Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)

Кафедра ____Автоматизації проектування обчислювальної техніки_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
(рівень вищої освіти)

_____Система захисту інформації в IoT–мережі_____
(тема)

Виконав: студент 2 курсу, групи СКСм-19-1
_____Ліхота О.І_____
(прізвище, ініціали)
Спеціальність _123 – Комп'ютерна інженерія___
(код і повна назва спеціальності)
Тип програми___Освітньо–професійна_____
(освітньо–професійна або освітньо–наукова)
Освітня програма_____
_____Спеціалізовані комп'ютерні системи_____
_____
(повна назва освітньої програми)
Керівник ___проф. Немченко В.П._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ___Чумаченко С.В.__
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
Кафедра Автоматизації проектування обчислювальної техніки
Рівень вищої освіти другий (магістерський)
Спеціальність 123 – Комп'ютерна інженерія
Тип програми Освітньо–професійна
Освітня програма Спеціалізовані комп'ютерні системи
(код і повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Ліхоті Орині Ігорівні
(прізвище, ім'я, по батькові)

1. Тема роботи Система захисту інформації в IoT–мережі

затверджена наказом по університету від 30.10.2020р .№ 1489СТ

2. Термін подання студентом роботи до екзаменаційної комісії. 15.12.2020 р.

3. Вихідні дані до роботи

мережа IoT, PDCA, STRIDE, система менеджменту інформаційної безпеки

4. Перелік питань, що потрібно опрацювати в роботі

алгоритми виявлення вразливостей системи безпеки, методи побудови безпечної IoT–системи, методи вдосконалення IoT–системи

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 16 слайдів

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Спец. частина	Проф. Немченко В.П.		12.12.2020

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	03.09.2020–07.09.2020	
2	Аналіз предметної області	11.09.2020–21.09.2020	
3	Аналіз джерел з проблемної галузі	25.09.2020–05.10.2020	
4	Аналіз загроз інформаційної безпеки IoT–систем	08.10.2020–19.10.2020	
5	Аналіз методів захисту інформаційної безпеки	22.10.2020–02.11.2020	
6	Розробка системи захисту інформації в IoT	05.11.2020–16.11.2020	
7	Оформлення пояснювальної записки	03.12.2020–14.12.2020	

Дата видачі завдання 03.09.2020 р.

Студент _____ _____

(підпис)

Керівник роботи _____ _____проф. Немченко В.П.__

(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 98 сторінки, 5 рисунки, 3 таблиці, 24 джерела за переліком посилань

Об’єкт дослідження – самоорганізована розподілена Internet of Things (IoT) система.

Предмет дослідження – метод побудови та вдосконалення безпеки бездротової IoT системи.

Мета роботи – дослідження методів виявлення та запобігання вразливостей інформаційної безпеки в IoT системі.

Оглянуті методи побудови IoT систем, основні протоколи безпеки та технології передачі даних. Проведено аналіз загроз та вразливостей інформаційної безпеки IoT систем, та запропоновані методи їх виявлення та запобігання за допомогою різних протоколів та інших технологій.

Запропоновано система побудування, розвитку та підтримки безпечної IoT системи.

ABSTRACT

Master's thesis contains 98 pages, 5 figures, 3 tables, 24 sources according to the list of links.

The object of research is a self–organized distributed Internet of Things (IoT) system.

The subject of research is a method of building and improving the security of a wireless IoT system.

The purpose of the work is to study methods of detecting and preventing information security vulnerabilities in the IoT system.

Methods of building IoT systems, basic security protocols and data transmission technologies are reviewed. The analysis of threats and vulnerabilities of information security of IoT systems is carried out, and the methods of their detection and prevention by means of various protocols and other technologies are offered.

A system for building, developing and maintaining a secure IoT system is proposed.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЕБУ – Електронні блоки управління

ІТ – Інформаційні технології

ОТ – Операційні технології

API – Application Programming Interface

CoAP – Протокол обмежених додатків

CSRF – Підроблення запитів між сайтами

DAR – Data at Rest

Denial of Service – відмова в обслуговуванні.

DIT – Data in Transit

DIU – Data In Use

DLP – Data Loss Prevention

ECDH – Еліптична крива Діффі–Хеллмана

ECDSA – Алгоритм цифрового підпису еліптичної кривої

GPS – Системи глобального позиціонування

HMAC – Hash–based message authentication

IAM – Identity and Access Management

IoT – Internet of Things

JTAG – Joint Test Action Group

MAC ID – Media Access Control ID

NAT–PMP – NAT–Port Mapping Protocol

QR – Quick Response Code

RFID – Radio frequency identification

SCADA – Supervisory Control And Data

SDP – Session Description Protocol

SSID – ServiceSetIdentifier

TLS – Transport Layer Security

XSS – Уразливості міжсайтових сценаріїв

ВСТУП

На ринку спостерігається початок широкого впровадження Інтернету речей (IoT) у споживчому секторі. Переносні прилади, розумна побутова техніка, освітлення та інші розумні пристрої стають масовими. Популярність розумних споживчих пристроїв очікується, що буде і надалі зростатання шаленими темпами.

Доповідь Verizon IoT прогнозує, що кількість підключень IoT для бізнесу збільшиться на 28% за рік з 2011 по 2020 рік. Такі галузі, як виробництво, енергетика, транспорт та роздрібна торгівля, вже застосовують Ініціативи IoT. У своєму документі з позиціонування промислового Інтернету речей за 2015 рік Accenture прогнозує, що до 2030 року. "Промисловий" IoT лише в США коштуватиме 7,1 трильйона доларів і підтримуватиме підвищення ефективності, безпеки, продуктивність та надання послуг.

Муніципалітети у всьому світі також приймають IoT, працюючи над тим, щоб стати розумними містами, які покладаються на дані, отримані тисячами різноманітних датчиків, розповсюджених по географічному регіону. У галузі охорони здоров’я ми також починаймо бачити, як буде виглядати IoT із виробниками, що вбудовують мережеві зв’язки та інтелект всередині таких пристроїв, як приліжкове обладнання пацієнта. Ми можемо побачити початок взаємозв’язків між особистим та діловим.

Можливості IoT, де розумні пристрої незабаром зможуть збирати інформацію та передавати цю інформацію постачальників медичних послуг через хмару. Транспортний сектор – ще одна захоплююча сфера, де концепція IoT – це підключені транспортні засоби, а інфраструктура для підтримки цих транспортних засобів набуває популярності. Крім того, експерименти з автомобілями без водіїв дадуть майбутнє, де буде можливість збирати та аналізувати дані датчиків з IoT для придорожнього обладнання стане ще більш важливим. В енергетичному секторі інтегровані та взаємопов’язані системи (наприклад, сучасні інтегровані системи підстанцій,

системи інтелектуальної мережі) мають тенденцію до підвищення рівня потужності автоматизація системи та віддалена доступність для доставки інформації широкому колу користувачів майже в реальному часі, а також контролювати кількість завдань для впорядкування операцій та ефективності.

1 АНАЛІЗ ТЕХНОЛОГІЇ «ІНТЕРНЕТ РЕЧЕЙ»

1.1 Історія технології «Інтернет речей»

Термін «Інтернет речей» вперше було сформульовано в кінці XX–го століття у 1999 році. Це концепція комунікації об'єктів (речей), які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини. Таким чином, всі пристрої в будинках, в автомобілях, на користувачеві виконують обробку інформації, її аналіз та обмін між собою та, залежно від результатів, приймають рішення і виконують певні дії. Але ця історія почалася значно раніше.

1) 1926 рік − Нікола Тесла сказав, що в майбутньому радіо перетвориться на «великий мозок», усі речі стануть частиною єдиного цілого, а технологічні машини будуть поміщатися в кишені.

2) 1990 рік − один з авторів протоколу TCP/IP Джон Ромкі створив першу у світі інтернет–річ – він підключив до Інтернету свій тостер.

3) 1999 рік − Кевін Ештон вводить в обіг термін «Інтернет речей».

4) 2008 рік − відбувся перехід від інтернету людей до Інтернету речей − кількість підключених до мережі предметів перевищила кількість осіб.

5) 2014 рік − ринок рішень у галузі інтернету речей (1,9 трильйонів доларів) перевищує обсяг ВВП однієї з найбільш динамічних економік світу − Індії (1,87 трлн доларів).

Один з основоположних принципів інтернету речей – у кожного пристрою, будь то пилосос, холодильник або пральна машина, є модуль підключення до інтернету з можливістю взаємодії з домашнім комп'ютером або смартфоном домовласника. Особливу роль в інтернеті речей відіграють засоби вимірювання, що забезпечують перетворення відомостей про

зовнішнє середовище в дані, що може зрозуміти машина, і тим самим здатні наповнити обчислювальне середовище значущою інформацією. Використовується широкий клас засобів вимірювання, від елементарних датчиків (наприклад, температури, тиску, освітленості), приладів обліку споживання (таких, як інтелектуальні лічильники) до складних інтегрованих вимірювальних систем [2].

Кілька систем, які «населяють» ваше житло, постійно стежать за станом будинку: чи знаходиться в приміщенні власник (якщо так, то потрібно включити йому світло), яка вологість повітря і так далі. По суті, вони роблять те, що раніше мала робити людина: створюють комфортні умови для проживання і за наказом власника виконують певні дії. Можна сказати, що будинок стає вашим союзником у боротьбі з побутовими труднощами. Наблизитися до реалізації інтернету речей, нехай навіть і не реалізувавши саму ідею в строгому сенсі, можна, додавши можливість віддаленого управління лампочкою або кавоваркою дуже зручно ще на підході до будинку доручити техніці зробити каву, включити світло в коридорі і підготувати комп’ютер. Це поки не повноцінний «інтернет речей»: всі ці пристрої спілкуються з людьми, а не один з одним. Важливо навчити пристрої взаємодіяти один з одним. Тоді керувати будинком будете не тільки людина, але і техніка.

1.2 Принципи роботи Інтернету речей

За визначенням, Інтернет є глобальною системою взаємозалежних комп’ютерних мереж, які використовують набір протоколів Інтернету (TCP/IP) для зв’язку пристроїв по всьому світу.

Термін Інтернет використовується для позначення конкретної глобальної системи взаємопов’язаних пристроїв. У простому визначенні Інтернету можна сказати, що Інтернет визначається як спосіб зв’язку, за допомогою якого можна отримувати, передавати інформацію між кількома пристроями, що може використовуватися для декількох операцій.

Це можуть бути фізичні пристрої, транспортні засоби, побутова техніка, електронні пристрої, датчики, виконавчі механізми, програмне забезпечення і так далі, які можна підключати і обмінюватися даними.

Унікальним аспектом IoT, в порівнянні з іншими мережевими системами, очевидно є наявність безлічі фізичних речей і пристроїв, відмінних від обчислювальних пристроїв і пристроїв обробки даних. На рис. 1.1 зображені типи пристроїв в моделі MCE–T. Модель розглядає IoT як мережу пристроїв, тісно пов’язаних з речами. Сенсорні і виконавчі пристрої взаємодіють з фізичними речами в навколишньому середовищі.

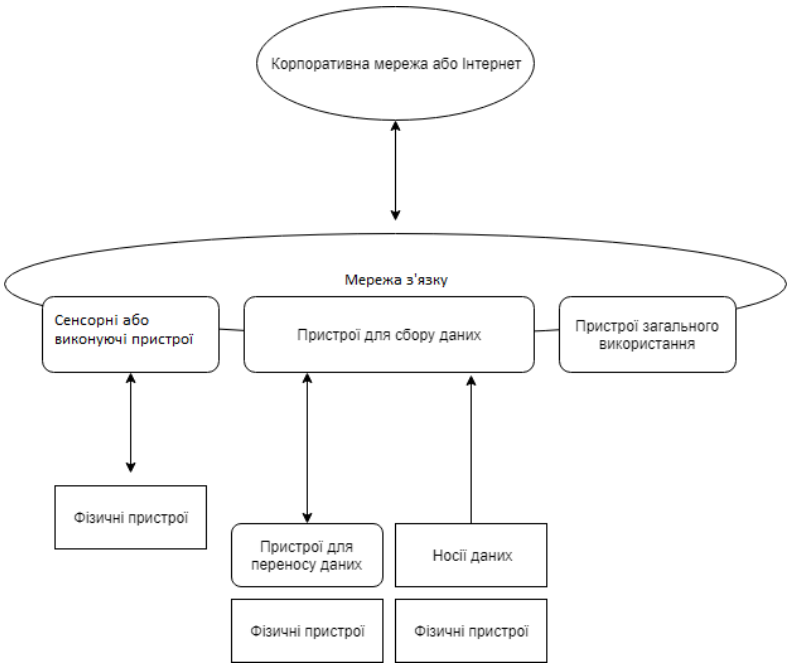

Рисунок 1.1 – Типи пристроїв і їх взаємозв’язок з фізичними речами

Ця модель проводить відмінність між пристроями перенесення даних і носіями даних. Як мінімум, пристрій завжди має можливості зв'язку і може мати інші електронні можливості. Прикладом пристрою перенесення даних є radio frequency identification(RFID)–бірка. У той же час носій даних – це елемент, приєднаний до фізичної речі з метою ідентифікації або інформування.

Технології, що використовуються для взаємодії між облаштуваннями збору даних і облаштуваннями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Приклади кожної з них нижче.

1) Радіочастотні: радіочастотні ідентифікаційні RFID–біркі, або радіопозначки.

2) Оптичні: штрих–коди і Quick Response Code(QR) – коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.

3) Гальванічне збудження: прикладом можуть служити медичні імпланти, які використовують електропровідні властивості людського тіла. В ході комунікації між імплантом і поверхнею гальванічна пара передає сигнали з імпланта на електроди, виведені на шкіру. Ця схема використовує дуже мало енергії, що дозволяє знизити розмір і складність імплантованого пристрою.

Останнім типом пристроїв з рисунку 1.1 є пристрої загального призначення. Вони володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT. Вдалим прикладом є технологія «розумного будинку», яка може інтегрувати практично будь–який пристрій в будинку в мережу для централізованого або дистанційного управлення.

Основними стовпами IoT–проектів або IoT–рішень є:

- датчики/пристрої;
- зв'язок;
- обробка даних;

– інтерфейс користувача.

По–перше, датчики або пристрої збирають дані з–поміж себе. Це може бути як просте показання температури, так і складне, як повний відеопотік. Як правило, використовують «датчики/пристрої», тому що кілька датчиків можуть бути об’єднані разом, або датчики можуть бути частиною пристрою. Наприклад, телефон – це пристрій з декількома датчиками (камера, акселерометр, GPS і так далі).

Необхідно відмітити, що будь то автономний датчик або повноцінний пристрій, на першому етапі дані збираються з середовища будь–яким чином. Потім ці дані відправляються в хмару, але для цього потрібен спосіб. Датчики/пристрої можуть бути підключені до хмари різними способами, включаючи мобільний зв’язок, супутниковий зв’язок, WiFi, Bluetooth, глобальні мережі з низьким енергоспоживанням (LPWAN) або пряме підключення до Інтернету через Ethernet.

У кожному варіанті є компроміс між енергоспоживанням, діапазоном і пропускною спроможністю. Вибір оптимального варіанту підключення залежить від конкретного додатка IoT, але всі вони виконують одну й ту ж задачу: передача даних до хмари.

Як тільки дані потрапляють в хмару, програмне забезпечення їх обробляє. Це може бути дуже просто, наприклад, перевірити, що показники температури знаходяться в допустимих межах. Або це також може бути більш складніші дії, наприклад, використовувати комп’ютерний зір на відео для ідентифікації об’єктів (наприклад, зловмисників у будинку). Але що відбувається, коли температура занадто висока або якщо у будинку є зловмисник? Ось де користувач має отримати сповіщення від програмного забезпечення.

Потім інформація стає корисною для кінцевого користувача. Це може бути зроблено за допомогою попередження для користувача (електронна пошта, текст, повідомлення тощо). Наприклад, текстове повідомлення, коли температура занадто висока в холодному сховищі компанії.

Крім того, користувач може мати інтерфейс, який дозволяє йому завчасно реєструватися в системі. Користувач може захотіти перевірити відеопотоки в своєму будинку через додаток для телефону або веб–браузер.

Однак це не завжди односторонній обмін інформацією. В залежності від програми IoT користувач також може виконувати дії і впливати на систему. Наприклад, користувач може віддалено регулювати температуру в холодильнику за допомогою програми на своєму телефоні.

Деякі дії виконуються автоматично. Замість того, щоб чекати, поки користувач відрегулює температуру, система може зробити це автоматично за допомогою заданих параметрів. І замість того, щоб просто подзвонити користувачеві, щоб попередити його про зловмисника, система IoT також може автоматично повідомляти відповідні органи [3].

Нині існує декілька «базових» технологій для побудови мереж, що можуть використовуватися для:

- Wi–Fi;
- Bluetooth;
- ZigBee.

Розглянемо їх детальніше.

1.3 Стандарт Wi–Fi

Wi–Fi – торгова марка Wi–Fi Alliance для бездротових мереж на базі стандарту IEEE 802.11. Ноутбук або комунікатор без підключення до мережі Інтернет сьогодні є лише шматком «заліза». Завдяки широкому використанню Wi–Fi для вирішення проблеми підключення до Інтернету цей термін став добре відомим.

Продукти, що призначалися спочатку для систем касового обслуговування, були виведені на ринок під маркою WaveLAN і забезпечували швидкість передачі даних від 1 до 2 Мбіт/с. Творець Wi–Fi – ВікХейз (VicHayes) знаходився в команді, що брала участь в розробці таких стандартів, як IEEE 802.11b, IEEE 802.11a і IEEE 802.11g. Зазвичай схема мережі Wi–Fi містить не менше однієї точки доступу і не менше одного клієнта.

Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів на швидкості 0,1 Мбіт/с кожні 100 мс. Тому 0,1 Мбіт/с – найменша швидкість передачі даних для Wi–Fi. Знаючи SSID мережі, клієнт може з'ясувати, чи можливе підключення до даної точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на підставі даних про рівень сигналу. Стандарт Wi–Fi дає клієнтові повну свободу при виборі критеріїв для з'єднання.

Для організації бездротової мережі в замкнутому просторі застосовуються передавачі зі всеспрямованими антенами. Слід мати на увазі, що через стіни з великим вмістом металевої арматури (в залізобетонних будівлях такими є несучі стіни) радіохвилі діапазону 2,4 ГГц іноді можуть взагалі не проходити, тому в кімнатах, розділених подібної стіною, доведеться ставити свої точки доступу. Потужність, яку випромінює передавачем точки доступу або ж клієнтської станції, що працює за стандартом IEEE 802.11, не перевищує 0,1 Вт, але багато виробників бездротових точок доступу обмежують потужність лише програмним шляхом, і досить просто підняти потужність до 0,2–0,5 Вт.

Забезпечення безпеки у Wi–Fi забезпечується завдяки шифруванню. Стандарт шифрування WEP може бути відносно легко зламаний навіть при правильній конфігурації (через слабку стійкість алгоритму). Незважаючи на те, що нові пристрої підтримують досконаліший протокол шифрування даних WPA і WPA2.

Багато старих точки доступу немають підтримки його і вимагають заміни.

Прийняття стандарту IEEE 802.11i (WPA2) в червні 2004 року зробило доступною більш ефективну схему автентифікації і шифрування, яка застосовується в новому обладнанні. Для реалізації протоколів WPA і WPA2 потрібно більш надійний пароль, ніж той, який зазвичай призначається користувачем.

Продукти для бездротових мереж, що відповідають стандарту IEEE802.11, пропонують чотири рівні засобів безпеки: фізичний, ідентифікатор набору служб (SSID – ServiceSetIdentifier), ідентифікатор управління доступом до середовища (MAC ID – Media Access Control ID) і шифрування.

Багато організацій використовують додаткове шифрування (наприклад, VPN) для захисту від вторгнення. На даний момент основним методом злому WPA2 є підбір пароля, тому рекомендується використовувати складні цифро–буквені паролі, що містять як маленькі так и великі літери, цифри та спеціальні символи у собі для того, щоб максимально ускладнити завдання підбору та злому паролю для зловмисника та зробити цю процедуру як найбільш довшою [4].

1.4 Стандарт Bluetooth

Bluetooth забезпечує обмін інформацією між такими пристроями як персональні комп’ютери (настільні, кишенькові, ноутбуки), мобільні телефони, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній, недорогій, повсюдно доступній радіочастоті для ближнього зв’язку. Бездротовий канал дозволяє цим пристроям повідомляти, коли вони знаходяться в радіусі від 1до 200 метрів один від одного (дальність сильно залежить від перешкод), навіть у різних приміщеннях.

Варто відзначити, що компанія AIRcable випустила Bluetooth–адаптер Host XR з радіусом дії близько 30 км. Для спільної роботи Bluetooth–пристроїв необхідно, щоб всі вони підтримували загальний профіль. Профіль – набір функцій або можливостей, доступних для певного пристрою Bluetooth. Технологія Bluetooth спирається на неліцензованому частотному діапазоні 2,4 ÷ 2,4835 ГГц. При цьому використовуються широкі захисні смуги: нижня межа частотного діапазону становить 2 ГГц, а верхня – 3,5 ГГц. Частота (положення центру спектра) задається з точністю ± 75 кГц. Дрейф частоти в цей інтервал не входить. Кодування сигналу здійснюється подворівневою схемою GFSK (Gaussian Frequency Shift Keying) логічного 0 і 1 відповідають дві різні частоти. В обумовленої частотній смузі виділяється 79 радіоканалів по 1 МГц кожен.

Для захисту Bluetooth–з'єднання передбачено шифрування даних, що передаються, а також виконання процедури авторизації пристроїв. Шифрування даних відбувається з ключем, ефективна довжина якого – від 8 до 128 біт, що дозволяє встановлювати рівень стійкості результуючого. Тому варто відразу відмітити, що правильно зконфігуровані Bluetooth–пристрої самовільно з'єднуватися не можуть, тому випадкових витік важливої інформації до сторонніх осіб не буває.

Залежно від виконуваних завдань специфікація Bluetooth передбачає три режими захисту, які можуть використовуватися як окремо, так і в різних комбінаціях.

1) У першому режимі – мінімальному (який зазвичай застосовується за умовчанням) – ніяких заходів для безпечного використання Bluetooth – пристрою не робиться. Дані кодуються загальним ключем і можуть прийматися будь–якими пристроями без обмежень. Це дуже не безпечний режим роботи захисту роботи Bluetooth.

2) У другому режимі здійснюється захист на рівні пристроїв, тобто активуються заходи безпеки, ґрунтовані на процесах упізнання/аутентифікації (authentication) і дозвол/авторизації (authorization). У цьому режимі визначаються різні рівні довіри (trust) для кожної послуги, запропонованої пристроєм. Рівень доступу може вказуватися безпосередньо в чіпі, і відповідно до цього пристрій отримуватиме певні дані від інших пристроїв.

3) Третій режим – захист на рівні сеансу зв'язку, де дані кодуються 128–бітовими випадковими числами, що зберігаються в кожній парі пристроїв, які беруть участь в конкретному сеансі зв'язку. Цей режим вимагає упізнання і використовує кодування/шифрування даних (encryption).

Другий і третій режими часто застосовуються одночасно. Головне завдання процесу аутентифікації полягає в тому, щоб перевірити, чи дійсно пристрій, що ініціює сеанс зв'язку, є саме тим, за яке себе видає.

Захисні функції Bluetooth повинні забезпечувати безпечну комунікацію на усіх рівнях зв'язку. Але на практиці, незважаючи на передбачену стандартом безпеку, в цій технології є цілий ряд істотних вад.

Наприклад, слабким місцем захисту Bluetooth–пристроїв є те, що виробники прагнуть надати користувачам широкі повноваження і контроль над пристроями і їх конфігурацією. В той же час сучасна Bluetooth–технологія має недостатні засоби для упізнання користувачів (тобто система безпеки Bluetooth не бере до уваги особу або наміри користувача), що робить Bluetooth–пристрою особливо уразливими до так званих spoofing–нападів (радіодезінформації) і неправильного застосування розпізнавальних пристроїв.

Можливість використання коротких паролів, що допускається стандартом, є ще однією причиною уразливості Bluetooth–з'єднання, що, як і у випадку з використанням простих паролів системними адміністраторами

комп’ютерних мереж, може привести до їх вгадування (наприклад, при автоматичному порівнянні з базою звичайних/поширених паролів) [5].

1.5 Стандарт ZigBee

ZigBee – назва набору мережевих протоколів верхнього рівня, що використовують маленькі, малопотужні радіопередавачі, засновані на стандарті IEEE 802.15.4. Цей стандарт описує бездротові персональні обчислювальні мережі (WPAN). ZigBee націлена на додатки, яким потрібен тривалий час автономної роботи від батарей і висока безпека передачі даних при невеликих швидкостях їх передачі.

Основна особливість технології ZigBee полягає в тому, що вона при відносно невисокому енергоспоживанні підтримує не тільки прості топології бездротового зв’язку («точка–точка» і «зірка»), а й складні бездротові мережі з комірчастою топологією з ретрансляцією і маршрутизацією повідомлень. Області застосування даної технології – це побудова бездротових мереж датчиків, автоматизація житлових і споруджуваних приміщень, створення індивідуального діагностичного медичного обладнання, системи промислового моніторингу та управління, а також при розробці побутової електроніки і персональних комп’ютерів.

Мережі, утворені за протоколом ZigBee почали розглядатися з1998 року, коли виникла необхідність в самоорганізованих системах зв'язку. ZigBee націлений на додатки, яким потрібен тривалий час автономної роботи від батарей і висока безпека передачі даних при невеликих швидкостях передачі. ZigBee працює в радіодіапазоні: 868 МГц в Європі, 915 МГц в США і в Австралії, і 2,4 ГГц в більшості країн в світі [6].

Так як ZigBee–пристрій велику частину часу перебуває в сплячому режимі, рівень споживання енергії може бути дуже низьким, завдяки чому досягається тривала робота від батарей. ZigBee–пристрій може активуватися (тобто переходити від сплячого режиму до активного) за 15 мс або менше, затримка його відгуку може бути дуже малою, особливо в порівнянні з Bluetooth, для якого затримка, що утворюється при переході від сплячого режиму до активного, зазвичай досягає трьох секунд.

Беручи до уваги такі критерії, як ціна чіпів, дешевизна і швидкість освоєння технології, низьке енергоспоживання і стійкість до завад, можна сказати, що ZigBee нерідко є зараз найкращим вибором для будь якого масштабу бізнеса. Чіпи для реалізації ZigBee випускають такі відомі фірми, як TexasInstruments, Freescale, Atmel, STMicroelectronics, OKI і так далі. Це гарантує низькі ціни на комплектуючі для даної технології. ZigBee – це технологія, що заповнює нішу низькошвидкісних бездротових мереж з низьким енергоспоживанням, призначених для систем управління з великою кількістю вузлів, таких як системи освітлення в будівлях, системи спостереження за парком промислового обладнання тощо.

Система безпеки відповідно до специфікації ZigBee побудована на 128–бітовому AES алгоритмі. Передбачені специфікацією ZigBee служби безпеки визначають створення ключів, управління пристроями і захист даних. ZigBee використовує 128–бітові ключі для реалізації механізмів безпеки. Ключ може бути асоційований або з мережею (і використовуватися рівнями ZigBee і MAC підрівнем) або з каналом зв’язку.

Архітектура безпеки розподіляється між мережевими рівнями.

1) Підрівень MAC здатний встановлювати надійний зв’язок з сусіднім пристроєм. Як правило, він використовує рівень безпеки, визначуваний верхніми рівнями.

2) Мережевий рівень управляє маршрутизацією, обробляє отримані повідомлення і може направляти запити. Вихідні фрейми використовуватимуть ключ відповідного каналу зв’язку згідно

маршрутизації, якщо він доступний; інакше для захисту корисного навантаження від зовнішніх пристроїв використовуватиметься мережевий ключ.

3) Рівень додатків встановлює ключі і робить транспортні послуги як об’єкту пристрою (ZDO), так і додаткам. Він відповідає також за поширення повідомлень про зміни в пристроях усередині мережі, які можуть виходити як від самих пристроїв (наприклад, проста зміна статусу), так і від центру управління безпекою (який може повідомити, що певний пристрій видаляється з мережі). Рівень також маршрутизує запити облаштувань центру управління безпекою і оновлення мережевого ключа від центру управління безпекою усім пристроям. Також,є дуже важливим те, що об’єкт облаштування ZDO підтримує усі політики безпеки пристрою. Наразі це один з ключових факторів, що потрібно розглядати у випадку використання данної техногогії.

1.6 Класифікація приладів, що використовують «Інтернет речей»

У запропонованій технології «Інтернет речей» розділений на промисловий і споживчий. До промислового зазвичай відносять розумний транспорт або підключення автомобілі (Connected Cars), розумне місто (Smart City), розумні мережі (Smart Grid) в енергетиці, розумні машини і цілі фабрики. До споживчого – носяться пристрої (Wearables), підключені пристрої (Connected Devices або Appliances), розумний будинок (Smart Home) та ін.

В наш час не всі напрями однаково перспективні. Harvard Business Review виділяє п’ять ключових ринків:

- connected wearables;
- connected cars;
- connected homes;
- connected cities;

– industrial internet.

Отже, розглянемо більш детально ці ринки.

1) Connected Wearables – це тип інтернет–речей, які ви можете взяти із собою або вдягнути на себе. Назва пішла від глаголу «to wear». Розумні годинник і інші носяться пристрої діють як розширення смартфона, надаючи користувачу миттєвий доступ до потужних додатків, електронній пошті, текстових повідомлень і мережі. Так як розумні годинники знаходяться в зародковому стані, вони схильні до порушень безпеки. Недавнє дослідження, проведене Hewlett–Packard, виявило критичні проблеми безпеки в кращих пристроях SmartWatch. Найбільш поширеною проблемою була недостатня авторизація користувача. Всі проаналізовані розумні годинники мали призначений для користувача інтерфейс, в якому була відсутня двухфакторна перевірка справжності або здатність блокувати облікові записи після кількох невдалих спроб введення пароля. До 30% протестованих розумних годин були сприйнятливі до збирання інформації. Дослідження також прийшло до висновку, що розумні годинники не мають необхідних протоколів шифрування. У той час як всі пристрої використовували шифрування SSL/TLS, 40 відсотків розумних годинників були уразливі для таких проблем, як SSL V2 і POODLE. Хмарні веб–інтерфейси, в яких 30% використовуваних пристроїв дозволяли хакерам ідентифікувати дійсні облікові записи користувачів за допомогою служб, що дозволяють їм скинути пароль. Крім того, у семи з десяти розумних годин були проблеми з оновленнями прошивки, що дозволяло завантажувати дані з–за відсутності шифрування.

2) Connected Cars – це транспортний засіб, який з’єднано з іншими автомобілями і пристроями, мережами і сервісами, які охоплюють велику інфраструктуру, включаю й ваш будинок і офіс. У цій сфері є декілька специфічних проблем безпеки. Управління роботою транспортного засобу: катастрофічні інциденти, що призводять до травм і судових позовів, можуть бути в найближчому майбутньому. Відомі дослідники в області кібербезпеки

Чарлі Міллер і Кріс Валасек продемонстрували кілька перевірок концепції, в ході яких їм вдалося контролювати гальмування і рульове керування автомобілем за допомогою адаптивної системи круїз–контролю. Незважаючи на те, що така атака є дорогою і має меншу вірогідність, ніж витік даних і несанкціонований доступ, в даний час ця глобальна аудиторія виявилася можливою. Та несанкціонований доступ до транспортних засобів: у викрадачів з'явився новий спосіб проникнення в заблоковані транспортні засоби. Багато автомобільних компаній вирішило замінити фізичні системи запалювання на системи без ключа, використовуючи мобільні додатки або бездротові брелоки. Ці нові механізми доступу означають, що способи отримання незаконного в'їзду включають в себе перехоплення бездротового зв'язку між транспортним засобом і мобільним додатком або між бездротовим брелоком і транспортним засобом, щоб отримати реєстраційні дані для входу. У New York Times є документовані методи, такі як пристрої емуляції бездротових ключів і «підсилювачі потужності», які збільшують діапазон бездротового сигналу при пошуку облікових даних для входу. Якщо власник знаходиться в будинку або іншому місці поруч з автомобілем, злочинці можуть отримати доступ, коли їх бездротовий брелок відгукнеться.

3) Connected Homes – це мережа, призначена для того, щоб пов'язувати і поєднувати декілька пристроїв, сервісів і додатків, починаючи від комунікацій, безпеки і домашньої автоматизації. Ці послуги та програми надаються через кілька взаємопов'язаних і інтегрованих пристроїв, датчиків, інструментів і платформ. Жителям будинку надається інтелектуальний і контекстуальний доступ і контроль в режимі реального часу, і господарі можуть управляти будинком як віддалено, так і всередині нього. Пристрої в екосистемі «розумного будинку» збирають інформацію про користувачів в їх найбільш випадкових і особистих умовах. Вони дають йому дуже конфіденційною інформації, яка має потенціал для експлуатації. Все було б добре, якби технологічні виробники дотримувалися свої обмеження і реєстрували тільки ті дані, які їм потрібні. Експлуатація приватного життя є

найбільш нагальною проблемою технології розумного будинку. Також такі пристрої можна використовувати як засоби для проведення інших хакерських атак.

4) Connected Cities. Концепція бере інновації і технології IoT і застосовує їх до потреб міста. Наприклад, в Connected Citie можуть використовуватися пристрої IoT для моніторингу та оптимізації потоку трафіку на дорогах, для виявлення пострілів і інших перешкод або для підключення комунальних лічильників. У недавньому минулому ідея розумних міст була концептуалізована тільки в науково–фантастичних фільмах і художніх книгах. Однак сьогодні ця ідея швидко переходить від творчих сфер в реальності. Подібно до того, як розумні міста виникають по всьому світу, вони також створили унікальну парадигму загроз безпеки Одна з основних проблем, пов'язаних з «розумними» містами і будівлями в них, полягає в тому, що обладнання і датчики, які передають дані, можуть бути легко зламані. Хакер може потім викликати проблеми з сигналом і всі види у більшому масштабі, такі як відключення метрополітену або закачування забруднюючих речовин в основне водопостачання. Виробники програмного і апаратного забезпечення часто випускають такі продукти, не замислюючись про реалізовані функції безпеки. Уряди часто перевіряють і тестують такі продукти, в основному на функціональність, але часто параметри кібербезпеки не враховуються. За оцінками експертів, в різних містах по всьому світу, включаючи Лондон, Вашингтон і Нью–Йорк, існує близько 200 000 датчиків контролю дорожнього руху, вразливих для маніпуляцій. На жаль, більшість виробників Smart Cities або не знають про кібербезпеку, або не мають персоналу, що володіє технічними ноу–хау для вирішення цих проблем.

5) Industrial Internet. Уявіть собі шосе, де автомобілі можуть безпечно переміщатися по місцю призначення без водія. Уявіть собі будинок, в якому здоров'я літній пацієнтки ретельно контролюється лікарем лікарні. Уявіть собі місто, яке значно скорочує відходи завдяки вбудованим датчикам

у водопровідні труби, будівлі, лічильники паркування тощо. Вони перестають бути частиною далекого майбутнього. Ці сценарії починають відбуватися зараз, завдяки зближенню машин і інтелектуальних даних в так званому Industrial Internet (Промисловий Інтернет). Промисловий Інтернет перетворює промисловість за допомогою інтелектуальних, взаємопов'язаних об'єктів, які значно підвищують продуктивність, знижують експлуатаційні витрати і підвищують надійність. Розміщення даних в хмарі (публічне чи приватне) є невід'ємним компонентом IIoT. Але це має величезне значення для безпеки. Традиційно виробники систем промислового контролю стверджують, що їх системи мають вбудований повітряний зазор. Наразі це не вірно, коли ці системи мають пряме або непряме підключення до Інтернету. IIoT буде сприяти розумінню того, що усі гаджети повинні мати вбудовані функції аутентифікації і безпеки [7].

2 ЗАГРОЗИ ФІЗИЧНИМ ОСОБАМ ТА ПІДПРИЕМЦЯМ ВІД IOT СИСТЕМ

IoT представляє велику кількість нових пристроїв, які будуть розгорнуті або вбудовані в організації системи. Дані, отримані з цих пристроїв, можуть бути проаналізовані та використані. У деяких випадках розгорнуті пристрої здатні виконувати завдання. Ці описані крайові пристрої стануть розповсюдженими і дозволять масовий збір даних. Аналіз цих даних дозволить зробити невидимі зв'язки, які можуть викликати занепокоєння щодо конфіденційності приватних осіб чи груп людей. У деяких випадках люди можуть навіть не знати про, що вони відстежуються або реєструються. У всіх випадках забезпечення безпеки кожного компонента в системі IoT важливо для збереження програм від несанкціонованого використання потужності IoT.

Ось кілька прикладів нових загроз та векторів атак, якими можуть скористатися зловмисники:

1) До систем управління, транспортних засобів і навіть людського тіла можна отримати доступ і маніпулювати ними, що може спричинити травми або гірше через несанкціонований доступ до систем фізичного зондування, (включаючи транспортний засіб, Supervisory Control And Data (SCADA — диспетчерське управління та збір даних) SCADA, імплантовані та неімплантовані медичні вироби, виробничі підприємства та інші кіберфізичні реалізації IoT

2) Постачальники медичних послуг можуть неправильно діагностувати та лікувати пацієнтів на основі модифікованої інформації про стан здоров’я або маніпулюючи датчиками даних.

3) Зловмисники можуть отримати фізичний доступ до будинків або комерційного бізнесу через атаки на електронні та віддалені керовані механізми замків дверей.

4) Втрата контролю над транспортним засобом може бути спричинена відмовою в обслуговуванні за допомогою внутрішньої шини зв'язку.

5) Важлива інформація щодо безпеки, така як попередження про непрацюючий газопровід, може залишитися непоміченою через DDoS атаку датчика IoT.

6) Критичні пошкодження інфраструктури можуть статися через перевизначення критичних характеристик безпеки або джерела живлення, температури або регулювання.

7) Зловмисні сторони можуть викрадати особисті дані та гроші на основі витоку конфіденційної інформації, включаючи особисту інформацію про стан здоров'я .

8) Непередбачуваний витік особистої або конфіденційної інформації може відбуватися шляхом агрегування даних з багатьох різних систем та датчиків, або злиття персональних даних, які були зібрані в умовах різної конфіденційност.

9) Незаконне спостереження через постійні можливості віддаленого моніторингу, що пропонуються дрібними пристроями IoT.

10) Маніпулювання фінансовими операціями.

11) Грошові втрати, спричинені неможливістю надати послугу.

12) Вандалізм, крадіжка або знищення активів IoT, які розміщені у віддалених місцях та не мають фізичної безпеки елементів керування.

13) Можливість отримати несанкціонований доступ до крайових пристроїв IoT для маніпулювання даними, використовуючи виклики пов'язані з оновленням програмного забезпечення та прошивки вбудованих пристроїв (наприклад, вбудованих у машини, будинки, медичні пристрої.

14) Можливість отримати несанкціонований доступ до корпоративної мережі шляхом компрометації крайових пристроїв IoT та використання переваги довірчих відносин.

15) Можливість створення бот–мереж шляхом компрометації великої кількості крайових пристроїв IoT.

16) Можливість видавати себе за пристрої IoT, отримуючи доступ до матеріалів, що зберігаються на пристроях, які покладаються на надійні сховища, що базуються на програмному забезпеченні.

IoT покладається на крайові пристрої, які збирають дані або виконують певні дії. Ці компоненти можуть мати форму автономних пристроїв, наприклад інтелектуальні датчики або розумні лічильники, можуть бути вбудовані у великі системи, такі як електронні блоки управління (ЕБУ) підключені до транспортних засобів. Ці крайові компоненти збирають, зберігають або обробляють дані. Вони об'єднані в мережу, або разом, або через якийсь шлюз, як правило, використовуючи радіочастотний зв'язок. Це дозволяє встановити зв’язок із серверною службою, часто розміщеною в хмарі.

3 РЕКОМЕНДОВАНІ ЗАСОБИ КОНТРОЛЮ БЕЗПЕКИ ІОТ СИСТЕМ

Наступні засоби контролю безпеки рекомендуються для організацій, що впроваджують можливості IoT. Ці елементи управління мають бути адаптованими до специфічних для IoT характеристик, щоб дозволити людям, які вперше застосовують IoT, запобігти багатьом пов'язаних з цим ризикам за допомогою цієї нової технології.

3.1 Аналіз впливу на приватне життя зацікавлених сторін і прийняття індивідуального підходу до ІОТ

IoT надає організаціям потужні інструменти для збору та аналізу даних. Ці дані подаються у різних формах, і у багатьох випадках із IoT є залишкові дані, які або збираються, або можуть бути зібрані за допомогою ретельного аналізу. Коли організації починають застосовувати IoT, ми можемо побачити розміщення датчиків, відеокамер та іншого обладнання, спрямованого на збір інформації. Ці компоненти IoT будуть широко використовуватися в громадських приміщеннях, а також у приватних будинках та в деяких випадках навіть використовуватися окремими особами. Багато компонентів IoT включатимуть використання системи глобального позиціонування (GPS), які можуть забезпечувати відстеження місцезнаходження осіб або активів цих осіб (наприклад, автомобілів/телефонів). Інший аспектом IoT є те, що багато систем IoT перекриваються щодо типів даних, які збираються. Таким чином, підвищується потенціал загальної суттєвої інформації, навіть якщо ці дві системи збору експлуатуються абсолютно різними сутностями. У цих випадках заповзятливі маркетологи чи зловмисники можуть цим скористатися та збирати дані для досягнення своїх цілей без відома осіб, які відстежуються. Однією з унікальних проблем, пов’язаних з приватністю в Інтернеті речей, є те, що незабаром з’явиться можливість переповнити

суспільство пристроями збору даних та датчики. Ці пристрої іноді будуть використовуватися зловмисно, а інколи можуть ненавмисно збирати інформацію про осіб, які не дали згоди на відстеження. Для власника системи буде важливо зрозуміти, які дії допустимі щодо даних, які збираються ненавмисно від приватних осіб.

Датчики IoT також будуть використовуватися таким чином, щоб покращити взаємодію з клієнтами. У цих випадках клієнт буде отримувати повідомлення про те, що він взаємодіє з якоюсь системою IoT. Яскравий приклад цього можна знайти в роздрібній галузі.

Слід точно враховувати, які дані зберігаються про кожного користувача, і вплив, який вони мають мати на відповідність та правила конфіденційності. На додаток до перевірки, що вся конфіденційна інформація захищена в достатній мірі, важливо також враховувати ризики до ланцюга поставок. Якщо компоненти, що складають вашу систему IoT, скомпрометовані в ланцюзі поставок, ризик вплив конфіденційної інформації є високим.

Інше питання стосується того, хто має доступ до конфіденціально збережених даних. Ці дані, швидше за все, будуть надані третім сторонам, тому доступ до будь–якої конфіденційної інформації слід реєструвати для аудиту та перевіряти на відповідність з політикою.

Враховуючи складність ситуації конфіденційності IoT, важливо для будь–якої організації витрачати відповідні ресурси для забезпечення захисту конфіденційної інформації зацікавлених сторін. При розробці IoT, дотримання принципів конфіденційності у проекті дозволить інтегрувати відповідні гарантії конфіденційності в межах системи. Цими принципами можна керуватися, розробляючи реалізацію різних компонентів, що входять до складу системи IoT. Робоча група з питань захисту даних у вересні 2014 р. опублікував вказівки про те, що всі зацікавлені сторони IoT повинні застосовувати ці принципи до впровадження в будь–якому регіоні світу. У наступних розділах представлений специфічний для IoT погляд на ці

принципи. Організації можуть використовувати для посилення своїх програм конфіденційності для підтримки розгортання IoT.

3.2.1 Принципи конфіденційності за дизайном

Користувачі систем IoT повинні бути поінформовані про всі дані, зібрані з них або про них, і повинні бути повідомлені про можливість відмовитися від практики збору даних на детальному рівні. Визнаючи занепокоєння, що багато які IoT пристрої можуть не мати належного користувальницького інтерфейсу, компанії повинні впровадити відповідні методи, щоб забезпечити вибір та повідомлення споживачів

У контексті системи IoT важливо врахувати потенційні наслідки ураження конфіденційності для всіх зацікавлених сторін до переведення системи в робочий стан. На початку аналіз буде зосереджений на типах даних, зібраних, щоб зрозуміти, які є конфіденційними та які норми мають застосовуються до кожного типу даних. Далі повинен бути більш поглиблений аналіз, щоб зрозуміти непрямі наслідки конфіденційності різних операцій та компонентів IoT. Як приклад, маючи справу з програмами, які відстежують підключені транспортні засоби, було б важливо зрозуміти, чи відстеження буде викривати моделі водіння, які, можуть бути простежені до окремої людини чи групи, у поєднанні з даними, зібраними іншими системами. Інший випадок, що стосується збору даних за допомогою розумних лічильників що подається комунальним компаніям для аналізу. Якщо доступ до цих даних не контролюється жорстко, зловмисники можуть визначити, коли людина не перебуває вдома, відкриваючи можливість фізичних нападів. Розглядаючи конфіденційність сукупних даних проти конфіденційності даних, зібраних єдиною системою, дозволять виявити потенційно серйозні проблеми конфіденційності до їх викриття або використанням недобросовісних осіб.

У січні 2014 року голова Федеральної торгової комісії зазначив, що зацікавлені сторони IoT мають відповідальність «зробити безпеку частиною процесу розробки продукту, зібрати мінімальний обсяг даних і повідомляти споживачів про несподіване використання їх даних та надавати спрощений вибір щодо цього використання». Організації, які застосовують можливості IoT, повинні це взяти до уваги та переконатися, що вони вбудували засоби контролю конфіденційності у свої системи, над пристроєм або спеціальні засоби контролю конфіденційності, які надає будь–який постачальник IoT.

3.2.2 Конфіденційність, закладена в дизайн

Організації, що впроваджують функціонал IoT, можуть зіткнутися з першим розумінням справжніх проблем їхньої конфіденційності. Таким чином, проведення аналізу для визначення елементів даних, які система IoT буде обробляти, є критичним. Це, в ідеалі, повинно проводитися у поєднанні з рекомендованим аналізом загроз і на самому початку проектування системи IoT. Як тільки буде досягнуто глибокого розуміння потенційних непрямих наслідків збору даних, відповідні гарантії можуть бути запроваджені в систему IoT з самого початку, а не після того, як було порушено проблему конфіденційності. Крім того, компаніям слід переглянути свою програму сповіщення про порушення персональних даних, щоб охопити ці аспекти пов’язані з IoT. Розглянемо усі варіанти, які можуть нам зустрітися.

1) Повна функціональність. Зазвичай існує баланс між цілями функціональності та безпеки, які необхідно підтримувати, щоб забезпечити систему, яка працює коректо, відповідає комерційним цілям і залишається безпечною. Те саме можна сказати про приватність. У випадку з IoT критично важливо, щоб компроміси між функціональністю, безпекою та конфіденційністю були зроблені на початку процесу проектування, щоб забезпечити однакове досягнення всіх цілей. Дотримуйтесь цих принципів

проектування конфіденційності для виявлення та реалізації тих компромісів, коли вартість цього є відносно незначною під час проектування системи IoT.

2) Наскрізна безпека. У межах IoT зібрані дані матимуть тривалий термін служби. Важливо враховувати повний термін служби зібраних даних, як в межах організації, так і в межах третіх сторін, яким вона надана. Зацікавлені сторони повинні бути поінформовані про те, коли дані надаються третім особам, засобам управління, що використовуються для їх захисту, а також як і коли дані видаляються. Захист життєвого циклу також застосовується до даних другого порядку (інформація про людей, яка виводиться або визначається на основі первинних даних). Наприклад, якщо датчик у вашому автомобілі збирає, як далеко, куди, як швидко та інші атрибути вашої водійської звички, тоді хтось може зробити висновок про різні речі про вас, наприклад, про ваші покупки чи робочі звички, або про те, з ким ви спілкуєтесь або взаємодієте. Власник даних (наприклад, автомобільна компанія) може стерти ваші основні дані після продажу вашого транспортного засобу, але насправді зберігати всю виведену інформацію (соціальний зв'язок, звички до покупок тощо).

3) Видимість та прозорість. Зацікавлені сторони повинні мати можливість легко ідентифікувати дані, зібрані з них для будь–якої конкретної системи IoT, а також для запланованого або потенційного використання цих даних. Зацікавленим сторонам також слід дозволити грубий збір даних і гранульований рівень. Наприклад, якщо програма відстежує їхні моделі руху (наприклад, для цілей страхування), користувач повинен мати можливість чітко дозволити використання своїх даних для цієї мети (грубо). Користувач також повинен мати можливість чітко санкціонувати окремі елементи даних, якщо це потрібно, наприклад, зберігання шаблонів руху або отриманої історії через GPS.

4) Повага до конфіденційності користувачів. Збереження конфіденційності інформації зацікавленої сторони з часом стане визначальним фактором для компаній у еру IoT. Маючи стільки можливостей

для неправильного використання конфіденційності користувачів, організації, які роблять необхідні кроки до захисту конфіденційної інформації будуть розглядатися набагато сприятливіше, ніж та, яка цього не робить. З огляду на це, важливо виховувати в організації культуру обізнаності щодо конфіденційності. Це може включати у себе призначення одного або декількох людей, що виступає за оцінку впливу на конфіденційність будь–якої нової системи IoT, що впроваджується. Цим людям в треба надати повноваження санкціонувати зміни конструкцій системи IoT у разі виявлення проблем конфіденційності. Конфіденційність користувачів також стосується непрямої логіки. У випадку деяких пристроїв IoT, наприклад розумних окулярів, користувач погодився з положеннями про конфіденційність, але сторона, що спостерігається, швидше за все, ні. Подальші дослідження повинно проводитися для розуміння наслідків та норм, необхідних щодо сценаріїв такого типу.

5) Оцінка впливу на конфіденційність. Керівництво ЄС WP29 також вказує на рекомендовану основу для проведення Оцінки впливу на конфіденційність. Якщо виявиться, що пристрій збирає, обробляє або зберігає інформацію, захищену конфіденційністю, застосовуватимуться більш жорсткі засоби контролю вимагати. Ці засоби контролю повинні поєднуватись із політикою та технікою. Наприклад:

– для надання пристрою може знадобитися більше адміністративних схвалень;

– слід провести огляд внутрішнім аудитом або дотриманням вимог, щоб визначити, чи є життєздатним наявність даних щодо IoT пристроїв;

– дані, що зберігаються на пристрої, повинні шифруватися з використанням досить потужних криптографічних алгоритмів;

– доступ до пристрою, як фізичний, так і логічний, повинен бути обмежений уповноваженим персоналом;

Існують різні рекомендації щодо вимог щодо конфіденційності, які слід враховувати залежно від регіону, зокрема:

– Північна Америка. Інтернет речей, конфіденційність та безпека у зв’язаному світі, звіт співробітників Федеральної торгової комісії;

– Європа. Рекомендації щодо конфіденційності для IoT, WP29 ЄС (Європейський дорадчий орган з питань захисту даних);

4 ЗАСТОСУВАННЯ ПІДХОДУ БЕЗПЕЧНОЇ СИСТЕМНОЇ ІНЖЕНЕРІЇ ДО АРХІТЕКТУРИ ТА РОЗГОРТАННЯ НОВОЇ СИСТЕМИ IoT.

Хоча деякі функціональні можливості IoT можуть просто складатися з датчиків, що подають дані в механізм аналітики, цілком ймовірно, що більшість можливостей з доданою вартістю IoT будуть результатом низки різноманітних компонентів, що працюють разом з даними, що враховують багато мереж. Оскільки ці системи є архітектурними, важливо визначити та внести вимоги до безпеки в конструкції, щоб врахувати реалізацію функціональних можливостей безпеки перед розгортанням. Стандартною практикою виконання цієї діяльності, яка може бути прийнята з проектування більш традиційних систем, є моделювання загроз.

4.1 Моделювання загроз

Посилання на моделювання загроз можна знайти в книзі Адама Шостака "Моделювання загроз: проектування для безпеки". Корпорація Майкрософт також визначає продуманий підхід до моделювання загроз, використовуючи кілька етапів для визначення серйозності загроз, запроваджених новою системою. Підхід до моделювання загроз (на основі Microsoft SDL):

1) Крок 1: Визначення активів. Це для каталогізації різних компонентів системи IoT, які будуть розгорнуті. Розглянемо не тільки пристрої IoT, але також сховища даних та додатки, якими пристрої спілкуються, та користувачів, які взаємодіють із системою.

2) Крок 2: Створення огляд системи/архітектури. Цей крок забезпечує надійну основу для розуміння не тільки очікуваних функціональних можливостей системи IoT, а й того, як зловмисник може неправильно використовувати систему. Почніть із процесу документування

очікуваних функціональних можливостей, а потім витратьте час розглянути та задокументувати випадки зловживання системою. Важливо також створити архітектурну схему, яка деталізує нову систему IoT та те, як система взаємодіє з іншими обчислювальними ресурсами підприємства та системами безпеки. Ця схема може також служити відправною точкою для визначення кордонів довіри, механізмів автентифікації та авторизації, а також реєстрації копій.

Створення архітектури системи допомагає шляхом аналізу випадків використання. Наступний приклад випадків використання із галузі охорони здоров'я може надати розуміння міркувань безпеки для впровадження IoT.

Після завершення подання логічної архітектури важливо визначити та вивчити конкретні технології, що складають систему IoT. Це включає розуміння та документування деталей нижчого рівня щодо пристроїв IoT, такі як тип процесора та операційна система. Це надасть інформацію, необхідну для розуміння конкретних типів вразливостей, які в кінцевому підсумку можуть виявитись, та визначає процеси, як і як часто виправлення та прошивка має застосовувати оновлення. Розуміння та документування протоколів, які використовуються кожним пристроєм IoT, також дозволить оновлювати архітектуру, особливо якщо в шифруванні виявляються прогалини, що застосовуються до даних, що передаються по системі та організації.

3) Крок 3: Розкладання системи IoT на окремі частини. На цьому етапі основна увага приділяється розумінню життєвого циклу даних під час їх проходження через систему. Розвиток цього розуміння дозволить виявити вразливі або слабкі місця в архітектурі безпеки, на які слід звернути увагу. Визначте та задокументуйте точки входу для даних у системі. У системі IoT ці точки входу, як правило, є датчиками певного типу. Простежте потік даних від точок входу та задокументуйте різні компоненти, які взаємодіють з цими даними у всій системі. Визначте головні цілі для зловмисників – це можуть бути проблеми всередині системи, яка агрегує або зберігає дані, або

це можуть бути високо цінні датчики, які потребують значного захисту для підтримки загальної цілісності системи. Наприкінці цієї діяльності буде добре зрозуміти поверхню атаки нової системи IoT. Розберемо ці загрози нижче в таблиці 4.1.

Таблиця 4.1 – Типи загроз та методи попередження цим загроза

Тип загрози	Опис IoT
Підробка ідентичності	Вивчіть систему на загрози, пов’язані з підміною ідентичності машини та здатністю зловмисника подолати автоматизовані довірчі відносини між пристроями. Уважно вивчіть протоколи автентифікації, що використовуються для встановлення захищеного зв'язку між різними пристроями (M2M) та між пристроями та програми, які використовують дані, що надаються цими пристроями. Вивчіть процес надання ідентифікаційних даних для кожного пристрою IoT та переконайтеся, що існують належні процедурні засоби контролю, щоб обмежити можливість впровадження неправдивого пристрою в систему.
Втручання в дані	Вивчіть шлях до даних у всій системі IoT. Визначте точки в системі, які надають можливість підробляти дані в пунктах збору, обробки, транспортування та зберігання. Уважно вивчіть реалізацію механізмів авторизації, щоб забезпечити ефективну боротьбу з фальсифікацією даних.
Репутація	Вивчіть дизайн системи IoT для вузлів у системі, які є критично важливими постачальниками даних. Ймовірно, це набори датчиків, які надають різні дані для аналізу. У випадку з IoT важливо мати можливість відстежувати дані до джерела та переконатися, що ці дані справді було передбачуваним джерелом. Вивчіть слабкі місця IoT–системи, які б дозволили б зловмисникові ввести неправдивий вузол, який подавав би погані дані в систему, намагаючись заплутати вищі процеси. передбачуваними функціональними можливостями систем IoT, наприклад незаконні операції відключені або не дозволені. Слід враховувати зміни стану та коливання часу (наприклад, порушення послідовності повідомлень.

Продовження таблиці 4.1

Тип загрози	Опис IoT
Розкриття інформації	Вивчіть шлях до даних у всій системі IoT, включаючи системи внутрішньої обробки. Переконайтеся, що будь–який пристрій, який обробляє конфіденційну інформацію, був ідентифікований і що введені належні засоби управління шифруванням для захисту від розголошення цієї інформації. Визначте вузли зберігання даних у системі IoT та переконайтеся, що застосовано елементи керування шифруванням даних у стані спокою. Вивчіть систему IoT на випадки, коли пристрої IoT вразливі до фізичного викрадення, і переконайтеся, що були розглянуті належні засоби управління, такі як нулізація ключа.
Відмова в обслуговуванні	Виконайте діяльність, яка відповідає кожній системі IoT бізнес–цілям, намагаючись забезпечити відповідне планування безперервності операцій. Вивчіть пропускну здатність, передбачену для кожного вузла в системі, і переконайтеся, що вона достатня для протистояння відповідним атакам Denial of Service(DoS – відмова в обслуговуванні). Вивчіть структури обміну повідомленнями (наприклад, шини даних), структури даних, неправильне використання змінних та Application Programming Interface (API), що використовуються у відповідних компонентах IoT, та визначте, чи є вразливості, які дозволять неправдивому вузлу заглушити передачі законного вузла.
Підвищення привілею	Вивчіть можливості адміністрування, що надаються різними пристроями IoT, що складають систему IoT. У деяких випадках існує лише один рівень автентифікації, який дозволяє конфігурувати деталі пристрою. В інших випадках можуть бути доступні окремі облікові записи адміністратора. Визначте випадки, коли в можливість розділити адміністративні функції від функцій на рівні користувача у вузлах IoT. Визначте слабкі місця в методах автентифікації, що використовуються вузлами IoT, щоб розробити відповідні засоби автентифікації в системі для захитсу ваших приладів та данних, користувачів, котрі вони використовують..
В обхід фізичної безпеки	Вивчіть механізми фізичного захисту, пропоновані кожним пристроєм IoT, і плануйте, де це можливо, пом'якшення щодо виявлених слабких місць. Особливо це стосується розгортань IoT, які розміщені у громадських або віддалених районах.

Продовження таблиці 4.1

Тип загрози	Опис IoT
Вторгнення в соціальну інженерію	Навчіть персонал для захисту від спроб соціальної інженерії та регулярно контролюйте активи на підозрілу поведінку
Помилки в ланцюзі постачання	Зрозумійте різні технологічні компоненти, що складають пристрої та системи IoT, та відстежуйте уразливості, пов’язані з будь–яким із цих технологічних рівнів.
Вторгнення в мережу	Регулярно контролюйте мережі на предмет підозрілої поведінки.

4) Крок 3а: Визначення захисної архітектури. Після декомпозиції системи IoT, чи не слід наступним кроком бути розробка архітектури для захисту системи? Чому б не дати їм умовно захисну архітектуру? Тут можуть бути введено деякі елементи Session Description Protocol (SDP). На основі коментарів Junaid я включила умовну схему на рисунку 4.1, яку ми можемо адаптувати до середовища IoT.

Рисунок 4.1 – Схема захисної архітектури середовища IoT

Після надання їм умовної архітектури захисту середовища IoT, потім перелічіть загрози та надайте детальну інформацію інструкції, як показано нижче.

5) Крок 4: Визначення та документування загроз. Популярну модель STRIDE можна застосувати до розгортання системи IoT. Використовуйте добре відомі сховища вразливостей, щоб краще зрозуміти навколишнє середовище, такі як загальна база вразливостей та експозиції MITRE [21]. Виявлення унікальних загроз для будь–якого конкретного екземпляру IoT керуватиметься цими типами загроз.

6) Крок 5: Оцінка загрози Оцінка ймовірності та впливу кожної загрози, виявленої на попередньому кроці, дозволяє розподілити відповідні рівні інвестицій для пом'якшення кожної загрози. Загрози з вищим рейтингом ризику, швидше за все, вимагатимуть зменшити великі суми грошей, оскільки вони, ймовірно, становлять загрозу, яка потребує негайного пом'якшення. На цьому етапі може бути використана будь–яка стандартна методологія оцінки загроз, включаючи підхід DREAD [22] від Microsoft.

4.2 Безпечний розвиток

Крайові пристрої IoT – це поєднання апаратного забезпечення, операційних систем, програмного забезпечення та програмного забезпечення.

Це означає, що по мірі створення нових пристроїв постачальники повинні знати про вразливі місця безпеки, що виникають на всіх рівнях стеку технологій.

Сюди входять такі речі, як зміцнення основної операційної системи (коли це застосовно) та пом'якшення специфічних для апаратного забезпечення вразливостей платформи. Пристрої IoT на межі також взаємодіють з багатьма іншими пристроями та системами, створюючи ефект система систем. Деякі крайні пристрої мають дуже обмежений код, побудований поверх цих різних фреймворків, операційних систем та платформ. Однак існують більш складні пристрої IoT, і для цього потрібно багато чого ті самі практики розробки безпечного програмного забезпечення, що і традиційні корпоративні або мобільні додатки. Сюди входить аналіз

коду на вразливості за допомогою використання засобів статичного та динамічного аналізу коду, а також виконання проникнення тести на програмне забезпечення для визначення вразливостей, які необхідно пом'якшити.

Такі організації, як Проект захисту веб–програм відкритих веб–програм (OWASP) працюють над забезпеченням безпечних вказівок щодо розробки для виробників пристроїв IoT. Топ 10 OWASP IoT визначає проблеми безпеки, які слід пом'якшити розробка пристроїв IoT. До них належать такі предмети, як:

- небезпечні хмарні та мобільні API;
- відсутність транспортного шифрування;
- Недостатня автентифікація та авторизація;

Постачальникам IoT буде важливо швидко набути досвіду інженерії безпеки, щоб забезпечити можливість розробки безпечних рішень IoT. Нарощування цього досвіду всередині є ще однією проблемою, оскільки витрати на підготовку персоналу, який розуміє дисципліну безпеки та виявляє вразливі місця, дуже великі. Такі організації, як Builditsecure.ly та I Am the Cavalry, можуть надати керівництво для досягнення цієї мети, однак інший цікавий підхід для розробників IoT полягає у використанні незалежних мисливців за помилками, які мають натовп. Такі сайти, як BugCrowd, дозволяють розробникам проводити незалежні аналітики безпеки, які проводять перевірку коду і навіть у деяких випадках перевіряють реалізацію обладнання, а потім подають результати виявлення вразливості.

Організаціям, які працюють над створенням методологій безпечного розвитку для Інтернету речей, слід розглянути питання про створення основи для безпечного розвитку. Структура повинна деталізувати безпечні практики кодування для вбудованих рішень, маніпуляції з параметрами та API. Використовуйте найкращі практики щодо захисту API від REST та SOAP/ ML для встановлення цих практик безпечного кодування для IoT. Також детально опишіть ризики безпеки, пов’язані з різними протоколами, для яких

можна використовувати зв'язку та рівні доступу, які слід надавати різним користувачам пристроїв IoT. Ключовим фактором розуміння належного контролю безпеки, який застосовується до реалізації IoT, є набір протоколів передачі даних та транспорту, що використовуються. Кожен з різних протоколів, доступних для використання IoT, підтримує різний рівень безпеки, і деякі з них можна поєднати, щоб забезпечити оптимально безпечну конфігурацію. Як розробники системи IoT, організації зіткнуться з розумінням цих протоколів і з тим, як використання одного з них впливає на необхідність використання протоколів вищого рівня, таких як протокол Transport Layer Security (TLS) для конфіденційності та автентифікації. Рисунок 5.1 надає огляд різних протоколів IoT, доступних для використання.

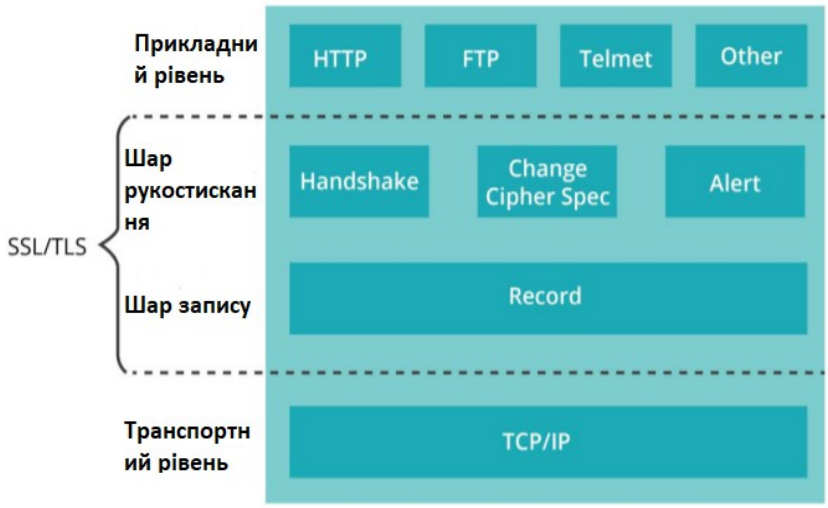

Рисунок 5.1 – Огляд різних протоколів IoT

Інша думка полягає в тому, що інструменти, що використовуються для реалізації самих протоколів зв'язку та безпеки, повинні бути ретельно вивчені. Наприклад, помилка Heartbleed, яка була викрита в квітні 2014 року, торкнулася лише частину TLS OpenSSL.

SSL – це протокол шифрування, який використовується для шифрування трафіку між веб–сайтом та його користувачем. Через

неправильну перевірку вводу в OpenSSL, помилка Heartbleed дозволила хакерам витягати дуже особисту інформацію про веб–користувачів із серверів, що використовують OpenSSL. Інші реалізації протоколів TLS не постраждали. (Наприклад, Microsoft, Mozilla та GnuTLS не постраждали). Навіть сьогодні багато вразливих пристроїв OpenSSL досі не виправлені: аналіз Джона Матерлі, творця скануючого інструменту Shodan, виявив, що станом на грудень 2014 року залишається недоступним 300 000 машин. Багато з них є «вбудованими пристроями», такими як веб–камери, принтери , сервери зберігання, маршрутизатори та брандмауери.

4.3 Огляд та оцінка вразливостей

Загальна система оцінювання вразливостей (CVSS) – це вільний і відкритий галузевий стандарт для оцінки важкості вразливостей системної безпеки комп’ютера чи системи. CVSS намагається визначити оцінку ступеня важкості для вразливостей, що дозволяє респондентам визначити пріоритети відповідей і ресурсів відповідно до загроз. Оцінки розраховуються на основі формули, яка залежить від кількох показників, які наближають простоту використання та вплив експлуатації. Бали знаходяться в діапазоні від 0 до 10, причому 10 позначає найбільш небезпечну загрозу або вразливість. Хоча багато хто використовує тільки базову оцінку CVSS для визначення небезпечності, існують також фактори, що впливають на доступність пом’якшень і наскільки широкі вразливі системи знаходяться в організації, відповідно.

1) Можливість експлуатації.

Вектор доступу (access vector, AV) описує можливий спосіб експлуатації уразливості:

– локальний (local, L) – вразливість експлуатується тільки локально;

– локально-мережний (adjacent network, A) – вразливість може експлуатуватися тільки з суміжних мереж;

– мережний (network, N) – вразливість може експлуатуватися віддалено.

Чим далі може перебувати джерело атаки, тим небезпечніше уразливість.

Складність доступу (access complexity, AC) визначає рівень складності атаки:

– високий рівень (high, H) – для експлуатації уразливості потрібно виконати певну послідовність дій;

– середній рівень (medium, M) – вразливість можна віднести ні до складної, ні до легкої;

– низький рівень (low, L) – вразливість експлуатується просто.

Чим нижче оцінка складності доступу, тим небезпечніше уразливість.

Метрика «автентифікація» (authentication, Au) описує спосіб автентифікації для експлуатації уразливості:

– багаторазова (multiple, M) – атакуючий повинен пройти автентифікацію два і більше разів;

– одноразова (single, S) – атакуючий повинен пройти автентифікацію один раз;

– нульова (none, N) – автентифікація не потрібно.

Чим менше раз потрібно проходити автентифікацію, тим небезпечніша уразливість.

2) Вплив.

Метрика «вплив на конфіденційність» (confidentiality, C) описує вплив уразливості на конфіденційність даних системи:

– нульове (none, N) – вплив на конфіденційність відстуній;

– часткове (partial, P) – частина інформація підвернена небезпеці;

– повне (complete, C) –вся інформація у небезпеці.

Чим сильніше вплив на конфіденційність даних в системі, тим небезпечніше уразливість.

Метрика «вплив на цілісність» (integrity, I) описує вплив уразливості на цілісність даних системи:

– нульове (none, N) – вплив відсутній;

– часткове (partial, P) – можна змінити частину даних;

– повне (complete, C) – можна змінити будь-які дані.

Чим сильніше вплив на цілісність даних в системі, тим більша уразливість.

Метрика «вплив на доступність» (availability, A) описує вплив вразливості на доступність системи:

– нульове (none, N) – вплив відсутній;

– часткове (partial, P) – вразливість може викликати в системі тимчасові відмови в обслуговуванні або зниження продуктивності;

– повне (complete, C) – вразливість може викликати повну відмову системи в обслуговуванні [10].

Чим сильніше вплив на доступність системи, тим більша вразливість.

Але це для стандарту версії два. Для більш нового стандарту є декілька нових, або просто замінених метрик. Замість «Автентифікації» тепер використовують «Потрібний рівень привілеїв» для проведення атаки.

Підхід до розрахунку метрики, заснований на кількості незалежних процесів автентифікації, які потрібно пройти атакуючому, недостатньо точно відображає зміст привілеїв, необхідних для експлуатації. Значення Multiple в базі зустрічається досить рідко і в основному використовується для вразливостей, інформація про яких недостатньо деталізована.

Значення Single не дозволяє визначити, чи потрібне для експлуатації доступ рівня привілейованого користувача або досить автентифікації стандартного користувача.

Також додали метрику «Необхідність взаємодії» з користувачем та «Межі експлуатації». Чи потрібні для успішної реалізації атаки будь-які дії з боку користувача атакується системи. Чи відрізняються експлуатований і атакується компоненти, тобто дозволяє чи експлуатація уразливості порушити конфіденційність, цілісність і доступність будь-якого іншого компонента системи.

Результати ми отримаємо за такими шкалами.

1) Base Score – це число представляє ранжування деяких якостей, притаманних вразливості, яка не змінюватиметься з часом або залежатиме від середовища, в якому з'являється вразливість. Базовий бал надходить з двох метрик: «Підпорядкованість до експлуатації» та «Субкорекція впливу».

2) Exploitability Subscore – базується на якостях вразливішого компонента – їхні оцінки визначають, наскільки вразливим ресурс. Чим вище комбінована оцінка, тим легше використовувати цю вразливість. Кожна метрика тут класифікується відповідно до значень, специфічних для себе, а не відповідно до числової оцінки.

3) Impact Subscore визначає, наскільки суттєво впливатимуть певні властивості уразливого компонента, якщо загроза успішно експлуатується.

Виходячи з всього вищезазначеного, можна зробити висновок, що для розрахунку ризиків інформаційної безпеки (рівня вразливості) підходить методика CVSS. Так як, технологія «Інтернет речей» дуже розповсюджена і може використовуватися у будь-якій сфері нашого життя, врахувати усі специфічні особливості встановлення, інтегрування та використовування подібних пристроїв дуже важко. А для того, щоб визначити основні проблеми безпеки та вразливості таких продуктів, можна використовувати CVSS, тому що вона використовує чіткі параметри, які можна визначити без особливих умов.

Також, слід зазначити, що технологія ще відносно молода, тому виробники прагнуть випускати нові продукти якомога частіше та робити їх, більш технологічними. Це сприяє тому, що вони економлять час на тестуванні своєї продукції. Так як, обрана в атестаційній роботі методика не займає багато часу, то вона ідеально підходить для аналізу вразливостей пристроїв, що використовують технологію «Інтернет речей» [11].

Проведемо оцінку загроз та вразливостей даних технологій, та побудуємо профіль загрози.

У зловмисника є можливість спробувати отримати підтвердження того, що користувач існує в системі. Ця вразливість добре описана у рейтингу OWASP-AT-002. Вона полягає в тому, що з відповідей від сервера на отримані ним дані автентифікації можна визначити, існує користувач в системі чи ні.

Якщо користувач вказав ім’я користувача, якого немає в системі, то сервер скаже про це, повернувши одну відповідь. Якщо ж користувач передав правильне ім’я користувача, але неправильний для цього користувача пароль, то сервер поверне вже іншу відповідь.

Таким чином зловмисник може ідентифікувати існуючих в системі користувачів, перебравши їх імена.

Якщо зловмисник отримає ім’я користувача в системі, то це сильно полегшить йому отримання пароля. Якщо ж зловмисник зможе підібрати і вірний пароль для існуючого користувача, то наступним його кроком буде підвищення привілеїв в системі.

Тепер ми можемо скласти базовий вектор для цієї вразливості.

Спочатку для стандарту CVSSv2.

1) Вектор доступу. У нашому випадку доступ до ресурсу зловмисник має з зовнішньої мережі. Тому ми даємо йому значення Network.

2) Складність. З огляду на те, що вірність чи не вірність даних користувачів підтверджує сервер, можна присвоїти значення Low.

3) Метрика «автентифікація». Атакуючий авторизується лише один раз, тож Single.

4) Метрика «вплив на конфіденційність». Так як, хакер має доступ до закритої інформації, то рівень уразливості Complite.

5) Метрика «вплив на цілісність». Так, як цілісності системи нічого не загрожує, то None.

6) Метрика «вплив на доступність». Доступність теж у безпеці, тож None.

Тепер складемо наш вектор: [AV:N / AC:L / AU:S / C:C / I:N/ A:N]. Тепер треба обробити це у спеціальних калькуляторах, що побудовані за цим стандартом. І отримаємо такі результати:

- CVSS Base Score: 6.8;
- Impact Subscore: 6.9;
- Exploitability Subscore: 8.2;
- Overall CVSS Score: 6.8.

Теперь перейдемо до CVSSv3. Звернемо увагу лише на ті метрики, що змінилися.

1) Необхідний рівень привілеїв. Так як автентифікації не потрібно, то None.

2) Необхідність взаємодії з користувачем. Так як зловмиснику не потрібно будь-яким чином взаємодіяти з користувачами, то ставимо None.

3) Межі експлуатації. Межі експлуатації не змінюються – Unchanged.

Складемо базовий вектор за CVSSv3:

[AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:N / A:N].

При обробці отримаємо такі результати:

- CVSS Base Score: 7.5;
- Impact Subscore: 3.6;
- Exploitability Subscore: 3.9;
- Overall CVSS Score: 7.5.

Афтентифікований користувач ThingsPro Suite в веб-панелі може змінювати дані свого облікового запису. Серед цих даних – логін, пароль, адресу електронної пошти та назву компанії. Для зміни цих даних веб-сервісу відправляється hypertext transfer protocol (HTTP)-запит.

Після зміни значення role з user на root і повторної відправки повідомлення, у відповіді сервера було зазначено, що роль поточного користувача змінена з user на root. Повторний вхід в цей аккаунт підтвердив підвищення привілеїв до root. Дану уразливість можна віднести до типу Broken Access Control, який посідає п’яте місце в рейтингу OWASP TOP 10 2017.

Тож, перейдемо до складання вектора за CVSSv2.

1) Вектор доступу. У цьому випадку доступ до ресурсу зловмисник має з зовнішньої мережі. Тому даємо йому значення Network.

2) Складність. Користувач може сам змінювати свої данні. Low.

3) Метрика «автентифікація». Атакуючий авторизується лише один раз, тож Single.

4) Метрика «вплив на конфіденційність». Так як хакер має доступ до закритої інформації, то рівень уразливості Complite.

5) Метрика «вплив на цілісність». Цілісність у даному випадку у небезпеці, тож – Complite.

6) Метрика «вплив на доступність». Доступність ресурсу може стати обмеженою, тому тут теж обираємо Complite.

Складемо базовий вектор: [AV:N / AC:L / AU:S / C:C / I:C / A:C].

- CVSS Base Score: 9.0;
- Impact Subscore: 10.0;
- Exploitability Subscore: 8.0;
- Overall CVSS Score: 9.0.

Вектор за CVSSv3.

1) Необхідний рівень привілеїв. Так як зловмисник змінює свій рівень привілеїв, то обираємо Low.

2) Необхідність взаємодії з користувачем. Так як зловмиснику не потрібно будь-яким чином взаємодіяти з користувачами, то ставимо None.

3) Межі експлуатації. Межі експлуатації не змінюються – Unchanged.

Отже базовий вектор: [AV:N / AC:L / PR:L / UI:N / S:U / C:H / I:N / A:N].

- CVSS Base Score: 6.5;
- Impact Subscore: 3.6;
- Exploitability Subscore: 2.8;
- Overall CVSS Score: 6.5.

Також автентифікований користувач може змінювати дані не тільки свого, а й будь-якого іншого облікового запису в системі. Це дуже корисно, якщо користувачеві потрібно змінити пароль для початкових користувачів root або admin, якщо він його забуде.

Однак для зловмисника це можливість підвищення привілеїв. Найпростішим варіантом використання цієї уразливості може бути зміна довільним користувачем з будь-яким рівнем привілеїв пароля для користувача root.

Сервер, отримавши такий запит, змінить пароль користувача root на вказаний в запиті і надалі атакуючий може увійти в систему як користувач root.

Ця вразливість також відноситься до типу Broken Access Control, який посідає п’яте місце в рейтингу OWASP TOP 10 2017.

Вектор доступу за CVSSv2.

1) Вектор доступу. У цьому випадку доступ до ресурсу зловмисник має з зовнішньої мережі. Тому даємо йому значення Network.

2) Складність. Користувач може сам змінювати свої данні. Low.

3) Метрика «автентифікація». Атакуючий авторизується лише один раз, тож Single.

4) Метрика «вплив на конфіденційність». Так як, хакер має доступ до закритої інформації, то рівень уразливості Complite.

5) Метрика «вплив на цілісність». Цілісність у даному випадку у небезпеці, тож – Complite.

6) Метрика «вплив на доступність». Доступність ресурсу може стати обмеженою, тому тут теж обираємо – Complite.

Складемо базовий вектор: [AV:N / AC:L / AU:S / C:C / I:C / A:C].

Та результати:

- CVSS Base Score: 9.0;
- Impact Subscore: 10.0;
- Exploitability Subscore: 8.0;
- Overall CVSS Score: 9.0.

Перейдемо до CVSSv3.

1) Необхідний рівень привілеїв. Так як зловмисник змінює свій рівень привілеїв, то обираємо Low.

2) Необхідність взаємодії з користувачем. Так як зловмиснику не потрібно будь-яким чином взаємодіяти з користувачами, то ставимо None.

3) Межі експлуатації. Наші межі експлуатації не змінюються – Unchanged.

Отже наш базовий вектор: [AV:N / AC:L / PR:L / UI:N / S:U / C:H / I:N / A:N].

Фінальні результати:

- CVSS Base Score: 6.5;
- Impact Subscore: 3.6;
- Exploitability Subscore: 2.8;
- Overall CVSS Score: 6.5.

5 СИСТЕМА БАГАТОРІВНЕВОГО ЗАХИСТУ БЕЗПЕКИ ДЛЯ АКТИВІВ IoT

IoT поєднує існуючі в екосистемі мережі інформаційних технологій (IT) та операційних технологій (OT) мільйони датчиків, пристроїв та інших розумних об'єктів. Це зближення значно розширює виклики безпеці, завдяки його збільшена ширина і глибина в порівнянні з існуючими мережевими підключеннями.

Мережами IT та OT керуються з урахуванням різних пріоритетів, і кожна з них має певні потреби в безпеці. Пріоритет IT-мережі повинна захищати конфіденційність даних. Основна увага в мережі OT приділяється фізичній безпеці та безпечному доступу до забезпечити експлуатаційну безпеку та безпеку працівників.

Завдяки зближенню цих двох середовищ, безпека IoT вимагає нового підходу, який поєднує фізичну та кібербезпеку. Результатом є покращена безпека працівників та захист всієї системи ззовні, а також всередині.

Організаціям, що працюють сьогодні в цифровому світі, потрібні рівні захисту, щоб повідомлення електронної пошти, яке потрапляє через брандмауер, зупинялося антивірусом поштового сервера, і якщо це вдасться через це, тоді його слід зупинити антивірус робочої станції. Якщо ворожа програма насправді закріплює на робочій станції палець, її слід виявити, коли вона працює на робочій станції, оскільки вона робить підозрілі або несподівані дії. Шукайте зв’язки з веб–сайтами в Інтернеті, які мають зв’язок з ворожою діяльністю, і блокуйте такі сайти, фільтруючи вихід на брандмауері.

Зловмисники не залишають доказів, захоплюючи веб-додатки, операційні системи та ще глибше в апаратному забезпеченні. Вони користуються перевагами звичайних кінцевих точок та мобільних пристроїв, пропускаючи повз і через мережеву безпеку, і навіть користуючись перевагами людського елементу, що керує пристроями.

На етапі проектування необхідно серйозно розглянути Моделювання загроз архітектури IoT, яке повинно враховувати гравців/ролі, використовувані компоненти, точки введення та виходу даних на всіх згаданих нижче рівнях, включаючи рівень пристрою. Різні сценарії загрози повинні бути продумані з численними випадками неправомірного використання, а потім передані команді розробників/збірників для розробки /збірки з використанням найкращих практик безпеки з подальшим тестуванням безпеки.

З точки зору споживачів IoT, перед реалізацією ініціативи IoT потрібно ретельно планувати. Безпека повинна бути ретельно продумана на всіх цих рівнях, оскільки одного або двох захищених шарів недостатньо, щоб забезпечити повну безпеку реалізація:

5.1 Мережевий рівень

Брандмауери призначені для фільтрації трафіку залежно від типу, порту та призначення. Брандмауери еволюціонували шляхом включення глибша аналітика, така як IPS та служби інспекції дорожнього руху, що дозволяє їм глибше заглянути в пакети та краще виявити зловмисний трафік. Такі пристрої є однією з найпростіших вихідних точок при реалізації шаруватого захисту. Часто шукайте відкриті порти в брандмауерах та маршрутизаторах. Відкриті порти – це запрошення хакерам.

Перевірте, чи маршрутизатори вразливі до неправильно налаштованих служб NAT–Port Mapping Protocol (NAT–PMP).

NAT–PMP – це протокол, який не має вбудованого механізму автентифікації та довіряє всім хостам, що належать до локального маршрутизатора мережі, тим самим дозволяючи їм вільно «пробивати» отвори через брандмауер. Неправильно налаштовані маршрутизатори до NAT–PMP послуги згадуються у 10 найпопулярніших загрозах Інтернету речей OWASP [24].

Здійснюйте управління мережевим доступом (NAC) для уніфікації технологій захисту кінцевих точок, таких як антивірус та вторгнення у профілактичних цілях. Антивірусні продукти захищають комп'ютери від шкідливих програм, наприклад, покладаючись на порівняння файлів підписи.

Виконуйте періодичну оцінку вразливості та переконайтеся, що автентифікація користувача та системи для мережі відповідають політиці безпеки вашої організації. Це включає сувору політику щодо паролів, пароль управління та періодична зміна паролів.

Вимкнути паролі гостя та за замовчуванням на мережевих пристроях, таких як маршрутизатори та шлюзи. Це слід зробити відразу після розпакування нового мережевого пристрою, перш ніж вводити їх у роботу у вашій мережі.

Рекомендується документувати всі MAC-адреси для кожного пристрою, щоб маршрутизатор призначав IP-адреси лише ці пристрої. Всім невідомим пристроям буде заблоковано доступ до мережі.

Для бездротових мереж використовуйте Wireless Protected Access 2 (WPA2) замість протоколу бездротового шифрування (WEP). WPA2 вимагає використання посиленого бездротового шифрування. Завжди використовуйте надійний складний пароль для бездротової мережі.

Також для бездротових мереж використовуйте кілька ідентифікаторів набору послуг (SSID), а не лише один. Це дозволяє мережі менеджер призначити різні політики та функції для кожного SSID, тим самим дозволяючи організації призначити пристрої в різні SSID на основі ризику та критичності. Сегментування вашої бездротової мережі таким чином гарантує, що якщо один пристрій зламається, інші пристрої не будуть порушені, оскільки вони знаходяться в іншому сегменті.

Використовуйте приватний попередньо спільний ключ (PPSK), щоб переконатися, що кожен датчик або пристрій надійно підключено до Wi-Fi.

Адміністратори можуть призначати унікальні та відкликані ключі кожному користувачеві та клієнту в мережі. Ці ключі визначають які дозволи

слід призначити пристрою, що з'єднується за допомогою цього ключа. Є технологічні компанії, які забезпечити цю можливість.

Дедалі частіше пристрої IoT зберігають свої дані в хмарі для аналізу. Важливо захистити ці дані належним чином за допомогою шифрування та інших засобів. (Наприклад, передача конфіденційних даних, таких як дані про охорону здоров'я від пристрій моніторингу пацієнта до хмарного сховища)

5.2 Прикладний рівень

IoT не вимагає абсолютно нового набору вказівок щодо безпеки програм та найкращих практик. Той самий набір вказівок на рівні додатків справедливий для будь-якої традиційної реалізації.

Якщо ваша організація пише власні програми, використовуйте відповідну автентифікацію та авторизацію. Шукайте будь-які паролі, залишені у вільному місці в коді програми (наприклад, жорстко закодовані логіни telnet або паролі, які залишились під час тестування).

Якщо організація використовує сторонні бібліотеки або бібліотеки з відкритим кодом, рекомендується підтримувати інвентаризацію цих бібліотек та постійно їх оновлювати. Також перевірте версію та відповідні уразливості у цих версіях, щоб ви могли уникнути використання цих вразливих версій. Це забезпечить можливість виправлень безпеки застосовуватись до сторонніх або відкритих бібліотек, що використовуються.

Перевірте наявність уразливостей міжсайтових сценаріїв (XSS) або підроблення запитів між сайтами (CSRF).

CSRF – це тип атаки зловмисним веб-сайтом, електронною поштою, блогом, миттєвим повідомленням або програмою, яка змушує браузер виконувати небажані дії дія на надійному сайті. XSS дозволяє зловмисникам вводити скрипт на стороні клієнта на веб-сторінки, які переглядають інші користувачі, або може використовуватися для обходу засобів контролю

доступу. OWASP рекомендує такі засоби сканування, як Zed Attack Proxy (ZAP) або Динамічне тестування безпеки додатків (DAST).

Попросіть у постачальника звіт про перевірку коду безпеки щодо будь-яких уразливостей, виявлених під час розробка платформи IoT та їх відповідне відновлення. Цей крок буде діяти як належна перевірка з бок. Перспектива статичного тестування безпеки додатків (SAST). Якщо споживач розробляє додаток, яке буде розміщений на вершині платформи IoT, SAST повинен виконуватися в додатку разом з тестування безпеки динамічних додатків(DAST).

Програми також можна керувати та розміщувати або надавати як послугу іншій організації. Навчити користувачів змінити паролі за промовчанням для послуги.

Небезпечні хмарні інтерфейси цитуються в OWASP Top 10 для IoT. Переконайтеся, що використовується https, і застосуйте блокування, коли досягнуто максимальної кількості дозволених спроб автентифікації або часу простою.

Використовуйте шифрування даних у стані спокою. Забезпечте конфіденційність даних під час транспортування, використовуючи потужне шифрування. Посолити або випадкові дані до хешованих даних, щоб ускладнити злом.

Шифрування даних під час транспортування повинно мати можливість враховувати обмежені ресурси і, отже, має бути невеликий розмір, легкий замість традиційного, щоб уникнути продуктивності вузькі місця.

Базова "нормальна" поведінка, щоб згодом виявити підозрілу поведінку. Джерело базової лінії руху може бути брандмауерами, маршрутизаторами, комутаторами, колекторами потоку та мережевими кранами. Тому що брандмауери та маршрутизатори пропускають трафік вони є ідеальним місцем для початку. З точки зору безпеки, як правило, найцікавішим є потік між внутрішнім хостом та інтернетом.

Однією з унікальних проблем веб-програм для пристроїв IoT є те, що вони, як правило, використовують нестандартні порти замість звичайні 80 або 443. Пристрої створені для прослуховування в інших портах. Найкраще використовувати стандартний сканер портів або здригатися до дізнатися, які веб–послуги пропонує певний пристрій. Скануйте нестандартні порти на пристроях IoT, оскільки багато хто цього не робить або використовувати стандартні.

Окрім додаткових механізмів втручання, інтерфейси фізичних пристроїв IoT можуть вимагати додаткового захисту. JTAG та непотрібні послідовний та інші інтерфейси виробника повинні бути видалені або захищені від фальсифікації перед масовим розгортанням. Приватні або секретні ключі слід зберігати в мікросхемі "захищеного елемента", яка працює в енергонезалежній пам'яті та обмежує доступ лише для авторизованих користувачів.

5.3 Рівень пристроїв

Деякі приклади пристроїв – датчики, шлюзи, що об'єднують дані, мобільні пристрої, камери, зчитувачі RFID, переносні та імплантовані пристрої. Залежно від галузі, можуть бути пристрої, які не є поширеними в інших галузях, і тому в цьому списку можуть бути відсутні конкретні вказівки щодо унікальних пристроїв.

Переконайтеся, що мікропрограма пристрою регулярно оновлюється, оновлюється та виправляється.

Подбайте про джерела файлів оновлення та про спосіб їх транспортування. Обов’язково відскануйте файли або перевірте їх цілісність перед тим, як встановлювати їх у свій пристрій. Перевірте «репутацію» файлу, яка може бути робиться різними способами. Кожен комп'ютерний файл має унікальну контрольну суму – відносно коротке математичне значення для файл. Ще однією репутаційною характеристикою файлу є те,

наскільки широко він використовувався. Такі оцінки створюють а контекст для файлу, вказуючи, чи відомо це як добре чи погано, чи це невідомий ризик стежити за ретельним контролем.

– заміна паролю з'єднання за замовчуванням для пристроїв Bluetooth;

– заміна паролю за замовчуванням та запровадьте надійну політику щодо паролів;

– укріплення пристрію, змінивши конфігурацію за замовчуванням, а не лише пароль;

– тестування перед розгортанням пристроїв. Функція “Fuzzing” надсилає пристрою несподівані вхідні дані та перевіряє, як він реагує на виявлення можливі дефекти;

– для мобільних пристроїв доступ до відбитків пальців надійніший. Застосовуйте блокування на основі простою та максимального числа спроб для автентифікації;

– пристрої та датчики повинні періодично тестуватися для забезпечення належної функціональності;

– обмеження даних, які збираються або агрегуються шлюзом, до того, що дійсно необхідно;

У медичній галузі переносні пристрої, такі як кардіостимулятори та імплантовані пристрої, вразливі до атак, що діють далеко від нешкідливого підслуховування до фатального злому. Зловмисники можуть надсилати несанкціоновані радіокоманди на перепрограмування пристрою або надішлють атаку відмови в обслуговуванні, щоб розрядити акумулятор пристрою. Щоб захистити ці пристрої від летального результату порушення, розгляньте можливість застосування пристрою проти глушення, щоб завадити зловмисникові встановити несанкціонований бездротовий зв'язок між пристроєм та віддаленим терміналом. Ці пристрої називаються «носими щитами». уповноважені особи, такі як лікарі, все ще можуть отримати доступ до даних, а інші – ні.

5.4 Фізичний рівень

Безпека на фізичному рівні давно була обов'язковою практикою у високо регульованих галузях, ще до IoT. Наприклад, комунальні та енергетичні компанії дуже суворо ставляться до того, хто отримує доступ до вестибюлів та дверей, які ведуть до критично важливих машин та пристроїв, оскільки одне порушення може призвести до катастрофічного відключення або великих штрафів. Подібно до того, як пристрої та датчики використовуються в ініціативі IoT, застосовуються ті самі уразливості. OWASP виявив слабкий фізичний захист у топ-10 вразливості IoT.

Як і у логічних системах, має існувати управління інфраструктурою управління фізичною ідентичністю та доступом. Лише уповноваженим особам повинен бути наданий доступ до захищених областей, таких як центри обробки даних, лабораторії та райони, де пристрої мають критичне значення. Значки повинні забезпечувати як найменший доступ.

Фізичні ключі слід надавати так само ретельно, як і захищені маркери.

Камери спостереження слід використовувати для відстеження пристроїв, розміщених навколо певної території. Камери повинні мати можливість панорамування вліво і вправо для сканування області, де реалізовані пристрої та датчики.

Документ, де розташовані пристрої. Якщо можливо, розробіть графічну карту, що показує, де в будівлі знаходяться активи IoT.

Беручи до уваги широкий спектр фізичних сайтів (у приміщенні, на відкритому повітрі), місць розташування (захищених сайтів проти захисту людей), огороджень та варіантів фізичного вбудування, засоби фізичного захисту є важливим елементом безпеки IoT. Багато пристроїв мають невеликий розмір і стикаються зі значним ціновим тиском. Незважаючи на це, захисні огородження, а також докази фальсифікації та механізми

реагування на фальсифікацію слід розглядати виходячи з рівня впливу різних фізичних векторів загроз. Захист від несанкціонованого втручання можна застосувати до корпусу, підрозділу вбудованого пристрою (наприклад, дочірньої плати з критичними компонентами процесора/пам'яті), а також криптографічний модуль (бажано апаратний). Якщо пристрій нерухомий у своєму середовищі та прикріплений до стіни, стовпа чи іншого кріплення, слід враховувати індикатори видалення фальшивок, щоб попередити операторів про несанкціоноване вилучення та крадіжку пристрою.

5.5 Рівень користувача

Людський рівень може бути найскладнішим у забезпеченні та найбільш сірою зоною, коли йдеться про пом'якшення ризиків. У цьому рівні так багато речей, які можуть піти не так, що складно вирішувати вимоги чорно–білих манер. До наведених нижче вказівок у цьому рівні можна дотримуватися легковажно або серйозно, залежно від готовності організації інвестувати. Найважливішим загальним керівним принципом тут є розвиток культури, що усвідомлює безпеку, та прищеплення обізнаності, підзвітності та відповідальності для того, щоб ініціатива працювала.

1) Визначте декількох лідерів, які є євангелістами з питань безпеки. Ці люди повинні мати особистість і потяг до бути на передових позиціях, щоб ініціатива IoT успішно працювала з найменшим викликом безпеці.

2) Постійно навчайте співробітників речам, яких слід уникати, наприклад, потрапляння на занадто добрі справжні пропозиції або навіть небажані пропозиції які виглядають як законні ділові запити.

3) Подібно до завантаження виправлень для пристроїв, користувачів слід навчити перевіряти репутацію будь–яких завантажень з Інтернету.

4) Навчіть кінцевих користувачів, як вони можуть допомогти у захисті своїх мобільних пристроїв, таких як вищезазначені практики блокування та надійні паролі. Вимкніть Bluetooth на мобільних пристроях,

коли він не використовується. Негайно повідомити про втрату мобільні пристрої та відновлені на карантин мобільні пристрої, щоб їх можна було сканувати на наявність фальсифікацій.

5) Винагороджуйте персонал, коли він виявляє вразливі місця.

6) Спростіть звітування про вразливості не лише працівникам, а й кінцевим користувачам. Надайте користувальницький інтерфейс на порталі повідомляти про них. Система винагород дає людям ініціативу повідомляти про них.

7) Документуйте всі активи IoT та види інформації, яку вони збирають. Ранжуйте їх за критичністю, щоб приділити більше уваги надіти ті, які є більш критичними для місії. Це застосовується підхід, заснований на оцінці ризику, особливо коли не всі IoT активам можна приділити однакову увагу.

8) Розширювати та застосовувати високі стандарти у контрактах з постачальниками та постачальниками послуг.

Зауважте, що у всіх вищевказаних рівнях обговорення йшли з точки зору споживачів IoT. Однак виробники пристроїв IoT також повинні знати про ці рівні, щоб вони могли стати на місце споживача та зміцнити свою продукцію. Виробники пристроїв можуть зосередитись лише на самому рівні пристрою, але їм також потрібно взяти на себе відповідальність і допомогти споживачеві усвідомити інші сфери, де слід посилити безпеку.

Таким чином, профілактика – найкращий спосіб запобігти тривожним інцидентам. Чим більше ці вказівки щодо безпеки на кожному рівні будуть сприйматися серйозно, тим успішнішою буде ініціатива IoT.

6 СИСТЕМА ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

Захист даних у різних станах вимагає застосування шифрування. Існує безліч криптографічних примітивів (шифрування, цілісність, автентифікація тощо), доступних у різноманітних криптографічних програмах/бібліотеках програмного забезпечення та апаратних модулях. Національний інститут стандартів і технологій (NIST) надає хороші рекомендації щодо алгоритмів, режимів та довжин ключів, які слід використовувати для захисту конфіденційної інформації. Алгоритми та розміри ключів слід вибирати, виходячи з мінімальних рівнів захисту, встановлених для криптографічної системи IoT.

Двома основними міркуваннями при виборі криптографічного набору для захисту інформації є рівень безпеки та продуктивність. Продуктивність особливо вірна при роботі з обмеженими, як правило, вбудованими пристроями, типовими для IoT. Криптографія еліптичної кривої (ECC) забезпечує потужні алгоритми, але малі розміри асиметричних ключів для:

- встановлення ключа шифрування (еліптична крива Діффі–Хеллмана – ECDH);
- цифрові підписи (алгоритм цифрового підпису еліптичної кривої – ECDSA) для операцій підпису повідомлень /даних;

У поєднанні з симетричним алгоритмом, таким як Advanced Encryption Standard (AES), цей криптографічний набір пропонує потужний криптографічний захист, придатний для пристроїв, що знаходяться в неблагополучному стані.

Визначення криптографічних алгоритмів та розмірів ключів для підтримки в пристрої IoT є лише одним із аспектів криптографічної головоломки. Ці алгоритми повинні працювати в довіреному середовищі, а ключі повинні зберігатися в захищених контейнерах. У більших системах дизайнери часто використовують модулі апаратного захисту (HSM) для зберігання ключів та операцій, однак HSM часто неможливі для IoT.

Натомість дизайнери повинні дослідити інші варіанти, такі як Trusted Execution Environment (TEE) та Trusted Platform Module (TPM).

Криптографічні реалізації, що використовуються в пристроях IoT, а також системи управління та збору даних повинні пройти перевірку перевірки криптографічного алгоритму та, можливо, перевірку відповідності криптографічного модуля за допомогою схем перевірки перевірки, таких як програма перевірки криптографічного модуля NIST (CMVP) та програма перевірки криптографічного алгоритму (CAVP).

6.1 Ідентифікація даних, класифікація, безпека

Організаціям, які застосовують можливості IoT, потрібно спочатку створити корпоративну політику безпеки даних, яка включає підходи до захисту даних IoT. Цей процес починається з чіткого завдання ідентифікації елементів даних, пов'язаних з ними класифікацій та інших атрибутів пристрою чи програми. Модель даних повинна не лише каталогізувати чітко визначену інформацію, яку пристрої IoT передають, отримують або зберігають як частину програми, але також за своєю суттю дані фізичного світу, які зовні або окремо можуть здаватися не чутливими або приватними. Фізичні вимірювальні значення, використання пристрою також потрібно збирати метрики тощо для того, щоб визначити політику захисту даних щодо захисту даних, що стосується не лише її програм, а й моделей використання пристрою. Це є вагомою передумовою для встановлення політики та декларацій щодо власності на дані (які стосуються даних програми, а також моделей використання пристрою), необхідних для наступне:

1) Захист даних у стані спокою (DAR). Залежно від складності пристрою IoT, можливо, багато елементів даних, специфічних для додатків, повинні бути зашифровані, коли вони активно не використовуються у виконуваних процесах. Пристрій повинен зашифрувати ці параметри за допомогою ключа шифрування DAR, надійно збереженого у фізично

загартованому, заблокованому криптографічному модулі, що знаходиться в пристрої. На додаток до конфіденційних даних додатків, усі секретні та приватні ключі, аутентифікація, контроль доступу та інші конфігурації безпеки повинні зберігатись зашифрованими, якщо це можливо. Захист DAR призначений для захисту приватної інформації (наприклад, медичних даних) у разі викрадення або втрати пристрою.

2) Захист даних при транзиті (DIT). Транзитні дані стосуються надсилання або отримання даних (додатків, команд управління, стану тощо) через лінію зв'язку або мережу. По можливості захист DIT повинен включати криптографічну конфіденційність (шифрування), алгоритми цілісності та автентифікації, що виконуються належним чином інтегрованим криптографічним модулем. Для забезпечення наскрізної безпеки DIT, коли це можливо, слід використовувати добре перевірені протоколи безпеки мережі та/або додатків.

Якщо симетричні ключі не надійно попередньо розміщені в пристроях IoT, системам управління пристроями та збору даних може знадобитися встановити одноразові або обмежені терміни використання ключів для шифрування даних на/з пристроїв. Для цього корисний повністю ефемерний або статико–фемерний обмін Діффі–Хеллмана (з використанням взаємно визнаних цифрових облікових даних), який забезпечить ключ шифрування з ідеальною прямою таємницею.

3) Захист даних, що використовуються (DIU). Захист даних, що використовуються на крайніх пристроях IoT, вимагає надійного середовища для виконання коду. Це включає як конфіденційність, так і цілісність даних. Довірене середовище виконання (TEE) надає цю можливість для використання на різних процесорах. Пристрої IoT на базі ARM можуть додатково використовувати для таких операцій такі технології, як TrustZone. Пристрої IoT, засновані на інших архітектурах, системі на мікросхемі (SoC) та унікальних платах, можуть мати додаткові доступні логічні та фізичні конструкції виконання. Вбудовані мікроконтролери повинні використовувати

безпеку запобіжники для запобігання зовнішньому маніпулюванню виконуваними файлами флеш–пам'яті та критичними елементами даних/ конфігурації На додаток до мікро–апаратного захисту, де це можливо, гарантоване використання захищених операційних систем, таких як WindRiver. Багато профілів пристроїв IoT скорочуються до невеликих, але потужних модулів SoC, здатних запускати різноманітні операційні системи із захищеним завантаженням, що мають суворий контроль доступу, надійні середовища виконання, мікроядра високого рівня захисту, розділення ядра та інші функції безпеки. Захищені, офіційно змодельовані мікроядра, такі як National ICT Australia (NICTA) seL4, створюють міцну основу для пристроїв IoT, що будуються з нуля.

4) Запобігання втраті даних (DLP). Запобігання втраті даних має вирішальне значення при плануванні та виконанні добре розробленого розгортання IoT. Очікується, що пристрої IoT, що використовуються в медичних, промислових контрольних, побутових та інших парадигмах розгортання, збирають і передають величезну кількість інформації. DLP забезпечує гарантію того, що конфіденційні дані не розповсюджуються за межами призначеної бази користувачів або мережі. Планування DLP слід проводити на початку розгортання та періодично, коли нові пристрої IoT вводяться в корпоративну мережу. Позначення елементів даних є важливою передумовою належного DLP і дозволяє точкам забезпечення політики, захистам XML, одностороннім діодам та іншим пристроям фільтрувати та регулювати подальшу передачу конфіденційних даних.

5) Політика цілісності даних та агрегування. Величезна кількість пристроїв IoT дозволяє створювати надзвичайно великі набори даних, корисні в різних системах аналізу даних. Важливим кроком в управлінні безпекою IoT є забезпечення того, щоб величезний обсяг даних у сукупності не порушував правил конфіденційності користувачів або системи. Політику агрегації необхідно враховувати в процесі планування конфіденційності

таким чином, щоб застосовуватись належний контроль. Чи враховуємо ми дані ІЦВ та відокремлений ІЦВ, а також агрегування чи очищення даних?

7 ВИЗНАЧЕННЯ ЗАСОБІВ КОНТРОЛЮ ЖИТТЕВОГО ЦИКЛУ ДЛЯ ПРИСТРОЇВ IoT

Елементи керування життєвим циклом для крайніх пристроїв IoT вимагають управління та моніторингу активів, щоб переконатися, що вони авторизовані, захищені та регулярно оновлюються за допомогою найновішої прошивки, програмного забезпечення та виправлень. Крім того, організація повинна мати задокументований метод надійного розпорядження активами IoT в кінці життєвого циклу. Визначте підхід до управління життєвим циклом для пристроїв IoT. Приклад такого життєвого циклу, який використовують прилади, що побудованы за технологиею IoT приведено на на рисунку 7.1.

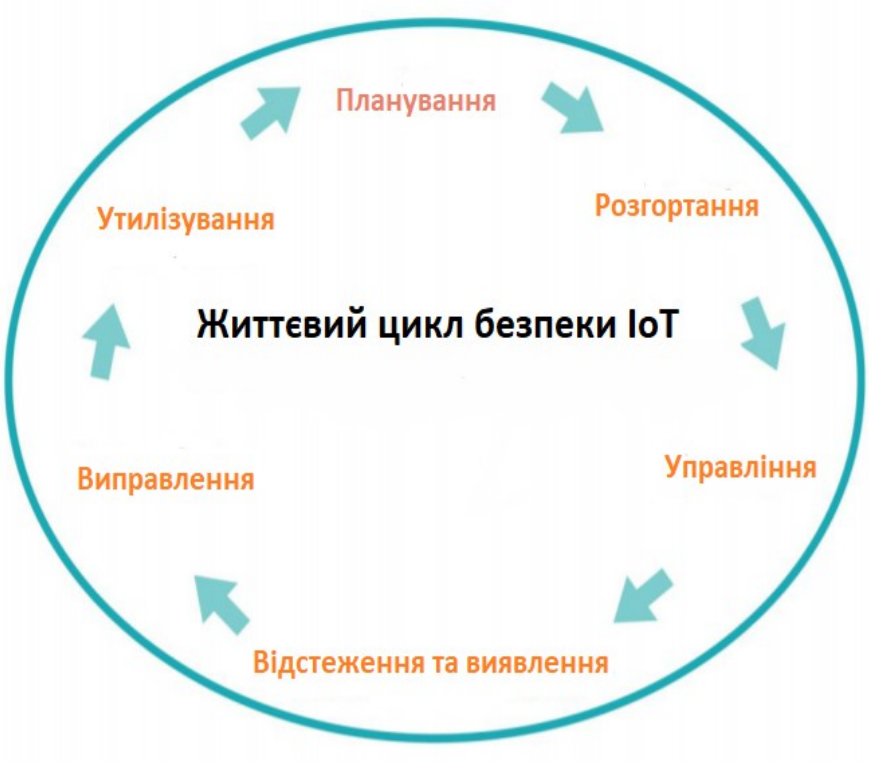

Рисунок 7.1 – Життєвий цикл для крайніх пристроїв IoT

7.1 План, розгортання та управління

Для кожного розгортання IoT враховуйте допоміжну інфраструктуру, необхідну для управління безпекою та моніторингу. Визначте відповідні інтерфейси до існуючого обладнання безпеки, оновлюючи мережеві архітектури, щоб сегментувати певні анклави IoT. Для цього можна використати план нижче.

1) Планування комунікацій:

– де буде знаходитись пристрій (корпоративна мережа, інше)?;

– публічно доступна IP–адреса (IPv4);

– план базової підготовки та переходу IPv6;

2) планування фізичної безпеки:

– планування середовища розгортання; де знаходиться пристрій; складова; яка фізична безпека (контроль доступу)?

3) Логічне планування безпеки:

– план зони безпеки;

4) Встановіть базову лінію поведінки, яку можна перевірити:

– яку можливість аудиту має пристрій?

– потрібно доповнювати іншими пристроями фіксації аудиту, які можуть контролювати трафік до/з пристроїв?

– які нормальні робочі пороги для пристроїв і що повинно викликати попередження (якщо це значення не перевищує);

5) Складіть план автентифікації/авторизації:

– документуйте ролі та послуги кожного типу пристрою;

– розмежування відповідних ролей безпеки;

– встановлення матриці контролю доступу для кожного пристрою;

– складання плану об’єднання пристроїв, якщо це необхідно;

6) Визначити критичність пристроїв та/або інформації, що підтримується пристроями.

– визначення необхідного рівня строгості реєстрації пристрою для криптографічного матеріалу;

– визначення наборів шифрів, необхідних для захисту даних та функцій пристрою;

7) Розробити тести розгортання та перевірки завантаження.

– перевірка інтеграції пристроїв IoT у функціонал безпеки, що надається інфраструктурою;

8) Оновлення підприємства і Архітектурна документація

– шаблони інтеграції IoT;

9) План обміну інформацією.

– якими даними можна поділитися?

– які дані будуть передані?

– які засоби контролю конфіденційності цих даних?

10) Встановіть конфіденційність, вимоги та засоби контролюю.

– конфіденційність даних у парі;

– чи можна довільно зменшувати дані без збереження необхідних засобів захисту;

11) Встановіть правила безпеки і пом'якшення наслідків

– багато пристроїв не підтримують автентифікацію/авторизацію;

– розробити пом'якшення для ризику, якщо потрібно;

– які наслідки електронного зловживання щодо безпеки зацікавлених сторін;

Надалі для розгортання системи треба слідувати наступним крокам:

- безпечні конфігурації для операційних систем крайових пристроїв IoT;
- встановлення ідентифікації пристрою (облікових записів та сертифікатів); Пристрої документування та інвентаризації (управління активами);
- первинне забезпечення ключових матеріальних і довірчих відносин;
- перевірка та перевірка оперативної безпеки;
    - Ви збираєте необхідні дані аудиту?;
    - Чи достатньо заблоковані рахунки тощо?;
- негативне тестування (необов’язково);

– за потреби розгорніть шлюзи;

Управління пристроями IoT включає управління самими крайовими пристроями, програмним забезпеченням та мікропрограмою, що завантажується на ці крайові пристрої, ліцензіями та застосуванням рутинних оновлень виправлень для зменшення вразливостей у пристроїв. Управління крайовими пристроями IoT може призвести до того, що на підприємстві керуватиме всіма активами одна точка, або у випадках, коли в більшій платформі вбудовано кілька пристроїв IoT, точка управління, швидше за все, буде вбудована в саму платформу, виконуючи роль моста пристрій нижчого рівня та сервер управління вищого рівня. Криптографічними ключами, сертифікатами або загальнодоступними секретами (якщо вони використовуються) також слід керувати на кожному пристрої.

У типових пристроях IoT є багато різноманітності – від датчиків низької потужності до ЕБУ в автомобілях. Для більшості крайових пристроїв IoT потрібно буде оновити один або кілька шарів у стеці технологій. Операційні системи можуть вимагати виправлення, прошивка може вимагати оновлення, і навіть спеціально створені програми можуть вимагати оновлення програмного забезпечення. Відстеження версій прошивки та програмного забезпечення, що працюють на крайньому пристрої IoT, є критичним аспектом управління активами та дозволить системним адміністраторам швидко розгортати необхідні оновлення на потрібних пристроях за мінімальний час. Обов’язково визначте та дотримуйтесь процедури регулярної перевірки наявності оновлень мікропрограми та програмного забезпечення, що працює на ваших пристроях IoT. Не думайте, що кінцевий постачальник повідомить вас про оновлення базового стеку технологій.

Переконатись, що ці оновлення є законними та не піддані фальсифікації, є настільки ж важливим, як і традиційні обчислювальні технології. Системні адміністратори повинні окреслити процес перевірки

достовірності та цілісності всіх оновлень, а також забезпечити наскрізний процес отримання, зберігання та оновлення пристроїв IoT.

Існують стандарти, які, ймовірно, можуть бути адаптовані до IoT для ефективного управління оновленнями мікропрограми. Як приклад, об’єкт управління оновленнями прошивки та програмний компонент Open Mobile Alliance.

Керуючий об’єкт, швидше за все, може бути витончено адаптований для підтримки оновлень мікропрограми та програмного забезпечення для крайових пристроїв. Сьогодні вже працюють постачальники, і Робоча група OMA Device Management створила специфікацію шлюзу, яка підтримує управління пристроями, що підтримують протоколи Bluetooth і ZigBee.

Звичайно, IoT стосується не лише крайових пристроїв, які збирають та передають дані, але також включає транспортні посилання, які переміщують ці дані, системи, що обробляють дані, та системи, які використовують дані. Також слідкуйте за версіями програмного забезпечення цих програм та систем та переконайтеся, що вони постійно оновлюються.

Через масштаби IoT організаціям важливо мати можливість керувати апаратним/програмним забезпеченням своїх IoT–пристроїв. Поруч із вищезазначеним, важливим є управління ліцензіями – це безпосередньо пов’язано з кількістю пристроїв, які ми маємо в навколишньому середовищі. Інвентаризація активів також повинна враховувати конкретні апаратні/ програмні версії пристроїв у середовищі.

Давайте розглянемо випадок безпеки у певній версії програмного забезпечення/прошивки пристрою IoT – без належного інвентаризації ми не можемо оцінити, "чи організація піддається ризику чи не впливає на організацію". Ще один випадок, про який я можу придумати, якщо для продукту відбувається оновлення мікропрограми, ми маємо проаналізувати, чи застосовне воно, тоді власник продукту повинен це визначити тому відображення власника до активу є дуже важливим для будь–якої інвентаризації активів навколишнє середовище. Відповідальність за

управління життєвим циклом активу IoT несе цей власник. Управління активами як інструмент/політика допоможе їм у цьому.

7.2 Криптографічний ключ та управління сертифікатами

Пристрої IoT найчастіше використовують певну комбінацію криптографічних ключів, сертифікатів або загальнодоступних секретів.

Коли використовуються ключі та сертифікати, слід подбати про те, щоб розглянути заходи безпеки, що викликаються при їх створенні, розповсюдженні та загальному управлінні. Такі міркування, як скасування, компромісне відновлення та первинна реєстрація кожного пристрою має бути продумано та адаптовано процеси на основі цінності інформації, що захищається.

Ключі не повинні бути доступними для сторонніх розробників. Підприємство повинно мати повний контроль над управлінням ключами та життєвим циклом ключів. Життєвий цикл ключа та сертифіката забезпечує безпеку матеріалу ключа та прив’язку ключів/сертифікатів до користувачів та пристроїв. Життєвий цикл також визначає обробку сертифікатів, які вважаються скомпрометованими, та процес знищення основних матеріалів, коли вони більше не потрібні. Інші аспекти життєвого циклу включають процеси відновлення ключів, коли це необхідно, а також процес, що використовується для оновлення ключів та сертифікатів, що розгортаються на всьому підприємстві регулярно.

Після того, як буде визначено комплексний життєвий цикл, можна буде вивчити можливості скористатися можливостями безпечної автоматизації, що надаються постачальниками. Автоматизація надання та повторного надання сертифікатів забезпечує впорядковані робочі процеси, однак важливо оцінити загрози, пов’язані з автоматизованою обробкою процесів, щоб не відкрити двері для нових векторів атак.

Кількість ключів і сертифікатів, розгорнутих у IoT, робить відстеження їх складним завданням. Це може спричинити необхідність збільшити термін служби сертифікатів пристрою, що полегшує адміністративний тягар повторного надання сертифікатів, але може також збільшити ризик того, що сертифікати можуть бути скомпрометовані та використані невідомо, не знаючи про це. Незважаючи на те, що не завжди можливо підтримувати консолідовану ситуаційну обізнаність про стан усіх сертифікатів та ключів в інвентарі IoT організації через сегментовані мережі та довірчі відносини, організації повинні прагніть робити це, коли це можливо.

Тривалість часу, протягом якого використовується певний ключ, є критичним фактором у визначенні ризику, пов’язаного з певним ключем. Наприклад, ключ, який мав необмежений криптоперіод, дозволив би зловмисникові витратити незліченні години на спроби виконати грубі атаки, а також забезпечив значні можливості для збору даних при спробах провести криптоаналіз. Вибираючи криптоперіод для ключів, важливо розуміти середовище, в якому ключі будуть зберігатися та використовуватися всередині. Ключі, які забезпечуються суворим захистом безпеки, часто можуть надаватися довше криптоперіоди проти ключів, які перебувають у менш захищених системах (наприклад, розумних лічильниках без схвалених модулів криптозв'язку FIPS 140–2). Обмеження терміну служби ключа також зменшує час, який має той, хто зламав ключ щоб скористатися цим ключем.

В енергетичному секторі NISTIR рекомендував забезпечити ключові терміни служби від 3 до 6 років для сертифікатів пристроїв, що надаються на комунальні послуги, з максимальним терміном служби 10 років. Обґрунтування цієї рекомендації ґрунтується на необхідності обмежити кількість матеріалу, пов’язаного з певним ключем, який можна зібрати на підтримку спроб криптоаналізу. Регулярне оновлення ключа гарантує, що корисні спроби зловмисників здійснити криптоаналіз обмежені, припускаючи, що використовуються досить сильні алгоритми та довжина ключів.

Сертифікати криптографічно пов’язані з парою відкритий/приватний ключ певної сутності. Оскільки пара ключів оновлюється, сертифікат, пов’язаний з парою ключів, також повинен бути оновлений. Є випадки, коли ключ залишається нерухомим вважається криптографічно звуковим може бути просто прив'язаний до нового сертифіката, однак організації слід розглянути можливість планування обмеження терміну служби кожного сертифіката пристрою, щоб забезпечити їх регулярне оновлення та захист від атак.

Швидше за все, не буде вказано термін дії деяких сертифікатів, наданих виробником IoT, що відкриває запитання, що стосуються рівня довіри до цих сертифікатів, і свідчить про необхідність складання плану якщо компрометація виробника сертифікована.

Рекомендований криптоперіод для конкретного ключа залежить від призначення та типу ключа. Зверніться до розділу 5.3.6 NIST SP 800–57, щоб отримати конкретні рекомендації за типом ключів.

Реєстрація та схвалення видачі сертифіката надійній стороні із сертифікатом PKI є важливим аспектом забезпечення безпеки впровадження PKI. Для пристроїв, які обробляють ідентифікаційну інформацію або іншу конфіденційну інформацію, слід подбати про використання процесу реєстрації, який за рівнем безпеки еквівалентний іншим елементам керування, що застосовуються для захисту даних.

Одним з найважливіших аспектів будь-якої реалізації управління ключами є чітке розуміння того, що потрібно робити у випадку компромісу або з крайнім пристроєм IoT, або, що є більш критичним. У випадку компрометації ключа пристрій або сертифіката слід дотримуватися стандартного процесу відкликання сертифіката, однак слід також провести розслідування компромісу, щоб зрозуміти, як був скомпрометований ключ/ сертифікат, щоб можна було вжити заходів з виправлення, обмеживши потенціал для повторення події.

7.3 Контроль і виявлення

Зазвичай фахівці з безпеки перевантажені захистом багатьох програм і пристроїв у той час, оскільки кожен фахівець із безпеки має 50–60 розробників програмних кодів, які можуть розробляти код з потенційними вразливостями. Отже, старі методи ручного тестування на проникнення та щоквартальні перевірки безпеки вже не є достатніми. Існує потреба в автоматизованому ручному тестуванні безпеки на регулярній основі з використанням інструментів динамічного моніторингу.

Для ефективної регулярної оцінки стану безпеки IoT все ще потрібне більш залучене тестування на проникнення.

Враховуючи IoT, фізичне тестування пристроїв з відкритим інтерфейсом Joint Test Action Group (JTAG) та послідовними інтерфейсами не може бути автоматизовано. Кмітливий користувач може скористатися перевагами налагодження апаратних інтерфейсів, які залишаються після масового розгортання. Оскільки з цього щокварталу проводити тестування на повне проникнення.

IoT також надає можливість використання аналітики великих даних разом із інструментами динамічного моніторингу для прогнозування загроз у реальному часі. Це дозволить організаціям швидше оговтатися від катастроф у безпеці. Рекомендується також перевірити стан здоров’я кожного пристрою IoT, щоб перевірити його жвавість та функціональність.

Також слід здійснювати моніторинг подій безпеки в інфраструктурі IoT, в ідеалі, цілодобово. Планування збору даних, що мають відношення до безпеки, та встановлення правил для ідентифікації подій або комбінацій подій, що представляють інтерес, слід проводити на початку життєвого циклу техніки. Подумайте про те, щоб аналітики з питань безпеки відповідали за моніторинг майже реального часу стану безпеки вашого впровадження.

Важливим є також відстеження вразливостей, пов’язаних з різними програмними компонентами реалізації IoT, а також останніми загрозами для типів пристроїв IoT. Подумайте про доручення цього обов’язку комусь відстежувати та звітувати про різні загрози для вашої конкретної реалізації IoT.

Оновити плани реагування на інциденти, щоб включити нові системи IoT та визначити процедури для обробки компромісних подій. Складіть плани викликів для аналітиків з питань безпеки для швидкої ескалації подій та бути готовими до вивезення команд інцидентів відповідачів для розслідування та усунення проблем.

Через велику кількість реалізацій IoT, швидше за все, багато крайових пристроїв будуть регулярно замінюватися. Важливо встановити політику та процедури безпечної утилізації приладів, що утримуються конфіденційна інформація або ключовий матеріал, який може забезпечити доступ до конфіденційної інформації. Пристрої, що містять конфіденційну інформацію, слід надійно протирати, включаючи видалення основних матеріалів та сертифікатів з кожного пристрою.

8 СИСТЕМА АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ДЛЯ РОЗГОРТАННЯ IoT СИСТЕМИ

Сценаріїв автентифікації IoT безліч. Компоненти IoT можуть взаємодіяти між собою, вимагаючи автентифікації машинно–машинного (м2м). Компоненти IoT можуть взаємодіяти з хмарними програмами, мобільними додатками, Інтернетом додатки або навіть безпосередньо з людьми. Одним із складних аспектів автентифікації та авторизації в Інтернеті речей є те, що багато пристроїв працюватимуть у обмежених умовах, що означає, що використовувані протоколи можуть обмежувати параметри автентифікації або що пристрої не зможуть використовувати певні можливості автентифікації, наприклад сертифікат– аутентифікація на основі.

Існує низка різноманітних випадків використання, пов’язаних з автентифікацією компонентів IoT у межах підприємства. Більшість із цих випадків використання можна абстрагувати для узагальнення вимог автентифікації в IoT до наступного:

- пристрій IoT автентифікується на іншому пристрої IoT;
- пристрій IoT автентифікується на шлюзі чи пристрої контролера, або навпаки;
- шлюз контролер перевіряє автентичність певної служби (у хмарі) або навпаки;
- різні програми автентифікуються для певної служби (у хмарі) ;
- користувач проводить автентифікацію на пристрої IoT (наприклад, лікар проводить автентифікацію на медичному імплантованому);
- адміністратор автентифікується на пристрої IoT (наприклад, Центр управління дорожнім рухом здійснює автентифікацію на стороні дороги обладнання) ;

Приклад використання роздрібної торгівлі може показати деякі запитання щодо захисту рахунків від компромісів. На рисунку х показано

випадки використання сигналізації та датчиків навколишнього середовища, що збирають дані з декількох крайові компоненти та обмін цими даними з різними мобільними пристроями. У цьому сценарії важливо забезпечити, щоб усі облікові записи були заблоковані в достатній мірі, щоб зменшити загрозу отримання зловмисником доступу до чутливих систем, які можуть призвести до фізичної шкоди.

Якщо ми вивчимо, як сьогодні реалізується автентифікація IoT, ми можемо побачити, що існує ряд доступних варіантів.

Ці параметри зазвичай включають:

- попередньо спільний ключ/загальний секрет;
- автентифікація на основі сертифікатів;
- автентифікація на основі токенів;

Ми також бачили випадки, коли компанії застосовували слабкі схеми автентифікації, такі як використання хешованого MAC для ідентифікації. Ці підходи можуть підтримувати простоту використання, однак вони не рекомендуються для реалізацій, де потрібна безпека платформи.

Можна використовувати спільні секрети, хоча вони можуть створювати значні накладні витрати на управління. Якщо використовується спільно–секретний підхід, переконайтеся, що схема базується на використанні коду автентифікації хеш–повідомлень, заданого NIST.

Алгоритм hash–based message authentication code (HMAC), який криптографічно пов’язує вміст і ідентичність повідомлення (наданий ключ). HMAC забезпечують функції аутентифікації походження даних та перевірки цілісності повідомлень. Прикладом схеми HMAC є HMAC–SHA–256.

Аутентифікація на основі сертифікатів може підтримувати такі протоколи, як TLS та DTLS. Одна з проблем автентифікації на основі сертифікатів пов'язана з розміром структури сертифіката X.509. Існує альтернативна структура, яка є оптимізовано для транзакцій автентифікації "машина–машина" та пристроїв, обмежених пам'яттю. IEEE визначив 1609.3 сертифікатів для використання з цифровим комунікаційним зв'язком

короткого діапазону, що використовується у зв'язку між транспортними засобами.

Структура сертифіката оптимізована для пристроїв, обмежених пам'яттю, і набагато менша, ніж стандартний сертифікат X.509.

Розробники повинні розглянути можливість переходу на сертифікати IEEE 1609.3, коли стикаються з обмеженими пристроями та середовищах.

Використання сертифікатів (незалежно від того, чи є X.509 чи 1609.3) створює ймовірну потребу в інфраструктурі відкритих ключів, яка централізовано управляє всіма сертифікатами, наданими пристроям. Сюди входять такі важливі функції, як надійна реєстрація та компромісне відновлення.

Схеми автентифікації на основі токенів, такі як OATH 2 та Федеральна автентифікація OpenID Connect, надають корисні альтернативи загальним секретам та сертифікатам, а також дозволяють запровадити комплексний контроль політики застосовано до вимог доступу до IoT.

Обраний метод автентифікації залежить від обмежень пристрою. Спільна секретна автентифікація вважається менш бажаною альтернативою автентифікації на основі сертифікатів. При спільних секретах накладні витрати, пов’язані з управлінням секретами, стають значними по мірі збільшення кількості пристроїв. Аутентифікація на основі сертифікатів вносить проблеми, пов'язані з обробкою сертифікатів та асиметричними алгоритмами, що використовуються для таких функцій, як встановлення автентичності ключів.

Для транзакцій між пристроями, будь то з однорангових пристроїв або з крайніх пристроїв до шлюзів чи розповсюджувачів, часто найкраще скористатися перевагами можливостей автентифікації, вбудованих безпосередньо в протоколи, які вони підтримують. Як наприклад, протокол обмежених додатків (CoAP) забезпечує чотири режими роботи. Кожен режим має рівень загрози що вимагає певного рівня автентифікації.

– без захисту – передбачає захист на іншому рівні протоколу;

– preSharedKey – симетричний ключ ділиться між групами, уповноваженими на спілкування;

– rawPublicKey – для кожного пристрою, що реалізує CoAP, надається єдиний асиметричний ключ;

– сертифікат – кожен пристрій, що реалізує CoAP, отримує сертифікат X.509;

У режимах CoAP режим “No Security” передбачає, що захист застосовується на іншому рівні протоколу. Режим preSharedKey забезпечує елементарну автентифікацію між пристроями, однак не рекомендується, враховуючи складність збереження захищений ключ та складність управління ключем. Режим preSharedKey покладається на використання одного ключа в мережі зв'язку пристрою. Хоча цього підходу може бути достатньо для невеликих кількостей пристроїв, він погано масштабується. Якщо ключ порушено, зміна клавіш на всіх пристроях, що беруть участь, стає трудомісткою та складною.

Кращими підходами до автентифікації за допомогою CoAP для транзакцій від пристрою до пристрою є використання режимів rawPublicKey та сертифікатів. Режим rawPublicKey вимагає надання унікальних асиметричних ключів для кожного пристрою, усуваючи занепокоєння, пов’язане із складанням одного ключа, що вимагає запиту всіх пристроїв. Режим сертифіката подібний до режиму preSharedKey, хоча додає додаткову міру довіри до сегментів пристроїв (на основі того, що емітент ЦС знаходиться у довіреному сховищі) та потужну підтримку відкликання. Зазвичай ви використовуєте цей режим під час використання інфраструктури відкритих ключів (PKI) для ваших пристроїв. Цей підхід є кращим для більш масштабних проектів, де використовуються велика кількість бездротових або дротових пристроїв, та які мають між собою зв’язок та різні потоки даних, котрі повинні бути захищені .

Вивчаючи інші протоколи IoT з точки зору автентифікації, ми можемо спостерігати наступне, у таблиці 8.1:

Таблиця 8.1 – Протоколи та параметри аутентифікації

Протокол	Параметри автентифікації	Аналіз
MQTT	Ім'я користувача/Пароль	MQTT дозволяє надсилати ім'я користувача та пароль, хоча рекомендує це пароль не повинен містити більше 12 символів. Ім'я користувача та пароль надсилаються зрозуміло, і тому важливо, щоб TLS використовувався при використанні MQTT.
CoAP	preSharedKey rawPublicKey сертифікат автентифікації	CoAP підтримує безліч варіантів автентифікації для пристрою на пристрій спілкування. Підключіть до Datagram TLS (D–TLS) для забезпечення конфіденційності вищого рівня послуги.
CoAP	preSharedKey rawPublicKey сертифікат	CoAP підтримує безліч варіантів автентифікації для пристрою спілкування. Це може вам дати можливість вибрати саме той алгоритм, що підходить вам найбільше.
XMPP	Доступно кілька варіантів, залежно від протоколу	XMPP підтримує різноманітні схеми автентифікації за допомогою простої автентифікації та рівень безпеки (SASL – RFC4422). Механізми включають односторонні анонімні як а також взаємну автентифікацію

Продовження таблиці 8.1

Протокол	Параметри	Аналіз

		зашифрованими паролями, сертифікатами та іншим засоби, реалізовані через рівень абстракції SASL.
DDS	Сертифікати X.509 (PKI) за допомогою RSA та DSA алгоритмів. Токени	Захист стандарту розподілу даних груп об'єктів керування (DDS). Специфікація забезпечує автентифікацію кінцевої точки та встановлення ключа для виконання подальшої автентифікація джерела. Обидва цифрові підтримуються сертифікати та різні типи маркерів ідентифікації/ авторизації.
Zigbee (802.15.4)	Pre–shared keys	Zigbee забезпечує автентифікацію як на мережі, так і на рівні програми (та шифрування) за допомогою використання головного ключа (необов'язково), мережі (обов'язково) та, за бажанням, Клавіші посилання програми [RBJ1].
Thread	(Бета–стандарт повинен бути звільнений)	Передбачається використання протоколу бездротової мережі IPv6 для розумного пристрою, який Thread використовуватиме цей протокол. Та щоб покращити параметри безпеки, що містяться в інших бездротових протоколах.

Продовження таблиці 8.1

Протокол	Параметри автентифікації	Аналіз

Zigbee (802.15.4)	Pre–shared keys	Zigbee забезпечує автентифікацію як на мережі, так і на рівні програми (та шифрування) за допомогою використання головного ключа (необов'язково), мережі (обов'язково) та, за бажанням, Клавіші посилання програми [RBJ1].
Bluetooth	Shared Key	Bluetooth надає послуги автентифікації за допомогою двох різних пристроїв, що з'єднуються в пару параметри, стандартне та просте сполучення. Стандартний метод сполучення – автоматичний; Метод простого сполучення включає людину в циклі для перевірки (слідуючи простому Diffie–Hellman exchange), що два пристрої відображають однаковий хеш встановлений ключ. Bluetooth пропонує як односторонню, так і взаємну автентифікацію «Введення ключа доступу» та «Немає в наявності» опції автентифікації пристрою.. Це теж треба враховувати, коли обираєш протокол.

Продовження таблиці 8.1

Протокол	Параметри автентифікації	Аналіз
Bluetooth–LE	Незашифровані дані автентифікований за допомогою	Bluetooth–LE вводить у світ Bluetooth двофакторну автентифікацію система, модель

	Підпис підключення Ключ розв'язання (CSRK) Ідентифікація пристрою/конфіденційність через розпізнавання особистості Ключ (IRK)	поєднання LE Secure Connections, яка поєднує – на основі можливість пристрою – доступно кілька доступних моделей асоціацій. В додаток, Еліптична крива Діффі Хеллман використовується для обміну ключами.
HTTP/REST	Базова автентифікація (прозорий текст) (методи TLS) BCIX2	HTTP/REST зазвичай вимагає підтримки протоколу TLS для автентифікації та послуги конфіденційності. Хоча базова автентифікація (де є облікові дані передано в чистому вигляді) можна використовувати під прикриттям TLS.

Процес вибору оптимальних механізмів автентифікації для вашого розгортання IoT можна керувати відповідями наступний набір питань та рішень проблем безпеки системи IoT, що представлений у таблиці 8.2.

Таблиця 8.2 – Питання для вибору оптимальних механізмів автентифікації

№	Питання	Рішення
1.	Чи вимагає ваша реалізація комунікації машина–машина?	Якщо так, вивчіть протоколи зв'язку пристрою та визначте, чи є вони підтримує автентифікацію.
2.	Чи підтримують ваші пристрої IoT один із	Якщо ні, розгляньте рівень шару, щоб включити автентифікацію вищого рівня

	комунікаційних протоколів, що надає послуги автентифікації?	послуги, такі як TLS або DTLS.
3.	Чи обмежений інвентар вашого пристрою IoT пам’яттю чи обробною потужністю?	Якщо так, розгляньте можливість співпраці з постачальниками для підтримки сертифікатів IEEE 1609.3
4.	Хто керуватиме вашими пристроями? Чи потрібно дистанційне управління?	Спочатку сплануйте своє впровадження. Створіть автентифікацію та доступ контрольної матриці та виберіть найсильніший підтримуваний метод автентифікації ожним крайовим пристроєм.
5.	Чи підтримують ваші пристрої IoT мережеві функції віддаленого управління, такі як SNMP або SSH	Заблокуйте кожен пристрій перед тим, як виставляти інформацію, щоб підтримувати лише авторизовану послуги управління. Встановіть політику та прооцедури віддаленого керування своїми пристроями за допомогою мережі.
6.	Чи реалізують ваші пристрої IoT інтерфейси RESTful?	Розглянемо підхід, заснований на маркерах, такий як OAUTH2. Переконайтеся, що дизайн автентифікації включає ключі API

Продовження таблиці 8.2

№	Питання	Рішення
6.	Чи реалізують ваші пристрої IoT інтерфейси RESTful?	Розглянемо підхід, заснований на маркерах, такий як OAUTH2, для автентифікації крайніх пристроїв. Переконайтеся, що дизайн автентифікації включає ключі API
7.	Чи підключаються	, які підтримують автентифікацію

	пристрої безпосередньо до служб у хмарі?	пристрою та додатків для хмарної служби.

Захист API є важливою частиною безпеки IoT. Постачальники IoT випускають відкриті API для продуктів, що надають багато нових різноманітних застосувань та можливостей. Цей пріоритет, наданий API, керує екосистемами в просторі IoT, і для постачальників IoT стає необхідним ставити безпеку на перше місце в локальному середовищі постачальника. Інша проблема полягає у тому, щоб не дати постачальнику зловживати своїм доступом до API в хмарі, де пристрої IoT можуть спілкуватися між собою, якщо їм надається глобальний доступ. Нам потрібно розробити модель безпеки, яка відповідає як місцевим потребам, так і глобальним потребам, пов’язаним із хмарою.

На додаток до Identity and Access Management (IAM), реалізація привілейованої системи управління користувачами відстежує діяльність та взаємодію адміністраторів, адміністративних консолей та додатків. Це особливо корисно у великих розгортаннях IoT та допомагає визначати політики облікових даних, примусово обертати паролі після кожного використання, видавати та видаляти облікові дані, реєструвати діяльність (наприклад, натискання клавіш для криміналістики).

Щодо ідентифікації споживачів, особливо в роздрібній торгівлі чи на транспорті, існує поняття централізованих систем, що базуються на політиці та базуються на згоді, що підтримує можливість споживачів давати згоду на:

- які їх атрибути чи інформація можуть бути чіткими;
- яку інформацію потрібно маскувати під час відображення;
- яку інформацію можуть використовувати сторонні аналітики та маркетинг;
- інші уподобання;

Це дуже пов'язано з дотриманням норм, але поєднання цих уподобань із політикою безпеки організації забезпечує а посилення системи безпеки.

Наявність централізованого IAM, який базується на політиці в усіх службах, де задіяні пристрої IoT, буде простішим в управлінні, ніж наявність розподіленого IAM для кожного пристрою IoT та пов'язаних додатків. Посилення та зміцнення однієї системи з єдиними загальними політиками є більш послідовним, ніж надання окремого authN/AuthZ для кожної послуги.

Існує багато проблем щодо конфіденційності щодо IoT, які необхідно вивчити. Одне із значних занепокоєнь викликає проблема захоплення даних із датчиків, про які споживач не знає. У цих випадках за особою спостерігають або відслідковують організації або іншою особою, не знаючи про це. У цьому сценарії існує багато питань, включаючи те, яким чином звертається особа, яка відстежується, та яку відповідальність несуть сторонні організації, щоб переконатись, що інформація вони збирають не отримано без явної згоди.

Нарешті, для нас буде важливо дослідити, який із набору, який не відповідає вимогам щодо конфіденційності (повідомлення, обізнаність, вибір, згода, доступ, застосування тощо) можна виконати за допомогою технічного контролю, а які однозначно не входять в архітектуру IoT.

Подібним чином, які елементи можна захоплювати та передавати разом із захопленими даними з точки зору атрибутів, які можуть зберігатися протягом усього життя їх потоку даних у всій системі IoT? Наприклад, якщо хтось погодився на певне використання їх даних під час збору, як це рішення залишається приєднаним до цих даних, коли вони передаються і передані та проаналізовані іншими гравцями IoT?

Чи можна позначати дані та домовлятися про "рукостискання" між партнерами по екосистемі, щоб забезпечити обробку даних лише відповідно до початкової згоди? Сюди входить будь–яка повторна ідентифікація після того, як дані були зібрані лише як анонімний елемент.

У висновках можна сказати, що технологія «Інтернет речей» ще дуже молода, тож більшість загроз, що існують через те, що розробники занадто швидко випускають нові продукти, та не тестують їх належним образом. У

всіх на меті лише якомога швидше стати лідерами у цій сфері. То ж, де, як не в цій сфері потрібен добрий аналіз загроз та повне розуміння ризиків інформаційної безпеки. Як було виявлено в атестаційній роботі, облікові дані для перевірки автентичності в хмарі, які використовуються в процесі настройки та експлуатації розгортання IoT, мабуть, являють собою найсерйознішу уразливість, яку зловмисники можуть легко використовувати, щоб отримати доступ до системи IoT і скомпрометувати її. Для захисту облікових даних рекомендується регулярно міняти пароль і намагатися не використовувати ці облікові дані на загальнодоступних комп'ютерах.

З аналізу можна зробити такі висновки. Компаніям треба більш ретельно підходити до тестуванню свого програмного забезпечення та приладів, та розраховувати усі ризики, що можуть бути. Так як, усі загрози, що були виявлені – це лише результати занадто швидкої розробки продукту. .

Тож, запорука успіху у цій справі – це спокій та розважливі дії. Треба с розумом підходити до розробки продуктів для технології «Інтернет речей» та мати на увазі досвід, що був набутий у інших сферах безпеки. Розглянуті у цій роботі загрози вже давно відомі, класифіковані та були досліджені у інших продуктах інших компаній.

Щоб забезпечити належний рівень безпеки для інфраструктури IoT, необхідна стратегія всебічного захисту. В рамках неї забезпечується захист даних в хмарі, захист цілісності даних при передачі в Інтернет, а також безпечне виробництво пристроїв. І все це дуже залежить від доброго аналізу усіх вразливостей та загроз. Саме завдяки цій методиці фахівці можуть проаналізувати всі загрози та вразливості, що можуть бути у системі або продукті.

Спираючись на показники базових метрик. Вхідних даннних та мождивостей підприемства, можна проаналізувати наскільки небезпечною є загроза і правильно побудувати комплекс дій, що можуть або запобігти збиткам або позбутися загрози зовсім. Звичайно усі дії повинні плануватися уповноваженими спеціалістами. Завдяки суворому ранжируванню загроз та

вразливостей, можна побудувати статистику загроз від найнебезпечніших до найменш небезпечних загроз.

Для повного розуміння ситуації, звичайно, треба робити більш глибокий аналіз з урахування особливостей використовування даного конкретного приладу та особливостей місця, де він буде встановлений. Це є дуже актуальним, для великих підприємств, які можуть ризикувати великими статками.

На основі всього вищесказаного ми можемо отримати таку блок–схему для побудування безпечної IoT мережі, як показано на рисунку 8.1. за допомогою, кроків, що описані у ній та у даній роботі спеціалісти можуть спроектувати та запровадити IoT мережу будь–якого масштабу та для будь–якого підприємства. Ця схема наведена на рисунку 8.1

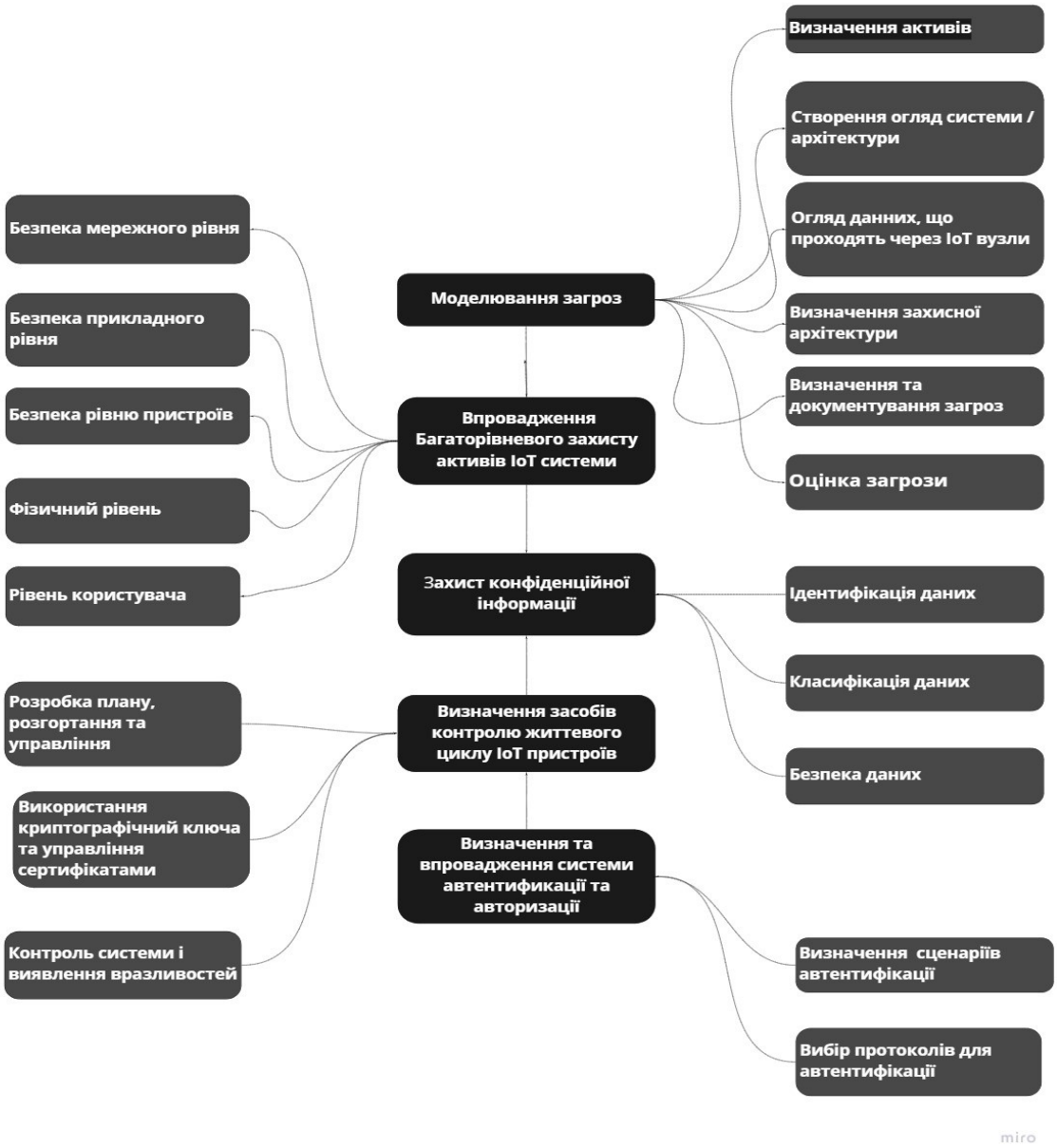

Рисунок 8.1 – Система побудови безпечної IoT мережі.

ВИСНОВКИ

«Інтернет речей» − єдина мережа, що об’єднує техніку, якою суспільство користується щодня, та віртуальний світ. Технологія не лише дозволяє віддалено керувати різними приладами, а й пов’язує їх між собою. Обмінюючись даними, речі починають «спілкуватися» один з одним.

Наразі технологія «Інтернет речей» є дуже затребуваною та популярною у всіх сферах нашого життя. Вона починається у нас вдома разом із колонками, кондиціонерами та холодильниками, і закінчується на величезних підприємствах та у космосі. Звичайно, що для великих та серйозних підприємств використовують зовсім іншу пристрої, аніж ті, що ми бачимо кожен день довкола нас.

Але у всіх них є одна велика проблема – безпека. Так як виробники у конкурентній боротьбі за ринок збуту хочуть стати лідерами ринку та швидше за інших випускати нові і нові продукти, то вони всі припускають одну й ту саму помилку. Вони недостатньо часу приділяють тестуванню приладів. З цього випливають дуже різні проблеми. Але, безперечно, найбільша з них це проблема, що стосуються інформаційної безпеки. В атестаційній роботі було розглянуто принципи роботи систем, що використовують технологію «Інтернет речей».

Щоб забезпечити належний рівень безпеки для інфраструктури IoT, необхідна стратегія всебічного захисту. В рамках неї забезпечується захист даних в хмарі, захист цілісності даних при передачі в Інтернет, а також безпечне виробництво пристроїв. І все це дуже залежить від доброго аналізу усіх вразливостей та загроз.

За допомогою сучасних практик, протоколів та технологій передачі даних було побудовано систему захисту інформації в IoT мережі. У цій системі було враховано усі фактори від людського до машинного. Вона включає в себе усі необхідні кроки для побудування системи, починаючи від

аналізу вхідних можливостей та внутрішнього потоку даних до фізичної безпеки приладів та конфіденційної інформації користувачів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ericsson Mobility Report: к 2018 году число устройств интернета вещейобойдет количество мобильных телефонов [Електронний ресурс]. – 2017. – Режимдоступу до ресурсу: https://itc.ua/news/ericsson–mobility–report–k–2018–godu–chislo–ustroystv–interneta–veshhey–oboydet–kolichestvo–mobilnyihtelefonov/.

2. Коротка історія інтернету [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://studway.com.ua/internet–rechey/ .

3. Internet of things: все, что нужно знать об интернете вещей и о будущем современной цивилизации [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.everest.ua/ru/ai–platform–2/analitika/iot–vse–chto–nuzhno–znat–ob–internete–veshhej–i–o–budushhem–sovremennoj–civilizacii/.

4. Пролетарский А. В. Беспроводные сети Wi–Fi / А. В. Пролетарский, И. В.Баскаков, Д. Н. Чирков // Беспроводные сети Wi–Fi / А. В. Пролетарский, И. В.Баскаков, Д. Н. Чирков. – Москва: Интуит, 2007. – С. 178.

5. Технология Bluetooth [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://www.sota1.ru/articles/articles_142.php3.

6. ZigBee Alliance. Specification. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://www.zigbee.org/en/spec_download/zigbee_downloads.asp.

7. Гордейчик С. В. Безопасность беспроводных сетей / С. В. Гордейчик, В.В. Дубровин // Безопасность беспроводных сетей / С. В. Гордейчик, В. В. Дубровин. – Москва: Телком, 2008. – (Горячая линия). – С. 288.

8. Overview of the Internet of Things [Електронний ресурс] // https://www.internetsociety.org/. – 2015. – Режим доступу до ресурсу: @ http://www.itu.int/rec/T–REC–Y.2060–201206–I.

9. State of the Market, The Internet of Things [Електронний ресурс] // Verizon. – 2019. – Режим доступу до ресурсу: http://www.verizonenterprise.com/resources/reports/rp_state–of–market–the–market–the–internet–of–things2015_en_xg.pdf.

10. Industrial Internet of Things Positioning Paper [Електронний ресурс] // Accenture. – 2015. – Режим доступу до ресурсу: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture–Industrial–Internet–of–ThingsPositioning–Paper–Report–2015.PDF.

11. IDC Futurescape for Internet of Things [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.idc.com/getdoc.jsp?containerId=prUS25291514.

12. Mitre Common Vulnerabilities and Exposures [Електронний ресурс] – Режим доступу до ресурсу: https://cve.mitre.org/.

13. SOHO Wireless Router (In)Security: Tripwire Vulnerability and Exposure Research Team (VERT) Report [Електронний ресурс] // 2018 – Режим доступу до ресурсу: http://www.tripwire.com/register/soho–wireless–router–insecurity/showMeta/2/.

14. Dan Geer Security of Things Forum [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://securityledger.com/2014/05/dan–geer–keynote–securityof–things–forum/.

15. Symantec Corporation Internet Security Threat Report [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://www.itu.int/en/ITUD/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf.

16. Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show Las Vegas [Електронний ресурс] // , Nevada January 6. – 2015. – Режим доступу до ресурсу:https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

17. Software Defined Perimeter (SDP) Specification Document v1.0 [Електронний ресурс] – Режим доступу до ресурсу: https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf.

18. Privacy and Data Protection Impact Assessment Framework for RFID Applications [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: http://cordis.europa.eu/fp7/ict/enet/documents/rfid–pia–framework–final.pdf.

19. Article 29 Data Protection Working Party: Opinion 8/2014 on the on Recent Developments on the Internet of Things [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://ec.europa.eu/justice/data–protection/article–29/documentation/opinionrecommendation/files/2014/wp223_en.pdf

20. Threat Modeling: Designing for Security by Adam Shostack [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: http://threatmodelingbook.com/index.html.

21. Microsoft Developer Network: The STRIDE Threat Model [Електронний ресурс] – Режим доступу до ресурсу: https://msdn.microsoft.com/enUS/library/ee823878(v=cs.20).aspx.

22. Microsoft Developer Network: Threat Modeling — DREAD [Електронний ресурс] – Режим доступу до ресурсу: https://msdn.microsoft.com/enus/library/ff648644.aspx.

23. MITRE's Common Vulnerabilities and Exposures [Електронний ресурс] – Режим доступу до ресурсу: https://cve.mitre.org/index.html.

24. OWASP's Top 10 Threats for Internet of Things [Електронний ресурс] – Режим доступу до ресурсу: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.