пропонують API-інтерфейси на базі

блокчейна. Ці API-інтерфейси, призначені для розробників, дозволять компаніям витрачати більше часу на поліпшення своїх сервісів, а не на створення для них програмно-апаратного комплексу для їх роботи. Використовуючи API-інтерфейси на базі блокчейна, компанії можуть забезпечити надійний захист своїх систем Інтернету речей [20].

Блокчейн здатний забезпечити захист ланцюжка поставок (див. Малюнок) і дозволяє локалізувати проломи безпеки Інтернету речей відразу після виявлення. Блокчейн допоможе у вирішенні кризових ситуацій, таких як масове відкликання продукції у зв'язку з підозрами з приводу її безпеки. Громадська доступність записів блокчейна дає можливість відстежувати походження товару аж до джерела сировини, а по транзакціях можна уточнювати всіх користувачів вразливих пристроїв Інтернету речей.

Роль блокчейна в зміцненні безпеки мереж ланцюжка поставок. При використанні блокчейна є можливість забезпечити з самого початку ланцюжка поставок доступ до незмінних записів для уточнення подробиць угод, що стосуються вироби, з метою виявлення дефектів. Блокчейн також дозволяє посилити профілактичні та оборонні заходи забезпечення інформаційної безпеки, які застосовуються нижчими учасниками ланцюжка поставок і власниками пристроїв

2.4.2 Хмарні платформи у мережах IoT

Перед лицем проблем, викликаних тривалим розширенням Інтернету речей (тенденція, яка, як очікується, буде ще більше посилюватися з настанням ери 5G), багато організацій звернулися до хмарних обчислень, особливо до хмарним рішенням Інтернету речей. Засновані на ідеї надання «орендованого простору для зберігання», хмарні рішення Інтернету речей можуть відповідати потребам організацій щодо інтеграції, обробки, масштабованості і найважливіших міркувань

Постачальники хмарних послуг запропонували організаціям рішення відповідно до їх різними бізнес-потребами. У міру того, як все більше підприємств

переносять свої робочі навантаження в хмару, щоб скористатися перевагами інфраструктури, ці постачальники також можуть розширювати функції своїх продуктів, щоб досліджувати нові можливості для бізнесу. Підприємствам, які вже скористалися хмарними сервісами, пропонується більше рішень, специфічних для IoT, що вимагають менших витрат, ніж ті, які зазвичай потрібні для виходу на ринок IoT, без істотного впливу на існуючу інфраструктуру продуктів.

З поширенням пристроїв IoT і необхідністю обробляти експоненціально збільшується обсяг даних, підприємства можуть стежити за розвитком хмарних рішень IoT. Тут ми проілюструємо деякі переваги, які організації можуть отримати від впровадження хмарних рішень Інтернету речей. Як приклад ми візьмемо додаток для спільного використання транспорту, зокрема досліджуючи його масштабованість за допомогою хмарних функцій IoT з урахуванням користувачів і сервісів, з якими воно, як очікується, буде мати справу після його запуску.

При необхідності розробники можуть швидше масштабувати додаток і легко враховувати необхідні зміни платформи, такі як точність часу для водіїв і пасажирів. Оскільки платформу можна розглядати як частину методології IoT - з користувачем, вузлом і периферією, що знаходяться в хмарі як «слабо пов'язаної архітектурою», хмарне додаток може бути спроектовано так, щоб отримувати періодичні винагороди і екстрені повернення. Він також може мати функції захисту від підробки/спуфинга на стороні сервера. Рішення IoT на основі хмарних обчислень призначені для використання строгих правил перевірки та ієрархічного управління правами для запобігання несанкціонованого вторгнення, оскільки вся хмарна середовище може бути скомпрометована; без тестів даних або сигналів від серверного терміналу команди не передаються пристрою або додатком [21].

Інтегроване з машинним навчанням і штучним інтелектом (AI), додаток може постійно вивчати дані для розробки продуктів і покращувати профілі водіїв і користувачів. Оскільки хмарні рішення мають кілька каналів для зв'язку, користувачі і водії можуть повідомляти про своє місцезнаходження, інформації про швидкість і профілях в режимі реального часу. Ці інтеграції також можуть допомогти водіям справлятися з непередбаченими ситуаціями і порушеннями

умов, негайно попереджаючи їх у міру необхідності або в режимі реального часу, або з затримкою в 10 секунд. Час простою скорочується на 0,01%, так як нові хмарні рішення пропонують потужні позасмугових можливості для адаптації до несподіваних ситуацій, таким як зміна сигналу мережі та датчіка.Potential attack vectors in cloud-based IoT infrastructures [22].

Платформи промислового Інтернету речей (англ. Industrial Internet of Things - IIoT) оптимізують витрати на активи, процеси і робочу силу, надають користувачам можливість приймати зважені та своєчасні рішення по всьому підприємству. Цілісний погляд на процеси і активи дозволяє зрозуміти взаємозв'язок і потенційний економічний ефект. Маючи такий погляд, користувачі можуть безпечно і ефективно виконувати завдання для досягнення стійкої пікової продуктивності. Можна виділити наступні переваги концепції промислового Інтернету речей:

Розглянемо підхід до захисту хмарних-платформ. Основним документом, що визначає цей підхід, є політика кібербезпеки. Програми захисту платформи IoT, що реалізуються відповідно до політикою кібербезпеки, повинні включати наступні розділи:

Керівництво і стандарти:

- керівництво. Вище керівництво та співробітники підрозділів безпеки повинні контролювати виконання програми безпеки. Такий контроль включає регулярні перевірки, внутрішні та зовнішні аудити;
- захищене середовище життєвого циклу безпечної розробки (SDLC). Перевірки безпеки повинні виконуватися на кожному циклі розробки;
- стандарти безпеки. Платформа і цикл розробки повинні відповідати міжнародним і національним стандартам як за допомогою сертифікації, так і іншими можливими способами;
- безпеку і конфіденційність, вбудовані в дизайн:
- безпечна архітектура. Повинні використовуватися кращі практики, включаючи управління ідентифікацією та доступом, шифрування даних (в спокої і

при передачі) і аналіз захищеності компонентів інфраструктури, платформи і додатків;

- Повинні використовуватися кращі галузеві інструменти та процеси для реалізації SDLC, в тому числі: вимоги безпеки, аналіз архітектури, моделювання загроз, огляд коду, статичний і динамічний аналіз коду, аналіз додатків, аналіз продуктивності і тестування на проникнення, а також огляд проблем безпеки в сторонніх і відкритих компонентах;
- конфіденційність. Повинні існувати процеси обробки і класифікації даних в додатках для реалізації і забезпечення дотримання заходів захисту конфіденційності даних відповідно до чинного законодавства і договорами;
- сторонні компоненти. Повинні регулярно перевірятися використовувані компоненти з відкритим вихідним кодом і сторонніх виробників на етапі визначення вимог безпеки, необхідно сканувати вихідний код з використанням інструментів безпеки і усувати виявлені вразливості;

Операції:

- управління ідентифікацією та доступом. Повинні бути впроваджені засоби управління доступом на основі ролей і криптографічні рішення, засновані на стандартах класифікації, маркування та обробки інформації. Всі вхідні і особисті дані повинні бути зашифровані на рівні продукту і конкретного проекту і підлягати контролю доступу;
- шифрування. Повинні дотримуватися стандарти маркування і обробки інформації і стандарти управління шифруванням, які забезпечують шифрування в стані спокою і при передачі. Дані повинні передаватися між різними компонентами IoT і платформою в зашифрованому каналі. Крім того, передача даних повинна бути обмежена за допомогою сегментації мереж;
- збереження даних. Дані повинні розміщуватися в центрах обробки даних відповідно до вимог законодавства;
- конфіденційність даних. Конфіденційність даних повинна бути захищена відповідно до вимог законодавства;

- локалізація і передача даних. Повинна бути можливість розміщення копії глобального примірника даних в окремому регіональному або локальному сховищі, щоб забезпечити мінімальну затримку, підвищену продуктивність запитів, конфіденційність даних а також мати кваліфікацію про локалізацію і передачі даних;
- виправлення. Оновлення, пов'язані з безпекою (в тому числі для програмного забезпечення з відкритим вихідним кодом), для виявлених вразливостей повинні встановлюватися якомога швидше;
- моніторинг безпеки. Повинні використовуватися інструменти моніторингу інфраструктури для виявлення підозрілих і зловмисних дій;
- інциденти. Повинен бути створений ситуаційний центр безпеки (SOC або аналогічний підрозділ), який реалізує провідні в галузі практики інформаційної безпеки і процедури реагування на інциденти кібербезпеки для реєстрації, обробки і моніторингу інцидентів у співпраці з іншими внутрішніми підрозділами;
- процедури контролю змін. Повинен бути визначений процес управління змінами при внесенні будь-яких змін в конфігурацію програми або його інфраструктури;
- вразливості. Повинна бути створена група реагування на інциденти в області безпеки для мінімізації ризиків, пов'язаних з уразливими безпеки, шляхом надання своєчасної інформації для керівництва та усунення вразливостей, включаючи програмне забезпечення та програми, обладнання та пристрої;
- аварійне відновлення і резервне копіювання. Повинен бути розроблений план аварійного відновлення і забезпечення безперервності бізнесу. План повинен включати в себе стратегію відновлення і процедури, призначені для відновлення операцій протягом певного часу після аварії. План повинен періодично тестуватися. Періодично повинні створюватися резервні копії даних;

Треті особи:

- провайдер інфраструктури. У разі використання послуг провайдера інфраструктури він повинен підтвердити захищеність своєї інфраструктури, наприклад провівши сертифікацію SOC2 типу 1 і типу 2;

- мережі. Системи та мережі середовища повинні бути логічно розділені, щоб забезпечити відповідність законодавчим, нормативним та договірним вимогам;
- співробітники, підрядники. Повинна проводитися перевірка всіх кандидатів на роботу і підрядників відповідно до чинних законів і правил;
- постачальники, Ліцензії будуть. Повинні відповідати стандартам та рівнями безпеки;
- аудити і тестування:
- внутрішні аудити. Повинні проводитися внутрішні аудити і пошук вразливостей і вживатися коригувальні дії для усунення виявлених проблем, які впливають на безпеку;
- зовнішній аудит. Повинні бути визначені правила і процедура проведення зовнішніх аудитів.

Приклади популярних хмарних платформ: Amazon Web Services, Google Cloud IoT, Microsoft Azure IoT Suite, Salesforce IoT, Oracle Internet of Things, Cisco IoT Cloud Connect, Bosch IoT Suite, IBM Watson Internet of Things, ThingWorx IoT Platform.

2.4.3 Порівняльний аналіз переваг блокчейну над хмарними технологіями

В рамках хмарної моделі пристрою Інтернету речей ідентифікуються, проходять аутентифікацію і з'єднуються через хмарні сервери, на яких виконуються обробка і зберігання даних. Навіть якщо самі пристрої знаходяться поруч один з одним, з'єднання між ними здійснюється через Інтернет.

При використанні централізованої хмарної моделі проблемою стають високі витрати на мережі Інтернету речей. Кожен блок архітектури Інтернету речей може стати вузьким місцем або точкою, збій якої призведе до відмови всієї мережі. Зокрема, пристрої Інтернету речей уразливі для DDoS-атак, злому, крадіжки даних і віддаленого захоплення управління. Зловмисники також можуть зламати систему

і незаконно використовувати її дані. А якщо пристрій Інтернету речей, поєднане з сервером, зламали, під загрозою може опинитися все, що з'єднується з тим же сервером [23].

Централізована хмарна модель вразлива для маніпуляцій. При зборі даних в реальному часі немає гарантій того, що інформація використовується за призначенням. Блокчейн дозволив би усунути багато проблем, перераховані в таблиці. Обмін повідомленнями між пристроями може відбуватися за тією ж схемою, що і фінансові транзакції в біткойн-мережі. Обмін інформацією управляється розумними контрактами.

Таблиця 2.5.

Рішення проблем безпеки хмари за допомогою блокчейен

Проблема	роз'яснення	Потенційне рішення на базі блокчейн
Витрати і обмеження потужності	Проблема, пов'язана з ростом числа пристроїв Інтернету речей	Немає потреби в централізованої системи: пристрої можуть захищено обмінюватися даними, а також автоматично виконувати дії за інструкцією.
недосконаліть архітектури	Будь-блок архітектутри Інтернету речей може стати вузьким місцем або точкою відмови, що виводить з ладу всю мережу	Захищений обмін повідомленнями між пристроями: ідентифікатори пристрою перевіряються, транзакції підписуються, це дає гарантії. Того, що відправник сообшщенія - той, за кого себе видає
Непродуктивні простої хмарних серверів і недоступність служб	Хмарні сервери можуть виходити з ладу через кібератаки, програмних помилок, а також проблем харчування, оздажденія і т.п.	Відсутність єдиної точки відмови: записи зберігаються на багатьох комп'ютерах пристроях, що містять ідентичні копії інформації.

Уразливість для маніпуляцій	Вероятность изменения информации и злоупотребления ею	Децентралізований доступ і незмінюваність: шкідливі дії можна розпізнати і запобігти. Взаємне блокування пристрою: якщо відбувається перехоплення контролю над оновленням блокченйа на одному з пристроїв, система його відкидає.

Блокчейн криптографически підписує транзакції і перевіряє підписи, щоб виключити можливість відправки повідомлень кимось крім реального упорядника. В результаті усувається можливість перехоплення, відтворення та інших атак. Тому, з'явилася нова технологія - Fog Computing (т.зв. «туманні обчислення»), яка усуває зазначені недоліки. Таким чином, децентралізація обчислень - невідворотна тенденція розвитку інтернету речей. У централізованих хмарних платформах IoT спостерігається дуже щільний трафік передачі повідомлень. Тут криється саме «вузьке місце» в масштабуванні рішень IoT для великої кількості пристроїв. Великий обсяг даних, зібраних від мільйонів пристроїв гостро ставить питання інформаційної безпеки як для окремих користувачів, так і для підприємств і організацій. Як показали відбуваються DoS-атаки на пристрої IoT, велике число недорогих пристроїв, підключених до інтернету безпосередньо - це головна проблема забезпечення безпеки в IoT. Централізовані хмарні платформи залишаються «вузьким місцем» в комплексних рішеннях IoT. Будь-яка несправність або помилка в цьому місці може вплинути на всю мережу [24].

Висновки до розділу 2

Досліджено головні взразливості пристроїв мережі Інтренту Речей. Зазначено ключові вектори атак та узагальнену статистику світових вразливостей та експлойтів.

Виокремлено особливості організації різних типів атак, та того, з яких пристроїв найчастіше вони надходили.

Проаналізовано приклади здійсннних кібер атак, та підкреслено наслідки до яких можуть призвести успішно проведені атаки. Безпека в IoT унікальна в тому, що повинна відбуватися ідентифікація, аутентифікація, зберігання та обробка інформації, в тому числі і фінансової.

Зазначено, що безпека доставки товарів, мультифакторна аутентифікація, автоматична фіксація передачі прав від одного контрагента до другого забезпечується п’ятьма кроками:

1) Оцінка цілей і ризиків.

2) Управління цілісністю системи.

3) Шифрування конфіденційних даних.

4) Для важливих систем використовувати апаратне забезпечення і стандарти.

5) Захист пристроїв з обмеженими можливостями за допомогою оверлейної мережі.

Проаналізовано основні положення безпеки пристроїв мережі IoT та досліджено основні засоби забезпечення безпеки мереж IoT.

Визначено принцип роботи технології блокчейну, а також підкрслено особливості функціонування найвідоміших хмарних платформ, які здійснюють регулюючу функцію для забезпечення безпеки технології Інтернету Речей

Зазначено переваги у вирішенні питянь безпеки за допомогую блокчейн при порівняні з хмарними технологіями, а такж проаналізоано доцільність використання стандартних підходів до забезпечення безпеки.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЗАХИСТУ МЕРЕЖІ IOT НА БАЗІ ЕКСПЛОЙТУ SIREPRAT

3.1 Дослідження експлойту SirepRAT у ОС Windos IoT core

29 липня 2015 року відбулася офіційна презентація нової версії операційної системи Windows 10 та вбудованої версії Windows 10 IoT. У назві нової операційної системи більш не присутній слів Embedded. На зміну Embedded приходить IoT, що означає Internet of Things (Інтернет речей) - нову концепцію Microsoft, що об'єднує воєдино пристрої, датчики, дані, сервера, хмарні технології

Windows 10 IoT - це еволюція більш ранньої версії Windows - Windows Embedded. Ви можете згадати банкомати під управлінням Windows XP і потребують серйозного оновлення. Ці банкомати та інші подібні пристрої працювали під управлінням Windows Embedded (XPe). Це урізана версія операційної системи Windows, яка буде добре працювати на менш потужному обладнанні, використовувати один сценарій використання або обидва варіанти.

Банк може використовувати цю ОС для банкомату, роздрібний торговець може використовувати її для системи POS (точки продажу), а виробник може використовувати її для простого прототипу пристрою. Однак Windows IoT - це не просто перейменована версія Windows для використання Інтернету речей, і не тільки для підприємств і великих корпорацій. Це очевидно в двох різних версіях ОС, IOT Enterprise і IoT Core [25].

IoT Core це урізана версія. Ви не одержуєте повний досвід Windows Shell; замість цього ОС може запускати тільки один додаток універсальної програми Windows (UWP) і фонові процеси. Однак IoT Core буде працювати на процесорах ARM. Ви б обрали IOT Core для запуску простих програм, які можуть не вимагати стільки безпосередньої взаємодії з користувачем. Наприклад, термостат Glas використовує IoT Core. А завдяки сумісності з ARM Ви можете запускати IoT Core на простих платах, таких як Raspberry Pi.

Ця особливість робить IoT Core відмінним вибором для швидких прототипів для виробників або одноразових проектів для любителів. Hackster, співтовариство розробників апаратного і програмного забезпечення, містить чимало унікальних прикладів IoT Core, в тому числі двері з розпізнаванням домашніх тварин, двері з розпізнаванням осіб, інформаційну панель smarthome і чарівне дзеркало. Це все проекти, які Ви могли б побудувати самостійно, якщо у Вас є необхідні навички. Microsoft навіть продемонструвала робота на базі Raspberry Pi, який використовував Windows IoT і взаємодіяв з голограмами. Він надає необхідні ресурси, тому Ви можете завантажити IoT Core для особистого використання з безкоштовною ліцензією.

Крім того, IoT Core на Raspberry Pi або Minnowboard може бути з'єднаний з датчиками і механізмами, такими як камери, PIR-датчики, сервоприводи і температурні датчики для розширеного використання. Це, в свою чергу, дозволяє Windows 10 передавати дані, зібрані цими датчиками, що є основною передумовою Інтернету речей.

Віддалене виконання коду можливо на пристроях Windows 10 IoT Core за допомогою SirepRAT, утиліти, розробленої дослідником безпеки Дором Азурі. Інструмент загальнодоступний і використовує службу тестування Sirep, яка використовує протокол зв'язку з тим же ім'ям. Оскільки він поставляється з можливостями віддаленого адміністрування, SirepRAT можна використовувати для відправки команд цільової мети Windows IoT Core [26].

Протокол Sirep / WPCon надає зловмисникам інтерфейс віддалених команд, який включає можливості RAT, такі як отримання / розміщення довільних файлів в довільних місцях і отримання системної інформації

Дослідник надає технічні деталі в офіційному документі, де, за його словами, атака можлива тільки за допомогою бездротової технології Ethernet. Іншими словами, уразливі тільки пристрої, підключені по кабелю. Це гарна новина, тому що більшість користувачів Інтернету речей покладаються на Wi-Fi для підключення своїх гаджетів до Інтернету.

У цьому методі використовується служба тестування Sirep, вбудована і працює на офіційних образах, пропонованих на сайті Microsoft. Цей сервіс є клієнтською частиною установки HLK, яку можна створити для виконання тестів драйверів/обладнання на пристрої IoT. Він обслуговує протокол Sirep/WPCon/TShell.

Протокол Sirep/WPCon надає зловмисникам інтерфейс віддалених команд, який включає можливості RAT, такі як отримання/розміщення довільних файлів в довільних місцях і отримання системної інформації.

Windows Hardware Lab Kit11 (Windows HLK) - це тестова середовище, що використовується для тестування апаратних пристроїв для Windows 10 і Windows Server 2006. Вона складається з сервера і клієнтського програмного забезпечення: сервер називається контролером HLK, а клієнт - це встановлене програмне забезпечення. на цільовому тестовому пристрої. Постачальники, які прагнуть офіційно поєднати своє обладнання і драйвери з цими версіями Windows, повинні пройти кваліфікацію через Програму сумісності обладнання Windows. Ця програма вимагає, щоб продукт пройшов набір тестів, складених Microsoft. Проходження цих тестів гарантує, що продукт відповідає вимогам Microsoft.

Фактично, HLK є наступником HCK12 (Hardware Certification Kit) і грає точно таку ж роль. Єдина відмінність - це список цільових версій Windows. Хоча HLK призначений для Windows 10 і Windows Server 2006, HCK призначений для наступних попередніх версій: Windows, Windows 8, Windows Server 2008 R2, Windows Server 2012.

Контролер HLK запускає серверне програмне забезпечення під назвою HLK Studio, яке надає графічний інтерфейс для управління тестовими пристроями, створення тестових сценаріїв (списків відтворення) і запуску реальних тестов.HLK on Windows IoT

Пристрій IoT грає роль тестової системи в описаній вище тестової установки HLK. Він приймає тестові завдання від контролера HLK і відправляє назад результати. Він також обслуговує спеціальні ping-запити (ping-запити для конкретних служб, а не ICMP) і рекламує себе за допомогою широкомовних пакетів

UDP. Всі перераховані вище функції реалізовані в одній DLL з використанням 3 портів TCP, які дозволені за умовчанням в брандмауері Windows пристрої.

```
reg query
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Defaults\FirewallPolicy\Fi
rewallRules | findstr -i sirep
    Sirep-Server-Service    REG_SZ
v2.28|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=29817|App=%systemroot%\system32\svcho
st.exe|Name=Sirep Server (Service)|Desc=Sirep Server (Service)|EmbedCtxt=Sirep Server|
    Sirep-Server-Ping    REG_SZ
v2.28|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=29819|App=%systemroot%\System32\svcho
st.exe|Name=Sirep Server (Ping)|Desc=Sirep Server (Ping)|EmbedCtxt=Sirep Server|
    Sirep-Server-Protocol2    REG_SZ
v2.28|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=29820|App=%systemroot%\System32\svcho
st.exe|Name=Sirep Server (Protocol 2)|Desc=Sirep Server (Protocol 2)|EmbedCtxt=Sirep Server|
```

Рис. 3.1. Основна Dll служби: testsirepsvc.dll

Шлях до образу служби Sirep веде до цієї DLL в C:\Windows\System32\testsirepsvc.dll. У ньому реалізовані основні сервісні функції, включаючи зв'язок і виконання завдань, відправлених з контролера HLK.

Сервер HLK діє як клієнт Sirep цієї служби Windows IoT. Було розглянуто логіку і реалізацію основних функцій, які пропонує цей сервіс: підпис мережі, оголошення пристрої.

У сервісу є дуже смілива мережева підпис, яка фактично стала принадою для початку копання, що призвело до цієї дослідницької роботи.

За замовчуванням ядро Windows IoT періодично відправляє безкоштовні UDP-пакети для реклами пристрої в локальній мережі. Це простий широкомовний пакет з унікальним ідентифікатором пристрою: 12-символьного шестнадцатеричной рядком (Unicode). Він вирушає на широкомовна адресу відповідні підмережі і інтерфейси. Фільтрація відповідних інтерфейсів виконується аналогічно тому, як фільтруються командні з'єднання, як описано нижче в цьому документі.

У свою чергу, контролер HLK очікує цих рекламних пакетів і становить список ідентифікаторів пристроїв у межах досяжності. Ці виявлені пристрої будуть доступні користувачеві на вибір в додатку HLK studio, яке працює на тестовому

сервері HLK. Відстеження джерела цих пакетів розкриває особистість відправника: службу перевірки Sirep [26].

Зокрема, він відправляється з виділеного потоку, що виконує ControllerWSA :: NameBroadcasterThreadProc. В кінцевому підсумку це викликає ControllerWSA :: SendBroadcastForDevice, який використовує ws2_32! Sendto наступним чином

```
WS2_32!sendto:
7730b260 e92d4ff0 push        {r4-r11,lr}
0: kd> db r1 L?0x74
0324f7e0  00 c0 ff ee 42 00 38 00-32 00 37 00 45 00 42 00  ....B.8.2.7.E.B.
0324f7f0  33 00 44 00 42 00 44 00-39 00 36 00 00 00 00 00  3.D.B.D.9.6.....
0324f800  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0324f810  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0324f820  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0324f830  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0324f840  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0324f850  00 00 00 00                                      ....
0: kd> k
 # Child-SP RetAddr  Call Site
00 0324f7c0 711b7cb8 WS2_32!sendto
01 0324f7c0 711b7e3c testsirepsvc!ControllerWSA::SendBroadcastForDevice+0xd0
02 0324f880 711b7abc testsirepsvc!ControllerWSA::NameBroadcasterThread+0xb0
03 0324fad8 77ae97e2 testsirepsvc!ControllerWSA::NameBroadcasterThreadProc+0xc
04 0324fae0 00000000 ntdll!RtlUserThreadStart+0x22
```

Рис. 3.2. ControllerWSA :: SendBroadcastForDevice використовує ws2_32! Sendto

Windows IoT Core в своїй конфігурації за замовчуванням дозволяє кілька вхідних підключень через брандмауер. 3 з них використовуються цим сервісом. Служба постійно прослуховує ці порти, кожен для своєї мети.

Як згадувалося вище, опису різних портів неоднозначні через еволюції протоколу. У наступному списку наведені обидві версії імен: спочатку ім'я, орієнтоване на IoT, потім ім'я, орієнтоване на Windows Phone:

1. 29820: Sirep-Server-Protocol2/WPConProtocol2. Використовується для командної взаємодії, використовуваного в цьому документі.

2. 29819: Sirep-Server-Ping/WPConTCPPing/WPPingSirep. Використовується для простої луна-служби, описаної вище.

3. 29817: Sirep-Server- Service/WPCon. Його унікальне призначення не досліджувалося і залишено для майбутніх досліджень (після того, як цілі були досягнуті з використанням сервісів на порте WPConProtocol2).

Авторизація вхідного з'єднання. Служба прослуховує порт Sirep-Server-Protocol2 і приймає команди, відправлені на нього в унікальній двійковій структурі. Результати відправляються назад ініціатору команди в простій двійковій структурі.

Наведемо логіку, яка визначає, чи дозволено новому з'єднанню відправляти команди пристрою. Ця логіка реалізована у функції ControllerWSA :: IsConnectionAllowed.

Фільтрація не базується ні на якій формі аутентифікації або навіть ідентифікації. По суті, будь-який віддалений клієнт може відправляти команди пристрою з єдиною вимогою, щоб відповідний мережевий інтерфейс пристрою був підключений за допомогою кабелю Ethernet (не по бездротовій мережі). Перевірка заснована виключно на деталях локального сокета, який отримав нове TCP-з'єднання. Зокрема, функція виконує свої перевірки структури SOCKADDR_IN, яка повертається з виклику API для getsockname:

```
; Attributes: bp-based frame

; int __fastcall ControllerWSA::IsConnectionAllowed(#20 *__hidden this, unsigned int)
public: int __cdecl ControllerWSA::IsConnectionAllowed(unsigned int)

var_28= -0x28
var_20= -0x20
var_1C= -0x1C

PUSH.W          {R4,R5,R11,LR}
ADD.W           R11, SP, #8
BL              __security_push_cookie
SUB             SP, SP, #0x1C
MOV             R3, R1
MOV             R5, R0  ; The ControllerWSA object
MOV             R0, R3
LDR             R3, =__imp_getsockname
MOVS            R2, #0x10
STR             R2, [SP,#0x28+var_28]
LDR             R3, [R3]
MOV             R2, SP
ADD             R1, SP, #0x28+var_20
MOVS            R4, #0
BLX             R3
CBZ             R0, loc_100094C8
```

```
loc_100094C8
ADD             R1, SP, #0x28+var_20
ADD.W           R0, R5, #0x2C ; this
BL              NetworkInterfaces::IsInterestingAddress(sockaddr_in *) ; R0 - socket address
CBNZ            R0, loc_100094E8 ; SUCCESS = r0 non-zero
```

Рис. 3.2. Перевірка структури SOCKADDR_IN

3.2 Використання SirepRAT у Windows IoT core на Raspberry Pi 3

Мета цієї праткичної частини була у тому, щоб продемонструвати наскільки легко можна отримати доступ до приладу IoT на базі ОС однііє з передових IT компаній – Microsoft.

Для підтвердження наскільки популярна ОС Windows IoT на ринку Інтернету речей в цілому було проведено опитування Робочою групою Eclipse IoT, AGILE IoT, IEEE і Open Mobile Alliance. Вищезазначені організації виступили одним із спонсорів онлайн-опитування, щоб краще зрозуміти, як розробники створюють рішення IoT. Це опитування проводилося щорічно 3 роки тому, і останнє видання 2019 року дозволило нам зробити наступні відповідні висновки:

• Windows займає друге місце (22,9%) в розробці рішень Інтернету речей (після Linux - 71,8%).

• Одним з основних секторів Інтернету речей, в якому використовується Windows, є шлюзи Інтернету речей.

• Більшість розроблюваних рішень IoT побудована на архітектурі ARM. Це, ймовірно, виправдовує нову підтримку ARM з боку Windows IoT. Ми припускаємо, що це може привести до більш широкого використання версії Windows IoT Core іншими, враховуючи той факт, що IoT Core - єдина версія Windows IoT, що підтримує ARM.

Рис.3.3. Тонкий клієнт Raspberri Pi 3 B

Підтримувані плати. Microsoft офіційно пропонує використовувати одну з наступних плат в якості пристроїв для розробки: AAEON Up Squared, DragonBoard 410c, MinnowBoard Turbot, Raspberry Pi 2, Raspberry Pi 3B. Microsoft надає найбільш повну документацію по цих пристроях. Для виконання цієї роботи було використано тонкий клієнт Raspberry Pi 3B.

Таблиця 3.1.

Характеристики тонкого клієнта Raspberri Pi 3 B

процесор:	SoC Broadcom серії BCM2837B0 (чотирьохядерний ARM Cortex-A53 1,4 ГГц з 64-бітної архітектурою)
Об'єм оперативної пам'яті:	1 Гб
Мережеві інтерфейси:	двохдіапазонний Wi-Fi (2,4 ГГц і 5 ГГц) 802.11ac, Bluetooth 4.1 (Classic і Low Energy); порт Ethernet
USB порти:	4 × USB 2.0
Відеовихід:	HDMI
Роз'єми плати:	DSI-коннектор для LCD дисплея; CSI - інтерфейс для камери; аудіовихід - гніздо 3,5 мм з підтримкою композитного відеовиводу; слот microSD (підтримка карт пам'яті до 64 Гб)
Роз'єм живлення:	micro USB
Напруга живлення:	5 В
Максимальний споживаний струм:	3 А

Було встановлено саму ОС на MicroSD карту пам’яті з допомогую офіційного інсталятор Windows IoT Dashboard.

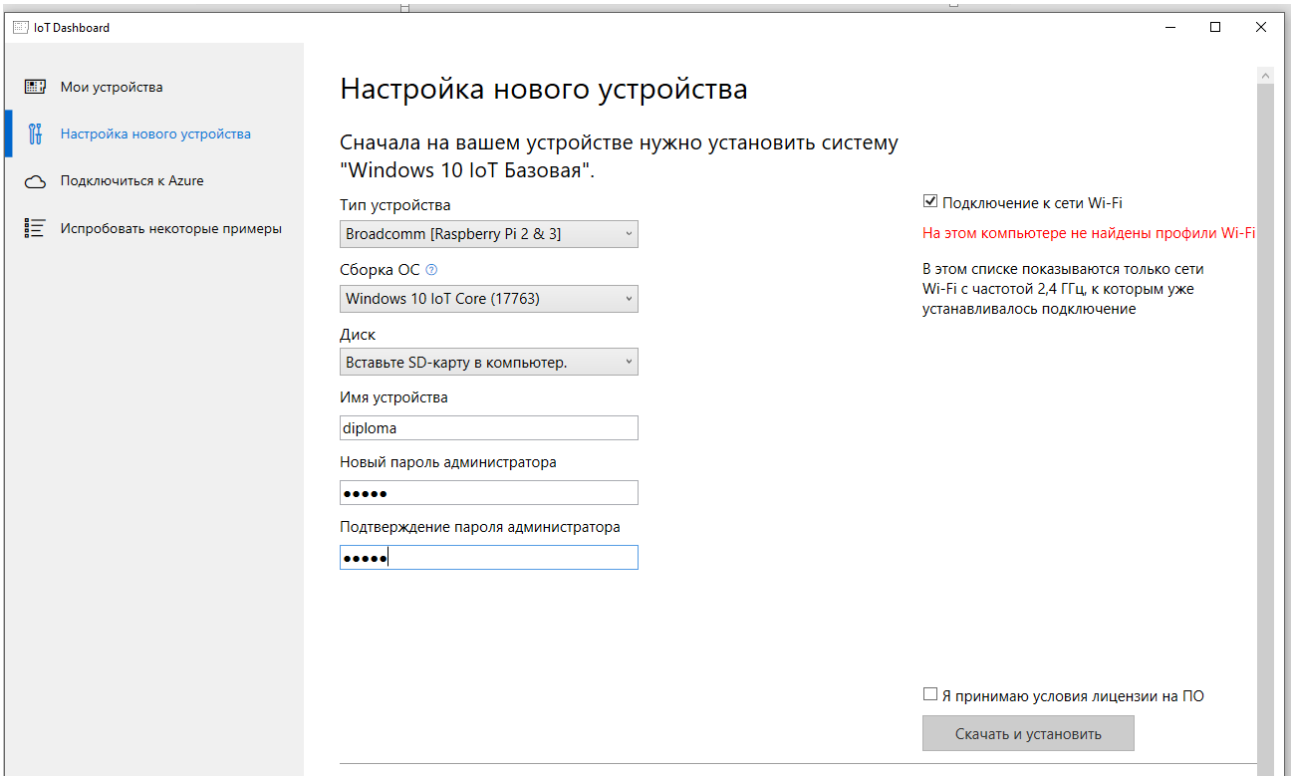

Рис. 3.4. Процесс встановлення Windows IoT Core

Після цього було запущено станцію та ознайомлено з її веб інтерфейсом.

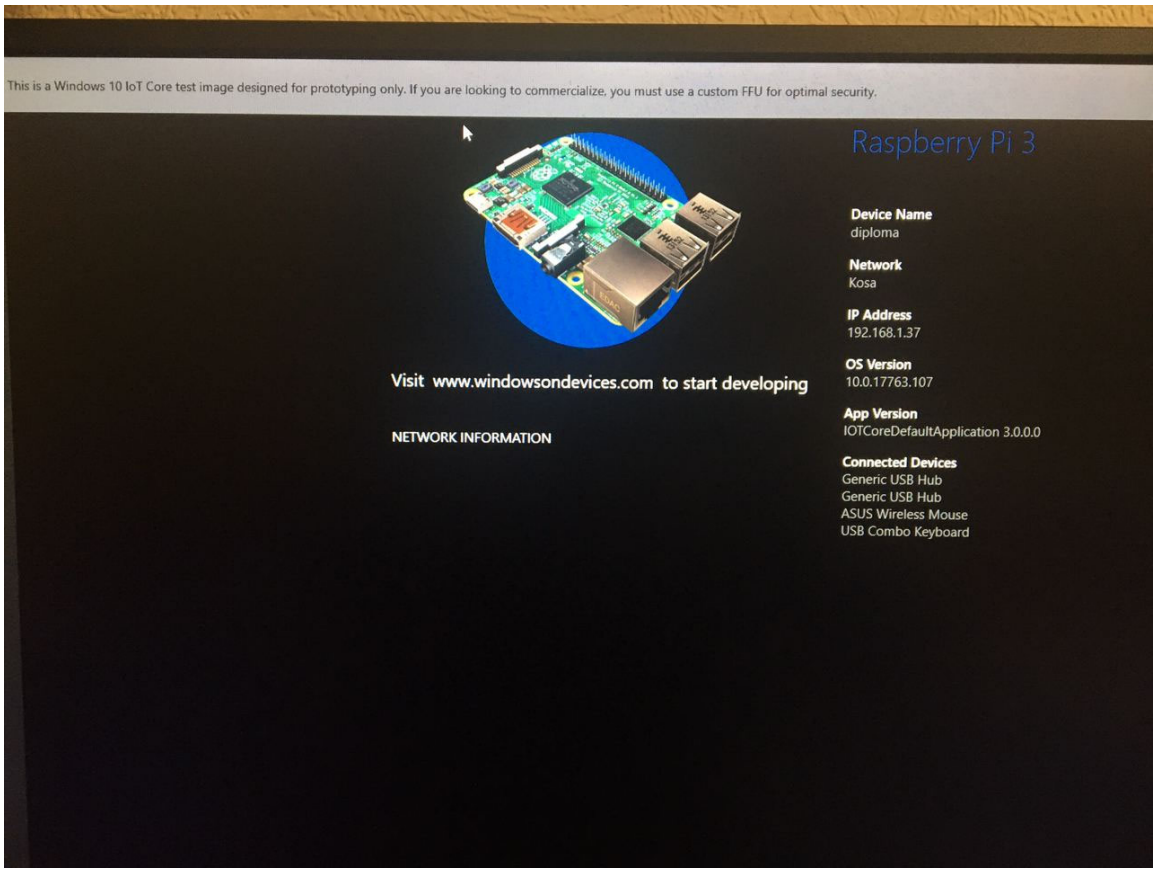

Рис. 3.5. GUI Windows IoT Core

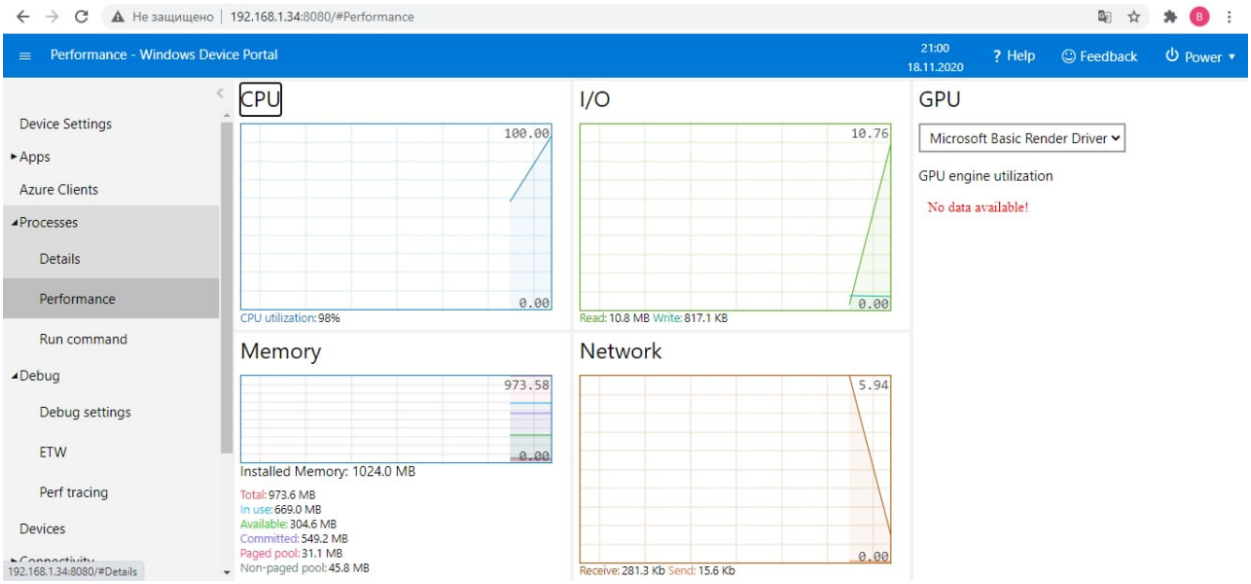

Рис. 3.6. Демонстрація робочої станції налаштованої для тестування

Як тільки було переконано що станція працює стабільно було перейдено до експлойту SirepRAT. Спершу було встановлено Python версії 2.7 та pip для нього. Для використання скрипту на версії 3 необхідно його адептувати та переписувати. Після цього було встановлено файл requirments.txt у середовище Python і експлойт готов до використання.

```
PS E:\SirepRAT-master> python -m pip install -r requirements.txt
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer mainta
ined. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pi
p.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting enum34>=1.1.10
  Downloading enum34-1.1.10-py2-none-any.whl (11 kB)
Collecting hexdump>=3.3
  Using cached hexdump-3.3.zip (12 kB)
Using legacy 'setup.py install' for hexdump, since package 'wheel' is not installed.
Installing collected packages: enum34, hexdump
    Running setup.py install for hexdump ... done
Successfully installed enum34-1.1.10 hexdump-3.3
```

Рис.3.7. Підготовка експлойту SirepRat до використання

Було опробувано стандартні команди запропоновані розробником SirepRAT нижче будуть скріншоти з командної строки.

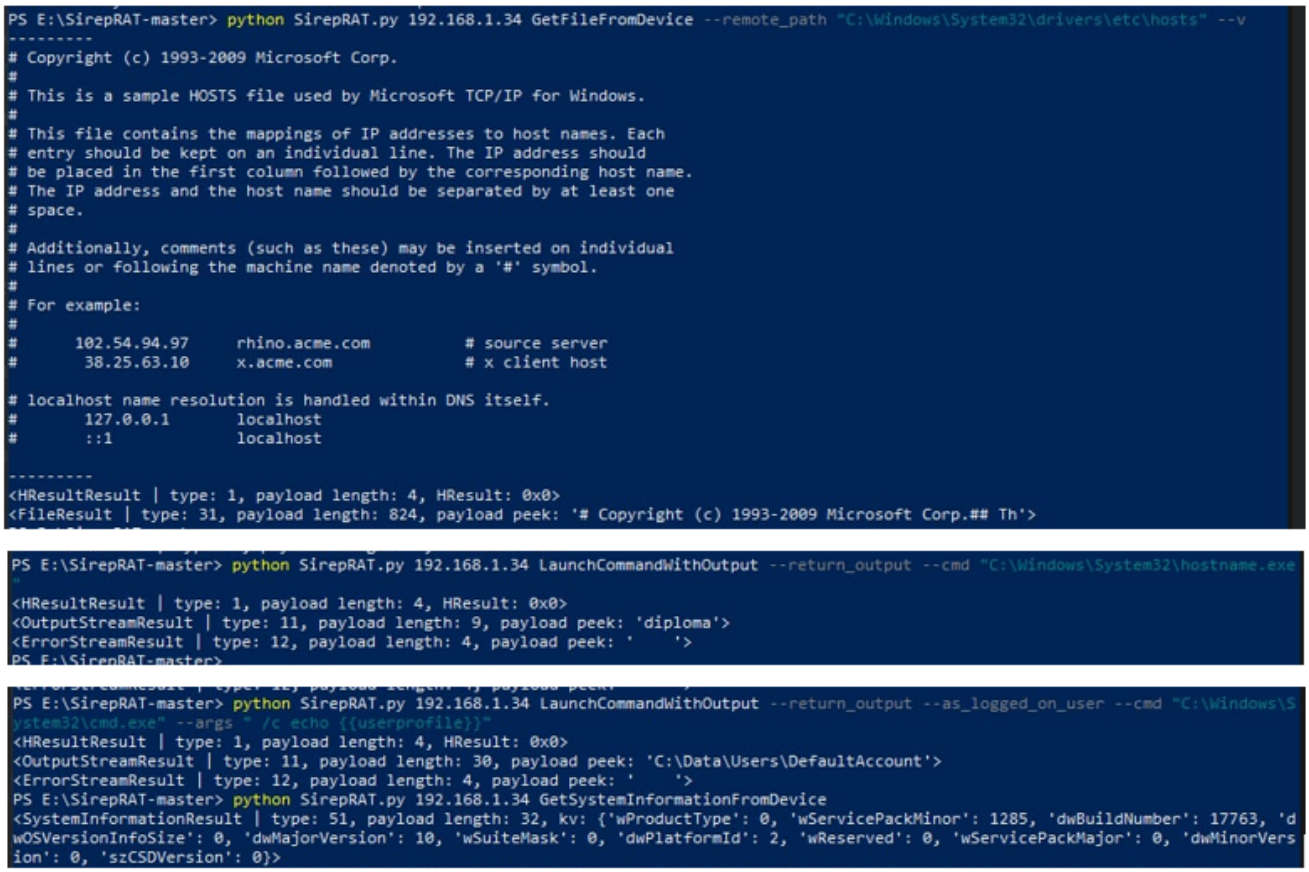

Рис. 3.8. Використання команд експлойту SirepRat

Таким чином було отримано повний доступ до ОС на станції без авторизації. На станції був встановлений пароль та любий вхід (напряму, веб-браузер) запрашував данні користувача. Використовючи даний експлойт можна завантажувати і викачувати дані з станції, запускати будь-яку команду і отримувати відповідь від станції без авторизації.

3.3 Розробка рекомендацій з захисту пристроїв мережі IoT

Виходячи з інформації що було зібрано та проаналізовано раніше в цій роботі, логічно дійшов до наступних кроків що забеспечать безпеку ваших Розумних Речей та мережі в котрій вони використовуються.

Безпеку мережі треба закаладати ще на етапі проектування. З боку споживача продуктів данного сегменту треба чітко розуміти який функціонал буде використовуватись та аналізувати наявні проблеми та вектори атак на ті чи інші

техології передачи інформації та ПЗ яке використовується. З іншого боку розробники товарів сфери IoT повинні враховувати безпеку на початку розробки будь-яких пристроїв для споживачів, підприємств або промислових підприємств бо в наш час багато компаній хочуть виграти технологічні перегони не зважаючи на явні недоліки та дири у своїх продуктах. Включення безпеки за замовчуванням має вирішальне значення, так само як і наявність самих останніх операційних систем і використання безпечного обладнання. Пристрої Інтернету речей, яким необхідно підключатися безпосередньо до Інтернету, повинні бути сегментовані в їх власні мережі і мати обмежений доступ до корпоративної мережі. Сегменти мережі повинні відстежувати аномальну активність, щоб можна було вжити заходів у разі виявлення проблеми. Шлюзи безпеки виступаючи в якості посередника між пристроями IoT і мережею, мають більшу обчислювальну потужність, пам'яттю і можливостями, ніж самі пристрої IoT. Реалізація додаткових заходів безпеки. Користувачам рекомендується включити брандмауери і використовувати протокол безпеки Wi-Fi Protected Access II (WPA2) для додаткового захисту. Рішення, що використовують веб-репутацію і контроль додатків, також забезпечують кращу видимість в мережі. Забезпечення безпеки в режимі реального часу з централізованої системи, як правило, не є гарною ідеєю, враховуючи, що пристрої будуть час від часу недоступні. Він повинен бути ізольованим, розподіленим і мати відмовостійкість.

Другим кроком при проектуванні мережі з використянням IP є стандартизація технологій та протоколів передачи інформації. Більша кількість різноманітних приладів та способів їх спілкування між одним породжує більшу кількість вразливих ланок, а як відомо що загальна безпека системи залежить від найуразлівішої ланки. Це добре прослідковується у прикладі що був наведеній вишче – потрапляння в межу казино через розумний термометр в акваріумі казино. Додатково рекомендується змінювати стандартні порти протоколів на унікальні для унеможливення скану мережі, особливо коли пристрій напряму спілкується з глобальною мережею в обхід локальної та роутеру. Але стандартизувати треба не тільки протоколи передачи інформації, а й централізоване ПЗ. Велика кількість

компаній на цьому ринку створює під свої унікальні пристрої й унікальне керуче ПЗ контре не буде працювати з програмами чи операційними системами інших розробників. З великої кількості різноматніного програмного забезпеченя випливає інша рекомендація – оновлення цього самого програмного забезпечення. Великий відсоток приладів використовується по принципу – встановив та забув отримуючи з них інформацію. Цей підхід являється в корні неправильним з огляду на те що програмне забезпечення залишається не оновленним та уразливим у продовж довгого часу. Не завжди є можливість оновлювати ПЗ для окремих пристроїв але рекомендується проводити планові оновлення та виїзди до приладів для оновлення якщо прямого доступу до приладу немає.

Моніторинг трафіку в мережі. Активне сканування на предмет аномального поведінки в мережі може допомогти користувачам запобігти будь-яким зловмисні спроби. Автоматичне і ефективне виявлення шкідливих програм також можна використовувати за допомогою сканування в реальному часі, що забезпечується рішеннями безпеки.

Наступна рекомендація стосується стандартни данних користувача що часто йдуть предстановлені в ПЗ приладів. При налаштуваннях пристроїв мережі IoT одним із перших шляхів є заміна стандартного користувача на унікального та заміна пароля на безпечний з дотриманням всіх правил його створення, опираючись на данні відомих та популярних зкомпромітованих паролів. Також необхіднно проводити планові зміни данних для авторизації.

Безпека API. Безпека індикаторів продуктивності додатків (API) важлива для захисту цілісності даних, що відправляються з пристроїв IoT на серверні системи, і забезпечення зв'язку з API тільки авторизованими пристроями, розробниками і додатками. Надійне шифрування критично важливо для захисту зв'язку між пристроями. Дані в стані спокою і при передачі повинні бути захищені за допомогою криптографічних алгоритмів. Це включає використання ключового управління життєвим циклом.PKI і цифрові сертифікати. Інфраструктура відкритих ключів (PKI) і цифрові сертифікати грають критично важливу роль в розробці безпечних пристроїв IoT, забезпечуючи довіру і контроль, необхідні для

поширення та ідентифікації відкритих ключів шифрування, безпечного обміну даними по мережах і перевірки особистості.

При правильному запуску блокчейн може принести велику користь системам Інтернету речей за рахунок зниження витрат і підвищення ефективності. Навіть в цьому випадку проникнення технології в середовища з підтримкою Інтернету речей далеко від оптимального. Наприклад, до 2021 року очікується, що тільки до 10 відсотків регістрів виробничих ланцюжків блоків будуть включати датчики IoT. Більш того, ще треба буде пройти довгий шлях, перш ніж більшість систем IoT стануть досить обчислювально компетентними, щоб справлятися з громіздкими реалізаціями блокчейнов.

Повинно використовуватись загальнодоступні хмарні платформи Інтернету речей, які можуть керувати віддаленим пристроєм за допомогою реплік пристрою. Ці копії систем пристроїв (включаючи ОС, базу даних, додатки і т. Д.), які іноді називають двійниками, дозволяють централізовано керувати безліччю копій пристроїв і відстежувати конфігурації. Основна конфігурація міститься в хмарі і використовується для відстеження змін та управління змінами.

Уніфікуючи основними засобами захисту платформи IoT залишается:

- засоби ідентифікації та доступу (IAM);
- засоби шифрування даних - як в спокої, так і при передачі по каналах зв'язку; (Захищені протоколи HTTPS, SSH і ін.);
- кошти міжмережевого екранування;
- кошти резервного копіювання і відновлення.
- Введеня блокчейну як систему безпечного і конфіденційного обміну повідомленнями про транзакції, децентралізація комунікацій
- Використання хмарних платформ Інтернету речей для ідентифікації, проходння аутентифікацію і з'єднання через хмарні сервери, на яких виконуються обробка і зберігання даних

Крім того, для підвищення ефективності використання процесів забезпечення і управління безпекою будуть потрібні засоби захисту і автоматизації наступних функцій:

- виявлення та інвентаризація активів;
- захищений віддалений доступ;
- запис сесій віддаленого доступу;
- туннелирование протоколів;
- захищена передача файлів;
- моніторинг пристроїв;
- управління оновленнями безпеки і оновленнями;
- управління антивірусним захистом;
- пасивний моніторинг мереж;
- створення звітів для керівництва та наглядових органів;
- сканування вразливостей, оцінка ризиків і ін.

Висновки до розділу 3

Досліджено ОС Windows IoT Core та експлойт що використовує вразливість у цій системі – SirepRAT.

Проаналізовано експлойт SirepRAT та примінено на практиці ці знання для отримання доступу на станцію Raspberry Pi 3B під керуванням ОС Windows IoT Core.

Досліджено сутність роботи та обміну данними між сервиісам ОС Windows IoT Core через котрі виконується віддалене керувіання за допомогою експлойту SirepRAT

Визначено що эксплойт SirepRAT працює на будь-якому Windows IoT Core-пристрої з офіційним образо Microsoft, тобто більшість приладів працючих на базі тонких клієнтів під керуванням данного програмного забезпечення є вразливими.

Продимонстровано що ніякої авторизації на самому пристрої для атаки не буде потрібно.

Перераховано та надано рекомендацій щодо захисту пристроїв, які здійснюють функціонування в мережах IoT.

ВИСНОВКИ

В магістерській роботі було отримано такі наукові та науково-практичні результати:

Проаналізовано основні терміни в IoT. Архітектура Інтернет речей складається з чотирьох основних рівнів, таких як: рівень датчиків, мережевого рівня, рівня обробки даних та прикладного рівня. Розглянуто еталонну модель IoT, її основні та додаткові рівні, а також переваги та недоліки IoT мереж.

Досліджено основні технології та протоколи передачі даних на довгі дистанції, які входять до складу мереж LPWAN: LoRaWAN, SigFox, NBIoT,Weightless-P. Здійснено порівняльний аналіз основних характеристик протоколів та технологій передачі даних на довгі відстані таких, як метод модуляції, діапазон частот, швидкість передачі даних, смуга частот, швидкість передачі даних, максимальний час автономної роботи пристроїв, частоти на яких працюють дані технології, рівень безпеки, дальність переді даних.

Визначені основні технології та протоколи передачі даних на короткі відстані, які входять до складу мереж WPAN та WLAN: Z-Wave, RFID, Bluetooth Low Energy та Wi-Fi HaLow. Здійснено порівняльний аналіз основних характеристик протоколів та технологій передачі даних на короткі відстані таких, як смуга частот, щвидкість передачі даних, радіус дії, пропускна здатність в каналі, вид модуляції, топологія, безпека.

Розглянуто топологію, яка використовується для передачі повідомлень в IoT. Здійснено порівняльний аналіз протоколів передачі повідомлень за такими показниками: протокол транспортного рівня, який використовується для передачі повідомлення до користувача IoT, призначення та особливості протоколу, а також операції, які він виконує в мережі IoT.

Долсідженно взразливості пристроїв мережі Інтренту Речей ,основні вектори атак та статистику використяних уразливостей та експлойтів, а також основні положення безпеки пристроїв мережі IoT

Описано засоби забезпечення безпеки мережі IoT, принцип роботи блокчейну та хмарних платформ для забезпечення безпеки Інтернету Речей, а також переваги у вирішенні питянь безпеки за допомогую блокчейно замість хмарних технологій.

Надано рекомендацій для захисту пристроїв мережі IoT

ПЕРЕЛІК ПОСИЛАНЬ

1. Alasdair Gilchrist. IoT Security Issues / Alasdair Gilchrist. –Berlin : De|G Press, 2017. – P. 149.

2. Drew Van Duren. Practical Internet of Things Security / Drew Van Duren, Brian Russell. – Birmingham : Packt Publishing, 2016. – P. 251.

3. С. Грінгард. Интернет вещей: Будущее уже здесь / С. Грінгард. – Москва : Альпина Паблишер, 2016. – P. 120.

4. Rapyder. [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0167739X1630694X

5. П. Лі. Архітектура интернета вещей. / П. Лі. – Москва : ДМК Пресс, 2018. – P. 410.

6. Aditya Gupta. A Practical Guide to Hacking the Internet of Things / Aditya Gupta. – Walnat : Apress, 2016. – P. 286

7. Rapyder. [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0167739X1630694X

8. Bureau of Labor Statistics. [Електронний ресурс] – Режим доступу: http://www.bls.gov/tus/

9. Ali Dorri. Blockchain for Cyberphysical Systems / Ali Dorri, Salil Kanhere, Raja Jurdak. – London : Artech House, 2020. – P. 248.

10. Mika Ylianttila. IoT Security: Advances in Authentication / Mika Ylianttila, Madhusanka Liyanage, An Braeken, Pardeep Kumar. – Hoboken : Wiley, 2020. – P. 85

11. Хабр. [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/unet/blog/410849/

12. Sravani Bhattacharjee. Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries / Sravani Bhattacharjee. – Birmingham : Packt Publishing, 2018. – P. 176

13. Security Magazine. [Електронний ресурс] – Режим доступу: https://www.securitymagazine.com/articles/93771-enterprise-internet-of-things-iot-cybersecurity

14. Sudhir Kumar Sharma. IoT Security Paradigms and Applications / Sudhir Kumar Sharma, Bharat Bhushan, Narayan C. Debnath. – Boca Raton : CRC Press, 2020. – P. 85.

15. Sudhir Kumar Sharma. Security and Trust Issues in Internet of Things / Sudhir Kumar Sharma, Bharat Bhushan. – Boca Raton : CRC Press, 2020. – P. 211.

16. Bureau of Labor Statistics. [Електронний ресурс] – Режим доступу: http://www.bls.gov/tus/

17. Aaron Guzman. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices / Aaron Guzman. – Birmingham : Packt Publishing, 2017. – P. 401

18. Ali Dorri. Blockchain for Cyberphysical Systems / Ali Dorri, Salil Kanhere, Raja Jurdak. – London : Artech House, 2020. – P. 248.

19. Pethuru Raj. Blockchain Technology and Applications / Pethuru Raj, Kavita Saini, Chellammal Surianarayanan. – Denmark : River Publishers, 2020. – P. 79.

20. М. Свон. Блокчейн: Схема новой экономики / М. Свон. – Москва : Олимп-Бизнес, 2017. – P. 83.

21. Ravi Sankar Kumar Dasari. SAP Cloud Platform: Tools and Services / Ravi Sankar Kumar Dasari, Kunal Kotak, Srinivas Mudapalli, Harikrishnadhar Sonnenahalli. – Bonn : SAP Press, 2018. – P. 678.

22. ResearchGate. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/figure/IoT-security-solutions_fig1_323912995

23. Trend Micro. [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/blockchain-the-missing-link-between-security-and-the-iot

24. Center for Internet Security. [Електронний ресурс] – Режим доступу: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-internet-of-things-iot/

25. Microsoft Azure. [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/ru-ru/overview/iot/security/

26. Github. [Електронний ресурс] – Режим доступу: https://github.com/SafeBreach-Labs/SirepRAT