МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2020 р.

На правах рукопису
УДК

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»

Тема: Система захисту інформації в IoT

Автор: Касьянов П. П.
Науковий керівник: д.т.н., проф. Толюпа С. В.
Нормоконтролер: д.т.н., проф. Толюпа С. В.

Київ 2020

ВСТУП

Актуальність роботи полягає у тому, що розвиток концепції Інтернету речей значно розширює можливості зі збору, обробки та поширення інформації. Інтернет речей відкриває потенціал для підвищення комфорту життя людини та збільшення ефективності у промисловому виробництві.

Незважаючи на перспективність технології, багато проблем ще повинні бути вирішенні для глобального впровадження об’єктів Інтернету речей у всі сфери людської діяльності, зокрема безпека і захист критичної інформації.

Мета дослідження: формування рекомендацій щодо використання засобів захисту об’єктів Інтернету речей на основі аналізу загроз функціонування об’єктів Інтернету речей.

Об’єктом дослідження є процес захисту об’єктів Інтернету речей від кіберзагроз.

Предметом дослідження є механізми захисту об’єктів Інтернету речей.

Дослідження проводиться методом аналізу загроз, інцидентів, атак та вразливостей об’єктів Інтернету речей.

Для досягнення поставленої мети було визначено наступні завдання:

- ознайомлення з концепцією Інтернету речей;
- дослідження стандартів, що регулюють об’єкти Інтернету речей;
- визначення основних принципів роботи Інтернет речей;
- визначення напрямків практичного застосування Інтернету речей;
- дослідження інцидентів та атак на об’єкти Інтернету речей;
- аналіз загроз інформаційної безпеки та вразливостей Інтернет речей;
- визначення базових компонентів безпеки об’єктів Інтернету речей;
- вироблення рекомендацій щодо забезпечення інформаційної безпеки об’єктів Інтернету речей.

Результати даного дослідження можуть бути використані для поглиблення знань у галузі Інтернету речей, зокрема з питань безпеки, включаючи вразливості, загрози, методи і способи захисту інформації. Оскільки Інтернет речей – це нове явище у технологічному світі, інформації про дану технологію дуже багато, але вона недостатньо структурована.

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

- IV Міжнародна науково-практична конференція «Прикладні системи та технології в інформаційному суспільстві» (AISTIS) (Київ, 2020), тема доповіді «Застосування програмного продукту Splunk machine Learning toolkit в системі управління інформаційною безпекою».
- Міжнародна наукова конференція «Динаміка сучасної науки – 2020» (Софія, 2020) тема доповіді: «Засоби захисту від BadUSB»

РОЗДІЛ 1. КОНЦЕПЦІЯ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Поняття Інтернету речей

Світ цілком і повністю поглинули інформаційні технології. Використання автоматизованих процесів стало буденністю для сучасного члена соціуму. Стрімке прагнення людини підвищити власний рівень комфорту продукує нові варіанти рішень простих та не зовсім проблем. Зв'язок із Всесвітньою мережею Інтернет відкриває нові можливості для електронної техніки. Автоматизація стала причиною переходу до нового етапу обробки даних, який дозволяє зневажати факт присутності людини в процесі перетворення інформації в дані.

Таким чином, сформувалося поняття Internet of Everything (Інтернет всього або Всеосяжний Інтернет), в склад якого входить Інтернет речей та традиційні пристрої підключені до мережі Інтернет (комп’ютери, смартфони, планшети і т.д.). Дане явище мало високий рівень впливу на значення та цінність мережевих підключень та з’єднань завдяки здатності не лише опрацьовувати інформацію, а й трансформувати її в певні дії. IoE відкриває нові можливості, розширює функціонал приладів і створює чудові умови для розвитку та існування людини, компанії, міста і навіть країни. Для всього цього необхідне злагоджене функціонування чотирьох компонентів: люди, процеси, дані, фізичні прилади [1]. Саме фізичні прилади стали основою для іншої, більш вужчої концепції формування сфери Інтернету речей.

Основою Інтернету речей вважають мережу фізичних об’єктів створених за технологією, яка дозволяє цим об’єктам вимірювати параметри власного стану або стану навколишнього середовища, оброблювати, зберігати та передавати цю інформацію.

Перше завдання IoT – це віддалений моніторинг і управління набором взаємозалежних мережевих пристроїв, кожен з яких може взаємодіяти з об’єктами інфраструктури та фізичного середовища.

Друге завдання – використання даних, одержуваних з кінцевих вузлів («розумних пристроїв» з можливістю підключення і зондування), для інтелектуального аналізу з метою виявлення тенденцій і взаємозв’язків, які можуть генерувати корисну інформацію для забезпечення додаткової вигоди, наприклад, заощадження ресурсів.

Особливу роль в IoT відіграють засоби вимірювання, що забезпечують перетворення відомостей про зовнішнє середовище в зрозумілі для машин дані і, таким чином, наповнюють обчислювальне середовище значущою інформацією. Використовується широкий клас засобів вимірювання, від елементарних датчиків (температури, тиску, вологи, освітленості), приладів обліку споживання (інтелектуальні лічильники) до складних інтегрованих вимірювальних систем. В рамках концепції Інтернету речей принциповим є об’єднання засобів вимірювання і мережі (таких, як бездротові сенсорні мережі, вимірювальні комплекси), за рахунок чого можлива побудова систем M2M (міжмашинної взаємодії).

Звідси витікає альтернативне визначення Інтернету речей як взаємозв’язку однозначно ідентифікованих вбудованих обчислювальних пристроїв в рамках існуючої інфраструктури Інтернету [3].

1.2 Історія виникнення Інтернету речей

Першим у світі пристроєм, який сміливо можна віднести до категорії Інтернету речей став вендінговий апарат з продажу Coca-Cola. В 1982 році, він був встановлений в Університеті Карнегі-Меллон. Апарат мав змогу передавати дані про залишок пляшок в відповідній ємності та про свій стан в цілому.

1990 роки стали часом зародження ідеї мережі, яка могла б забезпечити міжмашинну взаємодію. Одним із головних ідейних лідерів став керівник дослідницьких робіт в компанії Xerox PARC – Марк Вейзер. Він запропонував концепцію масштабного комп'ютерингу. В основі концепції полягало масове введення комп'ютерів та організацію зв'язків між ними, завдяки чому, машини мали б змогу самостійно вирішувати буденні завдання користувачів.

Вперше, ввести в масове використання Інтернет речей спробували такі корпорації як Microsoft та Novell. В 1993 році Microsoft запустила платформу «at Work», на меті якої було встановлення мережі для офісної техніки. Платформа містила в собі спеціальну операційну систему та протокол передачі даних. Головна ціль «at Work» полягала в створенні мережі та передачі функцій керування та контролю за нею комп'ютерам, що працювали під ОС Windows. Не дивлячись на всі можливі переваги такого рішення, платформа не здобула успіх та через деякий час була закрита. В 1994 році, схожий проект представила компанія Novell. Платформа «NEST» (Novell Embedded Systems Technology) давала змогу різним пристроям мережі підключатись до мережевої операційної системи NetWare та використовувати її протокол IPX для взаємодії з іншими учасниками мережі. Однак, «NEST» йшла стопами платформи «at Work» і досить швидко припинила своє існування.

1999 рік став проривним в сфері Інтернету речей. На презентації для керівництва «Procter & Gamble», Кевін Ештон, засновник дослідницької групи Auto-ID при Массачусетському технологічному інституті, провів доповідь про те, яким чином загальне впровадження радіочастотних міток RFID змінює систему керування логістичними ланцюгами в корпорації, а також сформулював загальну концепцію та термін IoT [2].

Паралельно цим подіям вчений Білл Джой, на Міжнародному форумі з економіки в Давосі, під час свого виступу запропонував ідею «Шести вебів». Ця ідея описувала шість типів інтернету майбутнього, в тому числі Інтернет речей. Білл спрогнозував появу речей які належали до створеної ним типології «Device-to-Device». Серед таких речей були: бездротові мобільні інтернет-мережі,

голосові помічники на основі штучного інтелекту, та комунікації між пристроями.

Період бурхливого розвитку Інтернету речей знайшов місце 2000-х роках. 90-ті були етапом формування теорії – створення концепцій, ідей, обговорень, тоді коли в 2000-х почався період втілення цих ідей в життя. Відбувся перехід від теорії до практики.

Масовий запуск різноманітних IoT-проектів призвів до «буму» на ринку товарів компаній, що займалися безпосередньо виготовленням Інтернет-речей. Продукція сфери IoT викликала неабиякий інтерес у покупців. Високий рівень попиту сприяв росту пропозиції. Таким чином було розроблено велику кількість користувацьких пристроїв, що відносилися до сфери IoT – від фітнес-браслетів до розумних дверей. Окрім того, свій початок беруть проекти неймовірних масштабів – розумні міста, виробництво, розумний транспорт, автомобілі під керуванням штучного інтелекту. Важливо відзначити, що вагомий внесок в розвиток IoT зробив активний прогрес в сфері інформаційних технологій, розповсюдження бездротового з’єднання з мережею Інтернет, виведенню на новий рівень швидкісних характеристик Інтернет-зв’язку , виникнення енергоефективних мереж дальнього радіусу дії та інше.

1.3 Нормативно-правова база та стандартизація Інтернету речей

Вперше закон, що безпосередньо пов'язаний з безпекою IoT, був прийнятий в Каліфорнії, в квітні 2018 року. Закон про безпеку IoT-пристроїв SB-327 «Інформаційна безпека: підключені пристрої » зобов’язує розробників розумних систем створювати для них унікальну пару логін/пароль. В 2015 році Європейський Союз сформував директиву з кібербезпеки, яка частково стосувалася IoT. Таким чином, почалась діяльність у сфері безпеки IoT.

Вже в кінці 2018 року Міжнародна організація з питань стандартизації, більш відома як ISO, розробила та опублікувала стандарт ISO/TR 22100–4:2018 Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT security (cyber security) aspects) («Безпека промислового обладнання – Зв'язок з ISO 12100 – Частина 4: Керівництво для виробників обладнання по розгляду відповідних аспектів інформаційної безпеки (кібербезпеки)». Даний стандарт стосується виключно промислового Інтернету речей (IIoT), однак це складова IoT, а отже робота в напрямку регулювання безпеки ведеться.

На сьогоднішній день, Україна не створила певних законів, чи стандартів які могли б регулювати діяльність в сфері IoT. Вплив на інформаційну безпеку в Україні мають наступні закон: Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про захист персональних даних», Концепція ТЗІ в Україні та інші.

Виходячи з сучасної ситуації недосконалості стану стандартизації Інтернету речей, можна виділити такі напрямки роботи:

1) Удосконалення стандартів IP та Ethernet з урахуванням всіх вимог та потреб сфери IoT. Таким чином, стандарти не втрачають нічого із свого функціоналу, але набувають нове для роботи та зв’язку з Інтернетом речей.

2) Формування сумісності стандартів IP та Ethernet з галузевими. Чимала кількість великих корпорацій, що займаються промисловою діяльністю почали виконувати стандартизацію власних технологій та протоколів. Це спричинило «розсинхронізацію» між світовими стандартами та «локальними», яку намагаються вирішити комісії з питань сумісності стандартів в сфері IoT.

3) Формування архітектурних моделей для сумісності різноманітних складових сфери IoT. На форумі з питань в сфері IoT - «IoT World Forum» представили архітектуру узагальненої моделі, що дозволить організувати зворотну сумісність між всіма складовими IoT. «IoT World Forum» запропонував еталонну графічну модель (Рис. 1.1), яка розподіляє компоненти архітектури за рівнями . Це дає змогу забезпечити «відкриту IoT-систему» з сумісністю.

Рисунок 1.1 – Еталонна модель сумісності Інтернет речей

4) Формування консорціумів для вирішення головних проблем сфери IoT. Великі корпорації об’єднують зусилля для організації консорціумів головна мета яких – вирішення проблем сумісності пристроїв Інтернету речей, а також певних питань сертифікації пристроїв. Таким чином, були сформовані Open Interconnect Consortium, OIC та Industrial Internet Consortium, IIC (Консорціум відкритої взаємодії та Консорціум промислового Інтернету відповідно) [5]. Головним завданням OIC виступає формування в межах Інтернету речей зворотну сумісність пристроїв між собою, сумісність між хмарними рішеннями та інфраструктурою шляхом створення нових специфікацій, програм сертифікації пристроїв та розробки відкритого коду. IIC в свою чергу займається процесами інтеграції цифрового світу в фізичний за допомогою впровадження програмних рішень промислового Інтернету речей. Використовуючи інноваційні полігони для випробувань своїх рішень та еталонні архітектури IoT, IIC визначає певну базу стандартів та напрямки яких слід дотримуватися в подальшій роботі.

Завдяки розширенню зворотної сумісності, IoT надає можливість реалізувати нові можливості в сфері автоматизації як промислових рішень, так і в сфері надання послуг, а також бізнес-моделі, які донедавна навіть не існували у вигляді концепції чи ідеї[4].

Розглядаючи питання глобальної стандартизації пристроїв IoT неможливо не згадати про діяльність Міжнародного союзу електрозв'язку (МСЕ-Т). Союз запропонував три глобальні ініціативи GSI (Global Standards Initiative).

Глобальна ініціатива розуміє під собою великий комплекс робіт, який виконується кількома різними дослідницькими комісіями союзу згідно з заздалегідь узгодженим планом роботи. Серед цих ініціатив варто виділити ініціативу стандартизації рішень сфери IoT - IoT-GSI (Global Standards Initiative on Internet of Things). Решта ініціатив стосується стандартизації мережі нового покоління – NGN(Next Gen Network)-GSI та системи телебачення в основі якої знаходиться протокол IPTV-GSI.

В рекомендаціях Міжнародного союзу електрозв'язку з кодовою назвою «Y.2060», постає питання огляду Інтернету речей. IoT представляє собою певну інфраструктуру, що сягає глобальних масштабів. Завдяки такому поширенню, функціонал цієї інфраструктури дає змогу надавати складні сервіси. Основою цих сервісів є мережа між фізичними та віртуальними речами. В даному контексті «річ» розуміється як предмет віртуального або ж фізичного світу. Особливою ознакою Інтернет речі є можливість її ідентифікації та підключення до мереж зв'язку. Такі можливості, як вимірювання показників, спрацьовування за певних умов, введення, зберігання та обробка даних є обов'язковими для пристрою IoT, який в свою чергу являє собою лише елемент обладнання.[2].

Отже, як висновок можна вважати, що стандарти потрібні для регулювання чотирьох найголовніших аспектів IoT:

- Зв'язок;
- Взаємодія;
- Конфіденційність;
- Безпека.

1.4 Головні альянси та союзи в сфері IoT

1.4.1 The AllSeen Alliance.

В 2013 році фонд Linux оголосив про створення «Альянсу AllSeen» для сфери Інтернету речей, побудованого на основі інфраструктури взаємодії IoT з відкритим початковим кодом «AllJoyn» Qualcomm. Альянс AllSeen має на меті створення спеціальних фреймворків для додатків, які за своєю специфікацією будуть універсальними. Для передачі даних використовуються такі технології, як Ethernet, WiFi, Bluetooth, ZigBee, Z-Wave, 6LoWPAN, PowerLine. Однією з важливих особливостей проекту є те, що він цілком і повністю крос-платформний. Проект підтримує всі основні настільні та мобільні операційні системи, включно з Linux, Android, Arduino, iOS, OS / X, Windows 7/8 / RT, та ігровий двигун Unity. «AllJoyn» покликаний дати можливість виробникам обладнання, постачальникам послуг та розробникам програмного забезпечення створювати сумісні пристрої та послуги IoT. Особливо, відмічається те, що «AllJoyn» дає можливість спеціальним системам безперешкодно виявляти, динамічно підключатися та взаємодіяти з довколишніми продуктами незалежно від бренда, транспортного рівня, платформи чи операційної системи.

1.4.2 The Open Interconnect Consortium.

Samsung, Intel та Dell в 2014 році об’єднуються для проектування загальних підходів, здатних спростити розробку протоколів, програмного забезпечення та пристроїв – майбутніх складових «цифрового світу» в рамках співтовариства Open Interconnect Consortium (OIC). Пізніше в консорціум увійшли Atmel, Broadcom та Wind River.

Головна мета співтовариства – розробка відкритих стандартів взаємодії пристроїв між собою, незалежно від їх виробників, призначення та керуючого програмного забезпечення.

1.4.3 The Thread Group.

В організацію The Thread Group, створену при підтримці компанії Alphabet, входять Samsung, Qualcomm, ARM Holdings та багато інших світових

технологічних компаній. Організація розробила та опублікувала стандарт мережевого протоколу обміну інформацією між пристроями, що формують Інтернет речей, та проводить сертифікацію пристроїв, що підтримують даний протокол.

Протокол Thread можуть використовувати різноманітні пристрої: лампи, замки, кондиціонери, термостати і так далі. Обмін інформацією між пристроями забезпечує їх спільну роботу. Наприклад, термостат може передавати кондиціонеру дані, необхідні для зміни режиму його роботи і підтримки певної температури в приміщенні.

Thread заснований на технології, яку розробила компанія Nest Labs. Пристрої підтримують між собою зв'язок по стандарту IEEE 802.15.4. Поверх протоколу Thread можуть працювати інші програмні платформи.

1.4.4 Apple HomeKit.

HomeKit – це програмний фреймворк від компанії Apple, який дозволяє своїм користувачам використовувати свій пристрій IOS для налаштування зв’язку між розумними домашніми пристроями та управління ними. Використовуючи службу HomeKit, користувачі можуть проектувати кімнати, елементі та дії. На основі цього вони можуть вмикати автоматичні дії в будинку за допомогою голосового асистента Siri або додатків.

Головна вимога до виробників полягала в програмі сертифікації MFI, а також в наявності сопроцесора шифрування в пристроях HomeKit.

1.4.5 Industrial Internet Consortium.

Консорціум був заснований в березні 2014 року для об’єднання організацій-розробників, що брали участь в створенні та просування технологій, необхідних для підвищення темпів росту промислового Інтернету речей. Учасники IIC спільно працювали над прискоренням комерційного використання передових технологій IIoT. В склад консорціуму входять малі та великі технологічні новатори, лідери вертикальних ринків, дослідники, університети та урядові організації. Завдяки численним заходам та програмам, IIC допомагає користувачам технологій, постачальникам, системним інтеграторам та

дослідникам досягати результатів в процесі цифрової трансформації всього підприємства. Консорціум займається розробкою стандартів та дає організаціям рекомендації, необхідні для стратегічного застосування технологій та рішень в сфері IoT[6].

1.5 Архітектура та еталонна модель IoT

У IoT мінімальною вимогою до пристроїв є підтримка ними можливостей зв'язку (рис. 1.1). Пристрої поділяються на категорії пристроїв переносу даних, пристроїв збору даних, сенсорних і виконавчих пристроїв, а також пристроїв широкого призначення наступним чином[7]:

- Пристрій переносу даних: пристрій переносу даних підключається до фізичної речі і непрямим чином з'єднує цю фізичну річ з мережами зв'язку.
- Пристрій збору даних: під пристроєм збору даних розуміється пристрій зчитування/запису, яке має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися непрямим чином за допомогою пристроїв переносу даних або напряму за допомогою носіїв даних, підключених до фізичних речей. В першому випадку пристрій збору даних зчитує інформацію на пристрої переносу даних і може додатково записувати інформацію, надану самими мережами зв’язку, на пристрій переносу даних. При цьому, для взаємодії між пристроями використовуються технології радіочастотного, інфрачервоного, оптичного та гальванічного збудження.
- Сенсорний та виконуючий пристрій: даний пристрій може виявляти та вимірювати інформацію, що відноситься до довколишнього середовища і перетворювати її в цифрові електричні сигнали. Також пристрій може перетворювати цифрові електричні сигнали, що поступають від інформаційних мереж в дії. Як правило, такі пристрої формують локальні мережі, обмінюються

один з одним даними за допомогою дротових чи бездротових технологій зв’язку та використовують шлюзи для підключення до мереж зв’язку.

- Пристрій загального призначення: пристрій володіє вбудованими можливостями обробки та зв’язку. Має можливість обмінюватися даними з мережами зв’язку з використанням дротових чи бездротових технологій. Такі пристрої включають обладнання та прибори, що відносяться до різних областей застосування IoT.

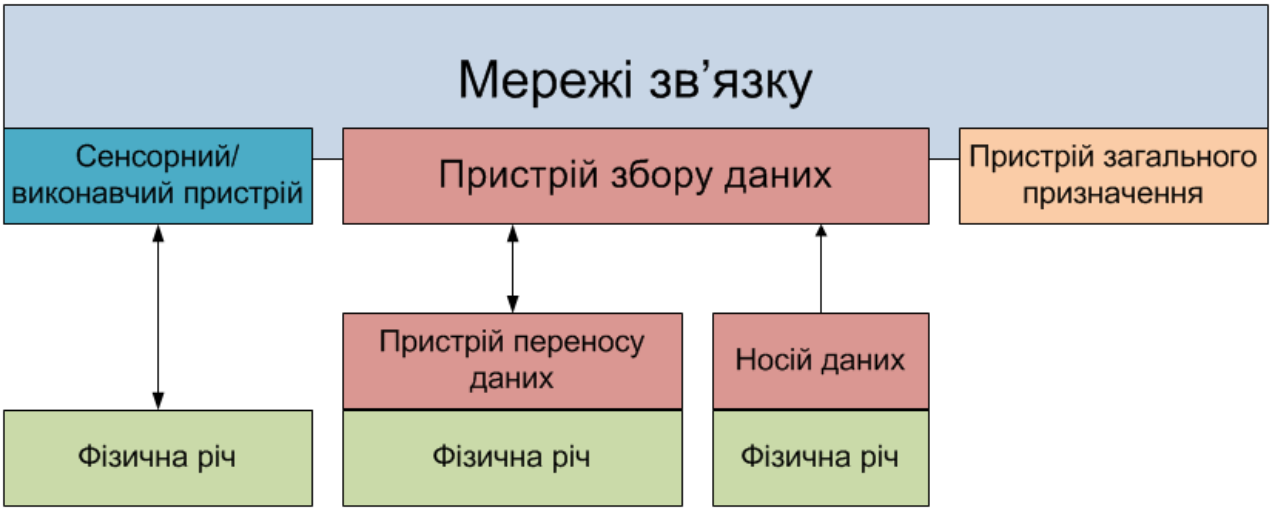

Рис. 1.1. Взаємозв’язок між пристроями та фізичним речами

Відповідно до рекомендації «Y.2060» еталонна модель покликана бути основою для стандартизації. Модель цієї архітектури дає розробникам розуміння того, які функції та можливості необхідні в IoT та яким чином вони взаємодіють між собою.

Модель складається з чотирьох рівнів:

- Рівень додатків: містить IoT додатки;
- Рівень підтримки послуг та підтримки додатків: загальні можливості являють собою типові можливості, які можуть використовуватися різними додатками IoT, такими як обробка чи зберігання даних[8]. Ці можливості можуть бути активовані спеціалізованими можливостями підтримки, наприклад, для створення інших спеціалізованих можливостей підтримки. Спеціалізовані можливості підтримки – це конкретні можливості, які призначені для

задоволення вимог різних додатків. В дійсності, вони можуть складатися з ряда груп чітко визначених можливостей, для того, щоб надавати різні функції підтримки різним додаткам IoT.

- Рівень мережі: можливості організації мереж надають відповідні функції керування мережевими з'єднаннями, такі як функції керування доступом і ресурсом транспортування, керування мобільністю та аутентифікація, авторизація та облік. Можливості транспортування – призначені для надання з'єднань для транспортування інформації в виді даних, що відносяться до послуг та додатків IoT, а також транспортування інформації контролю та керування, що відноситься до IoT.
- Рівень пристрою: можливості пристрою включають в себе пряму взаємодію з мережею зв'язку – пристрої здатні збирати та завантажувати інформацію безпосередньо в мережу зв'язку та можуть безпосередньо отримувати інформацію, наприклад, команди з мережі зв'язку; непряму взаємодію з мережею - отримання і завантаження інформації в мережу зв'язку непрямим способом, тобто за допомогою можливостей шлюзу; організацію спеціальних зв'язків в разі необхідності підвищеного масштабування або швидкого розсортування, пристрої мають можливість будувати мережу довільним чином; режим сну та пробудження – для економії енергії. Можливості шлюзу включають в себе підтримку декількох інтерфейсів (на рівні пристрою шлюз має можливість підтримувати пристрої, що з'єднані з використанням різних дротових та бездротових технологій, таких як шина локальної мережі контролерів (CAN), ZigBee, Bluetooth чи Wi-Fi); на рівні мережі шлюз має здатність обмінюватися даними з використанням таких технологій як комутована телефонна мережа загального доступу, мережа другого, третього покоління, мережа на базі технології довгострокового розвитку (LTE), Ethernet або цифрові абонентські лінії (DSL); перетворювати протоколи, в тих випадках коли для зв'язку на рівні пристрою використовуються різні протоколи рівня пристрою, наприклад, протоколи технологій ZigBee та Bluetooth, або коли для

зв’язку, що вимагає і рівень пристрою, і рівень мережі використовуються різні протоколи, наприклад, протокол технології ZigBee на рівні пристрою та протокол технології 3G на рівні мережі.

Окремо, необхідно звернути увагу на можливості керування. За аналогією з традиційними мережевими зв’язками, можливості керування IoT охоплюють традиційні класи недоліків, конфігурації, облік, показників роботи та безпеки, тобто керування несправностями (рис. 1.2).

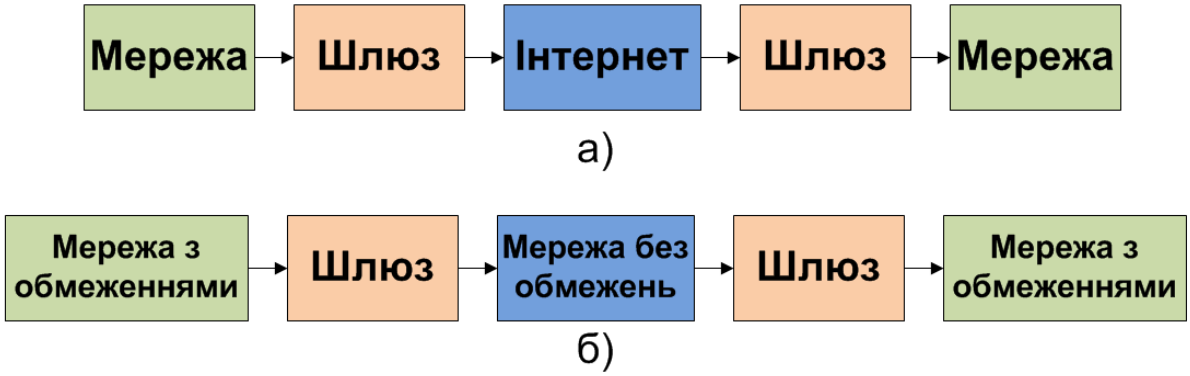

Рис. 1.3 Порівняння моделей передачі даних в Інтернеті та IoT. а) – Стандартна модель Інтернету, б) – модель IoT.

Можливість керування IoT може бути розділена на 2 категорії – загальні можливості керування та спеціалізовані[9]. Найважливіші загальні можливості керування в IoT включають:

- Керування пристроями. Наприклад, дистанційна активація і деактивація пристроїв, діагностика, оновлення прошивки або програмного забезпечення, керування робочим станом пристроїв;
- Керування топологією локальної мережі;
- Керування трафіком та перевантаженнями. Наприклад, виявлення умов перевантаженості мережі і реалізація зарезервованих ресурсів для термінових та життєво важливих потоків трафіку;

Спеціалізовані можливості керування тісно пов’язані з вимогами додатків, наприклад, вимогами за контролем лінії передачі електроенергії в «розумній» електромережі.

Існує два види можливостей забезпечення безпеки: загальні можливості забезпечення безпеки та спеціалізовані забезпечення безпеки. Загальні можливості забезпечення безпеки не залежать від додатків і включають:

- На рівні додатків: авторизація, автентифікація, захист конфіденційності та цілісності даних додатків, захист недоторканного приватного життя, аудит безпеки та антивірусне програмне забезпечення;
- На рівні мережі: авторизація, автентифікація, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;
- На рівні пристрою: автентифікацію, авторизацію, перевірку цілісності пристрою, керування доступом, захист конфіденційності та цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов’язані з вимогами додатків, наприклад, вимогами безпеки мобільних платежів (рис. 1.3).

Рис. 1.3 Еталонна модель IoT згідно з рекомендацією МСЕ-Т «Y.2060»

Сумісність між різними приладами користувача в сфері IoT досягається завдяки використанню загальних протоколів передачі даних[10]. Досить часто, компанії створюють власні стеки протоколів для обміну даними між пристроями (рис.1.4). Однак, протоколи різних фірм не можуть бути сумісні між собою і це спричинило б великі проблеми у формуванні IoT мереж якби не використання додаткових протоколів, які виконують роль мостів[7]. Завдяки цьому використання різних несумісних протоколів в одній операційні системі стає цілком реальним[9].

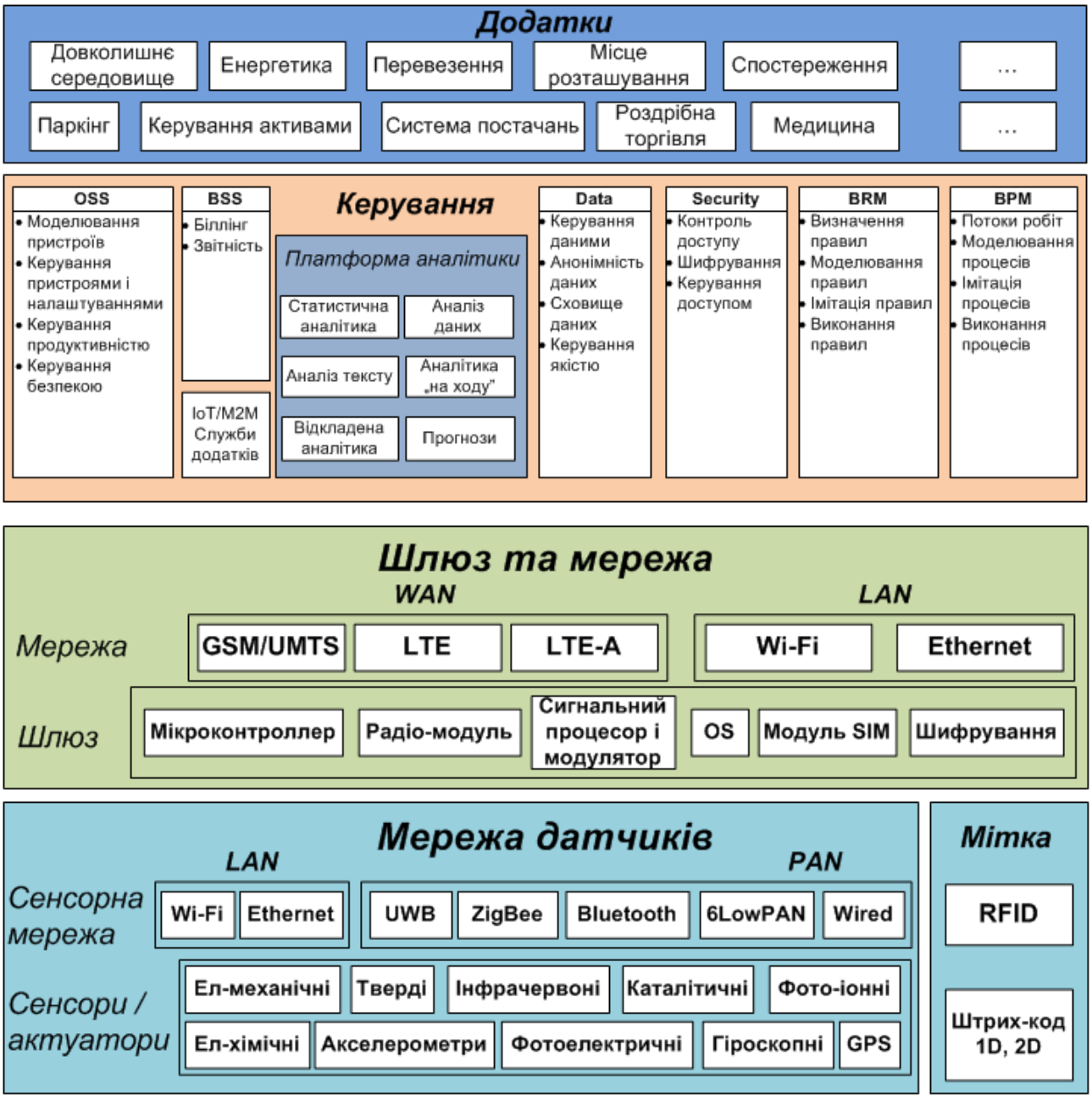

Рис. 1.4 Архітектура IoT

Однією з вимог до пристроїв Інтернету речей, є їхня ідентифікація. Даний аспект в умовах інтеграції IoT з Інтернетом вимагає використання IP-адреси як унікального ідентифікатора речі в мережі. Обмежений діапазон адресного простору в IPv4 провокує застосування IPv6, який має значно більший діапазон адрес[11].

Взаємодія речей відбувається на основі обраного протоколу, який в свою чергу обирається виходячи з функціональних можливостей та потреб. Обов'язковим фактором під час вибору протоколу є фактор безпеки: конфіденційність, цілісність, доступність.

Найбільш актуальними на сьогодні є протоколи бездротового зв'язку, а отже для великої кількості пристроїв найбільш ефективно буде використання саме таких протоколів[13].

Важливе місце в побудові системи IoT відводять таким характеристикам як ефективність роботи системи, відмовостійкість обладнання, адаптивність системи до змін та можливість самостійної реорганізації системи за певних умов.

Враховуючи всі вище перераховані вимоги, розробники почали використовувати стандарт IEEE 802.15.4. Його особливість полягає в можливості керування доступом з метою організації енергоефективних приватних мереж [12]. Даний стандарт став основоположником таких технологій, як 6LoWPAN, ZigBee.

ZigBee – являє собою специфікацію мережевих протоколів верхнього рівня - рівня додатків APS та мережевого рівня NWK, які використовують сервіси нижніх рівнів – рівня керування доступом до середовища MAC та фізичного рівня PHY, що є регламентованими стандартом IEEE 802.15.4. ZigBee разом з IEEE 802.15.4 описують регламент бездротових персональних обчислювальних мереж (WPAN). Специфікація ZigBee орієнтована на додатки, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях та можливість довготривалої роботи мережевих пристроїв від автономного джерела живлення.

Основними областями застосування технології ZigBee являються бездротові сенсорні мережі, автоматизація житлових будинків, медичне обладнання, системи промислового моніторингу та керування, а також побутова електроніка та периферія персональних комп'ютерів. Головна особливість технології ZigBee полягає в тому, що вона має змогу при низькому рівні енергоспоживання підтримує не лише прості топології мережі на кшталт «точка-точка», «дерево», «зірка», а й коміркову топологію, яка має здатність до самоорганізації та самовідновлення, з ретрансляцією і маршрутизацією повідомлень. Окрім того, специфікація ZigBee містить можливість вибору алгоритмів маршрутизації, в залежності від вимог додатків та стану мережі, механізм стандартизації додатків – профілі додатків, бібліотека стандартних кластерів, кінцеві точки, прив'язки, гнучкий механізм безпеки, а також забезпечує простоту розсортування, обслуговування та модернізації.

6LoWPAN – стандарт для взаємодії за протоколом IPv6 понад малопотужними бездротовими персональними мережами стандарту IEEE 802.15.4. Основною метою розробників було забезпечення взаємодії бездротових персональних мереж IEEE 802.15.4 з широко розповсюдженими мережами IP. Технологія орієнтується на додатки, які потребують бездротового підключення до Інтернету з низькою швидкістю передачі даних для пристроїв з обмеженими можливостями продуктивності та потужності. Наприклад, автоматизація будинків, офісів, виробництв. Не дивлячись на те, що така мережа здатна працювати автономно, забезпечення її підключення до Інтернету дозволяє розробникам надати нові можливості при керуванні такою мережею.

Адресація виконуються за рахунок присвоєння вузлам 128-бітну IP-адресу в ієрархічному порядку, пристрої IEEE 802.15.4 можуть використовувати 64-бітну адресу IEEE або (після об'єднання з PAN) 16-бітну адресу, унікальну в рамках PAN. Також існує PAN-ID для групи фізично сумісних пристроїв IEEE 802.15.4.

OTrP – Open Trust Protocol. Створений в 2015 році, протокол використовується для налаштування, оновлення та деінсталяції програмного

забезпечення, а також для керування конфігурацією безпеки в межах довірчого середовища.

Головним призначенням OTrP було додавання нового рівня сповіщень понад службою відкритих ключів PKI. З врахуванням того, що для роботи довірчих додаткіх необхідно використовувати захищене середовище (Trusted Execution Environment, TEE), створення нового протоколу, дозволило підвищити ступінь захищеності використовуваних систем, зробити їх роботу більш надійною за рахунок фізичного відділення обробки звичайних систем сповіщення на пристроях, що підключаються від підтримки прикладного трафіку, що пред'являє більш високі вимоги до безпеки.

В сфері IoT зустрічається дуже велика різноманітність пристроїв, що підключаються до мережі. Для кожного з них необхідно створювати власний механізм керування довірчими сервісами (Trusted Service Manager, TSM). Він відповідає за роботу з відкритими ключами, створення доменної зони для проведення безпечних розрахунків, підтримки роботи механізмів автентифікації ресурсів та завантаження додатків.

Зона дії OTrP знаходиться між службою TSM та пристроєм TEE. В роботі використовуються різноманітні механізми безпеки, що обслуговують з'єднання «точка-точка»: JSON Web Encryption (JWE), JSON Web Signature (JWS), JSON Web Key (JWK). Всі перераховані механізми рекомендовані одним із основних інститутів Інтернету, що займається стандартизацією – Інженерною радою IETF.

Для того, щоб пристрій, який підключається отримав можливість створити в собі захищене середовище TEE з підтримкою протоколу OTrP, йому необхідно надати пару унікальних ключів – публічний та приватний. Ці ключі виступають в ролі базового елементу довіри. Використовуючи їх, постачальники сервісів зможуть дозволити даному пристрою можливість виконати запуск довірчих додатків (Trusted Applications, TA).

X.509 – стандарт від MCE-T для інфраструктури відкритого ключа PKI та інфраструктури керування привілегіями PMI. Стандарт визначає основні формати даних і процедури розподілу відкритих ключів за допомогою

відповідних сертифікатів з цифровими підписами. Ці сертифікати надаються засвідчувальними центрам. Окрім того, X.509 визначає формат списку анульованих сертифікатів, формат сертифікатів атрибутів та алгоритм перевірки підпису методом побудови шляху сертифікування. Стандарт передбачає наявність ієрархічної системи засвідчувальних центрів для видачі сертифікатів.

Для випуск сертифікатів існує чітко визначена ієрархічна система засвідчувальних центрів. В цьому його головна відмінність від моделей заснованих на принципі мережі довіри, подібної до криптографічної технології PGP, де хто завгодно може випускати, підписувати та перевіряти на відповідність сертифікат. X.509 досить гнучкий для підтримки таких топологій як «міст» та «мережа», а також може бути використаний в P2P мережах.

1.6 Основні принципи та характеристики Інтернету речей

Існує три основні принципи на яких і сформована концепція Інтернету речей. Кожен з них, являє невід'ємну складову і не може бути замінений іншим. Інтеграція цих принципів дає можливість формувати сферу Інтернету речей з врахуванням всіх ризиків та складностей.

Перший принцип полягає в використанні поширеної інформаційно-комунікаційної структури, другий в можливості глобальної ідентифікації будь-якого об'єкту в системі, а третій в можливості обміну даними між об'єктами шляхом використання персональних мереж та Інтернету.

З певної точки зору, Інтернет речей досить кардинально відрізняється від Інтернету людей. Це пов'язано з самою концепцію IoT. Оскільки головна ідея полягає у існуванні системи без втручання людини в її структуру, роботу та процеси, то і відмінності базуються саме на цьому. Найбільш виразливими відмінностями є:

• Концентрація уваги системи на її об’єктах (речах фізичних та віртуальних) замість концентрації на користувачах – людях;

• Значно більша кількість підключених об’єктів, які складають структуру;

• Значно менші в порівнянні з Інтернетом людей розміри об’єктів системи та низькі ліміти швидкостей в каналах передачі даних;

• Концентрація процесів системи на зчитуванні інформації, а не на зв’язку між об’єктами;

• Потреба в формуванні нових інфраструктур та відповідних стандартів.

Згідно з Рекомендацією «Y.2060» МСЕ-Т, IoT – це інфраструктура глобальних масштабів для сучасного інформаційного суспільства. Дана інфраструктура надає послуги за допомогою організованих мереж зв’язку між об’єктами (між фізичними та віртуальними речами) при цьому використовуються цілком сумісні інформаційно-комунікаційні технології, що існують або такі, що знаходяться в процесі розробки.

Поняття «річ» розуміє під собою фізичний або віртуальний об’єкт як такий, що може бути повністю ідентифікований в системі або мережі, а також такий, який знаходиться в стані підключення до мережі засобами комунікацій.

Проблематика створення функціонуючих рішень в IoT полягає в наступному:

• Розміри та їх залежність від цілей, масштаб: Варто розуміти, що IoT у порівнянні з Інтернетом людей має більш широку концепцію та рамки застосування, це пов’язано з тим, що залежно від необхідних функцій та процесів, об’єкти взаємодіють у різних середовищах. В зв’язку з цим, необхідно забезпечити однаково ефективне функціонування речей, незалежно від розмірів та умов середовища.

• Самовідновлення та самоорганізація: Інтернет речей незалежний від впливу людини, чи комп’ютера, який залежний від користувача та того, яким чином він налаштований. Цей факт вимагає спроможності об’єктів адаптуватися до різних ситуацій, внаслідок яких інфраструктурі системи може знадобитись

реорганізація або відновлення після збою. Об’єкти повинні мати змогу незалежно ні від чого встановлювати зв'язок в разі необхідності.

- Об’єми даних та сховища: один із варіантів використання інфраструктури IoT полягає в постійному моніторингу, колективізації інформації з мережі датчиків та її зберігання. При цьому, вся ця інформація формуються на основі мереж великих масштабів, а отже її обсяги досить помітні, особливо коли інформація досягає центральних мережевих вузлів або серверів для її обробки. Термін який цілком описує це явище – «Big Data». Цей аспект потребує розробки нових технологій та методів обробки та зберігання інформації.

- Інтерпретація отриманої інформації: всі датчики та сенсори, що працюють в структурі рішення IoT передають інформацію для вузлів обробки в певному форматі. Це формує необхідність забезпечення чіткого перетворення інформації в дані, для подальшої обробки, в зв’язку з необхідністю постійної підтримки користувачів структури.

- Сумісність в робочих процесах: об’єкти які задіяні в довільному проекті Інтернету речей мають різні набори можливостей, а також характеристики. В зв’язку з цим, об’єкти можуть відрізнятися за інформаційно-комунікаційними та обчислювальними можливостями. До того ж, різні об’єкти в мережі, можуть працювати в різних умовах та середовищах, що викликає різницю в енергоефективності, швидкості передачі даних між цими пристроями. Для вирішення таких розходжень вкрай важливо розробити загальні стандарти та регламенти роботи.

- Авто-ідентифікація: у випадку, якщо рішення IoT розгортається в межах середовища, схильного до постійних змін – вкрай важлива підтримка автоматичного ідентифікування сервісів та об’єктів які їх надають, за допомогою семантичних засобів опису їхнього функціоналу та можливостей.

- Складність реалізації програмного забезпечення та додатків: необхідно сформувати регламент розробки додатків, який охоплює всі аспекти IoT для

забезпечення можливості надання всіх необхідних елементів керування об’єктами та їх підтримки з мінімальним рівнем використання ресурсів.

• Безпека об’єктів: враховуючи всі існуючі вимоги забезпечення захисту Інтернету, до Інтернету речей виникають додаткові, нові вимоги. Формування моделі, яка дозволить регулювати доступ різних сервісів або блокувати з’єднання зі сторонніми об’єктами в структурі IoT, та застосування особливих об’єктів завдання яких є захист бізнес-операцій від конкурентів. Беручи до уваги, той факт, що кожна річ підключається до мережі, варто зазначити, що це призводить до високих ризиків та загроз безпеці. Однією з важливих вимог безпеки в IoT є необхідність об’єднання різних принципів та методів забезпечення безпеки, що відноситься до багатьох об’єктів, мереж та користувачів.

• Увага до помилок та їх облік: Інтернет речей складається з об’єктів які постійно змінюються, мають динамічні показники та мобільний характер поведінки, відносно об’єктів Інтернету людей. В зв’язку з цим вони мають такий надлишковий аспект, як раптові зміни. Такі зміни можуть стати причиною збою чи помилки, що в свою чергу викликає підтримку рішень з боку структуризації та адаптації до змінених, нових умов.

• Енергоживлення та ефективність: залежно від задач об’єкти можуть бути мобільними та статичним. Однак в більшості рішень завжди є мобільні об’єкти, складність їх використання полягає в живленні від автономного джерела енергії. Одна з найважливіших вимог до джерела живлення – його розміри. Оскільки об’єкт має бути мобільним, то й живлення не має бути для цього проблемою. При проектуванні пристроїв увагу приділяють до процесорів, вибір часто падає на процесори з низьким рівнем енергозатрат та достатнім рівне потужності для виконання необхідних задач, а також на компоненти зв’язку від яких теж залежить використання енергії об’єкта. Додатково енергоефективність бере важливу участь в програмному забезпеченні. При розробці та впровадженні

нових протоколів, детально розглядають кожен можливий процес передачі інформації де кожен байт має бути аргументованим.

• Комунікації та бездротові технології: враховуючи вимоги енергоефективності найбільш популярними технологіями для комунікацій вважаються такі як 6LowPAN, WPAN, ZigBee. Натомість звичні для Інтернету людей технології GSM, UMTS, Wi-Fi та Bluetooth мало застосовуються в зв'язку з досить високими вимогами до елементів живлення пристроїв та речей в цілому.

Сфера IoT має наступні характеристики[12]:

• Можливість встановлення комунікацій: в сфері IoT, будь який пристрій може бути підключений до глобальної інформаційно-комунікаційної інфраструктури.

• Сервіси, які надають речі: Інтернет речі мають можливість надавати сервіси, що пов'язані з обмеженнями з боку захисту недоторканності приватного життя та семантичної відповідності між фізичним та відповідними їм – віртуальними речами. Для надання сервісів та послуг, що пов'язані з Інтернет речами, необхідно вносити зміни в технології як фізичного, так і інформаційного світу.

• Неоднорідність пристроїв: в IoT пристрої базуються на різноманітних апаратних платформах та мережах, це дає їм можливість взаємодії з пристроями та платформами інших послуг та сервісів використовуючи різні мережі.

• Динамічність станів: динамічність станів полягає у зміні режимів роботи пристроїв та об'єктів, наприклад, перехід з режиму сну в режим пробудження, знаходження в відключеному режимі. Також динамічним змінам підлягають такі характеристики пристроїв як місцезнаходження та швидкість. Окрім того, розглядаючи певний проект IoT як цілісну систему, то такий показник як кількість пристроїв, що входить до її складу також є динамічним, оскільки може змінюватися залежно від процесів та умов роботи.

• Масштаб інфраструктури: порівняно з Інтернетом людей, кількість пристроїв, що входить до сфери IoT буде в кілька разів більшою. Можна буде

спостерігати раптовий стрибок долі обміну інформацією, що ініційовано речами, по відношенню до інформаційного обміну, ініційованого людьми. Підвищиться значення керування даними, що створюються, їх процесам інтерпретації для використання в прикладних цілях.

• Зв'язок: встановлення зв’язку забезпечує два важливих фактори – доступність та сумісність. Перший розуміє під собою, можливість надання послуг та сервіс в будь який момент часу, коли це є необхідним, а другий – забезпечує можливість безпрецедентного обігу інформації в структурі, її створення та обробка.

1.7 Аналіз розвитку та перспективи впровадження концепції Інтернету речей

Майбутнє інформаційно-комунікаційної сфери дуже тісно пов’язане з розвитком та реалізацією концепції IoT. Чітка позиція МСЕ-Т та Європейського Союзу відносно сфери IoT дає неабияке підґрунтя для підвищення важливості розвитку технологій які сприятимуть розвитку Інтернету речей. До того ж, такі країни, як США, Китай та країни, що входять до складу ЄС внесли Інтернет речей до списку технологій майбутнього[13].

Інтернет речей став класичним прикладом концепції, яка випередила свій час. Сьогодні існує маса підходів, ідей, розробок, але не вистачає найголовнішого для IoT – універсальної інфраструктури передачі даних та єдиних стандартів. Домінуюча технологія – теж відсутня, замість неї – десятки, якщо не сотні галузевих варіантів реалізації IoT. Логічно зробити висновок із самої концепції IoT, що роль середовища для обміну інформації між об’єктами Інтернету речей мають виконувати мережі операторів мобільного зв’язку, які охоплюють на сьогодні більшу частину населення планети. Проблема полягає в

тому, що сучасні формати третього та четвертого покоління (3G та 4G відповідно) недостатньо добре підходять для масштабного розгортання інфраструктур IoT, це пов’язано з швидкістю передачі даних та затримками (рис. 1.5).

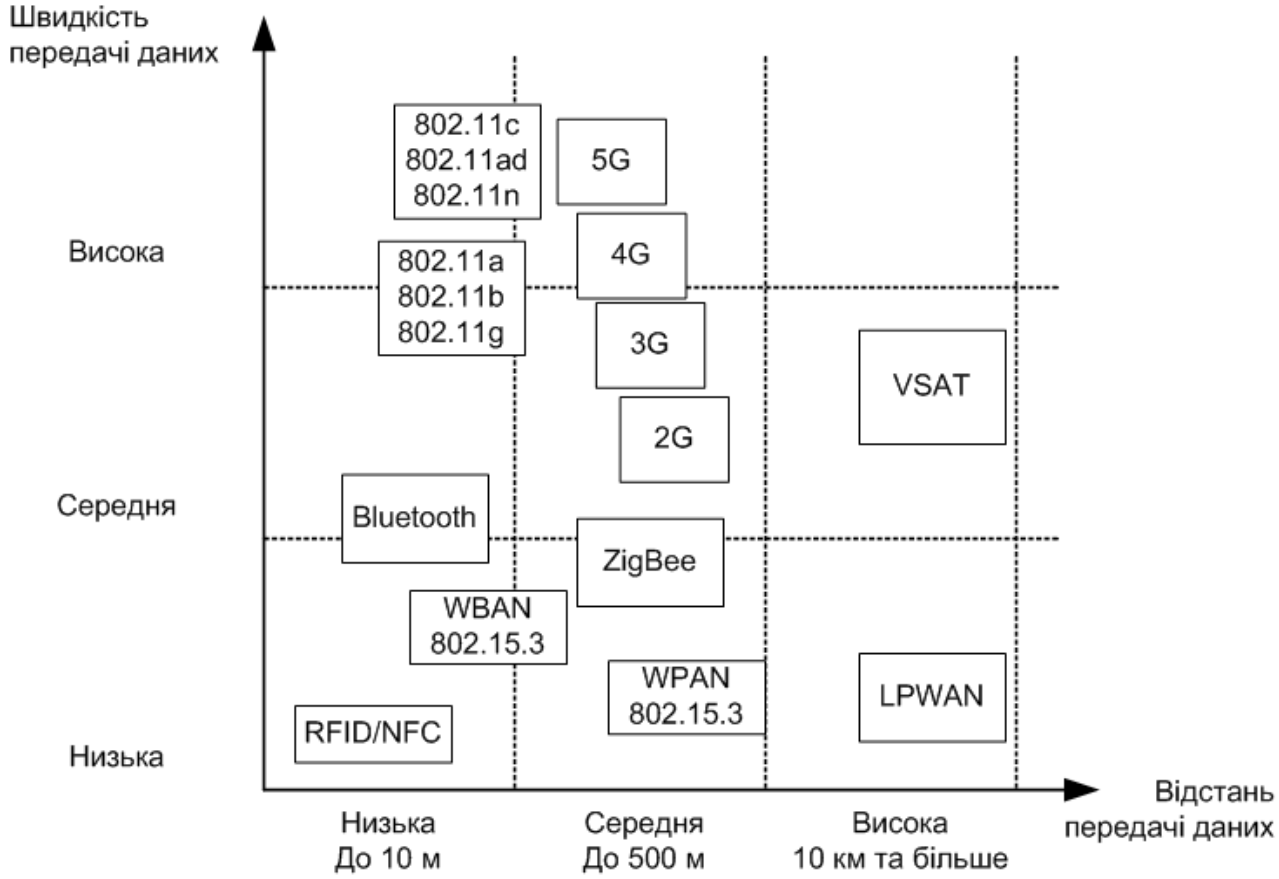

Рис. 1.5 Порівняння різних радіотехнологій, що використовуються в побудові мереж IoT

Наприклад, в США нормальним показником затримки в мережах LTE є значення в межах 50 мс – для Інтернету людей, та людського сприйняття це більш ніж достатньо, але у випадку міжмашинних інтерфейсів, що використовуються об’єктами IoT, необхідно отримати значення затримки в межах кількох мілісекунд. Такі значення можуть забезпечити лише мобільні мережі п’ятого покоління (5G). Власне, з їх широким застосуванням більшість виробників і пов’язують майбутнє швидкого розвитку IoT. А спостерігаючи тенденції 5G, досить скоро наступить момент, коли оператори розгорнуть по всьому світі технологію передачі даних п’ятого покоління, як універсальну технологію передачі даних[9]. Таким чином, галузеві технології на зразок

LPWAN найімовірніше будуть мати досить вузьке застосування, оскільки для таких технологій необхідно розгортати приватні спеціалізовані мережі, замість того, щоб використовувати вже існуючу інфраструктуру операторів зв'язку.

Ще одна проблема пов'язана з можливостями масштабування структур. Класична ситуація – інженери розробляють проект IoT, створюють прототипи і все працює саме так, як і було задумано, до тих пір, поки мережу формують лише кілька об'єктів. Коли проект починає швидко збільшувати кількість своїх об'єктів та кількість підключень вимірюється тисячами, виникають неочікувані технологічні проблеми, які просто неможливо було виявити на стадії прототипу. Як свідчать дані дослідження, що були проведені компанією «Cisco» в 2017 році серед майже 2 тисяч респондентів, близько 60% проектів зупиняються ще на стадії затвердження концепту. Експерти відмічають, що ініціативи IoT досить часто виглядають чудово на паперах,однак в реалізації виявляються набагато складніші, ніж будь-хто очікував. В число головних зупиняючих розробку факторів входять:

- Неможливість вірного розрахунку термінів реалізації проекту;
- Обмежена внутрішня експертиза;
- Недостатня якість даних;
- Відсутність інтеграції між командами впровадження;
- Перевищення витрат бюджету понад норми планованого.

Разом з тим, Інтернет речей дуже гостро поставив питання до сфери кібербезпеки. Оскільки в глобальних масштабах IoT, концепція переслідує ідею повсюдного впровадження, а це означає, що зловмисники зможуть отримати доступ не лише до найбільш детальних приватних даних користувачів, а й до важливих об'єктів критичної інфраструктури, транспорту, комунікаціям і тому подібне. При цьому, складність забезпечення захисту IoT-мереж стрімко збільшується по мірі включення до неї більшого числа об'єктів.

Судячи з усього, Інтернет речей очікує досить перспективне майбутнє. Ця концепція є прикладом об'єднання в собі всіх самих передових технологій. Поява

5G відкриває нові перспективи по розвитку інфраструктури IoT, інструменти роботи з «Big Data» дають можливість здійснювати глибокий та ефективний аналіз інформації, прикордонні обчислювання (Edge Computing) дозволяють суттєво зменшити навантаження на дата-центри та магістральні канали зв’язку за рахунок локальних обчислень. Великі надії покладають на використання штучного інтелекту в проектах IoT, за допомогою якого вдасться забезпечити зручне керування мережами та їх безшовне масштабування. Хмарні технології будуть основою для обробки та надійного збереження даних, а технологія блокчейну забезпечить нові послуги з високим рівне безпеки.

Розвиток таких технологій, як напівпровідникова електроніка, зв'язок, сенсори, смартфони, вбудовані системи, хмарні технології, мережева віртуалізація та програмне забезпечення, матимуть важливе значення для того, щоб фізичні пристрої могли працювати в мінливих середовищах і підключатися будь-де [13].

За даними IDC, міжнародної дослідницької маркетингової компанії, використання Інтернет речей підвищить глобальну продуктивність виробництва на 25%. Економічна цінність складає 11 трильйонів доларів, ринок пристроїв вартує 1,46 трильйонів доларів [14]. Кількість підключених пристроїв у 2016 році складає 4,8 тис. за хвилину, а до 2025 позначка зросте аж до 152 тис. Зважаючи на це 40% усіх даних будуть згенеровані пристроями IoT [16]. Темпи зростання і розвитку шалено швидкі, як і перспективи впровадження.

Перспектива IoT полягає в тому, що реальний світ буде все більше інтегруватися з віртуальним. Сьогодні в світі відбувається створення нових інтелектуальних вбудованих пристроїв. Це створить потік інформації в режимі реального часу, що зробить наші додатки більш обізнаними про події навколо.

Можна сподіватися на популяризацію нових додатків, які використовують ситуаційну інформацію, як-от інтелектуальність навколишнього середовища, соціальні пристрої, мережеві автомобілі та багато інших. Також існують програми, які дозволяють контролювати чи діяти в реальному світі. Рішення,

зроблені на віртуальній стороні, можуть відображатися в реальному середовищі. Це допоможе зекономити енергію, краще використовувати екологічні ресурси.

Перетворення величезної кількості необоротних даних на знання є однією з найбільших проблем, що стоять перед IoT. Існує цілий цикл обробки необроблених даних до створення бази знань. Можлива обробка даних включає генерацію статистики, агрегування даних, фільтрацію, кореляцію, контекстуалізацію та експозицію. Залежно від послуги або програми, чутливість до часу також є проблемою. Взагалі кажучи, інформація та знання, отримані з сенсорної мережі, будуть використовуватися для подальшого забезпечення інших процесів, таких як прийняття рішень або активація. Тому, складні ієрархічні цикли управління зворотним зв'язком можуть бути створені на основі отриманих сенсорних даних.

Очікування від IoT полягає в тому, що він впорається або, принаймні, значно зменшить ступінь необхідного втручання людини. Життєздатність IoT залежить від масштабованості, загальності, автономії та повноти управління [8].

На сьогоднішній день є основні виклики та наслідки, які потрібно вирішити, перш ніж масове впровадження IoT стане реальним [12].

1.7.1 Конфіденційність та безпека.

Оскільки IoT стає ключовим елементом майбутнього Інтернету та заважаючи на використання Інтернету речей для масштабних, а часом критично важливих систем, виникає потреба у вирішенні завдань надійності та безпеки:

- забезпечення довіри та якості інформації в спільних інформаційних моделях для забезпечення повторного використання в багатьох додатках;
- організація безпечного обміну даними між пристроями IoT та споживачами інформації;
- створення механізмів захисту від уразливих пристроїв.

1.7.2 Вартість в порівнянні зі зручністю.

IoT використовує технологію для підключення фізичних об'єктів до Інтернету. Для того, щоб впровадження IoT збільшувалося, вартість

компонентів, необхідних для підтримки таких можливостей, як ідентифікація, відстеження та механізми контролю, найближчими роками мають бути відносно недорогими.

1.7.3 Оперативна сумісність.

У традиційному Інтернеті взаємодія є основою вартості; перша вимога підключення до Інтернету полягає в тому, що "підключені" системи зможуть "говорити однією мовою" протоколів та кодів. На сьогоднішній день різні галузі використовують різні стандарти для підтримки своїх програм. Завдяки численним джерелам даних та неоднорідним пристроям, використання стандартних інтерфейсів між цими різними об'єктами стає важливим. Особливо це стосується програм, які підтримують перехресні організаційні та різні системи. Таким чином, системи IoT повинні мати високий ступінь сумісності.

1.7.4 Управління даними.

Управління даними є важливим аспектом Інтернету речей. Розглядаючи світ взаємопов’язаних об'єктів, що постійно обмінюються різними видами інформації, обсяг генерованих даних та процеси, пов'язані з обробкою цих даних, стають критичними.

1.7.5 Енергетичні проблеми на рівні пристрою.

Одним із найважливіших завдань IoT є взаємоз'єднання "речей" між собою, беручи до уваги енергетичні обмеження, адже зв'язок – це найбільш енергоємний процес на пристроях.

1.8 Напрями практичного застосування Інтернету речей

Широкий спектр приладів різної складності та функціональності відкриває нові можливості для використання інформації у світі. Інтернет речей має безліч застосувань у людському житті для його покращення. Розглянемо деякі з них [11].

1.8.1 Розумні міста.

Багато великих міст підтримали розумні проекти: Сеул, Нью-Йорк, Токіо, Шанхай, Сінгапур, Амстердам і Дубай. Функціональність розумних міст вимагає ретельного планування кожного етапу, з доступом до бази даних аеропортів, залізниць, можливістю відстеження транспорту. Згода уряду та громадян для впровадження технології Інтернету речей може значно покращити надання усіх можливих сервісів: зменшення трафіку, забезпечення безпеки, охорони здоров'я, соціалізації. Уявіть: громадянин взаємодіє з містом у будь-якій його точці і має доступ до усієї інформації починаючи від погодних умов і закінчуючи персональною інформацією.

1.8.2 Розумний дім та будинок.

Підключені через Wi-Fi домашні пристрої (телефони, телевізори, принтери і т.д.) стали частиною домашньої IP-мережі. Сучасні технології вже дозволяють керувати побутовою технікою через смартфон. Обидва типи пристроїв можуть бути використані як шлюзи для програм IoT. Багато компаній розглядають питання про розробку платформ, які інтегрують автоматику будівлі з сферою розваг, моніторингом охорони здоров'я, моніторингом енергії та моніторингом бездротових датчиків у житлових та будівельних середовищах. За концепцією Інтернету речей розумні будинки та будівлі можуть керувати багатьма пристроями та предметами, наприклад, інтелектуальним освітленням, інтелектуальним середовищем та медіа, контролем повітря та центральним опаленням, енергією та безпекою.

Бездротові сенсорні мережі (WSN) з технологією інтеграції в Інтернет речей забезпечують інтелектуальне управління енергією в будівлях, на додачу до очевидних економічних та екологічних переваг. Інтернет разом із системами енергоменеджменту надає доступ до енергетичної інформації та систем керування будинками з ноутбука або смартфона, розташованого в будь-якій точці світу. Майбутнє Інтернету речей забезпечить інтелектуальні системи управління будинком, які можна розглядати як частину набагато більшої інформаційної системи, що використовуватиметься власниками об'єктів у

будівлях для управління енергозатратами та енергозапасами та для підтримки будівельних систем.

1.8.3 Розумна енергія та енергосистеми.

Розумна енергосистема, інтегруючи інформаційні та комунікаційні технології в електричну мережу, дозволяє здійснювати в режимі реального часу двосторонній зв'язок між постачальниками та споживачами, створюючи більш динамічну взаємодію з потоком енергії, що допоможе забезпечити енергоефективність ефективніше та стабільніше. Основними елементами інформаційно-комунікаційних технологій будуть технології зондування та моніторингу для потоків енергії; інфраструктура цифрових комунікацій для передачі даних через мережу; розумні лічильники з домашнім дисплеєм для інформування про використання енергії; системи координації, контролю і автоматизації для агрегування та обробки різних даних.

Багато додатків з використанням Інтернету речей можуть бути використані для розумних енергосистем, таких як промислова і сонячна енергія, ядерна енергетика, транспортні засоби, лікарні та управління потужністю міст.

Такі системи можуть взаємодіяти зі звичайними електромережами, у майбутньому відкриваючи двері у напрямку використання енергетичної системи з низьким вмістом вуглецю, інтегруючись з поновлюваними джерелами енергії та зеленими технологіями, що створює багато переваг для споживачів за рахунок економії коштів завдяки ефективному використанню енергії.

1.8.4 Розумне здоров’я.

Постійна увага, необхідна для госпіталізованих пацієнтів, може забезпечуватися за допомогою безперервного моніторингу фізіологічного стану датчиками Інтернет речей. Сенсори використовуються для збирання інформації про стан здоров’я, а з використанням шлюзів та хмар для аналізу та зберігання інформації отримані дані бездротовими мережами надходять для подальшого аналізу. Цей процес замінює виконання одноманітних операцій медичним працівником через регулярні проміжки часу з метою перевірки життєвих показників пацієнта, натомість забезпечує безперервний автоматичний потік

інформації. Таким чином, одночасно покращується якість догляду за допомогою постійної уваги та знижується вартість послуг за рахунок зменшення вартості традиційних способів догляду, крім збору та аналізу даних.

1.8.5 Розумний транспорт і мобільність.

Рівень розвитку транспорту є одним із чинників, що вказують на добробут країни. Застосування моніторингу стану доріг та попередження про проблеми є одним із найважливіших застосувань IoT. Основною ідеєю концепції інтелектуального транспорту та мобільності є застосування принципів участі натовпу та залучення учасників. Процес починається з того, що користувач визначив бажаний маршрут, і позначив вибоїни на дорогах в додатку смартфону.

Концепція розумного транспорту має три основні розгалуження: аналіз транспорту, контроль транспорту та підключення до транспортних засобів. Аналіз транспорту – це прогнозування попиту та виявлення аномалій. Маршрутизація транспортних засобів та контроль швидкості, на додачу до управління трафіком, насправді тісно пов'язані із способом підключення до транспортних засобів, і в цілому регулюються декількома технологіями.

IoT як можливість використаний для електромобілів є важливим засобом зменшення вартості палива та впливу на глобальне потепління, також привернула значну увагу водіїв. Уряд у багатьох країнах підтримує дослідження систем контролю за продуктивністю літій-іонної батареї для електромобілів. Представлена система була розроблена для виявлення функцій літій-елементної батареї. Це рішення було вбудовано в багато основних функцій, таких як динамічне тестування продуктивності літійної батареї, віддалене спостереження за допомогою, онлайн– налагодження та корекцію помилок, що може істотно знизити витрати на технічне обслуговування.

1.8.6 Розумні заводи та виробництва.

Розробка розумного заводу додала нові цінності у виробничу революцію шляхом інтеграції штучного інтелекту, машинного навчання та автоматизації

роботи знань та зв'язку M2M з виробничим процесом. Розумний завод принципово змінить процес розробки, виготовлення та вантаження продуктів. У той же час це поліпшить безпеку працівників та захист навколишнього середовища шляхом мінімізації викидів та зменшення кількостей інцидентів. Досягнення у тому, як машини спілкуються з іншими об’єктами, і саме тому перехід процесу прийняття рішень від людей до технічних систем означає, що виробництво стає "розумнішим". Автоматизація, робототехніка та автономна мобільність є засобами для інтелектуального виробництва, проте зв'язок M2M, увімкнений "індустріальним" Інтернетом, відкриває повний зміст смарт-фабрики та інтелектуального виробництва на основі концепції Big Data. Розумне виробництво в цьому контексті посилається на аналітичні можливості, пропоновані обсягом та різноманітністю даних, які породжує мережева економіка, для оптимізації промислових процесів. Таке рішення передбачає менший проміжок часу для обслуговування, оптимізацію процесів та зменшення споживання енергії.

1.8.7 Розумне середовище.

Навколишнє середовище відіграє важливу роль у житті людини. Люди, а також тварини, птахи, рибки та рослини можуть постраждати у нездоровому середовищі. Створення здорового навколишнього середовища постає нелегкою проблемою через відходи промисловості та транспортні перевезення, а безвідповідальна діяльність людини є щоденними чинниками, які роблять шкоду навколишньому середовищу. Навколишнє середовище потребує розумних способів та нових технологій для моніторингу та управління.

Моніторинг показників навколишнього середовища є важливим для того, щоб оцінити його поточний стан для прийняття коректного життєвого рішення відповідно до зібраних даних з систем моніторингу, і визначити необхідний напрямок управління для ефективного споживання та використання ресурсів на додаток до зменшення відходів заводів та транспортних засобів, і навіть спрогнозувати стихійне лихо.

У навколишньому середовищі існує багато програм Інтернету, які можна розділити на дві основні категорії: контроль ресурсів навколишнього середовища, а також контроль якості та захисту довкілля.

Контроль ресурсів стосується всіх природних ресурсів: тварин, птахів та риб, вугілля, нафти, землі, лісів, прісної води, повітря та важких металів, включаючи золото, мідь та залізо. Усі ці ресурси, ймовірно, суттєво вичерпуються, впливаючи на деякі чинники, включаючи забруднення, відходи та зловживання. Відновлювані ресурси включають сонячне світло, вітер які можуть скеровуватися для найефективнішого використання в якості джерел альтернативної енергії.

Іншим аспектом навколишнього середовища є прогнозування погоди та моніторинг. IoT може забезпечити високу точність моніторингу погоди за допомогою обміну даними та інформацією. Це дозволяє погодним системам збирати дані з різних транспортних засобів на дорозі та здійснювати бездротовий зв’язок з метеорологічними станціями для підтримки даних, що включають температуру повітря, барометричний тиск, видимість або світло, рух та інші необхідні дані. Датчики, встановлені на будівлі, інтегрують транспортні засоби з IoT, допомагають збирати дані про погоду, які потім зберігаються в хмарах для аналізу. Сенсорна мережа IoT дозволяє контролювати рівень радіації навколо ядерних установок для запобігання виявлення та розповсюдження витоків.

Стихійні лиха є основними катастрофічними подіями в результаті природних процесів Землі і включають в себе повені, виверження вулканів, землетруси, урагани, лісові пожежі, хуртовини та інші геологічні процеси. Можна уникнути або зменшити вплив стихійних лих шляхом поширення ряду сенсорних систем для різних видів стихійних лих і зв'язок цих систем з науково-дослідними та рятувальними станціями, лікарськими та поліцейськими ділянками, а також для створення оголошень.

IoT принесе значні прибутки у сільське господарство, додаючи великий потенціал в економії ресурсів. За допомогою мереж датчиків і доступу до науково-дослідних баз, можна контролювати процес вирощування рослин та

інші сільськогосподарські виробництва, засновані на управлінні ресурсами, такими як погода, вода і сонячне світло. Крім того, IoT для моніторингу навколишнього середовища може допомогти в оцінці шкідливості викидів з заводів, виявлення лісових пожеж або прориву в сільському господарстві.

1.9 Висновки до розділу

Термін «Інтернет Речей» вперше був застосований у 1999 році. Однак тоді світ технологій докорінно відрізнявся від сучасного, адже ще не відбувся масштабний сплеск популярності смартфонів, що значно вплинув на хід розвитку технічного прогресу.

Згідно з рекомендацією Y.2060 «Огляд Інтернету Речей» IoT – це глобальна інфраструктура інформаційного суспільства, що забезпечує провідні послуги за рахунок організації зв’язку між речами (фізичними чи віртуальними) на основі сумісних інформаційних і комунікаційних технологій, що вже існують або лише розвиваються.

У концепції важливими поняттями також є «речі» – фізичні або віртуальні об’єкти, які можуть бути ідентифіковані і об’єднані через комунікаційні мережі; та «прилад» – частина обладнання з обов’язковими можливостями комунікації та необов’язковими можливостями із сенсорингу/зондування, з приведення у дію речі, збору, обробки і зберіганню даних. Прогнозують, що найближчим часом кількість приладів зросте до 50 млрд., що автоматично вимагає змін у протоколах та організації Інтернету.

Інтернет речей як концепція може здійснити революцію у наших життях впровадившись та ставши надійним помічником у всіх можливих галузях людської діяльності: від охорони здоров’я до розумної промисловості. Об’єднана мережа датчиків та індикаторів, що відслідковують фізіологічний

стан людини, ймовірність настання стихійного лиха, шкідливість промислових викидів та енергозатратність будинку вже об’єктивна реальність.

Перш ніж Інтернет Речі стануть невід’ємною частиною людського життя, розробникам доведеться подолати ряд викликів, найважливішими з яких є різнопланова стандартизація і забезпечення інформаційної безпеки на усіх етапах збору, передачі, обробки та зберігання даних.

РОЗДІЛ 2. ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ОБ’ЄКТАХ ІНТЕРНЕТУ РЕЧЕЙ

Безпека будь якої системи, завжди залежить від об’єктів, та підсистем які до неї входять. У випадку, коли до вже сформованої системи додають нові компоненти, об’єкти та пристрої, рівень безпеки цієї системи обов’язково змінюється, але в гірший бік. Це відбувається в інформаційних та комунікаційних системах, які отримують в свій розпорядок нові пристрої Інтернету речей. Паралельно з новими корисними послугами та можливостями, пристрої IoT беруть на себе роль потенційної вразливості для поточної системи[16].

Загрози, що приносять з собою Інтернет речі, є абсолютно практичними. Протягом останніх років, більшість випадків з порушення кібербезпеки та здійснення кіберзлочинів були здійснені за допомогою використання IoT-пристроїв. На основі даних про інциденти в кіберпросторі легко зробити висновок, що кількість атак на системи, що містять пристрої IoT зростає прямопропорційно росту кількості пристроїв IoT.

В липні 2019 року, компанія Check Point сформувала звіт «Global Threat Index». В даному звіті було оформлено рейтинг десяти найбільш часто використовуваних вразливостей в кібератаках. 3 місця з 10 зайняли вразливості Інтернету речей. Дві з них були критичними вразливостями, які надавали можливість виконувати код зловмисника на маршрутизаторі віддалено та вразливість за допомогою якої успішно обходили механізми автентифікації маршрутизатора. Ці недоліки безпеки IoT дають змогу зловмисникам ініціалізувати шкідливий програмний код, захопити керування пристроями та отримати доступ до інформації. Таким чином, система була б повністю скомпрометована[16].

2.1 «Big Data» та IoT дві сторони однієї монети

«Big Data» - поняття, що існувало ще до того, як IoT почали використовувати в ролі одного із найбільш актуальних засобів для проведення аналітичних досліджень[14].

Загалом, «Великі Дані» це інформація, яка була отримана з кінцевих пристроїв в системі IoT, потім інтерпретована та надана в ту частину системи, яка займається обробкою цієї інформації. Таким чином відбувається перехід від «Little Data» до «Big Data». Кінцева інформація, має наступні властивості:

- Швидкість;
- Достовірність;
- Обсяг;
- Різноманітність.

Такі властивості характерні для даних, які можна структурувати, або навпаки, працювати з неструктурованими. Швидкість та достовірність даних розуміються, як швидкість з якою інформація може бути опрацьована та точність яка властива отриманим даним.

Інтернет речей вимагає практичного рішення цього питання: створення та розробка програмного забезпечення та апаратних засобів, які дозволять в режимі реального часу виконувати обробку безперервного потоку даних та їхнє аналізування. Пов’язано це з тим, що інформація зчитується кінцевими датчиками, сенсорами та іншими фізичними об’єктами кожної хвилини, якщо не секунди та передається на вузли обробки та передачі даних.

Важлива частина концепції «Big Data» полягає в тому, що дані потрібно не лише накопичувати, але і відповідним чином проводити їхню обробку. Звідси виходить завдання «навчити» пристрої Інтернету речей виконувати корисну для системи роботу. При цьому, традиційні алгоритми, як обробки даних, так і керування системами цілком не ефективні, оскільки «Big Data» часто можуть бути не структуровані, не повні, а що ще більше важливо – в більшості випадків,

вони не підходять під заздалегідь відомі закономірності. Таким чином, існує задача для отримання нового ефективного алгоритму керування «Big Data», який в подальшому може бути ефективно використаний на кінцевих пристроях із значно меншими затратами. Саме такими пристроями, як правило, і виступають пристрої Інтернету речей.

Друга важлива компонента концепції «Big Data» є транспортування даних та зберігання їх в «хмарах». Це необхідно для того, щоб Інтернет речі могли отримати доступ до загальної бази знань, а також для того, щоб локалізувати ресурсоємні процеси в хмарних сервісах, де питання енергоспоживання та доступних ресурсів вже вирішений, та не стоїть так гостро, лишивши собі лише прості, енергоефективні функції та завдання.

Застосування традиційних підходів для обробки «Big Data» не тільки не ефективно, але і часто просто неможливо. Проблема полягає не стільки в величезних об’ємах ресурсів необхідних для обробки, скільки в складності взаємозв’язків в середині самих даних. Емпіричний метод втратив свою актуальність через неможливість обробки великого числа параметрів та тривалості фіксації кожного параметру окремо.

Але водночас комп’ютери ідеально підходять для виконання цієї задачі. Вони здатні порівнювати велику кількість даних між собою на різних рівнях та вибірках для виявлення закономірностей. Окрім того, такі задачі через свою природу чудово поділяються на паралельні потоки, що також чудово йде на користь сучасним багатоядерним процесорам та розподільним хмарним платформам. Кінцева ефективність такої роботи досить низька (результат приносять лише тисячні долі відсотка), але результат може виправдати всі сподівання, оскільки досить часто, його неможливо чи вкрай малоймовірно отримати іншим шляхом. З цієї точки зору, процес можливо порівняти з добуванням золота. Необхідно обробити тонни руди, щоб отримати кілька грам дорогоцінного металу. Важлива особливість роботи з «Big Data» на комп’ютерах полягає в тому, що практично нічого не потребується для роботи, окрім безпосередньо стандартного апаратного забезпечення (процесори, пам'ять,

накопичувачі, мережа) та електроенергії. А всі ці компоненти на сучасній стадії розвитку науки та техніки стають все більш дешеві з кожним роком[15].

Розглядаючи всі недоліки «Big Data», виокремити такі головні проблеми:

- Ієрархічна система фреймворків. Великі проекти використовують розгалужену систему хмарних сервісів для забезпечення достатньо високої швидкості обробки даних та їх аналізу. Зниження навантаження на одну підсистему за рахунок інших, дозволяє зменшити об’єм даних для обробки, але продукує множину підсистем, за безпеку яких необхідно спостерігати. Така децентралізація викликає проблеми з безпекою.
- Проміжне ПЗ. Деякі не реляційні бази даних вимагають високого рівня конфігурації безпеки, але не отримують його в достатньому обсязі, натомість використовується проміжне програмне забезпечення яке має на меті виконувати роль засобів безпеки.
- Сховища та процеси зберігання даних. В архітектурі «Big Data», інформація розподіляється по кількох рівнях в залежності від потреб проекту відносно продуктивності та визначених об’ємів коштів. Більшість даних з високим пріоритетом значущості часто зберігаються в пам'ять флеш-носіїв. В разі блокування доступу до пам'яті, виникає ефект формування процедури розподілу даних за рівнями.
- Кінцеві вузли. Засоби безпеки, пов’язані з кінцевими вузлами в системах IoT, мають підтверджувати автентичність усіх кінцевих об’єктів, інакше результати аналізу будуть непридатні.
- Функції безпеки в режимі реального часу. В зв’язку з великою кількістю інформації, висока вірогідність факту помилкових спрацьовувань відносно безпеки. Вкрай необхідно розробити механізм, мета якого вчасне виявлення та реагування на такі спрацьовування. Пов’язано це з необхідністю збереження ресурсів для обробки реальних проблем та порушень норм безпеки.

- Пошукова система для інформації. Головні елементи системи – модулі для збору та обробки інформації. Тому реалізація безпеки повинна враховувати загрози як зовнішні, так і внутрішні.
- Ідентифікація та керування доступом. Для системи вкрай важливо працювати лише з ідентифікованими користувачами та об’єктами. Важливо, щоб процедура автентифікації користувача була обов’язковою та регулювала процедуру визначення рівнів доступу.
- Система пост-аудиту. Мета системи – проведення аудиту інфраструктури, виявити факт втручань, атак, їхній вплив та наслідки на систему в цілому для майбутнього запобігання.
- Метадані. Метадані є важливим елементом під час обробки даних отриманих з кінцевих вузлів, оскільки їхня мета – надавати розширену інформацію про отримані дані. Їхня особливість полягає в необхідності швидкого аналізу, оскільки чим швидше вони будуть опрацьовані, тим нижче ризик витоку інформації. Важливо проводити аудит користувачів, які мають зв'язок з вказаним типом даних, оскільки вони можуть стати вразливістю для системи.

В якості завершення, можна відмітити наступне:

1) «Big Data» - це не лише самі дані в великих об’ємах, але й способи та методи їх обробки;

2) На основі «Big Data» можливо створити алгоритми керування IoT;

3) Розподіл задач і функцій на групи для пристроїв IoT та хмарних сервісів дозволяє вирішувати задачі більш ефективно;

4) Для обробки «Big Data» необхідні спеціальні алгоритми, в основному побудовані на машинному навчанні;

2.2 Головні вразливості пристроїв IoT

Вразливостей, що існують та активно використовуються злочинцями існує багато, але певні з них мають найбільшу популярність. Згідно з класифікацією OWASP існує 10 основних категорій вразливостей систем безпеки в проектах IoT[24].

2.2.1 Недостатній рівень фізичної безпеки.

Відсутність засобів фізичного захисту дозволяє потенційним зловмисниками отримати доступ до конфіденційної інформації, яка в майбутньому може бути використана для реалізації віддаленої атаки чи отримання локального контролю над пристроєм[17].. Одна з проблем екосистеми IoT полягає в тому, що її компоненти розміщені в просторі і часто встановлюються в публічних та незахищених місцях. Це дає можливість зловмисникам отримати доступ до пристрою та взяти його під контроль чи використати для доступу до всієї мережі. Зловмисник має можливість:

1. Отримати мережеві та фізичні налаштування пристрою та встановити замість нього власний пристрій для прослуховування або зниження продуктивності мережі;
2. Здійснити злам RFID зчитувача;
3. Встановити апаратну закладку;
4. Інфікувати шкідливим ПЗ;
5. Викрасти дані;
6. Фізично вивести пристрій з ладу.

2.2.2 Небезпечні налаштування по замовчуванню.

Пристрої чи системи поставляються з небезпечними налаштуваннями по замовчуванню або не мають можливості зробити систему більш безпечною, обмежуючи користувачів в налаштуваннях конфігурації[18]. Будь який виробник бажає заробити якомога більше та витрати якомога менше, в пристрої може бути реалізовано чимало розумних функцій, але при цьому не забезпечена можливість конфігурування безпеки. До складних наслідків може призвести відсутність таких функцій безпеки:

1. Відсутність перевірки паролів на надійність.

Занадто прості паролі легко піддаються зламу шляхом брутфорсу. Необхідна перевірка паролів, яка лише за виконанням всіх вимог стійкості паролів приймає зв’язку «логін/пароль». Нерідко, людська природа стає причиною до зламів. Досить часто користувач в надії на непотрібність інформації якою він користується, встановлює дуже простий пароль для простішого користування.

2. Відсутність можливості створення облікових записів з різними правами.

Розмежування прав користувача та адміністратора допомагає запобігти випадкових критичних змін в системі користувачем, а також відмовити в наданні важливих функцій в разі зламу облікового запису користувача, оскільки доступ до них має лише адміністратор. Розмежування прав та привілеїв відповідно до ролей дозволяє створити певний «розподіл обов’язків», що забезпечить систему яка слідкує за тим, щоб користувачі могли виконувати лише необхідні для роботи дії, не більше, не менше.

3. Відсутність логування.

Логування є однією з важливих вимог більшості сучасних стандартів в сфері інформаційної безпеки та комп'ютерних мереж. Ведення журналу подій та процесів може значно спростити розслідування інцидентів безпеки, в разі такого інциденту, журнал подій надасть можливість виявити всі причини інциденту та його наслідки при подальшому розслідуванні та використати отримані дані в майбутньому для покращення політики безпеки. Під час логування створюється файл журналу, в який заносяться всі події в системі, дії всіх користувачів, а також відсутня можливість змінювати та редагувати журнал. Таким чином, інформація в журналі цілком надійно захищена та достовірна.

4. Відсутність сповіщень про події безпеки.

Реалізація системи моніторингу дає можливість відповідним особам вчасно приймати рішення та запобігати інцидентам. Лише журналу логування замало, вкрай необхідно Сформувати компонент системи безпеки на основі

інформаційно-комунікаційної структури. Головним завданням системи є робота в режимі реального часу для виявлення неправомірних дій в мережі.

2.2.3 Відсутність можливості керувати пристроєм.

Відсутність підтримки безпеки на пристроях, розгорнутих в виробництві, включно з керуванням активами, керування оновленнями, безпечний вивід з експлуатації та моніторинг систем і реагування. Пристрої IoT часто являють собою «чорну скриньку». В них не реалізована можливість слідкувати за станом роботи, ідентифікувати які служби та процеси запущені та з чим вони взаємодіють. Не всі виробники дають здатність користувачам IoT-пристроїв повністю керувати операційною системою та запущеними додатками, а також перевіряти цілісність та легітимність завантаженого ПЗ чи встановлювати патчі оновлення на ОС. Під час атак, прошивка пристрою може бути переконфігурована так, що відновити її буде неможливо, залишається лише перепрошити пристрій[19].

2.2.4 Небезпечна передача та збереження даних.

Відсутність можливості шифрування чи контролю за доступом до конфіденційних даних в будь якому місці екосистеми, в тому числі при збереженні, при передачі чи під час обробки[20]. Пристрої Інтернету речей збирають та зберігають дані про довколишнє середовище, в тому числі різну персональну інформацію. Скомпрометований пароль, можна замінити, але викрадені дані з біометричного пристрою – відбиток пальця, сітківка ока, біометрія обличчя – ні. В той же час, IoT-пристрої можуть не лише зберігати в собі дані в незашифрованому вигляди, але і передавати їх в по мережі. Якщо передачу даних в відкритом вигляді по локальній мережі ще можна хоч якось пояснити, то у випадку з бездротовою мережею чи передачею через Інтернет, вони можуть стати легко здобутком будь кого. Сам користувач може використовувати безпечні канали зв’язку для передачі даних, але шифрування паролів, що зберігаються, біометричних та інших важливих даних повинен забезпечувати виробник пристроїв. До складних наслідків може призвести відсутність таких функцій безпеки:

1. Відсутність шифрування в каналах.

За результатами опитування HP Study, понад 70% користувачів під час передачі даних мережею, користуються сервісами які не мають служб шифрування. Так само близько половини мобільних додатків під час підключення до хмарних сервісів, Інтернету, локальних мереж – не мають захищеного з'єднання. Таким чином вірогідність прослуховування трафіку та імовірність успішної атаки типу MITM – дуже висока. Завдяки цьому, зловмисник отримує всі дані які надсилає користувач, оскільки виконує роль вузла між кінцевими пристроями.

2. Відсутність шифрування в каналах локальної мережі.

Такий сценарій цілком можливий і в локальних мережах, в тих випадках коли зловмисник отримав доступ до мережі.

3. Відсутність застосування SSL / TLS.

Протокол SSL / TLS був розроблений для застосунку в браузерах, але пізніше завдяки своїм якостям, став одним із найбільш якісних стандартів для комунікацій в мережі Інтернет[56]. Сьогодні протокол широко використовується в таких цілях, як: передача платіжних реквізитів та даних покупця, віддалений доступ до панелей адміністрування віртуальних інфраструктур розгорнутих в хмарі, передача локальних даних до сховищ розміщених в хмарних сервісах, автентифікація серверних послуг в мобільному програмному забезпеченні і т.д[57]. В теорії, SSL / TLS має здатність забезпечувати головні фактори безпеки – цілісність, доступність, конфіденційність комунікацій програмного забезпечення, як з боку серверів так і з боку клієнтів.

4. Застосунок SSL / TLS з неправильним налаштуванням.

В процесі активного обміну інформацією, безпека з'єднання в першу чергу залежить від повної перевірки криптографічного сертифікату, який надає сервер. Також, перевірка стосується таких складових як набір шифрів. Наступні ознаки, забезпечують цілком безпечне з'єднання з сервером:

- Орган сертифікації, що видав сертифікат – діючий;

- Сертифікат – актуальний за терміном дії та не є відкликаним;
- Домен до якого підключається клієнт, повинен обов’язково бути в списку імен доменів сертифікату.

2.2.5 Недостатній рівень захисту конфіденційності.

IoT-пристрої збирають інформацію про те, що і хто їх оточує, в ому числі це стосується і людей, що нічого не підозрюють. Викрадені чи неправильно оброблені дані про користувача можуть як ненавмисно дискредитувати людину, так і використовуватися при шантажуванні. 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 чи захищені вони, а також чи прописані політики зберігання даних. Інакше, при недотриманні цих умов, у користувача можуть виникнути проблеми з законодавством. До складних наслідків може призвести відсутність таких функцій безпеки:

1. Збір особистих даних.

Чим більше обсяг інформації про особи збирається пристроєм, тим більше необхідно ресурсів для забезпечення захисту. Персональні дані завжди цінувалися серед зловмисників, оскільки відкривали досить широкий спектр для атак. Заслуговує уваги закон про обробку персональних даних, прийнятий Європейським Союзом. «Загальний регламент про захист даних» вирішує питання, стосовно обмеження можливостей колективізації інформації про людину, яка перевищує значення та обсяг максимально необхідний для виконання певних дій.

2. Перевірка та налаштування дозволів.

Відсутність можливості налаштувати систему збору інформації наражає користувача на небезпеку. В разі її цілковитої відсутності, користувач не отримає персональний досвід від користування пристроєм, або навпаки, система збирає та оброблює всю можливу інформацію.

2.2.6 Використання небезпечних чи застарілих компонентів.

Використання застарілих або небезпечних програмних компонентів або бібліотек, які можуть дозволити скомпрометувати пристрій[21]. Це включає небезпечне налаштування платформ операційної системи і використання сторонніх програмних або апаратних компонентів із скомпрометованого ланцюга постачань. Один уразливий компонент може звести нанівець всю налагоджену безпеку. На початку 2019 року експерт Пол Маррапіз виявив уразливості в P2P-утиліті iLnkP2P, яка встановлена більш ніж на 2 мільйони пристроїв, підключених до мережі: IP-камерах, радіонянях, розумних дверних дзвінках, відеореєстраторах.

Перша вразливість CVE-2019-11219 дозволяє атакуючому ідентифікувати пристрій, друга - вразливість автентифікації в iLnkP2P CVE-2019-11220 - перехоплювати трафік у відкритому вигляді, включаючи потокову передачу відео і паролі.

2.2.7 Відсутність безпечних механізмів оновлення.

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 оновлення. 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 перевірений на цілісність перед установкою, відсутній захист проти відкатів (захист від повернення до попередньої, більш вразливою версії) або відсутні повідомлення про зміни безпеки через оновлення. До складних наслідків може призвести відсутність таких функцій безпеки:

1. Шифрування файлів оновлення.

Зазвичай оновлення відбуваються за допомогою бездротових технологій з’єднання, таким чином зловмисник зможе перехопити файли оновлення, впровадити шкідливий код, та повторно надіслати його пристрою.

2. Відсутність налаштування параметрів шифрування.

Всі дані що передаються та зберігаються повинні бути зашифровані в обов’язковому порядку, для уникнення факту перехоплення або підміни зловмисниками.

3. Підтвердження оновлень безпосередньо перед завантаженням.

Варто завжди перевіряти оновлення перед тим, як підтвердити їхнє завантаження до системи. Зловмисники мають можливість представити інфіковане ПЗ під виглядом оновлення для довіреної програми, до того ж, ПЗ матиме всі необхідні цифрові сертифікати та підписи.

4. Конфіденційні дані в оновленні.

Під час процесу оновлення, програмний код, облікові дані, що знаходяться в файлі прошивки можуть бути перехоплені зловмисником. Особливо важливо, якщо оновлення мало виправити відому «діру» в безпеці. Таким чином, зловмисник отримає знання про метод виправлення та одразу зможе працювати над тим, як обійти цей метод.

5. Погіршення роботи.

В разі, якщо після застосунку оновлення, система стала працювати гірше, варто негайно зробити «відкат», оскільки оновлення цілком можливо несло в собі шкідливий код.

2.2.8 Небезпечні інтерфейси екосистеми.

Небезпечний веб-інтерфейс, API, хмарні або мобільні інтерфейси в екосистемі поза пристроєм, що дозволяє компрометувати пристрій або пов'язані з ним компоненти навіть без підключення до нього. Загальні проблеми включають в себе відсутність автентифікації або авторизації, відсутність або слабке шифрування, а також відсутність фільтрації введення і виведення. Використання небезпечних веб-інтерфейсів, API, хмарних і мобільних інтерфейсів дозволяє скомпрометувати пристрій або пов'язані з ним компоненти.

Для захисту необхідно змінювати користувача і пароль за замовчуванням, переконатися, що веб-інтерфейс не схильний до міжсайтового скриптингу, SQL-ін'єкцій або CSRF-атак. Також повинен бути реалізований захист від атаки на паролі методом перебору. Наприклад, після трьох спроб невірного введення паролю обліковий запис повинен блокуватися і дозволяти відновити пароль тільки через апаратне скидання. До складних наслідків може призвести відсутність таких функцій безпеки:

1. Перевірка інформації POST та GET запитами.

Метод перебору облікових записів з використанням можливості отримання відповіді інтерфейсу за допомогою введення заздалегідь неправильних облікових даних.

2. Відсутня система блокування облікового запису.

3. Доступ до каналів мережі передачі даних.

Існує можливість отримати інформацію, за допомогою аналізатора трафіку. Таким чином, важко запобігти витоку даних, якщо канали не ізольовані в повній мірі.

4. Використання ін’єкцій в веб-сайтах.

Це клас атак, що містить в собі різні варіанти та способи реалізації. Атака основана на впровадженні сторонніх команд або даних в працюючу систему з метою модифікації робочого процесу системи, результатом чого стає доступ до інформації, або можливість дестабілізації роботи системи в цілому.

Загалом розрізняють такі види ін’єкцій:

- SQL-ін’єкція – атака спрямована на модифікацію SQL-запитів до бази даних[35]. Завдяки цій ін’єкції зловмисник може отримати доступ до інформації яка знаходиться в базі даних, частіше всього сервера чи веб-сайта.
- PHP-ін'єкція – використовується для обходження засобів безпеки веб-сайтів створених за допомогою мови програмування PHP. Суть методу полягає в ін’єкції шкідливого програмного коду до коду веб-додатку на серверній стороні сайту, це дозволить виконати різноманітні команди, частіше

використовується для впровадження бекдорів в сервер на якому розміщується сайт.

- XSS, міжсайтовий скриптинг – вид вразливостей веб-сайтів, результатом їх успішного використання являється можливість внесення шкідливого коду в структуру веб-сторінки, яку переглядають інші користувачі[34]. Внаслідок чого, цей код виконується на стороні клієнта користувача який переглянув сторінку.
- Xpath-ін’єкція – застосовується для модифікації запитів до бази даних XML. Внаслідок чого зловмисник отримує доступ до конфіденційної інформації.

5. Керування сесією між клієнтом та сервером.

Сесія визначає період підключення користувача до ресурсу, з моменту першого встановлення з’єднання та до моменту відключення[36]. Протягом цього періоду, захищений вміст який надає сервер повністю доступний для авторизованого користувача[25]. Сесія колективізує всі можливі облікові дані користувача, поки він знаходиться в межах одного домену, а також створює спеціальний ідентифікатор, який використовується сервером при всіх запитах веб-сторінки домену для ідентифікації користувача. Зловмисник може використати дані користувача, для входу до системи з його правами, в разі успішного викрадення. Але варто врахувати, якщо система має перевірку IP-адрес сесій та заборону на наявність більше одного з'єднання в одній сесії, то спроба буде безуспішна.

2.2.9 Небезпечні мережеві сервіси.

Непотрібні або небезпечні мережеві служби, запущені на самому пристрої, особливо відкриті для зовнішньої мережі, що ставлять під загрозу конфіденційність, цілісність, достовірність, доступність інформації або допускають несанкціоноване віддалене управління. Небезпечні мережеві служби можуть бути схильні до атак переповнення буфера і DDoS-атак. Відкриті мережеві порти можуть бути просканові 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 та на SSH. Після отримання доступу до цих служб зловмисники можуть завантажити на пристрій шкідливе ПЗ або отримати доступ до цінної інформації. До складних наслідків може призвести відсутність таких функцій безпеки:

1. Сервіси, що мають вразливості.

При обміні даними, пакети передаються по відповідним мережевим портам, які прив’язані до певних IP-адрес, за допомогою протоколів TCP або UDP транспортного рівня моделі OSI[31]. Всі порти, які використовуються мають шанс бути атакованими. Ризик атаки виникає на основі таких показників, як версія служби, що пов’язана з цим портом, коректність налагоджень, рівень стійкості паролю, що використовується в захищених сервісах. Всього існує 65,535 як TCP-портів, так і UDP-портів. Серед цих портів, особливу увагу слід приділити тим, які працюють з такими службами як: FTP, DNS, HTTP, Telnet, SSH, SNMP та ін.

2. Переповнення буферу обміну.

Переповнення буферу обміну – входить в список найпоширеніших типів атак в сучасному Інтернеті[46]. Принцип роботи полягає в використанні програмних помилок. З використанням цих помилок можливо досягти порушення кордонів пам’яті, викликати аварійне завершення додатків, виконати шкідливе ПЗ від імені користувача. Особливо складна ситуація у випадку, коли програма була запущена від імені адміністратора системи. Таким чином, зловмисник зможе отримати контроль над ОС жертви. Для запобігання цього, слід використовувати обліковий запис звичайного користувача, при цьому обліковий запис адміністратора варто використовувати лише у випадках, коли операції вимагають права адміністратора.

3. Відмова в обслуговуванні.

Denial of Service - атака, ціль якої будь якими силами вивести з ладу сервер[52]. Атаки цього класу не націлені на отримання певної конфіденційної

інформації, але часто використовується як основа для ініціалізації більш складної атаки.

Distributed Denial of Service - підтип DoS атаки, що має таку ж ціль, що і DoS, але для виконання застосовують не одну робочу станцію, а декілька, чи навіть мережі. Атаки цього типу націлені на використання помилок в системі, внаслідок чого атакований сервіс відмовляє в роботі і в обслуговуванні сервісу, що значно ускладнює можливість його відновлення.

Будь-яка атака на систему формує собою спробу ідентифікації вразливості системи безпеки жертви та її подальшу ініціалізацію для кінцевого отримання інформації, чи нанесення деструктивного впливу на систему. Тож успіх атаки на 50% залежить від професіоналізму зловмисника, його цілеспрямованості, та цінності інформації, і на 50% від некомпетентності системного адміністратора, чи системи безпеки в цілому.

4. Використання відкритих портів з технологією UPnP.

UPnP побудований на основі стандартів та технологій TCP/IP, HTTP і XML, його мета – швидке налагодження приватної мережі з доступом до Інтернету[47]. З використанням UPnP комп’ютери, роутери, розумні телевізори, сканери, принтери об’єднуються в одну суцільну мережу. Ця технологія забезпечує відсутність пере направлення портів при маршрутизації трафіку в мережі[48]. В більшості маршрутизаторів, така технологія ввімкнена за замовчуванням. Проте, саме зручність і є проблемою в безпеці. Завдяки цій технології будь-який прилад може підключитися до мережі та виконувати свої зловмисні дії[49].

2.2.10 Слабкий або жорстко вказаний пароль.

Використання легко зламуваних, загальнодоступних або незмінних облікових даних, включаючи бекдори у вбудованому програмному забезпеченні або клієнтському програмному забезпеченні, яке надає несанкціонований доступ до розгорнутих систем. Дивно, але до цих пір найбільшою вразливістю є використання слабких паролів, паролів за замовчуванням або паролів, злитих в мережу. Незважаючи на очевидність необхідності використання стійкого

паролю, деякі користувачі досі не змінюють паролі за замовчуванням. Цим у червні 2019 року скористалося шкідливе ПЗ Silex, яке протягом однієї години перетворило на «цеглу» близько 2000 пристроїв Інтернету речей. А до цього відомий всім ботнет і хробак Mirai встиг заразити 600 тисяч пристроїв Інтернету речей, використовуючи базу з 61 стандартних зв'язок «логін/пароль»[38].

1) Відсутність багатофакторної автентифікації.

Розширена автентифікація, метод контролю доступу до комп'ютера, в якому користувачеві для отримання доступу до інформації необхідно пред'явити більше одного «доказу механізму автентифікації». До категорій таких доказів відносять:

- Знання – інформація, яку знає суб'єкт. Наприклад пароль, пін-код.
- Володіння – річ, якою володіє суб'єкт. Наприклад електронна або магнітна карта, токен, флеш-пам'ять.
- Властивість, якою володіє суб'єкт. Наприклад біометрія, природні унікальні відмінності: особа, відбитки пальців, райдужна оболонка очей, Капілярні візерунки, послідовність ДНК.

Ще до появи комп'ютерів використовувалися різні відмінні риси суб'єкта, його характеристики[41]. Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності та вартості впровадження. Всього виділяють три фактори автентифікації:

- Фактор знання: щось, що ми знаємо – пароль. Це таємні відомості, якими повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або особистий ідентифікаційний номер (PIN). Парольний механізм може бути досить легко реалізований і має низьку вартість. Однак він має істотні недоліки: зберегти пароль в таємниці часто буває складно, зловмисники постійно вигадують нові способи крадіжки, злому і підбору паролю. Це робить парольний механізм нестійким до зламів. Більшість секретних питань, на кшталт " де ви

народилися?" – елементарні приклади фактору знань, тому що вони можуть бути відомі широкій групі людей або бути досліджені.

- Фактор володіння: щось, що ми маємо - пристрій автентифікації. Тут важливий факт володіння суб'єктом, якимось неповторним предметом. Це може бути особиста печатка, ключ від замка, для комп'ютера це файл даних, що містить характеристику. Характеристика часто вбудовується в особливий пристрій автентифікації, наприклад пластикову карту, смарт-карту. Для зловмисника дістати такий пристрій більш складно, ніж зламати пароль, а суб'єкт може відразу ж повідомити в разі крадіжки пристрою. Це робить даний метод більш захищеним, ніж парольний механізм, однак вартість такої системи більш висока.
- Фактор властивості: щось, що є частиною нас – біометрика. Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос або особливість очей. З точки зору суб'єкта, даний спосіб є найбільш простим: не треба ні запам'ятовувати пароль, ні переносити з собою пристрій автентифікації. Однак біометрична система повинна володіти високою чутливістю, щоб підтверджувати авторизованого користувача, але відкидати зловмисника зі схожими біометричними параметрами. Також вартість такої системи досить висока. Але, незважаючи на свої недоліки, біометрична система захисту залишається досить перспективним фактором.

2.3 Інциденти безпеки в сфері IoT

Розділ присвячений прикладам шкідливого ПЗ, що було створено зловмисниками для проведення атак в сфері IoT.

2.3.1Дамба Боуман-Авеню.

Дамбу Боуман Авеню (Bowman Avenue Dam) в містечку Рай-Брук побудували, щоб захистити прибережні території від повеней в період розливу річки Блайнд-Брук. Розміри цієї споруди невеликі: створ всього п'ять метрів, висота - не більше шести. Якби дамба вийшла з ладу, нічого страшного б не сталося, - хіба що підвали будинків в довколишніх кварталах затопило водою.

У 2013 році американські спецслужби виявили, що хакери зламали систему управління дамбою. Втім, ця історія практично не мала наслідків: по-перше, обладнання відключили від Інтернету на час ремонту, по-друге, навряд чи крихітну дамбу можна віднести до критичних об'єктів інфраструктури.

Місцева влада висловили припущення, що хакери атакували Боуман Авеню помилково - їх справжньою метою була велика гребля зі схожою назвою в Орегоні, яка використовується для зрошення прилеглих територій. Можливий і інший варіант: маленька дамба була для хакерів тренувальним об'єктом.

Пізніше з'ясувалося, що дамбу атакували іранські хакери, які займалися зламом банківських систем і встигли порушити роботу Citigroup, Wells Fargo, Bank of America і ще декількох фінансових організацій. Хоча їм не вдалося отримати доступ до даних клієнтів, вони успішно сповільнювали роботу сервісів або виводили їх з ладу.

Головним обвинуваченим у нападах на дамбу Боуман Авеню і банки США був названий Хамід Фіруза. Крім нього звинувачення були пред'явлені ще шістьом хакерам. Залучити злочинців до відповідальності було неможливо - Іран не видав би своїх громадян американцям, і все ж ця історія показує, що вистежити зловмисників, які орудують в віртуальному світі, цілком реально.

2.3.2 Системи екстреного сповіщення.

У квітні 2017 року близько півночі в Далласі завили півтори сотні аварійних сирен (зазвичай вони попереджають про наближення торнадо). До речі, незадовго до цього кілька будинків в місті постраждали від смерчу. Через кібератаку систему не вдалося вимкнути автоматично, - фахівцям довелося зробити це вручну.

Згодом з'ясувалося наступне. Сирени для системи оповіщення в Далласі поставляє компанії Federal Signal. Пояснюючи причини хаосу, представник міської влади мимохідь зауважив, що для запуску сирен використовується тональний код певної частоти. Зазвичай зашифровані сигнали керуючого центру передаються через метеорологічну службу за допомогою двотональних багаточастотних аналогових сигналів або аудиосигналів з частотної маніпуляцією. У Сполучених Штатах для таких цілей зарезервована частота 700 МГц.

Фахівці вважають, що хакери просто записали і відтворили аудиосигнали, які передавалися під час щомісячних тестових запусків системи. Очевидно, хакери непогано вивчили систему аварійного оповіщення і знали, на яких частотах вона працює і які коди використовує. Парадокс полягає в тому, що докладний опис роботи подібних систем можна без зусиль знайти у відкритому доступі.

Після події мер Далласа публічно пообіцяв, що винні будуть покарані, однак зловмисники так і не були знайдені.

2.3.3 Mirai ботнет, що покорив IoT.

Коли в жовтні 2016 року було опубліковано вихідний код ботнету Mirai, веб-журналісту з питань інформаційної безпеки Брайану Кребсу не довелося довго гадати на кавовій гущі, щоб передбачити: «У найближчий час Інтернет наповнять атаки нових численних ботнетів, що використовують у своїй роботі небезпечні маршрутизатори , IP-камери, цифрові записуючі пристрої та інші легкозламувані онлайн-пристрої». Як відомо, журналіст сам став однією з перших цілей ботнету Mirai. Наскільки пророкування пана Кребса виявилося пророчим?

Зараз, через три роки, можна констатувати, що ця подія мала величезний ефект, а його негативний вплив все ще продовжує стрімко зростати:

- Команда одних з кращих в області інформаційної безпеки інженерів і дослідників, які входять в групу NETSCOUT ATLAS Security Engineering &

Response Team (ASERT), за минулі три роки зуміла ідентифікувати і станом на сьогоднішній день відстежує більше 20 000 варіантів шкідливого коду Mirai[29];

- Дослідники з ASERT відзначають, що за рік частота глобальних DDoS-атак, що здійснюються за підтримки IoT-ботнетів, зросла на 39% на кінець 2019 року.
- За цей же період інженери ASERT зафіксували приголомшливе зростання на 776% числа DDoS-атак, трафік яких на своєму піку досягав швидкостей від 100 до 400 Гбіт / с.
- Також, працюючи в тісному партнерстві з компанією Reversing Labs, команда ASERT підготувала і представила графік, який ілюструє хронологію появи нових варіацій ботнету Mirai за останні три роки (рис. 2.1).

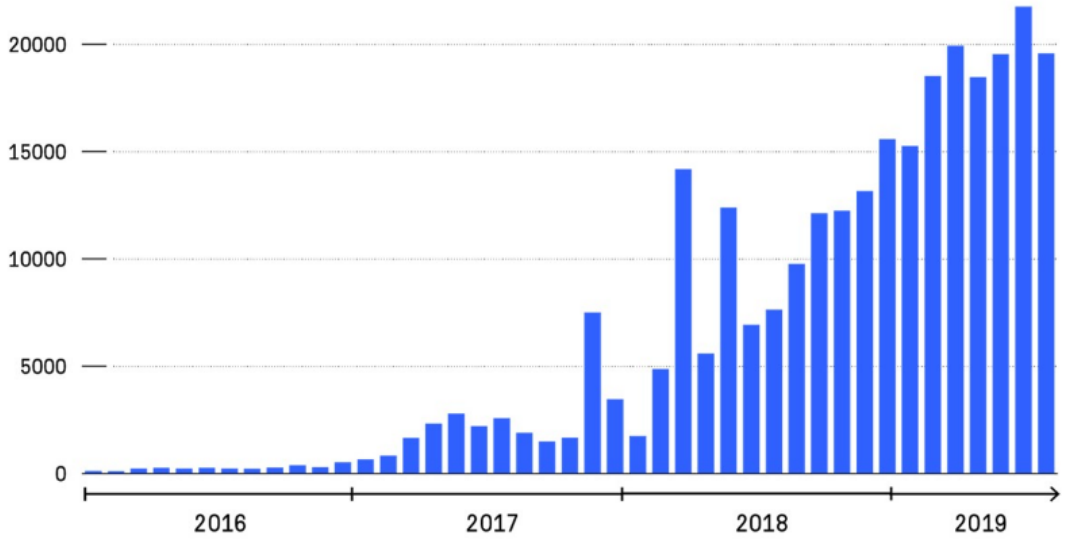

Рис. 2.1 Часова шкала появи нових варіацій ботнету Mirai протягом 2016-2019 рр.

В 2016 році ботнет Mirai, здавалося, був скрізь. Він націлювався на маршрутизатори, DVR-системи, IP-камери і багато іншого. Загалом, на все, що стосувалося Інтернету речей[30]. Ботнети працюють, заражаючи групи комп'ютерів і інших пристроїв, підключених до Інтернету, а потім змушують ці заражені машини атакувати системи або працювати над іншими цілями скоординованим чином.

Mirai пішов за пристроями з обліковими даними адміністратора за замовчуванням, або тому, що ніхто не змінив їх, або тому, що виробник жорстко закодував їх[28]. Ботнет захопив величезну кількість пристроїв. Навіть якщо

більшість систем були дуже потужними, то велике число обробників могли працювати разом, щоб досягти більшого, ніж зміг би потужний зомбі-комп'ютер самостійно.

Mirai захопив майже 500 000 пристроїв. Використовуючи цей груповий ботнет IoT-пристроїв, Mirai пошкодив сервіси, такі як Xbox Live і Spotify і веб-сайти, такі як BBC та Github, орієнтуючись безпосередньо на DNS-провайдерів. З такою кількістю заражених машин Dyn (постачальник DNS) був зупинений DDOS-атакою з трафіку об'ємом в 1.1 терабайт. DDOS-атака працює, наповнюючи ціль величезною кількістю Інтернет-трафіку, більше, ніж ціль може обробити. Це призводить веб-сайт або службу жертви до уповільнення роботи або до повного відключення від Інтернету[33].

Початкові творці програмного забезпечення Marai були арештовані, визнали себе винними і отримали умовний термін. Якийсь час Marai був вимкнений. Але достатня кількість коду вижила для інших злочинців, які перейняли Mirai і змінили його відповідно до своїх потреб. Тепер існує велика кількість варіантів Mirai.

18 березня 2019 року дослідники безпеки в Palo Alto Networks оприлюднили, що Mirai був змінений і оновлений для досягнення тієї ж мети в більшому масштабі. Дослідники виявили, що Mirai використовує 11 нових видів експорту, довівши загальну кількість до 27, і новий список облікових даних адміністратора за замовчуванням, для проби. Деякі зміни націлені на бізнес-обладнання, включаючи телевізори LG Supersign і бездротові презентаційні системи Wipg-1000.

Mirai може бути ще більш потужним, якщо він може взяти на себе бізнес-обладнання та командувати бізнес-мережами. Нові функції надають ботнету велику площу для атаки. Зокрема, наведення промислових ланок також надає йому доступ до більшої пропускної здатності, що в кінцевому підсумку призведе до більшої потужності ботнету для DDoS-атак.

Цей варіант Mirai продовжує атакувати клієнтські маршрутизатори, камери та інші пристрої, підключені до мережі. Для деструктивних цілей, чим

більше пристроїв інфіковано, тим краще. За іронією долі, шкідливий вірус був розміщений на веб-сайті, який займався просуванням бізнесу, який мав справу з "електронною безпекою, впровадженням та моніторингом сигналізації."

На даний момент до Інтернету підключено вже більше вразливих IoT-пристроїв, ніж кількість людей, що живе на нашій планеті. І число таких пристроїв збільшується щодня на 7 млн. У більшості користувачів всіх цих IoT-пристроїв - будь то домашній маршрутизатор або система відеоспостереження промислових масштабів - існує небезпечна помилкова думка про їх стан захищеності: користувачі впевнені, що IoT-пристрої можна просто підключити до Інтернету , і вони будуть безпечно працювати. Однак, реальність далека від їх наївної впевненості.

Більшість виробників IoT-пристроїв набагато більше стурбовані стратегіями виходу на ринок, ніж реалізацією в своїх продуктах надійних можливостей в сфері безпеки. В результаті більшість IoT-пристроїв все ще поставляються на ринок з попередньо встановленими іменами користувача та паролями, з включеними мережевими сервісами, які не потрібні для даних продуктів, а також великою кількістю вразливостей, виправлення для яких у вигляді оновлення програмного забезпечення з'являються дуже рідко і з великою затримкою, або взагалі не виходять.

Іншими словами, лавиноподібне поширення IoT-пристроїв для зловмисників дуже нагадує шведський стіл, де «можна брати все, що можна з'їсти». Наприклад, в першій половині 2019 року NETSCOUT honeypots (мережеві ресурси для дослідження інформаційної безпеки, що представляють собою приманку для зловмисників) зареєстрували понад 61 220 унікальних спроб, які використовували стандартні або попередньо записані облікові дані адміністратора для доставки одного з різновидів шкідливого ПЗ Mirai. Більш того, великі оператори ботнетів постійно сканують нові пристрої, що з'являються у Всесвітній мережі, і, за словами Гарі Сокрайдера (Gary Sockrider), директора з технологій безпеки NETSCOUT, новий IoT-пристрій піддається реальній загрозі

зараження шкідливим кодом Mirai або його різновидом вже протягом перших 60 секунд, після його стартового підключення до Інтернету.

Але нові IoT-пристрої - не єдине, що шукають великі оператори ботнетів у Всесвітній мережі. Вони також прагнуть використовувати недавно виявлені вразливості Інтернету речей. Багато сил направлено в DevOps і на прискорення процесу розробки. Однак зловмисники роблять те ж саме. Їх дослідники перетворюють нові експлойти в атаки на цілі протягом 5 днів .

Цілком очевидно, що найближчим часом виробники IoT-пристроїв не мають наміру істотно збільшувати інвестування в безпеку своїх продуктів. У той же час, збереження статус-кво, коли практично відсутнє керування безліччю пристроїв, здатних до міжмашинної взаємодії, що з'єднуються з системами всередині і поза мережею - це прямий шлях до катастрофи.

Головне питання, яке зараз стоїть перед IT-відділами, командами з управління мережами і службами інформаційної безпеки, полягає в наступному: як зменшити вплив атак, сила яких зростає з кожним днем? Для зменшення ризику успішної атаки варто взяти до уваги наступне:

- Покращена видимість.

Постачальники послуг висловлюють стурбованість з приводу негативного впливу DDoS-атак на основі IoT на їх мережі та їх клієнтів. Тим часом, 46% постачальників послуг навіть не здійснюють моніторинг вихідних і проміжних DDoS-атак. Відсутність видимості в цій області викликає занепокоєння, так як подібні атаки також чинять негативний вплив на агломерації маршрутизаторів користувачів і негативно позначаються на якості обслуговування клієнтів. В ідеалі, кожна організація повинна своєчасно виявляти і успішно протистояти, як вихідним і проміжним DDoS-атакам, так і вхідним DDoS-атакам.

- Сегментація мережі.

В епоху Інтернету речей сегментація мережі стає важливою як ніколи. Численні вразливі пристрої IoT примножують негативний вплив мережевих атак зловмисників і повинні бути ізольовані, щоб запобігти їх несанкціоноване

підключення з іншими системами і додатками по всій організації. Наприклад, одну частину мережі слід виділити для промислового IoT-обладнання, іншу - для систем клімат-контролю, третю - для принтерів і т. д.

- Багаторівневий захист від DDoS-атак.

Ботнети, засновані на шкідливому ПЗ Mirai, можуть використовуватися для запуску атак на рівні додатків, об'ємних атак (volumetric), націлених на переповнення смуги пропускання, а також багатовекторних атак, які можуть об'єднувати в собі кілька цілей і методів. Тому кращі практики захисту від DDoS-атак покладаються як на локальний захист від атак на рівні додатків, так і на хмарний захист від величезних об'ємних атак.

2.3.4 IoT-ботнет Dark-Nexus.

Експерти компанії Bitdefender виявили новий IoT-ботнет Dark Nexus, який атакує роутери Dasan Zhone, DLink і ASUS, а також відеорекордери, теплові камери та інші аксесуари. Ботнет існує близко року, і в даний час в його склад входять не менше 5 тисяч пристроїв, розташованих в Китаї, Південній Кореї, Таїланді, Бразилії та Росії, і які часто виступають в якості зворотних проксі[28].

Дослідники пишуть, що хоча Dark Nexus має чимало спільного з іншими ботнетами такого роду, спосіб розробки деяких його модулів робить Dark Nexus більш потужним і надійним, ніж конкуренти. Наприклад, корисні навантаження компілюються для 12 різних архітектур ЦП і динамічно доставляються в залежності від конфігурації жертви.

Відзначаючи схожість Dark Nexus з ПЗ Qbot та Mirai дослідники Bitdefender пишуть, що основні функції та модулі ПЗ все ж «в основному оригінальні» і отримують регулярні оновлення. Так, за період з грудня 2019 року по березень 2020 року було випущено більше 30 версій Dark Nexus (версії з 4.0 по 8.6).

Щоб скомпрометувати пристрій після виявлення, ботнет використовує як готові списки облікових даних, так і експлойти[40]. Для цього застосовуються

два модулі, один синхронний і один асинхронний, але обидва намагаються експлуатувати Telnet і заздалегідь складені списки облікових даних.

Щоб закріпитися на пристрої Dark Nexus використовує цікавий, на думку дослідників, підхід: спираючись на список процесів, ПЗ виробляє своєрідного роду оцінку ризиків. Таким чином, шкідливий код містить білий список процесів, включаючи їх ідентифікатори, і виходячи з цього Dark Nexus вирішує, які процеси нормальні, а які потрібно негайно перервати.

Атаки, що здійснюються цим ботнетом, в цілому досить типові, за винятком однієї команди: browser_http_req. Це складний і елемент, з можливістю налаштування, який займається маскуванням трафіку під нешкідливий, який міг би генерувати браузер.

Також фахівці помітили, що в деяких версіях ПЗ є проксі-сервери socks5, що вже зустрічалося в ботнетах, побудованих на базі Mirai, TheMoon і Gwmndy. Ймовірно, в майбутньому оператор Dark Nexus планує продавати доступ до цих проксі.

2.3.5 IoT-ботнет Ares.

IoT-ботнет Ares в основному атакує Android-приставки виробництва HiSilicon, Cubetek і QezyMedia. ПЗ не використовує будь-яких вразливостей, але заражає пристрої, доступні за допомогою налагоджувальних портів Android Debug Bridge (ADB).

Хоча за замовчуванням ADB відключений на більшості пристроїв, деякі гаджети все ж поставляються з включеним ADB (найчастіше на порті 5555). В результаті зловмисники, що не пройшли автентифікацію отримують можливість віддалено підключитися до уразливого пристрою і отримати доступ до командної оболонки ADB, яка зазвичай використовується для установки і налагодження додатків.

В даний час Ares вважається одним з найбільш активних Mirai-ботнетів.

Хоча Ares виразно намагається заражати будь-які доступні через ADB пристрої, за даними WootCloud, зараз ботнет складається в основному з вищезазначених Android-приставок (але, на думку дослідників, це може в будь-

який момент змінитися). Поки скомпрометовані пристрої використовуються лише для пошуку і зараження нових хостів і кінцева мета операторів ПЗ невідома.

Побудована на базі Mirai загроза здатна виконувати проксування трафіку, а також може використовуватися для проведення DDoS-атак. Однак вразливі Android-пристрої в корпоративних середовищах можуть стати відмінним плацдармом для хакерів і можуть використовуватися зловмисниками, як точки проникнення в корпоративні мережі.

2.3.6 ПЗ VPNFilter.

VPNFilter - це шкідливе ПЗ завдання якого інфікування мережевих пристроїв, в основному маршрутизаторів. Понад 500 тисяч пристроїв інфіковано в більш як 50 країнах по всьому світі. ПЗ виділяє серед інших модульна архітектура, здатність відновлення роботи після перезавантаження інфікованого пристрою, здійснення збору всією інформації, що циркулює в мережі, модифікація мережевого трафіку для внесення деструктивних дій.

Вивчивши поведінку цього шкідливого ПО на мережевому обладнанні, можна відзначити кілька основних особливостей даного ПЗ:

- крадіжка облікових даних веб-додатків;
- моніторинг протоколів Modbus SCADA;
- виведення пристрою з ладу.

Складність захисту і виявлення даного ПЗ обумовлена характером атакованих пристроїв - роутери і мережеві накопичувачі знаходяться на мережевому периметрі, слабо захищені і, як правило, не містять IDS / IPS-систем з огляду на технологічну простоту і обмеженість ресурсів, характерних для embedded/IoT-пристроїв.

Шкідлива програма VPNFilter являє собою модульну платформу, що складається як мінімум з двох основних компонентів: дропперу і керуючого модулю.

Після зараження пристрою на нього встановлюється так званий дроппер, здатний «пережити» перезавантаження пристрою, і завантажує на нього основний модуль.

Основний модуль, що не зберігається при перезавантаженні, може здійснювати збір файлів, виконання команд, фільтрацію даних і управління пристроями. Також деякі версії цього модулю містять функції самознищення і виведення пристрою з ладу шляхом перезапису критичних областей пам'яті мережевого пристрою.

Крім того, існує кілька допоміжних модулів, що володіють функціоналом мережевих сніфферів для збору мережевого трафіку, моніторингу протоколу SCADA Modbus, а також комунікаційний модуль для взаємодії зі зламаними пристроями через мережу Tor.

ПЗ сканує 23, 80, 2000 і 8080 TCP-порти для виявлення і атаки на нові пристрої під управлінням Linux / Busybox.

На даний момент вектор зараження і завантаження першого модуля VPNFilter не зовсім зрозумілий, але відомі деталі завантаження і управління зараженим пристроєм. Після того як шкідлива програма завершила ініціалізацію, вона починає завантажувати сторінки Photobucket.com (сайт зберігання зображень). Шкідлива програма завантажує перше зображення з галереї, на яку посилається URL, а потім переходить до вилучення IP-адреси сервера завантаження. IP-адреса витягується з шести цілочисельних значень для широти і довготи GPS в інформації EXIF.

Якщо звернутися і отримати зображення з photobucket.com не вдалося, ПЗ намагається отримати зображення з домену toknowall.com. Також існує і «запасний варіант» у вигляді прослуховувача, який очікує підключення до зараженого пристрою із застосуванням спеціалізованих тригерів.

2.3.7 Reaper.

ПЗ поширюється через експлуатацію різних вразливостей в пристроях D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys і Synology. Саме це відрізняє

Reaper від інших IoT-ботнетів, які, як правило, покладаються на Telnet-сканери та списки облікових даних за замовчуванням.

Згідно з аналізом Arbor Networks, Reaper, найімовірніше, був створений в Китаї і орієнтований на місцевий ринок, де його здають в оренду. Ботнет здатний влаштовувати SYN-, ACK- і HTTP-флуд, атаки з відображенням або посиленням через DNS і інші види DDoS.

За оцінками дослідників з компаній Qihoo 360 Netlab і Check Point, в даний час до складу ботнету входить близько 2 млн пристроїв. В основному це IP-камери, мережеві IP-відеореєстратори і цифрові відеореєстратори.

Код шкідливого ПЗ, що використовується для створення ботнету, включає фрагменти коду Mirai, але при цьому містить ряд нових функцій, що відрізняють Reaper від конкурентів. Головна його відмінність полягає в методі поширення. Якщо Mirai шукає відкриті Telnet-порти і намагається скомпрометувати пристрій, використовуючи перелік поширених дефолтних або ненадійних паролів, то Reaper в основному застосовує експлоїти для захоплення контролю над уразливими пристроями і додавання їх до C&C-інфраструктурі.

В даний час Reaper використовує експлоїти для вразливостей в пристроях D-Link (моделі DIR-600 і DIR-300), маршрутизаторах і системах відеоспостереження Netgear (ReadyNAS Surveillance, DGN1000, DGN2200), маршрутизаторах Linksys (моделі E1500 / E2500), IP-камерах GoAhead, JAWS, Vacron і AVTECH. Reaper також атакує маршрутизатори MicroTik і TP-Link, мережеві накопичувачі Synology NAS і сервери Linux.

На даний момент організатори ботнету працюють над його розширенням, додаючи нові експлойти і пристрої. За словами експертів Qihoo 360 Netlab, списки очікування C&C-серверів ботнету включають понад 2 мільйони інфікованих гаджетів.

Поки ботнет не здійснив жодної DDoS-атаки. ПЗ включає середовище для виконання скриптів на мові Lua, що дозволяє операторам додавати модулі для різних завдань, наприклад, DDoS-атак, перенаправлення трафіку та ін. Крім того,

Reaper включає 100 відкритих DNS-резолверів. Дана функціональність дозволить ботнету з легкістю здійснювати атаки типу DNS-ампліфікація.

2.3.8 GhostDNS.

ПЗ формує ботнет, який зламує роутери зі слабкими паролями і перенаправляє своїх жертв на підроблені банківські ресурси. За допомогою фальшивих сторінок зловмисники прагнуть отримати реєстраційні дані і реквізити жертви, щоб викрасти гроші з рахунку.

Скрипт змінює дані DNS в налаштуваннях маршрутизатора, і всякий раз, коли користувач намагається перейти на сайт однієї з фінансових установ країни, він опиняється на фішинговому ресурсі злочинців. Шкідлива мережа складається з декількох.

GhostDNS структура включає в себе понад 50 сайтів мета яких – підміна оригінальних сайтів банківської інфраструктури. Також, в своєму розпорядженні GhostDNS має модулі для обходу системи захисту роутерів звичайних користувачів, структуру шкідливих DNS-серверів, інтерфейс для керування та планування атак. ПЗ здатне проникати в прошивку більше маршрутизатора та використовувати зламаний пристрій для ідентифікації та реалізації нових жертв. Кількість моделей які схильні до атаки перевищує 70 різних пристроїв.

Під час проведення атаки на підміну DNS-серверу, відвідувачеві фішингового сайту дуже складно визначити підробку. Це пов’язано з тим, що сторінка-підробка відображає ту ж саму адресу, що і оригінальний ресурс. Незалежно від додатку, що використовується для встановлення з’єднання , маршрутизатор завжди буде перенаправляти користувача на сайт злочинців.

Для даного ботнету характерні такі складові:

- Shell DNSChanger. Це система, задача якої пошук відкритих портів, та використання shell-макросів, які можуть виконувати підбір паролів та ре конфігурацію налаштувань маршрутизатора. Після виявлення, скрипт використовує метод брутфорсу для зламу пристрою.

- Js DNSChanger. JavaScript-модуль для підміни адреси DNS-сервера на маршрутизаторі жертви, пошук решти пристроїв, що знаходяться в локальній мережі. В разі знаходження таких пристроїв, скрипт відправляє payload на цей пристрій та намагається взяти його під контроль.
- PyPhp DNSChanger. Набір створений за допомогою мов програмування Python та PHP та використовується в центрі керування та планування атак. Даний набір скриптів був завантажений на більше ніж сотню серверів хостингу Google Cloud. PyPhp DNSChanger має сканер, який користується ресурсами Masscan та Shodan. Для використання API Shodan, зловмисники викрали ключ одного з дослідницьких проектів Github. Набір скриптів налічує в собі 69 скриптів для проведення процедури зламу близько 50 різних маршрутизаторів.

2.4 Загрози інформації, що циркулює в пристроях IoT

Пристрої Інтернету речей часто стають об’єктами для отримання НСД до персональних даних користувачів. У зв’язку з високим рівнем інтеграції таких пристроїв у повсякденне життя людей, вони мають змогу отримувати та оброблювати великий обсяг конфіденційної інформації[28]. Враховуючи той факт, що рівень захисту такої інформації в об’єктах IoT досить часто вимагає уваги, то імовірність викрадення таких даних – висока. Зловмисники, або компанії які отримали цю інформацію, мають можливість використовувати її для власних потреб.

2.4.1 Мобільні додакти, як агенти збору інформації.

Карта активності The Global Heat Map, що була складена компанією Strava на основі даних фітнес-трекерів, розкрила місцезнаходження військових баз США. В таких зонах бойових дій, як Сомалі, Сирія, Ірак, Афганістан, Джибуті

карта активності цілком темна, тобто така, що не відображає інформації, за виключенням кількох окремих місць. Мова йде, саме про місця розміщення американських військових. Журналісти виявили на мапі як вже відомі бази, так і координати нових, які спецслужби намагалися зберегти в тайні.

Strava – це мобільний додаток для відстеження тренувань за допомогою GPS та соціальна мережа для тих, хто займається фітнесом. Користувачами Strava являються близько 27 мільйонів людей по всьому світі, включно з користувачами популярних фітнес-трекерів Fitbit та Jawbone.

Карта The Global Heat Map була опублікована в листопаді 2017 року, вона складена на основі даних, отриманих протягом 2015-2017 років (Рис. 2.2).

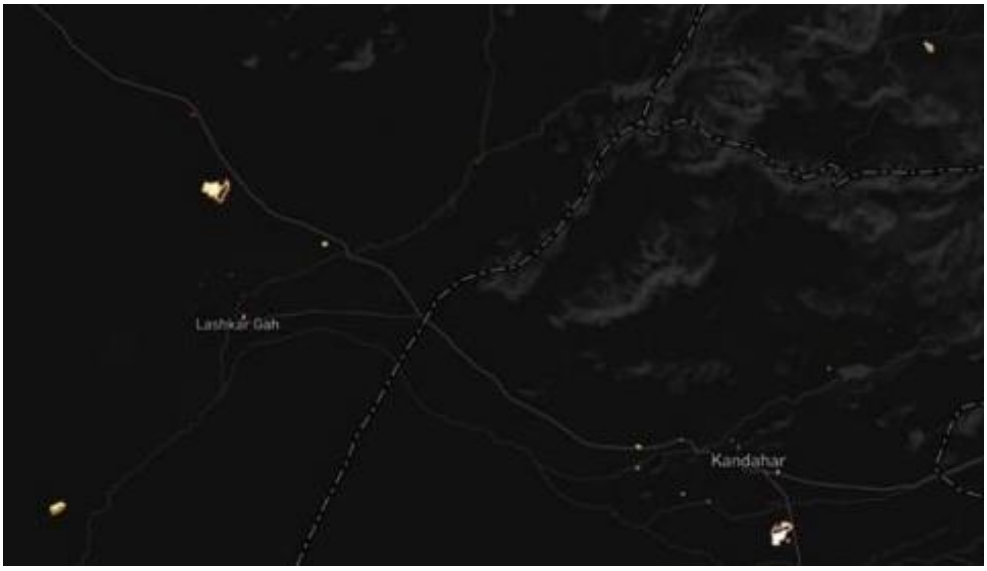

Рис. 2.2 Карта активності користувачів Strava

2.4.2 Годинники-шпигуни.

Додаток від компанії Nibaya став причиною шпигування за дітьми та нападів на них. Серйозна вразливість була виявлена в дитячих годинниках TicTocTrack, яка дозволяла отримати доступ до місцезнаходження годинника,вбудованого мікрофон. Для «повноцінного» користування годинником необхідно було встановити додаток. З його допомогою батьки мали змогу отримати інформацію про місцезнаходження дитини, послати сигнал тривоги чи використовуючи мікрофон, прослухати, що відбувається поряд з годинником. Однак, ніхто не врахував сценарію, за яким зловмисник отримує доступ до годинника на рівні зі справжніми батьками. Зловмиснику достатньо

створити обліковий запис TicTocTrack та використовувати запити до кінцевих точок OData. Відсутність якісної перевірки команд, що поступають до сервера дає змогу отримувати доступ до даних різних облікових записів та модифікувати їх.

2.4.3 Вразливості «Смарт-TV».

Телевізори компанії Sony під керуванням ОС Android, отримали діру в захисті в вигляді двох вразливостей додатку Photo Sharing Plus в Sony Smart TV[20]. Додаток призначений для обміну фотографіями та мультимедійним контентом між смартфоном та телевізором:

- CVE-2019-11336 – дає змогу в обхід авторизації отримати доступ до паролю точки доступу Wi-Fi, яка створюється під час запуску додатка Photo Sharing Plus; Точка доступу необхідна для підключення користувачів, які бажають виконати процес обміну або демонстрації медіа контенту. Зловмисник може отримати пароль з журналів логування API Photo Sharing Plus. Доступ до API легко отримати використовуючи домашню або корпоративну мережу.
- CVE-2019-10886 – зловмисник має змогу переглянути вміст файлів, що містяться в пам'яті пристрою використовуючи штатне ПЗ. За стандартними налаштуванням файли зберігаються в директорії «/data/user/0/com.sony.dtv.photosharingplus/files /». Розширює спектр вразливості можливість отримати доступ до кореневого каталогу та файлів, включно з інформацією про пароль використовуючи веб-адресу "http://[ip_tv]:10000/ contentshare/image/".

Обидві вразливості надають можливість як отримати конфіденційну інформацію так і завантажити шкідливе ПЗ до системи.

2.4.5 Бортові системи автомобіля.

Відмички та розбите скло - це вже в минулому. Сьогодні для зламі автомобілів все частіше використовуються ноутбуки та спеціальне комп'ютерне обладнання.

Автомобільна кіберзлочинність зростає просто-таки загрозливими темпами. Наприклад, в Лондоні в минулому році зловмисники, зробивши дублікат радіо-брелок для розблокування іммобілайзера, викрали понад 6000 автомобілів. Кількість викрадень з використанням високотехнологічних засобів збільшується пропорційно тому, як машини «розумнішають»[23].

Ось кілька прикладів того, як зараз хакери можуть зламати і викрасти автомобіль:

- У квітні цього року американцеві вдалося викрасти машину всього за 12 хвилин. Причому він це зробив за допомогою ноутбука. Зловмисник розкрив автомобіль і завів мотор, використовуючи ноутбук і спеціальний електронний пристрій. Він просто підійшов з ноутбуком і якимось невідомим пристроєм до машини, розкрив її, сів і поїхав. Вся процедура зайняла 12 хвилин. Відео викрадення автомобіля було опубліковано поліцією Х'юстона. При цьому організація Crime Stoppers пообіцяла 5 тисяч доларів тому, хто допоможе затримати хакера.
- Слід зазначити, що зловмисникам зовсім не обов'язково перебувати біля автомобіля при його зламі. У лютому цього року одному хакеру вдалося зламати авто, яке перебуває на іншому континенті.
- Хакери періодично доводять, що можуть зламати навіть самі високотехнологічні автомобілі. Так, влітку 2014 року на симпозіумі з інфобезпеки команді китайських студентів вдалося з легкістю зламати самий технологічний і просунутий автомобіль сучасності - електрокар Tesla Model S. За допомогою спеціальних засобів вони увійшли в бортовий комп’ютер машини і почали керувати склопідйомниками, блокуванням дверей і клаксоном. При цьому електрокар знаходився в русі. Студенти не стали керувати мотором і гальмами, але показали, що і це цілком можливо.
- У США хакерам вдалося перехопити управління рухомим на швидкості 110 км/год Jeep Cherokee через Інтернет. Вони змусили працювати омивачі, кондиціонер і радіо. У рухомому автомобілі несподівано ввімкнувся

кондиціонер, а радіо саме налаштувало якусь хіп-хоп-станцію. Потім включилися двірники. Програмісти також показали, що можуть заглушити мотор, відключити гальма і заблокувати машину. Це був експеримент, в кінці якого на екрані бортового комп'ютера з'явилися усміхнені обличчя зломщиків. Хакери просто хотіли довести вразливість сучасних авто. Але потенційна ймовірність справжнього злому виявилася настільки високою, що виробник вирішив відкликати понад 1,4 млн. Автомобілів для виправлення уразливості.

2.4.6 Порушення кордонів безпеки мережі, шляхом використання IoT-об’єктів.

Акваріум, обладнаний комплексом розумних пристроїв для вимірювання температури, рівня солоності води, та системою годування рибок став об’єктом атаки зловмисників[22]. В межах казино, з’єднання з автоматизованою системою акваріуму було виконане на основі VPN-з'єднання, відокремлене від решти мережі. Хакери атакували досить незвичний для казино пристрій, отримали помилку в програмному коді та скористалися нею для обходу традиційних засобів захисту казино. Це дозволило зловмисникам закріпити факт своєї присутності в системі та почати її сканування. За результатами сканування – вони виявили нові діри в безпеці і скористалися ними. Таким чином, хакери вийшли за межі ізольованого VPN-з’єднання та проникли в локальну мережу казино, після чого викрали базу даних з VIP-гравцями закладу.

2.4.7 Вороги в домі.

Побутова техніка в сфері IoT одне з найпоширеніших її явищ, а отже – одне з найслабкіших місць в безпеці. Платформа LG SmartThinQ на основі штучного інтелекту, головна ідея якої підвищення комфорту життя користувачів за рахунок здатності віддаленого керування домашньою технікою та системою в цілому[26]. Однак саме цю платформу спіткала вразливість під назвою HomeHack. Даний тип вразливості можливий за рахунок використання мобільних додатків LG SmartThinQ. Вразливість дає змогу отримати контроль над реальним обліковим записом користувача системи, а разом з тим і над всіма об’єктами які знаходяться в системі LG SmartThinQ[27]. Таким чином, досить

легко отримати зображення з камери розумного пилососа, отримати персональну інформації від всіх побутових предметів які беруть участь в платформу.

Проте завдяки оперативним діям, компанії LG, платформа LG SmartThinQ швидко обзавелася оновленням, яке виправляло дану вразливість. Але важливим фактом варто відмітити те, що оновлення необхідно встановлювати в ручному режимі, а отже деякі пристрої можуть досі мати вразливість, через неуважність користувачів.

2.4.8 Викинутий – не означає безпечний.

Досить часто пристрої Інтернету речей після того, як вони виходять з ладу, або втрачають свої функції за певних обставин і не мають можливості їх відновити – просто викидають на смітник[45]. Але хто задумується про те, чи правильно вони чинять з точки зору інформаційної безпеки? Після того, як пристрої опинилися на смітнику, вони все ще можуть зберігати інформацію про користувачів, про мережі в яких вони знаходилися, певні зашифровані або відкриті дані. Таким чином, зловмисник має змогу отримати інформацію без особливого втручання в цільову систему або життя жертви.

Експеримент компанії Limited Results довів, що просто списати пристрій – безвідповідально. В якості об’єкту використовували розумну лампу компанії LIFX. Розумною, її визначають такі можливості як повне керування за допомогою смартфона та можливість зміни «температури» світла. Лампу підключили до бездротової мережі, залишили на певний час, а потім вимкнули та демонтували корпус. Аналіз інформації, яка лишилася в пам'яті неробочої лампи, дав можливість зрозуміти, що навіть в такому стані – лампа зберігає дані. Такими даними виступили пароль від точки доступу Wi-Fi, до якої підключалась лампа, приватний RSA-ключ та навіть кореневий сертифікат.

Легко зрозуміти, за результатами експерименту, що такі вразливості властиві різним об’єктам IoT.

2.5 Висновки за другим розділом

Особливість сфери IoT полягає в тому, що разом з комфортом в життя людини, вона приносить небезпеку. І коли мова йде про небезпеку, то це справді, небезпека для життя людини. Якщо раніше кібератаки могли спричинити деструктивні дії наслідками яких були фінансові або матеріальні збитки, то з повсюдним використанням продуктів IoT загрозі піддається життя. Усвідомлюючи такий рівень відповідальності, компанії-виробники повинні ставитися з надзвичайною відповідальністю до своїх продуктів, а саме до функцій безпеки.

Знайти експлойти які необхідні для того, щоб скористуватися вразливістю якогось елемента побутової техніки, електричного автомобіля чи навіть кардіостимулятора – простіше простого. В наш час, хакери не лише створюють експлойти для наживи, а й згодом, поки вразливість актуальна, публікують їх у вільний доступ. Таким чином, загрози безпеці сфери IoT виходять за рамки віртуального світу і здатні причинити безпосередньо фізичний вплив. Завдяки поширенню цього явища, досить скоро такий вид тероризму, як кібернетичний буде з’являтися на перших шпальтах газет, частіше ніж звичайний тероризм.

Завдяки спільноті OWASP, було сформовано список найбільш потенційних проблем в сфері інформаційно-комунікаційної безпеки пристроїв Інтернету речей. Завдяки цьому вдалося визначити напрямки для вирішення можливих вразливостей та загроз.

В даному розділі продемонстровано небагато загроз, із тих що існують насправді, але вони властиві пристроям IoT. Приклади є аргументом того, що будь який пристрій, який має підключення до мережі Інтернет може стати точкою входу для зловмисника.

Інциденти кібербезпеки, що наведені в даному розділі атестаційної роботи, мали лише матеріальні, репутаційні та фінансові збитки, а також витоки конфіденційної інформації. Насправді, враховуючи беззаперечні факти існування терористичних угрупувань, наслідки майбутніх кібератак будуть

вимірюватися в кількості жертв. Адже широкий спектр застосування продуктів IoT в таких галузях, як медицина, промисловість та транспорт без належного забезпечення захисту може призвести до людських жертв.

Окрему увагу потрібно приділити питанням збору конфіденційної інформації виробниками смарт-пристроїв. Завдяки таким виробникам, досить часто інформація опиняється в руках третіх осіб або в руках хакерів.

Для попередження атак та ліквідування наслідків цих атак на проекти IoT (як на самі пристрої, так і на цілі мережі та інфраструктури) необхідно створити систему рекомендацій стосовно дій для забезпечення необхідного рівня захисту. Дана система враховує всіх учасників взаємодії з об’єктами IoT, як виробника так і кінцевого користувача. Наступний розділ містить інформацію про основні причини слабкого захисту об’єктів IoT та розподілену систему рекомендацій для підвищення рівня захисту.

РОЗДІЛ 3. БЕЗПЕКА ІНФОРМАЦІЇ В ОБ’ЄКТАХ IOT

Основа будь яких елементів безпеки полягає в визначенні причин та факторів, які являються визначними для рівня безпеки, аналізуванні та дослідженні причинно-наслідкових зв’язків в кібератаках на проекти IoT, які завершились успіхом. Враховуючи всі ці аспекти, необхідно створити ефективну

систему рекомендацій, застосування яких вирішить проблему низького рівня захищеності.

3.1 Головні причини слабкого захисту фізичних об’єктів IoT

Сьогодні, більшість виробників приділяє увагу функціоналу своїх пристроїв, для надання максимального спектру послуг, але не звертає достатньої уваги на питання, які стосуються механізмів захисту як пристроїв, так і користувачів. Це пов’язано з прагненням компаній максимально мінімізувати витрати на виробництво.

Компанії слідкують ідеології постійного оновлення, знову і знову ті ж самі пристрої з тим самим функціоналом випускаються в новій «обгортці» без суттєвих змін, але якщо вони є, то точно не в площині безпеки пристрою. Лише великі агломерати виробників здатні застосовувати хоч мінімальні елементи захисту, оскільки для цього потрібно часові та грошові ресурси у великих обсягах. Тому, для існування на ринку, виробники використовують компоненти та складові, які виготовлені різними виробниками:

- Процесори;
- Камери;
- Датчики;
- Модулі зв’язку;
- Накопичувачі і т.д.

Будь-який компонент в пристрої, який зібрано подібним чином, може містити вразливість, але відомо про неї буде, лише коли пристрій зійде з конвеєра, це в гіршому випадку. В кращому – пристрій проходить етап тестування. Протягом кількох тижнів, пристрій тестують у відповідних лабораторіях вивчаю всі можливі недоліки як в апаратному, так і в програмному

спектрі. Однак, через конкуренцію на ринку, виробник поспішає відправити товар на «прилавок», жертвуючи процедурою тестування.

Досить часто, час від розробки концепції пристрою та до його впровадження в використання складає від 2х до 4х місяців, в такі терміни – технічно неможливо виконати повноцінну перевірку та тестування.

До 90% пристроїв під час аналізу експертами, виявилися недостатньо захищеними[21]. Вирішити це питання неможливо, в зв'язку з тим, що виробник, чи компоненту, чи пристрою до якого він входить, не випускає ні функціональних, ні таких, що стосуються систем безпеки оновлень. Але якщо і випускаються такі оновлення, то сама процедура, досить часто несе в собі загрозу:

- Користувач може не знати про оновлення;
- Оновлення може бути встановлено лише в ручному режимі;
- Під час оновлення може виникнути збій, який виведе пристрій з ладу;
- Оновлення можуть погіршити роботу тих, чи інших компонентів пристрої, що вимагає або відновлення попередньої прошивки, або терміновий випуск наступного оновлення.

3.2 Необхідні складові успішних атак на проекти IoT

Виконавши детальний аналіз випадків кібератак на проекти в яких використовувалися об'єкти та механізми Інтернету речей в другому розділі атестаційної роботи, я маю можливість виокремити конкретні аспекти, що відіграли важливу роль при інфікуванні, компрометації та внесенні деструктивних дій, що властиві об'єктам, які виступили в ролі цілей для атак:

- Стандартна або не стійка до зламу пара «логін/пароль». Даний фактор є одним з найбільш розповсюджених, оскільки саме завдяки такій вразливості та методу брутфорсу паролів, був розповсюджений один з найбільш небезпечних та відомих на сьогоднішній день ботнетів Mirai. В 6 з 10 випадків, користувачі залишають стандартні налаштування облікового запису користувача пристрою, або ненавмисно випускають цей момент з огляду, що дає можливість зловмиснику використовувати базу стандартних даних облікових записів при процедурі зламу[37]. Бази таких зв'язок в формі «логін/пароль» є у вільному доступі в мережі Інтернет, при чому їхня кількість постійно зростає. Більше того, під час масштабних витоків баз користувачів різних сервісів, втрачені дані у вигляді «логін/пароль» часто потрапляють до таких «словників» для використання в майбутньому. Решта 4 з 10 випадків поділяються на два типи:

  - Перший – успішний, користувач розуміє важливість інформації та забезпечення її захисту і встановлює надійний пароль та логін.
  - Другий – безнадійний, користувач встановлює пароль, але настільки слабкий, що для зловмисника, він не становитиме жодної проблеми, під час спроби зламу.

Ще гірше в даному випадку, коли обліковий запис користувача і обліковий запис адміністратора, є одним і тим самим. Таким чином, дуже просто отримати цілковитий доступ до всіх систем пристрою та його ПЗ.

- Недоліки ПЗ та помилки в програмному коді. Такий фактор, стоїть одразу після фактору не стійких до зламу зв'язок «логін/пароль». Досить часто при проектуванні програмної складової пристрою, виробник намагається заощадити на функціях та механізмах безпеки заради високої енергоефективності, більшого об’єму пам'яті або вищої швидкодії ніж у конкурентів. Велика доля пристрої IoT замість захищеного протоколу HTTPS, використовує HTTP для зв’язку між пристроєм та веб-інтерфейсом керування, при цьому протокол HTTP є цілком незахищеним на сьогоднішній день та застарілим. Таким чином, виробник цілком свідомо наражає своїх користувачів та клієнтів на небезпеку[45].

Більшість шкідливих ПЗ були розроблені за таким набором функціоналу, який повністю відповідає відомими програмним помилкам та недолікам у певних моделях та версіях пристроїв. Це дає змогу автоматично використати даним ПЗ всі знайдені вразливості та отримати необхідний для зловмисника доступ до пристрою. Дана процедура вимагає високого рівня як програмних так і технічних навичок злочинця.

- Складність або неможливість оновлення ПЗ та ОС і при цьому відсутність підтримки з боку виробника для усунення загроз і вразливостей. Досить часто користувачі ігнорують оновлення своїх пристроїв в площині як програмного забезпечення так і операційної системи в цілому[58]. В зв'язку з цим, велика кількість пристроїв залишається незахищеною навіть, якщо виробник надає оновлення безпеки. Відсутність системи автоматичних оновлень компонентів суттєво підвищує ризики успішного проведення атак. Оскільки досить часто, фізичні об'єкти можуть знаходитись в таких місцях, в які людині складно потрапити, для запуску або повноцінного керування процедурою оновлення. Більше того, користувач може навіть не здогадуватися, як про те, що його пристрій має вразливість і знаходиться в небезпеці, так і про те, що виробник надав оновлення для вирішення цієї вразливості. Враховуючи це, масштаби наслідків зростають надзвичайно швидко у випадку, якщо подібне станеться в об'єктах критичної інфраструктури. Оскільки навіть декілька секунд недієздатності пристрою, можуть спричинити як фінансові збитки, так і спричинити поламки обладнання та інші надзвичайні ситуації. А якщо до цього, ще додати час необхідний на відновлення роботи пристрою, його оновлення та повторний запуск в роботу, то зловмисник матиме можливість «рухатися» далі по об'єктам структури.

- Відсутність системи шифрування та використання застарілих протоколів. Досить часто, з метою тієї ж економії, виробники обирають компоненти з метою забезпечити мінімальний набір необхідних функцій пристрою, таким чином, пристрої мають досить обмежені в продуктивності

апаратні можливості. Особливо, якщо порівнювати з сучасними персональними комп’ютерами, планшетами та смартфонами. Для застосування достатньо криптостійкого шифрування, такого як AES-128 чи AES-256, пристрій не зможе ані нормально виконувати свої функції, ані провести процедуру повноцінного шифрування даних. В зв’язку з цим, виробники не вносять системи захисту даних на основі криптографічних перетворень до списку мінімально необхідних функцій та можливостей пристрою. Або все ж таки вносять, але не без «ложки дьогтю» - використовуються одні з найпростіших алгоритмів. Вони дуже легко піддаються зламу і таким чином, хоч і є видимість захисту, але насправді захист відсутній.

- Конфігурація мережі, що сповідує ідеологію відкритих портів. За таких налаштувань, зловмисник виконуючи сканування, дуже легко знайде лазівку в елементах безпеки і отримає доступ як до веб-інтерфейсу, так і до портів, які використовуються для віддаленого службового адміністрування пристрою[50]. Навіть при використанні міжмережевих екранів, пристрій не буде захищено, якщо до такої конфігурації додати нестійкі «логін/пароль». В разі, якщо зловмисник отримав доступ до одного з пристроїв мережі, є великий шанс, що він має змогу отримати доступ і над іншими пристроями, виконати сканування всіх об’єктів мережі та продовжити атаку на сумісні частини мережі або іншу віддалену ціль[51].

Таким чином, ми розуміємо які особливості варто взяти до уваги проаналізувавши основні вектори атак на пристрої IoT, це дає нам можливість перейти до наступного кроку – формування системи рекомендацій. Однак варто враховувати, що вирішення проблем в площині безпеки пристроїв лягає не лише на плечі користувачів, а й виробників. Отже система має враховувати цей факт, тож і складатися вона буде з двох категорій рекомендацій: рекомендації з використання та необхідних дій для забезпечення необхідного рівня безпеки конфіденційних даних та унеможливлення НСД для користувачів (до групи

користувачів входять як фізичні, так і юридичні особи) та категорія рекомендацій присвячена для виробників об’єктів IoT.

3.3 Блокчейн як спосіб захисту інформації в об’єктах Інтернету речей

Оскільки кожен пристрій Інтернету речей є потенційною точкою входу для зловмисників, то порушення безпеки може привести до витоку конфіденційної інформації в великих масштабах або зробити пристрої Інтернету речей уразливими до кібератаки.

Рішенням проблеми безпеки пристроїв Інтернету речей може стати блокчейн. Ця революційна технологія є різновидом розподіленого реєстру і найбільшою мірою відома як основа криптовалюти біткойн. Блокчейн автоматично використовуючи технологію децентралізації зберігає дані в різних місцях, а не в одному центральному сховищі, завдяки чому забезпечується більш високий рівень захисту цих даних[63].

Результатом об'єднання цих двох передових технологій стала поява Інтернету речей на базі технології блокчейн (Blockchain Internet of Things), який також називається BIoT. Інтеграція технології блокчейн в пристрої Інтернету речей дозволяє знизити ймовірність хакерської атаки завдяки зменшенню кількості потенційних точок входу. Оскільки блокчейн усуває необхідність в інтеграції головного управління в мережі Інтернету речей, такі мережі можуть захищати себе самі. Пристрої Інтернету речей, об'єднані в одну групу, можуть автоматично припиняти роботу або відправляти повідомлення користувачам, якщо їм необхідно виконувати підозрілі завдання, які виходять за рамки їх звичайного функціоналу. В результаті це може істотно знизити ймовірність атак на пристрої Інтернету речей[64].

Крім того, крім зменшення кількості потенційних точок входу для хакерів, BIoT також веде захищений від НСД запис всіх дій, які можна легко відстежувати вздовж всього ланцюжка. Використання шифрування і розподіленого реєстру не дозволяє користувачам змінювати записи, так що ця технологія особливо корисна компаніям, бізнес яких пов'язаний з фінансовими операціями, аудитом і моніторингом ланцюга постачань. Такий рівень прозорості також робить блокчейн оптимальним рішенням для розумних контрактів, оскільки ця технологія дозволяє автоматично оформлювати угоди при виконанні певних умов, наприклад після прибуття відправлення в пункт призначення. Крім того, технологію блокчейн можна використовувати в розумних містах для захисту різних пристроїв (наприклад, підключених вуличних ліхтарів).

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 та 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.

В найближчому майбутньому з'являться різні 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.

Цілком ймовірно, що BIoT стане частиною стратегії по захисту пристроїв Інтернету речей в найближчі місяці і роки. Об'єднання технології блокчейн і Інтернету речей посприяє максимальному розкриттю потенціалу останнього завдяки зменшенню властивих йому ризиків безпеки і дозволить організаціям освоювати інноваційні бізнес-моделі.

3.4 Основні засоби захисту об’єктів IoT

Базуючись на класифікацій вразливостей та загроз, наведеній в попередніх пунктах, можна сформувати наступні класи категорій системи рекомендацій для максимального зниження ризиків імовірності реалізації загроз та використання вразливостей. Відповідно до категорій вразливостей, що були розглянуті в 2-му розділі виконано класифікацію контрзаходів:

1 клас. Відсутній захист веб-інтерфейсу:

- Зміна всіх стандартних логінів та паролей користувачів, якщо їх декілька, під час першого налаштування перед початком роботи;
- Створення веб-інтерфейсу з заздалегідь продуманим внутрішнім кодом, для уникнення можливостей використання ін'єкцій таких видів: SQL, SQLi, XSS, Xpath, CRLF, LDAP, XXE;
- Використання таких облікових даних, які не мають впливу з внутрішнього чи зовнішнього трафіку мережі.
- Використання надійних механізмів відновлення облікового запису та окремо паролю, для ліквідування можливості отримати інформацію про актуальний обліковий запис зловмисником[59];

- Використання системи перевірки стійкості паролю або жорстке введення правил до формування паролів;
- Введення системи блокування користувачів, шляхом блокування їх облікових записів після виявлення 3 невдалих спроб входу до системи керування.

2 клас. Слабкий механізм або відсутність автентифікації/авторизації:

- Вживання лише стійких паролів;
- Використання системи ролей користувачів для контролю та заборони доступу до функцій;
- Забезпечення достатнього рівню захисту акаунтів користувачів;
- Використання дво- або багато-факторної автентифікації;
- Використання безпечної системи відновлення паролю;
- Використання системи повторної перевірки та автентифікації користувача для надання доступу до критично важливих функцій або налаштувань об’єкта[60];
- Можливість налаштування параметрів управління паролями.

3 клас. Небезпечні мережеві сервіси:

- Підтримка робочого стану лише необхідних для повноцінної роботи об’єкта мережевих портів;
- Використання сервісів, стійких до атаки переповнення буферу обміну;
- Використання служб, стійких до Dos та DDoS атак;
- Вимкнення функцій UPnP для обмеження можливих підключень до мережі Інтернет.

4 клас. Відсутність шифрування в процесах передачі та збереження даних:

- Використання актуальних версій протоколів SSL / TLS для шифрування даних;
- Використання актуальних версій інших протоколів, стійких до зламу в разі неможливості використання SSL / TLS;

- Використання лише сертифікованих стандартів та алгоритмів шифрування та відмова від застосування «самописних» протоколів.

5 клас. Недостатній рівень захисту конфіденційності:

- Дозволяти збір лише тих даних, від яких залежить нормальна робота пристрою;
- Забезпечення шифрування зібраної інформації для збереження в межах пристрою;
- Забезпечення високого рівня захисту конфіденційної інформації, що збирається пристроєм, впродовж всього часу її життя в межах всієї інфраструктури проекту IoT;
- Надання доступу до конфіденційної інформації лише особам, які мають на це повне право.

6 клас. Відсутність можливості керувати пристроєм:

- Використання систем моніторингу за процесами;
- Забезпечення можливості безпечного виведення пристрою з експлуатаці;
- Надання можливості перевірки цілісності та легітимності завантаженого ПЗ;

7 клас. Використання небезпечних чи застарілих компонентів:

- Перевірка всіх програмних компонентів на цілісність та актуальність;
- Перевірка всіх апаратних компонентів на відсутність вразливостей;
- Виключення можливості вказати такі налаштування системи, які можуть бути небезпечними для неї.

8 клас. Виключення можливості небезпечної конфігурації безпеки:

- Розмежування привілеїв за допомогою системою ролей для користувачів та адміністраторів;
- Застосування систему ведення журналів подій, легування;
- Застосування системи сповіщення та моніторингу подій безпеки;

9 клас. Недостатній захист ПЗ та прошивки пристроїв:

- Шифрування файлів оновлення;
- Введення системи автоматичного оновлення пристрою;
- Регулярна перевірка оновлень;
- Використання зашифрованого з’єднання між пристроєм та точкою надання оновлення;
- Перевірка файлів оновлення на цілісність та легітимність перед встановленням;

10 клас. Недостатній рівень фізичної безпеки:

- Використання можливостей для блокування фізичного доступу до пристрою за виключенням легітимних користувачів;
- Використання носіїв даних, стійких до знищення;
- Використання системи шифрування даних;
- Фізичне блокування USB-портів які не є необхідними для роботи пристрою;

3.5 Рекомендації, щодо надання достатнього рівня захисту об’єктів IoT від кібератак

Існує 4 підходи для забезпечення безпеки Інтернету речей:

- Безпека пристроїв.

Використання апаратних та фізичних засобів забезпечення цілісності як ПЗ, шляхом використання шифрування та криптографічних сертифікатів, так і цілісності «тіла» пристрою контролюючи фізичний доступ до нього.

- Контроль пристроїв.

Використання автоматизованих систем оновлення, для регулярної перевірки їх наявності та цілісності перед встановленням. Для оновлення використання захищених ліній зв’язку, бажано бездротових.

- Безпека взаємодій і зв'язку.

Використання технологій шифрування даних та каналів передачі інформації.

- Контроль взаємодій.

Застосування систем моніторингу, сканування, легування та аналітики подій та процесів в режимі реального часу[61].

Першочергові дії, що необхідні, для налаштування інформаційної безпеки об’єкту на початку його введення та використання є такими:

- Виконання перевірки об’єктів на наявність вразливостей системи безпеки, в разі її існування в апаратній та програмній складовій;
- Створення набору мінімально необхідних стандартів безпеки для всіх об’єктів, що входять в межі структури, їх подальше вдосконалення та документація;
- Застосування створених стандартів протягом всіх процесів виробництва та обслуговування об’єктів;
- Імплементація достатнього рівня безпеки об’єктів до життєвого циклу рішення, під час процесу розробки;
- Виявлення та аналіз критично важливих інформаційних ресурсів;
- Застосування в роботі систем сповіщення, моніторингу подій та реагування;
- Застосування технологій захисту на основі IPS/IDS;
- Формування списку дій та інструкцій для ліквідації наслідків інцидентів безпеки.

Процес повноцінного захисту інфраструктури проекту IoT вимагає стратегії, яка враховує всі можливі ризики існування та виявлення вразливостей[62]. Згідно зі стратегією необхідно, забезпечити захист таких

складових, як дані в хмарі, цілісність даних в процесах їх передача шляхом використання мережі Інтернет, об’єкти структури.

Ефективна стратегія безпеки, може бути сформована лише на основі інформації та даних отриманих командами спеціалістів, які беруть участь в процесах виробництва, тестування, розгортання, та обслуговування всіх складових проекту IoT[44].

3.5.1 Виробники об’єктів IoT, обладнання та інтегратори.

Першу сходинку в процесі забезпечення займають фізичні та юридичні особи, які займаються виготовлення, компонуванням обладнання, інтегратори, які створюють продукти на основі рішень різних виробників, та постачальники пристроїв та обладнання для розгортання мереж організації IoT.

Для таких осіб та органів керування протягом життєвого циклу об’єктів IoT варто застосовувати наступні рекомендації та вимоги:

- Формування та дотримання списку мінімального набору компонентів для забезпечення всіх цільових послуг та функцій пристрою. Наявність додаткових інтерфейсів та органів керування надають можливість використання їх з метою компрометації пристрою.
- Забезпечення механізму захисту об’єкту від несанкціонованого доступу для фізичного втручання в його роботу. Необхідно розробити процедуру виявлення фізичного втручання в корпус пристрою або в межі фізичної безпеки пристрою. Застосування датчиків руху чи ідентифікаторів, що реагують на зміну стану пристрою чи його складових. Дана інформація може бути надіслана в систему реагування, моніторингу або безпосередньо операторам пристрою.
- Створення додаткових рішень для підвищення рівня безпеки. Під час створення концепції варто приділити увагу фінансовій складовій та розподілити її таким чином, щоб частина капіталу була вкладена в функції безпеки і не мала наслідків для зміни собівартості пристрою. Як приклад, використання сховищ з шифруванням наданої в них інформації.

- Формування політики безпеки при наданні оновлень. Штатне ПЗ вимагає постійного оновлення та вдосконалення, протягом всього циклу використання пристрою. В зв’язку з цим, необхідно сформувати такі засоби та методи надання пристроям оновлень та їх автоматичного встановлення, які б виключали можливість НСД до каналів передачі пакетів оновлення та необхідність їх ручної перевірки, встановлення та налаштування.
- Застосування лише визнаних стандартів розробки та введення в використання ПЗ. Необхідно в край ретельно продумати та спланувати всі етапи життєвого циклу ПЗ. В залежності від цього, будуть обиратися різні типи платформ, формування функцій та послуг, інструменти.
- Увага до використання ПЗ з відкритим кодом. Дане ПЗ дозволяє підвищити швидкість проходження етапів розробки, але необхідно врахувати, що у кожного такого компонента, є спільнота, яка забезпечує його підтримку. В разі слабкої активності, кінцевий користувач отримає продукт, який матиме безліч недоліків в зв’язку з тим, що спільнота не підтримує свій компонент надаючи йому виправлення та оновлення.
- Увага під час процесів інтеграції рішень. Маса обходів системи захисту ПЗ відбулася завдяки недолікам в роботі між інтерфейсами API та бібліотеками. Деякі функції, що забезпечуються шляхом використання API можуть бути цілком безкорисні в деяких рішеннях. Необхідно виконувати обов’язкову перевірку всіх інтерфейсів інтегрованих рішень та компонентів на наявність вразливостей.

3.5.2 Спеціаліст із процесів розгортання рішень та мереж IoT.

Друга сходинка безпеки, лягає на плечі персоналу, який займається питаннями з розгортання рішень IoT та впроваджує їх в робоче середовище. Також, він займається налаштуванням обладнання, взаємодії пристроїв в мережі їхнього зв’язку між собою та хмарними рішеннями.

Для таких спеціалістів з питань налаштування об’єктів IoT складено наступні рекомендації та вимоги:

- Безпека в процесах розгортання обладнання. Обладнання IoT часто розміщується в середовищі, яке саме по собі є небезпечним, як приклад громадський транспорт, приміщення або в місцях які виключають можливість контролювання місцезнаходження пристрою. В такому випадку вкрай важливо, забезпечити найбільший рівень захисту пристроїв від НСД. Вся конструкція має бути надійно захищена від фізичного впливу, як середовища так і можливих зловмисників, а також увагу необхідно приділити вразливим елементам пристрою та інтерфейсам які за своєю концепцією завжди відкриті до підключень. Зловмисник обов'язково скористується цими вразливостями для впливу на роботу пристрою чи системи в цілому.
- Створення спеціальних «контейнерів» безпеки. Під час процедури розгортання проекту, пристрої потребують паролі та ключі автентифікації, які створюються за допомогою хмарних сервісів та служб. Ключі необхідно зберігати в місці, яке захищено фізично, навіть по завершенню процедури розгортання проекту. Інфікований пристрій може використовувати отриманий ключ для інфікуванні всієї мережі.

3.5.3 Оператор об'єктів проекту IoT.

Третя сходинка в процесу формування цілісної стратегії безпеки проектів в сфері IoT залежить від оператора об'єктів. Персонал, що належить до даного типу, має наступні обов'язки:

- Довгостроковий моніторинг стану пристрою та його роботи;
- Регулярний огляд об'єктів;
- Перевірка оновлень пристроїв та їх встановлення;
- Надання послуг з відновлення пристроїв (після збоїв або природних катаклізмів);
- Складання плану аудитів мережі та їх проведення.

Такий спектр завдань виконує команда всередині компанії і складається вона з фахівців у сфері інформаційних технологій, технічного захисту інформації та фахівців вузьких галузей які пов'язані з проектом IoT.

Для таких команд з питань обслуговування об’єктів IoT складено наступні рекомендації та вимоги:

- Своєчасне оновлення системи. ОС в цілому та всі необхідні для роботи драйвери мають бути найбільш актуальної версії. Таким чином, зловмисники не матимуть можливості використовувати вразливості минулих версій або недоліки застарілого ПЗ.
- Застосування антивірусного ПЗ. В разі можливості встановлення антивірусного ПЗ до ОС об’єкта, що знаходиться в межах проекту, вкрай необхідно цим скористуватися. Такий захід допоможе підсилити захист окремих пристроїв системи.
- Регулярне проведення аудитів. В першу чергу, аудит інфраструктури проекту на присутність в ньому інцидентів безпеки, допомагає реагувати на проблему з безпекою. Багато ОС має штатні засоби логування подій та процесів. Для достатньої усвідомленості їх необхідно регулярно переглядати та аналізувати для того, щоб переконатися у відсутності проблем та інцидентів системи безпеки. Дані журналів можна легко надсилати окремим каналом до служб аналізу подій в хмарному середовищі.
- Захист інфраструктури IoT фізичними засобами. Одні з найбільш серйозних атак на системи безпеки та керування інфраструктурами різних проектів сфери IoT були здійснені за рахунок використання фізичного доступу до об’єктів. Важливе рішення в безпеці – захист всіх компонентів та відкритих інтерфейсів від атак.
- Захищення даних облікових записів хмари. За рахунок використання, облікових записів для автентифікації в хмарних середовищах та сервісах, які безпосередньо пов’язані з проектом, зловмисник має змогу отримати доступ до системи IoT та вчинити деструктивні дії. Для захисту зв'язок «логін/пароль» необхідно регулярно змінювати пароль, не використовувати паролі пов’язані з особистою інформацією користувача та слабкі до зламу паролі.

Залежно від направлення дій об’єкта IoT, їхні можливості відрізняються між собою. Більшість пристроїв мають спрощену ОС, яка забезпечує хоч і невеликий набір функцій, але достатній для повноцінної роботи. Однак до проектів IoT входять комп’ютери з стандартними ОС, які мають свої особливості. Враховуючи цей фактор, варто вказати, що надані вище рекомендації з налаштування засобів безпеки можуть бути застосовані в різній мірі. Необхідно застосовувати рекомендації, якщо такі наявні, від виробника пристрою.

Вкрай важливо, звернути увагу на вибір пристроїв та компонентів під час проектування IoT. Це пов’язано з тим, що деякі пристрої можуть бути застарілими або обмеженими в функціоналі. Вони можуть не володіти можливістю шифрування даних, бездротовим підключенням до мережі Інтернет або не мати можливості надавати інформацію для аудиту. В разі використання подібних пристроїв, необхідно використовувати майстри з’єднань та польові шлюзи, які допомагають об’єднувати небезпечні пристрої в одну групу та керувати нею. Таким чином, забезпечуються функції автентифікації, шифрування сеансів, надання команд з хмарних сервісів та інше.

Система рекомендацій поділяється на дві категорії: рекомендації користувачеві та рекомендації для виробника. Обидві категорії представлені у вигляді списків дій, необхідних для забезпечення захисту користувачів, пристроїв IoT та інформації в цих пристроях.

Категорія користувачів пристроїв IoT:

1. Використовувати лише стійкі до зламу паролі та виконувати обов’язкову зміну логіну та паролю облікового запису, що надається виробником за замовчуванням. Політика формування паролів наступна: при створенні паролю, вкрай важливо використовувати цифри, літери латинського алфавіту в різних регістрах, символи. Імена облікових записів необхідно змінити з стандартних «user», «root» на нестандартні, але такі, що не мають зв’язку зі справжніми іменами чи даними власника облікового запису.

2. Чітке та покрокове налаштування мережі та міжмережевих екранів, перевірка всіх доступних портів у мережі на наявність таких, які не є необхідними для повноцінного функціонування пристрою та не використовуються для віддаленого доступу. Додатковий фактор, для підвищення статусу захищеності – використання розмежування мережі пристроїв від критичних об’єктів інфраструктури за допомогою різних мережевих технологій, наприклад VLAN.

3. Слідкувати за станом оновлень та своєчасно виконувати оновлення як ОС пристрою, так і ПЗ. В разі виявлення вразливості пристрою, уникнути якої без втручання виробника неможливо, то необхідно максимально точно дотримуватися порад для мінімізації негативних наслідків даної вразливості, або в короткі терміни вивести пристрій з експлуатації та чекати на оновлення, яке може виправити вразливість.

4. Відповідна процедура утилізації пристроїв. Перед утилізацією пристрою, вкрай необхідно впевнитися, що в його накопичувачах та інших компонентах не залишилося жодних даних або їх фрагментів, які зловмисник міг би використати для власних цілей. Такі дані можуть представляти інформацію про мережу, її засоби зв’язку, налаштування, сертифікати криптографічних перетворень і т.д. Для повної очистки пристрою перед утилізацією варто виконати процедуру «жорсткого скидання» до заводських налаштувань. Таким чином пристрій виглядатиме, як новий, в плані ПЗ і не буде містити важливої інформації.

5. Уникати використання пристроїв, бувших у використанні. Даний клас пристроїв є досить небезпечним, оскільки вони могли бути навмисно модифікованими для вчинення деструктивних дій, наприклад, створення шлюзів віддаленого доступу, бекдорів, викрадення даних, інфікування пристроїв, що знаходяться в цій же мережі.

Категорія виробників пристроїв IoT:

1. Захист має бути обов’язковою складовою життєвого циклу пристроїв. Виробник зобов’язаний проводити регулярний аудит безпеки

продуктів, оперативно реагувати на виявлення помилок та проводити їх виправлення за допомогою оновлень ПЗ.

2. В заводських налаштуваннях ввести політику стійкого паролю. Пристрій при потраплянні до користувача має містити основний обліковий запис з такими налаштуваннями зв'язки «логін/пароль», які будуть стійкими до брутфорсу. Пароль варто використовувати згенерований за допомогою генераторів випадкових чисел, для кожного пристрою та надаватися разом с пристроєм у вигляді скретч-наліпки. Таким чином, користувач буде впевнений, що він буде першим, хто побачить пароль. В разі неможливості застосування таких механізмів захисту, варто забезпечити функцію примусової зміни стандартних налаштувань пристрою. Під час першого увімкнення пристрій має реагувати на підключення або спроби використання функцій, наступним чином - пристрій викликає екран зміни «логіну/паролю» щоразу[42]. Таким чином, пристрій лишається з заблокованим функціоналом, і не наражає решту системи на небезпеку. При цьому, політика оформлення паролю має слідувати наступним вимогам: використання цифр, літер латинського алфавіту в різних регістрах, символи.

3. Сформувати автоматизовану систему оновлень. Така система повинна в автоматичному режимі проводити аудит оновлень ПЗ пристрою та виводити про це повідомлення для користувача. Також, в налаштуваннях пристрою має бути графа яка відповідає за автоматичну перевірку цілісності файлу оновлення та автоматизована процедура його встановлення. Додатково необхідно ввести звичайний планувальник оновлень, за допомогою якого можна запланувати час оновлення на період, коли пристрій не бере активної участі в роботі системи.

Важливо, щоб виробник займався питанням розробки та стандартизації нових алгоритмів криптографічного захисту. Або вводити в використання існуючі. Головною вимогою до алгоритмів є криптостійктість та достатня ефективність в площині використання ресурсів пристрою. Найбільш

підходящими алгоритмами, на сьогоднішній день визнано алгоритми GBPA та ANU.

3.6 Дослідження WiFi-модулю ESP8266 на потенційні загрози, як складової пристрою IoT

WiFi-модуль ESP8266 від ESPRESSIF - це популярний недорогий (дешевше 2 доларів США) WiFi-модуль, який встановлюють на друковані плати. Він часто використовується для проектів IoT і легко програмується за допомогою Arduino IDE або Mongoose OS і його IDE через Інтернет. Модулі ESP8266 закриті металевим екраном. Під екраном знаходиться мікросхема WiFi/CPU і мікросхема FLASH пам'яті з послідовним інтерфейсом SPI (рис. 3.1).

Рис. 3.1. Зовнішній вигляд Wi-Fi модулю ESP8266

3.6.1 Загальні відомості та характеристики пристрою.

ESP8266 - плата-модуль Wi-Fi на базі популярного чіпсета ESP8266EX. На борту плати знаходиться мікросхема Flash-пам'яті об'ємом 2 МБ, чіп ESP8266EX, кварцовий резонатор, два індикаторних світлодіоди і мініатюрна антена з доріжки на верхньому шарі друкованої плати у вигляді змійки. Flash-пам'ять необхідна для зберігання програмного забезпечення. При кожному включенні живлення, ПЗ автоматично завантажується в чіп ESP8266EX.

За замовчуванням модуль налаштований на роботу через «АТ-команди». Керуюча плата посилає команди - Wi-Fi модуль виконує відповідну операцію.

Але всередині чіпа ESP8266 ховається цілий мікроконтролер, який є самодостатнім пристроєм. Прошивати модуль можна на різних мовах програмування.

Характеристики пристрою наведені в табл.3.1.

Таблиця 3.1

Програмно-апаратні характеристики WiFi-модуля ESP8266

Модуль:	ESP8266 з чіпом ESP8266EX
Вихідний інтерфейс:	UART
Обсяг Flash-пам'яті:	2 МБ
Бездротовий інтерфейс:	Wi-Fi 802.11 b / g / n 2,4 ГГц
Режими роботи:	• Клієнт (STA) • Точка доступу (AP) • Клієнт + Точка доступу (STA + AP)
Напруга живлення:	3,3 В

Струм:	до 250 мА
Габарити:	25 × 15 мм

3.6.2 Несанкціонований доступ.

Оскільки дані модулі часто використовують як в пристроях які виготовляються компаніями так і саморобних проектах на базі різних плат, то можна зробити висновок, що модуль дуже поширений. Найбільшу важливість представляє Flash-пам'ять, так як вона виконує роль сховища для ПЗ та завантажувача ПЗ в чіп ESP8266EX для виконання.

Для того, щоб отримати доступ до пам'яті – необхідно демонтувати захисний екран. Захисний екран і мікросхема FLASH можуть бути легко демонтовані за допомогою технічного фена з регулюванням температури (приблизно 370 ° C). Для цього процесу необхідно менше хвилини (рис. 3.2).

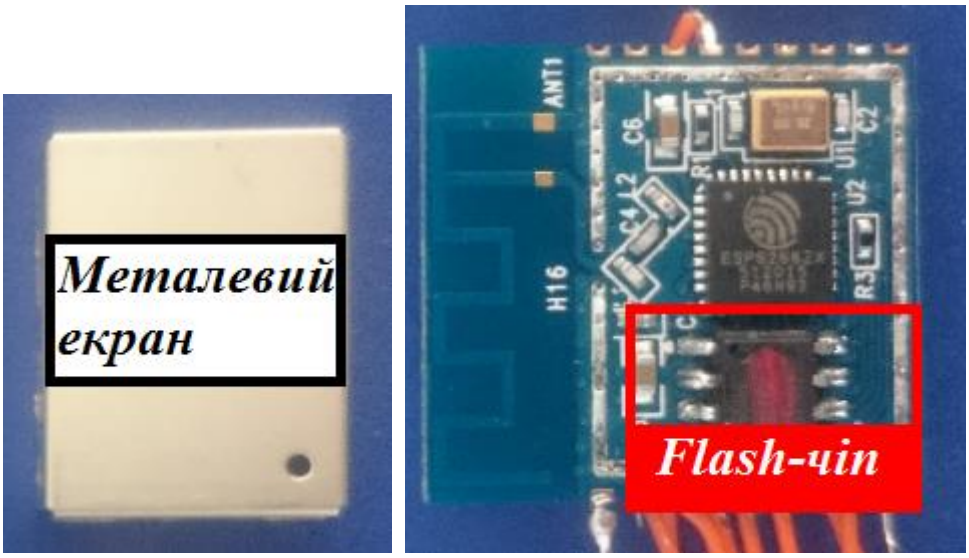

Рис. 3.2 Демонтований металевий екран WiFi-модуля ESP8266

Демонтовану мікросхему пам'яті потрібно помістити в програматор і вибрати в його ПЗ найменування, відповідне найменуванню мікросхеми, надрукованому на її корпусі (рис.3.3).

Рис. 3.3 Програматор

Наступний крок, зчитування інформації за допомогою ПЗ Revelprog IS(рис. 3.4)

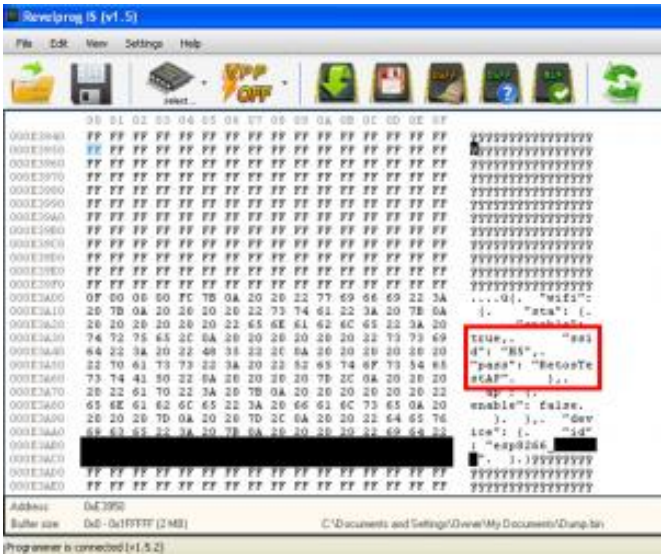

Рис. 3.4 ПЗ програматора

Таким чином, ми отримали вміст, що знаходився в пам'яті. Було отримано дані про заданий SSID мережі Wi-Fi і його пароль, які зберігаються в ESP8266 у вигляді відкритого тексту.

Для проведення такої атаки, зловмиснику не потрібно складних інструментів, достатньо лише програматора та технічного фена, які дуже просто придбати.

3.6.3 Висновки дослідження

У результаті даного дослідження було виявлено порушення безпеки як апаратної так і програмної складової пристрою. Таким чином, використання WiFi-модуля ESP8266 може стати причиною компрометації як окремого пристрою так і мережі, в якій він знаходиться. І ця проблема стосується як звичайних громадян, що не стосуються критичних структур, так і проектів де такий модуль використовується. Шляхи уникнення даної вразливості та багатьох інших загроз інформаційні безпеці наведені в наступному пункті атестаційної роботи.

3.7 Висновки до третього розділу

Об’єкти IoT мають на меті ідею підвищення комфорту людських життів та ефективності їх діяльності. Але при недостатньому рівні уваги до питань безпеки, необхідно бути готовим до інцидентів інформаційної безпеки об’єкту, що спричиняють збитки, які неможливо врегулювати.

Безпека Інтернету речей складається з двох компонент – безпека з боку користувача пристрою, та з боку виробника, які повинні забезпечувати надійний пароль, дотримання базових норм та правил безпеки та надання оновлень, ПЗ, аудит відповідно. Захисту підлягають всі об’єкти, як фізичні так і віртуальні, що входять до інфраструктури проекту IoT.

Одним із найбільш перспективних способів захисту інфраструктури IoT являється технологія блокчейн, яка колективізує не лише дані отримані з кінцевих точок, а й дані про самі кінцеві точки, їх роботу та стан. На початкових етапах, ці дані захищені від змін, а механізм децентралізованого розподілу

інформації по сховищах дає можливість надійно зберігати дані. Тому розвиток сфери IoT, частково залежить від розвитку технології блокчейн.

У даному розділі було визначено основні причини недостатнього рівня захисту об’єктів інфраструктури IoT та проведено інформаційно-аналітичну роботу, результатом якої стали дані для визначення основних факторів та вразливостей ,які сприяли порушенню периметра системи безпеки, базуючись на результатах аналізу кібератак на ці об’єкти. Було проведено практичне дослідження WiFi-модуля ESP8266, який часто використовують в мережевих IoT-пристроях, на наявність потенційних загроз безпеці як цього пристрою, так і структури до якої він може бути підключений. На основі отриманих результатів аналітичних робіт та досліджень було сформовано розподілену систему рекомендацій для кожної категорії користувачів IoT рішень, враховуючи ролі та потреби цих користувачів, та саму інфраструктуру IoT.

ВИСНОВКИ

На сьогодні, навіть в такому стані, IoT займає лідируючі позиції, як одна з найбільш перспективних технологій автоматизації процесів обробки, передачі та збереження інформації. Враховуючи мультифункціональність та багатогранність рішень IoT, вони можуть бути введені в найрізноманітніші галузі життя людини, її сфери роботи з метою покращення якості надання послуг та сервісів. Комбінуючи технології хмарних та туманних обчислень, блокчейн та штучного інтелекту, Інтернет речей може взяти на себе роль революційної технології.

Незважаючи на всі чудові можливості, якими володіє IoT, питання нормативно-правової бази та стандартів залишається проблемним місцем технології, оскільки розрив між темпами технічного розвитку технології, та темпами нормативної бази лише зростає. Відсутність єдиних стандартів

провокує компанії вигадувати власні для задоволення своїх потреб, але в масштабах ринку, це лише призводить до розриву єдиного шаблону безпеки.

Інша більш критична проблема – безпека пристроїв та інформації, яку вони оброблюють. Таким чином, хакери вдало користуються недоліками систем безпеки: злам систем сповіщення, проникнення в сотні тисяч пристроїв, віддалене керування автомобілями, викрадення баз даних казино і т.д.

За умови таких проблем, кіберзагрози здобувають фізичний вплив, наслідки якого можуть вартувати не лише фінансових збитків, а й людських життів.

Спільнота OWASP виділила 10 найбільш частих проблем пов’язаних з проблемами безпеки в IoT. Варто дослухатися до рекомендацій та настанов спеціалістів, оскільки від цього залежить робота як комерційних проектів так і критичних структур. Складова безпеки повинна брати участь у всіх етапах життєвого циклу продкту.

Нажаль, кіберзлочинці завжди попереду, вигадуючи нові засоби, інструменти та шукаючи нові вразливості в існуючих пристроях, це вимагає від структур безпеки завжди бути в режимі повної готовності для відбиття можливих атак.

Головне завдання атестаційної роботи полягало у розробці системи захисту інформації в сфері IoT шляхом застосування системи розподілених рекомендацій для максимально можливого підвищення рівня безпеки пристроїв сфери Інтернету речей. Для цього, в роботі було наведено існуючі приклади використання проектів Інтернету речей в різних галузях та розгляд їх можливостей та функцій у відповідних галузях. Також проаналізовано загрози інформації які можуть становити пристрої в проектах. Було виконано аналітичне дослідження шкідливого ПЗ та відомих інцидентів кібербезпеки в історії IoT. Було виконане процес практичного дослідження для виявлення рівня захищеності WiFi-модуля ESP8266.

Мета даної дипломної роботи – підвищити рівень захищеності об’єктів Інтернету речей і для досягнення мети було проведено такі заходи:

- Виконано аналіз особливостей роботи та функціонування фізичних та віртуальних об’єктів IoT;
- Виконано дослідження стандартів та нормативно-правової бази;
- Розглянуто імовірні загрози пристроїв Інтернету речей;
- Виконано детальний аналіз інцидентів у сфері інформаційно-комунікаційної безпеки за участі об’єктів IoT;
- Визначено, які фактори є основоположними в низькому рівні захисту пристроїв;
- Розроблено систему рекомендації для підвищення рівня захисту проектів IoT.

Отже, головним результатом атестаційної роботи є ефективна система розподілених рекомендацій для всіх учасників сфери IoT, яка має здатність забезпечити вищий рівень захисту пристроїв Інтернету речей та користувачів даної технології.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Эванс Д. Ответы на два самых частых вопроса про Всеобъемлющий Интернет [Электронный ресурс] / Д. Эванс // Cisco. – 2013. – Режим доступа: https://www.cisco.com/c/ru_ua/about/press/2013/04042013f.html.

2. Росляков А.В. Интернет вещей: учебное пособие / А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.

3. Програмно-апаратна технологія для навчання технологіям Інтернету Речей: навчальний посібник / [А.В. Пархоменко, А.В. Туленков, О.В. Соколянський, Я.І. Залюбовський]. – Запоріжжя: Дике Поле, 2017 – 120 с.

4. Кранц М. Интернет вещей стандартизуется [Электронный ресурс] / М. Кранц // Cisco. – 2015. – Режим доступа: https://www.cisco.com/c/ru_ru/ about/press/press-releases/2015/07-30a.html

5. Стандарты Интернета вещей [Электронный ресурс] // I-o-T Интернет вещей. – 2016. – Режим доступа: http://i-o-t.ru/standarti-interneta-veshey/.

6. IoT Leaders you Must Know [Electronic resource] // Linknovate Stories. – 2018. – Access: https://blog.linknovate.com/iot-leaders-you-must-know/.

7. Ватаманюк А. И. Домашние и офисные сети под Vista и XP: Популярный самоучитель: учебное пособие / А. И. Ватаманюк – СПб.: Питер, 2008. – 256 с.

8. IoT Standards and Protocols [Electronic resource] // Postscapes. – 2016. – Access: https://www.postscapes.com/internet-of-things-protocols/.

9. Mohammed Z. K. A. Internet of Things Applications, Challenges and Related Future Technologies / Z. K. A. Mohammed, S. A. A. Elmustafa // World Scientific News. – 2017. – №67(2) . – p. 126-148.

10. Patel K. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges / K. Patel, S. Patel // International Journal of Engineering Science and Computing. – 2016. – №5. – p. 6122 – 6131.

11. Evans D. The Internet of Things. How the Next Evolution of the Internet is Changing Everything [Electronic recourse] / D. Evans // Cisco. – Access: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

12. Connecting the IoT: The road to success [Electronic resource] // IDC. – 2015. – Access: https://www.idc.com/infographics/IoT.

13. Kanellos M. 152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things [Electronic resource] / M. Kanellos // Forbes. – 2016. – Access: https://www.forbes.com/sites/michaelkanellos/2016/ 03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#7523c7e34b63.

14. Alberti A., Singh D. Internet of Things: Perspectives, Challenges and Opportunities: conference report / A. Alberti, D. Singh // Research Gate. – 2013. – №5. – 7 p.

15. Ravindra S. Understanding the relationship between IoT and Big Data [Electronic resource] / S. Ravindra // Jaxenter. – 2017. – Access: https://jaxenter.com/relationship-between-iot-big-data-138220.html.

16. Gross G. 9 Key Big Data Security Issues [Electronic resource] / G. Gross // Alien Vault. – 2016. – Access: https://www.alienvault.com/ blogs/security-essentials/9-key-big-data-security-issues.

17. Toms L. 5 Common Cyber Attacks in the IoT – Threat Alert on a Grand Scale [Electronic resource] / L.Toms // Global Sign. – 2016. – Access: https://www.globalsign.com/en/ blog/five-common-cyber-attacks-in-the-iot/.

18. Loukas G. Cyber-Physical Attacks: A Growing Invisible Threat / G. Loukas. – MA, USA: Butterworth-Heinemann Newton. – 2015. – 270 p.

19. Тадтаев Г. Холодильник атакует: как киберпреступники используют бытовую технику [Электронный ресурс] / Г. Тадаєв // РБК. – 2016. – Режим доступа: https://www.rbc.ru/technology_and_media/13/11/2016/5825cf889a79475b671ff971.

20. Ализар А. Умный холодильник выдал хакерам пароль от Gmail [Электронний ресурс] / А. Ализар // Хакер. – 2015. – Режим доступа: https://xakep.ru/2015/08/25/ smart-fridge/.

21. Goodin D. Smart TV hack embeds attack code into broadcast signal—no access required [Electronic resource] / D. Gooodin // Arstechnica. – 2017. – Access: https://arstechnica.com/ information-technology/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/.

22. «Умные» телевизоры Samsung можно взломать через функцию Wi-Fi Direct [Электронный ресурс] // Securitylab. – 2017. – Режим доступа: https://www.securitylab.ru/news/485988.php.

23. ITI Capital. Взлом казино через умный аквариум и DDoS биржевых брокеров: новые атаки на сферу финансов [Электронный ресурс] // Habr. – 2017. – Режим доступа: https://habr.com/company/iticapital/blog/334396/ .

24. Взлом Tesla [Электронный ресурс] // Kaspersky Lab. – 2017. – Режим доступа: https://www.kaspersky.ru/blog/hacking-tesla-model-x/18169/.

25. Internet of Things Top Ten [Electronic resource] // OWASP. – 2014. – Access: https://www.owasp.org/images/7/71/ Internet_of_Things_Top_Ten_2014-OWASP.pdf.

26. What Is Account Enumeration? [Electronic resource] // Affinity Security Services. – Access: https://affinity-it-security.com/what-is-account-enumeration/.

27. 2100 – Username Enumeration [Electronic resource] // Hacking-Lab. – Access: https://www.hacking-lab.com/cases/2100-web-security-username-enumeration/index.html.

28. User Enumeration: Too Much Information [Electronic resource] // Microfocus. – 2014. – Access: https://community.softwaregrp.com/t5/Protect-Your-Assets/User-Enumeration-Too-Much-Information/ba-p/273785#.Wxo4ZEj4nIV.

29. Top 5 Most Common Network Vulnerabilities: Default Log-In Credentials [Electronic resource] // Perspective Risk. – 2014. – Access: https://www.perspectiverisk. com/top-5-common-network-vulnerabilities-default-login-credentials/.

30. 2014 Trustwave Global Security Report [Electronic resource] // Trustwave. – 2014. – Access: https://www.trustwave.com/Resources/Library/Documents/2014-Trustwave-Global-Security-Report/.

31. 2016 Trustwave Global Security Report [Electronic resource] // Trustwave. – 2016. – Access: https://www.trustwave.com/Resources/Library/Documents/2016-Trustwave-Global-Security-Report/.

32. Сетевой трафик. Словарь терминов [Электронный ресурс] // Setup. – Режим доступа: http://www.setup.ru/wiki/Сетевой%20трафик.

33. Перехват паролей с помощью Wireshark [Электронный ресурс] // Network Guru. – Режим доступа: https://networkguru.ru/wireshark-perekhvat-paroley/.

34. Атака через Inrternet: учебное пособие / [И.Д. Медведовский, А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков]. – СПб: НПО "Мир и семья-95", 1997. – 296 с.

35. Запобігання міжсайтового скриптинга [Електронний ресурс] // Yii Framework. – Режим доступу: https://yiiframework.com.ua/uk/doc/guide/topics.security/.

36. SQL-инъекция [Электронный ресурс] // Национальная библиотека им. Н. Э. Баумана. – Режим доступа: https://ru.bmstu.wiki/SQL-инъекция.

37. Nagaradjane V. Session Management Using PHP, Part 1: Cookie-based Sessions [Electronic resource] / V. Nagaradjane // Open Sourse. – 2008. – Access: https://opensourceforu.com/ 2008/12/session-management-using-php-part-1-cookie-based-sessions/.

38. Account lockout. Dicttionary [Electronic resource] // Computer Hope. – 2017. – Access: https://www.computerhope.com/jargon/a/accolock.htm.

39. Сложность пароля [Электронный ресурс] // Википедия. – Режим доступа: https://ru.wikipedia.org/wiki/Сложность_пароля.

40. Горчаков Д. Как обезопасить свою электронную почту от взлома [Электронный ресурс] / Д. Горчаков // ITC ua. – 2014. – Режим доступа: https://itc.ua/articles/ kak-obezopasit-svoyu-elektronnuyu-pochtu-ot-vzloma/.

41. Epp D. Credential Theft and How to Secure Credentials [Electronic resource] / D. Epp // Microsoft. – 2014. – Access: https://technet.microsoft.com/en_us/security/ dn920237.aspx.

42. Двухфакторная аутентификация: что это и зачем оно нужно? [Электронный ресурс] // Kaspersky Lab. – 2014. – Режим доступа: https://www.kaspersky.ru/blog/what_is_two_factor_authenticatio/4272/.

43. Небезопасное восстановление паролей (Weak Password Recovery Validation) [Электронный ресурс] // Персональный компьютер. – 2011. – Режим доступа: http://dammlab.com/bezopasnost-pk/nebezopasnoe-vosstanovlenie-parolej-weak-password-recovery-validation.html.

44. Угроза привилегированных пользователей и методы по её устранению [Электронный ресурс] // PPT.ru. – 2016. – Режим доступа: http://ppt.ru/guide/ news/136623.

45. Role Based Access Control [Electronic resource] // NIST. – Access: https://csrc.nist.gov/projects/role-based-access-control.

46. Geer D. Securing risky network ports [Electronic resource] / D. Geer // CSO. – 2017. – Access: https://www.csoonline.com/article/3191531/network-security/securing-risky-network-ports.html.

47. Buffer Overflow [Electronic resource] // OWASP. – Access: https://www.owasp.org/index.php/Buffer_Overflow.

48. UPnP Device Architecture version 1.1 [Electronic resource] // UPnP Forum. – 2008. – Access: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf.

49. Wisniewski C.UPnP flaws turn millions of firewalls into doorstops [Electronic resource] / C. Wisniewski // Naked Security. – 2013. – Access: https://nakedsecurity. sophos.com/ 2013/02/05/upnp-flaws-turn-millions-of-firewalls-into-doorstops/.

50. Moore H. Security Flaws in Universal Plug and Play: Unplug, Don't Play [Electronic resource] / H. Moore // RAPID7. – 2013. – Access:

https://blog.rapid7.com/ 2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play/.

51. Using UDP Services [Electronic resource] // Microsoft. – 2017. – Access: https://docs.microsoft.com/en-us/dotnet/framework/network-programming/using-udp-services.

52. Hart J. NCSAM: Understanding UDP Amplification Vulnerabilities Through Rapid7 Research [Electronic resource] / J. Hart // RAPID7. – 2016. – Access: https://blog.rapid7.com/2016/10/31/understanding-udp-amplification-vulnerabilities-through-rapid7-research/.

53. Denial of Service [Electronic resource] // OWASP. – Access: https://www.owasp.org/index.php/Denial_of_Service.

54. Greenberg A. Hacker lexicon: What is Fuzzing? [Electronic resource] / A. Greenberg // Wired. – 2016. – Access: https://www.wired.com/2016/06/hacker-lexicon-fuzzing/.

55. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack [Electronic resource] // Wired. – 2014. – Access: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WxpPqEj4nIV.

56. Атака “человек посередине” [Электронный ресурс] // Secure List. – Режим доступа: https://securelist.ru/threats/man-in-the-middle-attack-glossary/.

57. Карев А. Разбираем уязвимости проверки сертификатов SSL и TLS в небраузерном софте [Электронный ресурс] / А. Карев // Хакер. – 2018. – Режим доступа: https://xakep.ru/2018/03/08/ssl-tls-fuckup/

58. Кудрявцев Д. А. Исследование протоколов SSL/TLS / Д. А. Кудрявцев, В. С. Тебенькова, Е. Л. Кротова // Материалы всероссийской научно-технической конференции "Автоматизированные системы управления и информационные технологии". – Пермь: ПНИПУ, 2015. – с. 572-575.

59. What data can we process and under which conditions? [Electronic resource] // European Commision. – 2018. – Access: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en.

60. Using Granular Permissions. Adaptive Server Enterprise 15.7 SP100 [Electronic resource] // Sybase. – 2013. – Access: http://infocenter.sybase.com/help/index.jsp?
topic=/com.sybase.infocenter.dc01672.1572/html/sec_admin/CIHGCEAI.htm.

61. Improving Usability of Password Management with Standardized Password Policies / [B. AlFayyadh, P. Thorsheim, A. Jøsang, H. Klevjer] [Electronic resource] // European Commision. – 2018. – Access: http://folk.uio.no/josang/papers/ATJK2012-SARSSI.pdf

62. Ревнивых А.В. Мониторинг информационной инфраструктуры организации [Электронный ресурс] / А.В. Ревнивых, А.М. Федотов // Cyberleninka. – Режим доступа: https://cyberleninka.ru/article/n/monitoring-informatsionnoy-infrastruktury-organizatsii.

63. Макаревич О.Б. Регистрация и анализ событий безопасности в информационных системах [Электронный ресурс] /О.Б. МакаревичИ.А. Шелудько // Cyberleninka. – Режим доступа: https://cyberleninka.ru/article/n/registratsiya-i-analiz-sobytiy-bezopasnosti-v-informatsionnyh-sistemah.

64. Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge [Electronic resource] // I-SCOOP. – 2018. – Access: https://www.i-scoop.eu/ blockchain-distributed-ledger-technology/blockchain-iot/.

65. Shaik K. Why blockchain and IoT are best friends challenge [Electronic resource] / K. Shaik // IBM. – 2018. – Access: https://www.ibm.com/blogs/ blockchain/2018/01/ why-blockchain-and-iot-are-best-friends/.