ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Аналіз та захист від атак на мережі Інтернету речей (IoT)»

Виконав студент 4 курсу, групи КІД-42
спеціальності 123 Комп'ютерної інженерії
освітньо-професійної програми «Комп'ютерна інженерія»
(шифр і назва спеціальності)
Кліменченко І.С.
(прізвище та ініціали)
Керівник Сосновий В.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Розмаїлов Д. О.
(прізвище та ініціали)

КИЇВ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Інститут ННІІТ

Кафедра Комп'ютерна інженерія

Ступінь вищої освіти Бакалавр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
Лащевська Н. О.
«___»_____ 2024 року

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Кліменченко Ігор Сергійович
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: Аналіз та захист від атак на мережі інтернет речей(IoT)

керівник бакалаврської роботи: Сосновий В.О.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від « 27 » лютого 2024 року.

2. Строк подання студентом бакалаврської роботи 5 червня 2024 року

3. Вихідні дані бакалаврської роботи:

1)Аналіз та види загроз

2) Інструменти загроз

3) Наукова та технічна література, рекомендації.

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити)

1) Аналіз структури незахищених мереж та розробка вимог до захисту;

2) Дослідження концепцій загроз та аналіз надійної мережі

3) Рекомендації щодо захисту мережі

5. Перелік графічного матеріалу
1) Мета, об’єкт та предмет дослідження
2) Виявлення та аналіз основних типів атак на мережу
3) Різноманітність технологій атак
4) Висновки

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Аналіз науково-технічної літератури	03.04.2024 р.	виконано
2.	Ідентифікація та аналіз основних загроз безпеці Інтернет речей	07.04.2023 р.	виконано
3.	Рекомендації щодо захисту від атак	24.04.2023 р.	виконано
4.	Способи захисту інформації в мережі з використанням VPN	29.04.2023 р.	виконано
5.	Висновки	04.05.2023 р.	виконано
6.	Створення презентації	08.05.2023 р.	виконано
7.	Підготовка доповіді	09.05.2023 р.	виконано

Студент _____ Кліменченко І.С.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Сосновий В.О.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента **Кліменченко Ігора Сергійовича**
на тему: **«Аналіз та захист від атак на мережі інтернет речей(IoT)»**

Актуальність: Маючи сьогодні понад мільярд користувачів, Інтернет став каналом, через який люди та компанії регулярно отримують доступ до корисної інформації, виконують такі завдання, як банківські операції та здійснюють покупки в різних торгових точках. Поява соціальних мереж також зробила Інтернет цінним майданчиком для бізнесу та інших організацій, де вони можуть здійснювати важливий брендинг та інші важливі взаємодії з клієнтами, часто приносячи при цьому значні прибутки. Однак, незважаючи на цю зручність, існує вразливість до збоїв. Тому тема бакалаврської роботи є своєчасною та актуальною.

Позитивні сторони:

1. Робота зосереджена на аналізі та захисті мереж Інтернету речей (IoT), що є актуальною та важливою проблемою в сучасному світі інформаційних технологій.

2. Дослідження містить рекомендації та методи забезпечення безпеки мереж IoT і, таким чином, має практичне застосування.

Недоліки:

1. Незважаючи на те, що в цій статті представлено доволі широкий огляд теми, масштаби дослідження можуть бути обмежені, особливо порівняно зі складним ландшафтом кібербезпеки, що швидко змінюється.

2. Можливо, бракує конкретних прикладів або кейсів успішних або невдалих атак на мережі IoT.

Вищезгадані зауваження не впливають на загальну позитивну оцінку бакалаврської роботи.

Висновок: робота заслуговує оцінку **«відмінно»**, а студент – **Кліменченко Ігор Сергійович** гідний присвоєння кваліфікації: бакалавр з комп'ютерної інженерії, за спеціалізацією Комп'ютерна інженерія.

Якість бакалаврської роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	
Має практичну цінність	
Проект-частина комплексної теми	

Підпис рецензента

_____ _____
(П.І.Б.)

_____
(посада, науковий ступінь, вчене звання)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Кліменчнеко І.С. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 123 Комп'ютерна інженерія
освітньо-професійної програми Інформаційні технології
(шифр і назва спеціальності)
на тему: «Аналіз та захист від атак на мережі інтернет речей(IoT)»
Бакалаврська робота і рецензія додаються.
Директор інституту _____ _____
(підпис) (прізвище та ініціали)

Довідка про успішність

Кліменченко І.С. за період навчання в інституті
(прізвище та ініціали студента)
ННІІТ з 2020 року по 2024 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ _____
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Кліменченко І.С.*** обрав тему роботи, метою якої було розробити рекомендації щодо підвищення захисту інтернет речей та аналізу загроз. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи ***Кліменченко І. С.*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану бакалаврську роботу студента ***Кліменченко Ігора Сергійовича*** на оцінку **«відмінно»** та присвоїти йому кваліфікацію: бакалавр з комп'ютерної інженерії за спеціалізацією Комп'ютерна інженерія.
Керівник бакалаврської роботи _____ .
(підпис) (прізвище та ініціали)
"____" _____ 2024року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Кліменченко І.С.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.
Завідувач кафедри Комп'ютерна інженерія
(назва)

_____ _____
(підпис) (прізвище та ініціали)
"____" _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 67 сторінок, 30 рисунків, 20 джерел.

Об'єкт дослідження – безпечне функціонування мережі інтернет речей(IoT).

Предмет дослідження – аналіз та способи захисту від атак на мережі інтернет речей.

Мета роботи – дослідити та розробити рекомендації для підвищення захисту та функціонування інтернет речей.

Методи дослідження – опрацювання технічної літератури за темою, аналіз експлуатаційної документації, проведення тестування інструментів, порівняльний аналіз сервісів.

Досліджено поняття безпечного функціонування мережі інтернет речей та особливості їх роботи.

Виокремлено новий порядок денний для покращення безпеки на рівні окремих стеків.

Проаналізовано різні типи вразливостей та рекомендовано контрзаходи.

Перераховано технічні вимоги до системи, враховуючи наступне, а саме, необхідність підвищення ефективності системи. Типи загроз та наслідки їх використання, особливо для погано захищених систем.

Розроблено рекомендації щодо покращення захисту інформаційних систем.

ABSTRACT

Text part of the bachelor's thesis: 67 pages, 30 drawings, 20 sources.

The object of consideration - is the unemployed functions of online speech (IoT).

The subject of consideration - is analysis and methods of protection against attacks on smaller Internet speeches.

Meta-Robots - Review and develop recommendations for improving the sustainability and functioning of online speech.
Methods of provision - work of technical literature on the topic, analysis of operational documentation, testing of tools, additional analysis of services.

It has been proven that oven-free functions include both online processing and individuality in work.
During the day, a new procedure has been established for replenishment without baking on smooth ridges.
Various types of aggressiveness and preferred counter-approaches are analyzed.
The technical solution for the systems has been redesigned, at the same time it is necessary to increase the efficiency of the systems. Types of downloads and enjoyment in the US, especially for some secure systems.

Recommendations have been developed to improve the storage of information systems.

ЗМІСТ

ВСТУП

У XXI столітті Інтернет речей (IoT) є однією з найважливіших і розповсюдженіших технологій яка надає нам можливість з'єднувати мільйони об'єктів навколишнього середовища в єдину мережу, щоб зробити наше життя ефективнішим, зручнішим і безпечнішим.

Проте, зростання розвитку інтернет речей, збільшує і кількість потенційних загроз. Сталість систем, зв'язаних з мережею Інтернету речей, нині стоїть перед викликами безпеки, що вимагають комплексного аналізу та захисту.

У цій кваліфікаційній роботі я розглянув виклики та загрози, які ставлять під загрозу системи IoT, провів аналіз типових атак, які можуть бути спрямовані на пристрої Інтернету речей, та розробив стратегії захисту, які дозволять забезпечити їхню надійність та безпеку.

По іншому кажучи у цьому дослідженні я збираюся поглибитися у деталі Інтернету речей, розкрити їхню вразливість та вивчити шляхи захисту, щоб забезпечити майбутнє, в якому ця захоплива технологія буде продовжувати перетворювати наш світ, залишаючи його безпечним і стійким.

Інтернет речей (IoT) став це не просто технологічний прорив, а й невід'ємна частиною нашого повсякденного життя. Він взаємодіє більшістю наших домашніх пристроїв, будинками, транспортом та навіть нашими власними тілами, створюючи значний рівень зв'язку та зручності. Проте, разом з цими перевагами приходить і ризик.

Більшість систем IoT вразливі до: крадіжки даних, відмови пристроїв та інші атаки стають все поширенішими, ставлячи під загрозу як наше приватне життя, так і інфраструктуру критичних галузей, таких як медицина та енергетика.

У цьому розділі кваліфікаційної роботи я взяв на себе завдання розглянути та проаналізувати ці ризики та атаки, щоб розкрити їхні причини та наслідки. Я дослідив нові методи, які використовуються зловмисниками для зламу систем IoT, і виробив стратегії та визначив методи для захисту від таких загроз.

Це дослідження розкриє не тільки проблемну сторону Інтернету речей, але й практичні способи забезпечення безпеки та стійкості цих систем. Я не тільки покладався на сучасні технології кібербезпеки, але й звернувся до основних принципів і практик, які допоможуть зберегти довіру до світу Інтернету речей.

1. ВПРОВАДЖЕННЯ ІНТЕРНЕТУ РЕЧЕЙ (IOT): ВИЗНАЧЕННЯ ТА ПЕРСПЕКТИВИ

1.1 Визначення та важливість Інтернету речей (IoT)

Перед тим як створювати будь-яку систему захисту , необхідно розробити та проаналізувати модель системи, яку потрібно захистити, щоб виділити її основні характеристики та загрози, які вона може реалізувати [1, 2].

Рис. 1.1 Інтернет речей: мережева архітектура та архітектура безпеки

Інтернет речей (IoT) – взагалі це підключення різних фізичних пристроїв (від домашніх пристроїв, таких як пилосос чи телевізори, до промислових систем, таких як датчики виробництва та елементи інфраструктури) до Інтернету та здатність цих пристроїв взаємодіяти між собою та з іншими системами без необхідності

людського втручання. Сутність IoT полягає в створенні "розумного" середовища, де різні пристрої можуть автоматично збирати, обробляти та обмінюватися інформацією для досягнення поставлених цілей.

Термін «інтернет речей», зобов'язаний своєю появою Кевіну Ештону, який в 1997 р, працюючи на компанію Proctor and Gamble, застосував технологію радіочастотної ідентифікації (RFID) для керування системою поставок. Завдяки цій роботі в 1999 році його запросили в Масачусетський технологічний інститут, де він з групою однодумців організував дослідний консорціум Auto-ID Center. З тих пір Інтернет речей звершив перехід від простих радіочастотних міток до екосистеми і індустрії. Аж до 2012 р ідея підключення речей до Інтернету переважно відносилася до смартфонів, планшетів, ПК і ноутбуків. По суті, до тих пристроїв, які в усіх відношеннях виступають в якості комп'ютера. До цього, з моменту появи перших боязких зачатків Інтернету (таких як створена в 1969 р мережу ARPANET), більшості технологій, на яких будується Інтернет речей, просто не існувало.

Значення Інтернету речей в сучасному світі важко переоцінити. Ось кілька ключових аспектів, які підкреслюють його важливість:

Зручність та комфорт: Насамперед пристрої Інтернету речей роблять наше життя простіше і комфортніше. Наприклад, розумні домашні пристрої дозволяють успішно контролювати такі аспекти вашого будинку, як температура в приміщенні та освітлення, за допомогою мобільного додатка або голосового помічника.

Використання у виробнитстві: Промисловість впровадила IoT для вдоско налення та прискорення виробничих процесів, відстеження ресурсів та управління обладнанням. Наприклад, виробничі компанії використовують датчики IOT для слідкування за станом обладнання, прогнозування потреб у технічному

обслуговуванні, а також для запобігання нещасним випадкам та зменшення простоїв обладнання.

Медицина: У галузі медицини Інтернет речей використовується для віддаленого моніторингу стану пацієнтів, надання невідкладної медичної допомоги та скорочення часу реагування на надзвичайні ситуації. Наприклад, Носимі пристрої, які вимірюють частоту серцевих скорочень та інші ознаки привітання, можуть надсилати ці дані до медичного центру для аналізу та обробки за необхідності.

Економіка: Користуючись перевагами Інтернету речей, ми можемо автоматизувати процес управління, щоб ефективніше використовувати такі ресурси, як енергія та вода. Наприклад, інтелектуальні зрошувальні системи використовують дані датчиків для оптимізації часу та обсягу поливу, зменшення витрати води та споживання енергії.

Інтернет речей відкриває безмежні можливості для покращення різних аспектів нашого життя. Але водночас приходить і необхідність забезпечити безпеку та захист цих систем від загроз. У наступних розділах ми розглянемо аспекти атак та ризиків.

1.2 Зростання зацікавленості у розвитку та використанні IoT

Інтернет речей (IoT) в останні роки набирає все більше інтересу як у повсякденному житті так і у бізнес-сферах. Зростання зацікавленості у розвитку IoT впливає на багато сфер сучасного життя, від побутових пристроїв до промислових систем та інфраструктури.

1.2.1 **Застосування IoT у повсякденному житті**

Однією з головних причин зростаючого інтересу до розвитку Інтернету речей є його практичність у повсякденному житті. Сьогодні все більше побутових пристроїв стають "розумними" завдяки підключенню до інтернету. Від "розумних" пилососів, якими можна керувати віддалено за допомогою смартфона, до "розумних" термостатів, які автоматично регулюють температуру всередині будинку відповідно до зовнішньої температури, Інтернет речей перетворює наші оселі на більш комфортні місця.

Інтернет речей також пропонує нові можливості для збору та аналізу даних про наше повсякденне життя. Завдяки датчикам та підключенню до Інтернету ми можемо відстежувати наші звички, стан здоров'я та споживання енергії і приймати більш обґрунтовані рішення. Це дуже допомагає слідкувати за здоровьям.

1.2.2 **Промислові та комерційні застосування IoT**

У промисловому та комерційному секторах IoT надає дуже багато можливостей для підвищення продуктивності, оптимізації процесів та підвищення загального прибутку. Промислові компанії використовують IoT для моніторингу та підтримки виробничих ліній, прогнозування потреб у технічному обслуговуванні та автоматизації процесів, які раніше вимагали участі людини.

Застосування IoT доволі значне у сфері роздрібної торгівлі, де магазини використовують "розумні" системи інвентаризації та аналізу даних покупців для покращення обслуговування та оптимізації асортименту.

1.2.3 Вплив зростання зацікавленості у розвитку IoT

Загалом, зростання зацікавленості у розвитку та використанні IoT відкриває нові горизонти для технологічного прогресу і суспільного розвитку:

Економічний розвиток: Розвиток IoT сприяє створенню нових ринків продуктів та послуг, що стимулює економічний розвиток. Компанії, що спеціалізуються на розробці IoT-рішень та здійснюють значний вклад у розширення та модернізацію глобального бізнесу.

Соціальний вплив: IoT змінює наше повсякденне життя, роблячи його більш зручним та комфортним. Від інтелектуальних домашніх пристроїв до медичних систем віддаленого моніторингу.

Оптимізація ресурсів: IoT допомагає оптимізувати використання ресурсів, таких як електроенергія, вода та інші, що сприяє збереженню енергії та зменшенню викидів, що впливають на навколишнє середовище.

Кібербезпека: Розвиток IoT ставить під загрозу приватність та кібербезпеку, оскільки збільшує кількість пристроїв, підключених до Інтернету. Це стимулює інновації в галузі кібербезпеки та сприяє розвитку нових методів захисту від кіберзагроз.

Глобальні зміни: Впровадження IoT може мати глибокий вплив на розвиток міст, транспортних систем, сільського господарства та інших секторів, що сприяє створенню "розумних" та ефективних міст та громад.

Ці технології не лише полегшують наше життя та роботу, але й мають потенціал для революційних змін у різних галузях, від охорони здоров'я до екології. Однак, разом з новими можливостями приходять і нові виклики, особливо в сфері кібербезпеки, які потребують уважного аналізу та вироблення ефективних стратегій захисту.

Технологія Інтернету речей (Internet of Things) посіла третє місце за кількістю впроваджених або запланованих до впровадження технологій у північноамериканських та європейських організаціях у 2023 році. Більше половини (57%) північноамериканських та європейських організацій наразі використовують IoT у своїй діяльності — Statista

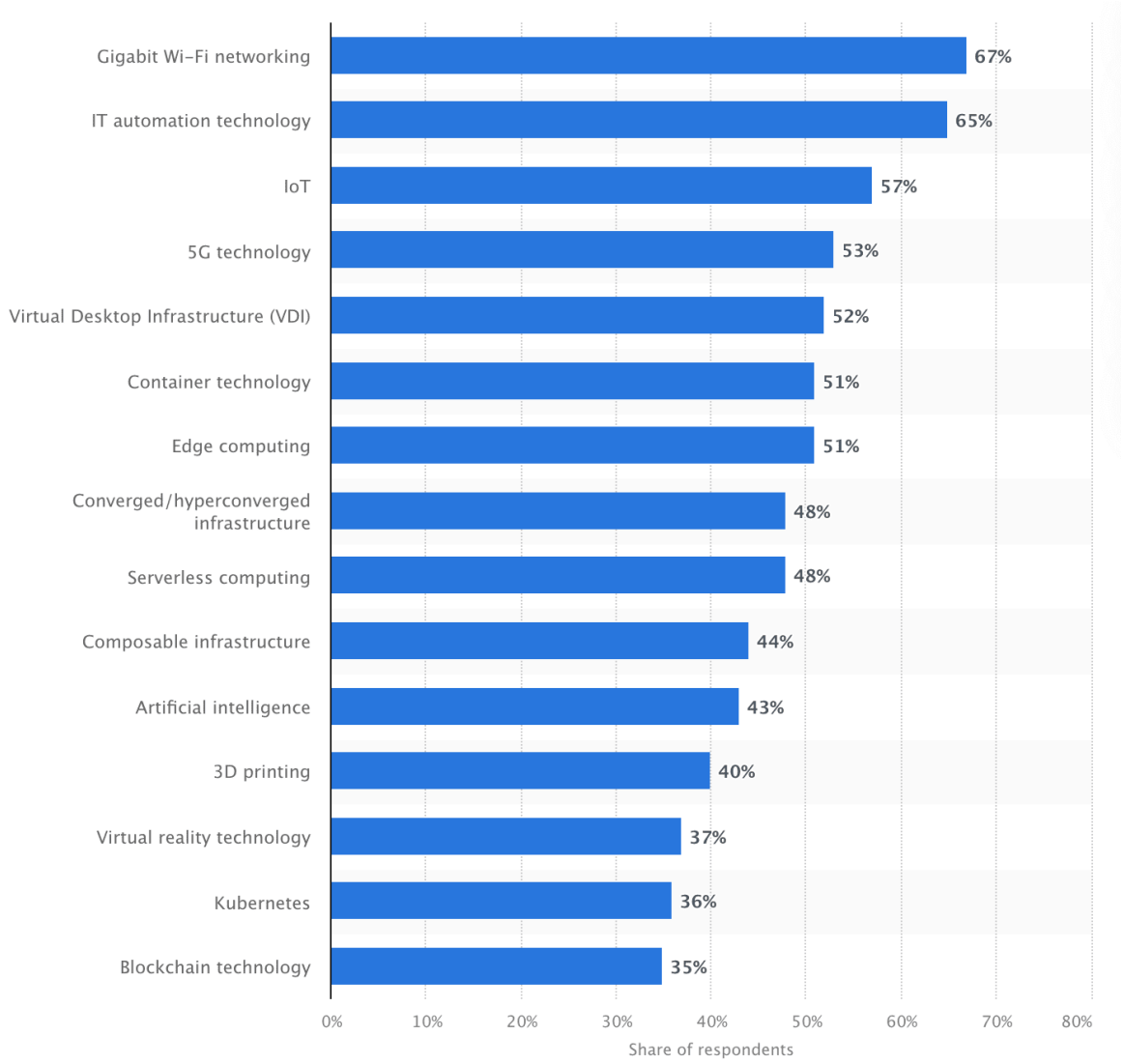


Рис. 1.2 (Статистика впровадження технологій в організаціях)

У 2021 році близько 41,9% американських домогосподарств мали пристрої розумного дому, і, за прогнозами, до 2025 року цей показник зросте до 48,4%.

Зростаючий попит на розумні пристрої в автомобілях збільшує розмір світового ринку автомобільного Інтернету речей. До кінця 2023 року дохід від ринку автомобільного Інтернету речей досягне, за оцінками, $397,2 млрд. До 2028 року - $882млрд — Allied Market Research.

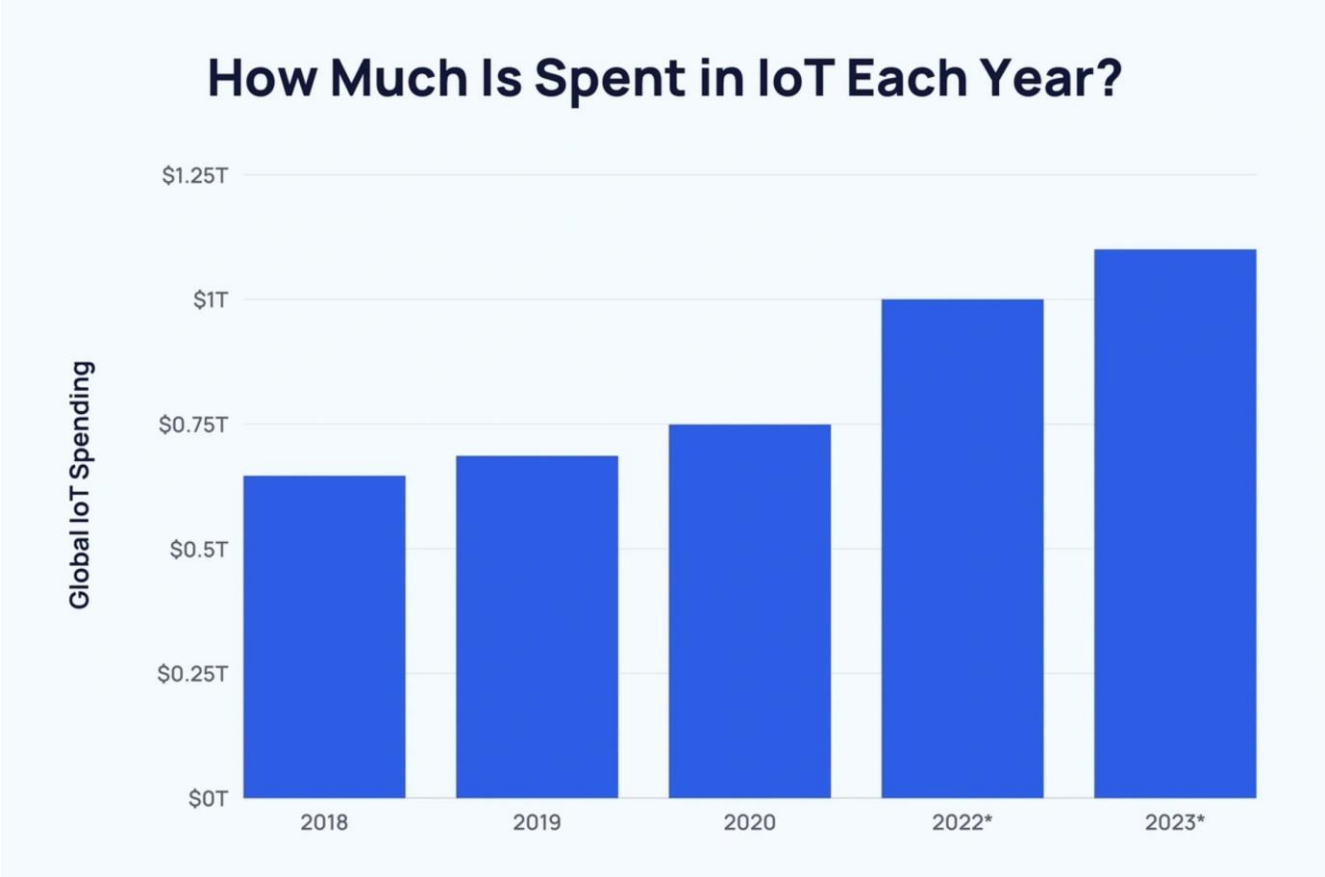


Рис. 1.3 (Річні витрати на IoT у світі)

Розділ 1.2 про зростання зацікавленості у розвитку та використанні Інтернету речей (IoT) розкриває різноманітні аспекти цього явища, яке сьогодні стало важливим стимулом для технологічного та економічного розвитку. Побутові та промислові застосування IoT не лише полегшують наше життя, але й створюють нові можливості для ефективного використання ресурсів, підвищення продуктивності та покращення якості послуг. Однак зростання зацікавленості у використанні IoT також вимагає уваги до кібербезпеки та приватності, оскільки збільшується кількість підключених пристроїв та потенційних кіберзагроз. У цілому, розвиток IoT відкриває широкі перспективи для технологічного прогресу та соціальних змін, і важливо продовжувати вивчати його вплив та реагувати на виникаючі виклики.

1.3 Області застосування IoT та їх потенційні переваги

Інтернет речей (IoT) відкриває широкі можливості застосування у різних сферах життя та бізнесу, що сприяє появі нових технологій та інновацій. У цьому розділі ми розглянемо основні області застосування IoT та їх потенційні переваги.

1.3.1 Смарт-будинок і побутові пристрої

Одними з найпоширеніших застосувань IoT є розумні будинки та побутова техніка. Розумний будинок включає в себе різні пристрої, підключені до Інтернету, які можуть взаємодіяти між собою. Це можуть бути "розумні" пилососи, освітлення, дверні замки, системи безпеки та інші пристрої.

Основні переваги таких систем у зручності та ефективності. Система розумного будинку дозволяє користувачам керувати різними аспектами свого житла з будь-якого місця за допомогою смартфона або голосових команд. Наприклад, вони можуть регулювати температуру в кімнатах, дистанційно керувати освітленням або навіть відкривати і закривати двері, що робить життя комфортнішим і ефективнішим.

1.3.2 Медицина

Дуже важливою областю застосування IoT є сфера медицини. Смарт-медицина використовує різноманітні датчики та пристрої, які можуть відстежувати стан здоров'я людей, передавати дані медичним працівникам та навіть автоматично реагувати на певні ситуації.

Одна з головних переваг полягає в покращенні діагностики та лікування. За допомогою IoT, лікарі можуть отримати доступ до важливих даних про стан здоров'я пацієнтів в реальному часі, що дозволяє їм рано виявляти та ефективно лікувати різноманітні захворювання.

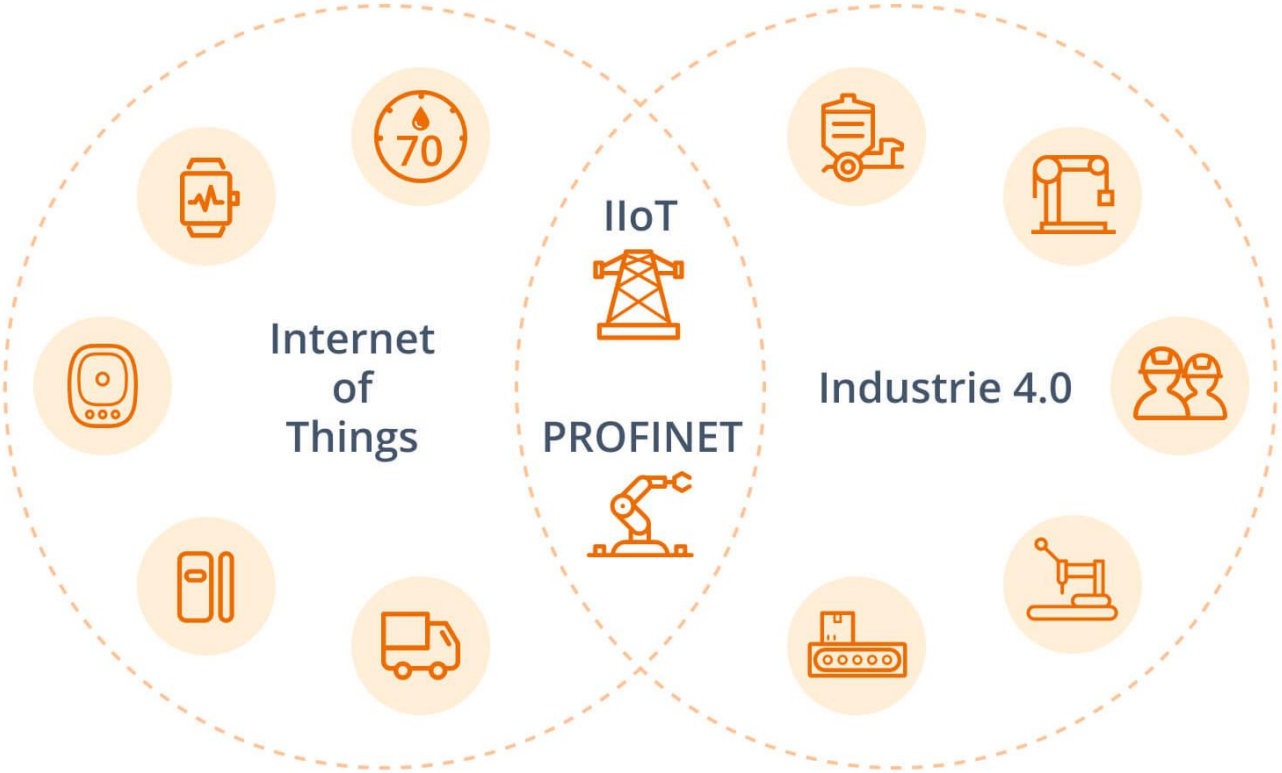


Рис. 1.4 Промислові застосування та "розумні" міста

Зазвичай у промисловому виробнитстві IoT застосовується для контролю та управління процесами, включаючи виробничі лінії, транспортні системи та логістичні операції. Водночас, у "розумних" містах технології IoT використовуються для покращення управління міською інфраструктурою, зменшення заторів на дорогах та підвищення якості життя мешканців.

Вище перечисленні можливості IoT значно впливають як на повсякденне життя, так і на промисловість и виробнитство, проте виникають і інші важливі питання, а саме щодо кібербезпеки, і усіх її аспектів(захист персональних даних та інших важливих факторів які потребують повного аналізу та відповідних дій.

Хотілося б трохи більше акцентувати увагу саме на охороні здоровья та яке місце тут займає IoT.

Отже, які саме потенційні переваги впровадження IoT в охорону здоров’я та як пристрої IoT у сфері охорони здоров’я сприяють розвитку галузі?

Швидка медична допомога: Одна з найбільш очевидних переваг інтернет речей у медицині та охороні здоров'я це можливість дистанційно, за допомогою пристроїв контролювати стан здоров’я своїх пацієнтів, що дозволяє людям звертатися за допомогою в будь-який час і з будь-якого місця. Це не лише покращує зручність та невідкладну допомогу, але й сприяє більшій доступності медичної до помоги.

Профілактика: Профілактика часто є найкращим засобом. Тут рішення для охорони здоров’я IoT пропонують інструменти відстеження та моніторингу, які дають пацієнтам змогу керувати своїм здоров’ям, змінювати звички, покращувати спосіб життя та виявляти ранні ознаки проблем зі здоров’ям.

Зручність та вигода: пристрої Інтернету речей у сфері охорони здоров’я та датчики дають пацієнтам можливість самостійно контролювати стан свого здоров’я, зменшуючи потребу в частих консультаціях. Водночас великі дані, зібрані за допомогою додатків Інтернету речей у сфері охорони здоров’я, роблять ці візити більш вражаючими,оскільки лікарі мають підрукою інформацію.

Медичні дані: До сьогоднішнього часу люди мали відвідувати лабораторії та особисто консультуватися з лікарями або володіти кількома приладами для вимірювання таких показників, як артеріальний тиск, частота серцевих скорочень, рівень глюкози чи кисню в крові. До речі компактні пристрої інтернет речей тепер забезпечують регулярне відстеження та статистику в додатках для здоров’я.

Стан здоров’я та діагностика: за допомогою пристроїв якими ми можемо відстежувати стан нашого здоров'я, ми можемо передбачити певні зміни у нашому організмі та виявити певні симптоми, що дасть швидке розуміння станну нашого здоров'я та пришвидшить процес поставлення точних діагнозів.

Спрощення управління охороною здоров’я: програми інтернет речей в охороні здоров’я перестають бути лише індивідуальними потребами а й включають системне вдосконалення. Певні типи медичного інтернету речей полегшують оцінку ефективності та стану обладнання разом із загальною статистикою захворювань.

Оптимізована медикаментозна терапія: ефективна медикаментозна терапія є ключовою для успіху лікування. Системи моніторингу здоров’я Інтернету речей геніально розроблені, щоб максимізувати ефективність медикаментозного лікування, забезпечуючи оптимальну прихильність пацієнтів і ефективність.

Сприяння дослідженню: IoMT це дійсно цінний інтрумент для досліджень. Це дає змогу вченим приділити більше уваги на сладних завданнях та не аналізувати великий обсяг даних вручну.

Тобто інтернет речей мають неаби який вплив на охорону здоров’я і в цілому на покращення повсякденного життя.

1.4. Ризики та загрози для безпеки IoT

Звичайно Інтернет речей (IoT) це багато можливостей для комфортного та ефективного життя, але він також має вразливу систему, яка може поставити під загрозу як особисту безпеку, так і функціонування системи в цілому. У цьому розділі розглядаються основні ризики та загрози безпеці Інтернету речей

Рис. 1.5 Схема Ризиків та загроз для мереж IoT

1.4.1 Недостатня кібербезпека пристроїв

Більша частина пристроїв IoT успішно вийшли на ринок, включаючи той факи що вони не мають достатньої безпеки та захисту даних.

Через недостатню безпеку та захист виникають різноманітні атаки, різних видів: від зламу паролів до вірусів та іншого шкідливого ПО. Тому варто прибігти до певних дій, адже зловмисники можуть використовувати ці вразливості для отримання персональних даних, також це може призвести до більш маштабних атак.

1.4.2 Невідповідність стандартам та регулятивам

Ще одна досить велика проблема у тому що багато виробників на звертають уваги на стандарти безпеки коли створюють свій товар що може у подальшому створити для вас проблеми такі як втрата даних або відмова у роботі пристрою або цілої системи

Наслідки можуть бути у тому що користувачі стануть більш вразливи до кібератак тому деякі пристрої будуть обмежені у використанні.

1.4.3 Несанкціонований доступ до особистих даних

Однією з невідємних частин у функціонуванні мережі інтернет речей є передача даних, це є у більшості приладів(камери, термостати, інша техніка). Це підвищує ризик того що дані можуть бути перехоплені і використанні проти вас.

Доступ до персональних даних може призвести до порушень приватності користувачів і недовіра до розробника, тим самим створюючи масові фінансові втрати для підприємств.

1.4.4 Недостатня захищеність мережі IoT

Тому мережі доволі вразливі цілі для потенційних кібератак, тим більш у більшості випадків вони не захищенні, Зловмисники можуть безліччю різних способів взламати мережу, викрасти дані або перешкодити її нормальній роботі, також можливе впровадження шкідливого програмного забезпечення, що є навіть більш серйозною проблемою.

Дані загрози вимагають вивчення і повного аналізу, тому у цій кваліфікаційній роботі я детально розглянув багато типів атак та проаналізував їх.

1.5. Мета та обгрунтування дослідження

Основною метою дослідження є:

- Ретельний аналіз потенційних загроз та вразливостей систем IoT.

- Виявлення основних видів кібератак, що спрямовані на пристрої та мережі IoT.

- Розробка ефективних стратегій та методів захисту від кіберзагроз для систем IoT.

- Встановлення рекомендацій для забезпечення безпеки в мережах IoT у майбутньому.

- Актуальність та значущість дослідження полягає у наступних аспектах:

Стрімкий розвиток Інтернету речей: Збільшення кількості пристроїв, підключених до Інтернету, призвело до зростання загроз кібербезпеці. Для забезпечення безпеки цих систем важливо дослідити потенційні загрози та розробити стратегію захисту.

Збільшення кількості кібератак: Кібератаки на системи Інтернету речей, включаючи атаки на промислові системи, медичні прилади та споживчі пристрої, зростають з кожним роком. Розуміння цих загроз і розробка ефективних стратегій захисту є значним викликом.

Можливі наслідки кібератак: Кібератаки на системи Інтернету речей можуть мати серйозні наслідки, включаючи порушення конфіденційності, крадіжку

конфіденційних даних, втрату фінансових активів і навіть загрозу здоров'ю та безпеці людей. Щоб цього не сталося, вкрай важливо мати стратегію безпеки.

Загрози кібербезпеці постійно оновлюються Загрози кібербезпеці постійно змінюються і розвиваються, тому важливо постійно аналізувати і оновлювати стратегії захисту, щоб протистояти новим і вдосконаленим загрозам.

Загалом, дослідження в галузі аналізу та захисту від атак на мережі Інтернету речей мають важливе значення для забезпечення безпеки та стабільності цих систем у сучасному цифровому світі.

Також я визначив що розвиток інтернету речей веде за собою і загрозу та ризики кібератак. Більшість пристроїв не достатньо захищенні щоб протидіяти ним і у подальших розділах я проаналізував конкретні атаки та методи захисту мережі інтернет речей від них.

Однак важливо зазначити, що є як можливості, так і проблеми. Наше дослідження виявило перспективи поліпшення зв'язку, підвищення продуктивності та зручності, а також нових можливостей для розвитку бізнесу з впровадженням Інтернету речей.

В цілому, грунтуючись на цьому аналізі того, що таке Інтернет речей, які загрози він представляє і які у нього очікування, ми зможемо розробити ефективну стратегію захисту і прогнозування майбутнього розвитку цієї важливої технології.

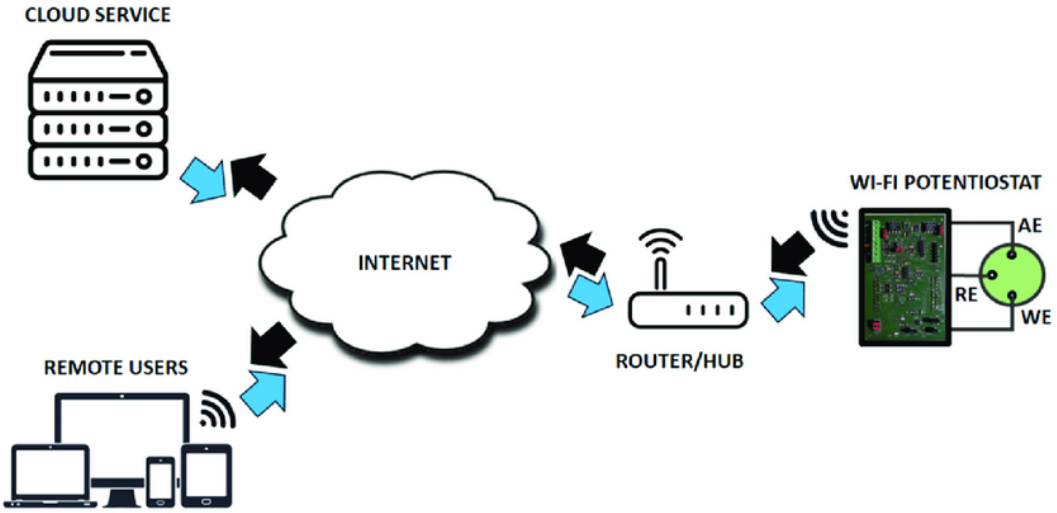


Рис. 1.6 Схема звичайної незахищенної мережі

Технології Інтернету речей відкривають нові можливості для моніторингу та управління навколишнім середовищем. За допомогою датчиків і збирачів даних IoT може відстежувати якість повітря, води, рівень забруднення, температуру та інші параметри навколишнього середовища. Це дозволить більш ефективно контролювати і управляти такими екологічними проблемами, як забруднення, виснаження ресурсів і зміна клімату.

Крім того, IoT може відігравати ключову роль у вирішенні проблем в сфері охорони здоров'я та медицини. Віддалений моніторинг показників здоров'я, автоматичне виявлення та реагування на медичні проблеми, а також покращення систем телемедицини - все це можливо завдяки розвитку IoT.

2. АНАЛІЗ АТАК НА МЕРЕЖІ IOT. ОГЛЯД МОЖЛИВИХ АТАК

2.1 Огляд типових атак на мережі IoT

Мережі Інтернету речей (IoT) стають все більш важливими цілями для кіберзлочинців через їхню поширеність і відносну незахищеність.

2.1.1 Деніал сервісу (DoS) та Розподілений деніал сервісу (DDoS)

Атаки DoS та DDoS є одними з найпоширеніших та досить ефективних способів атаки на мережі IoT. Під час атаки DoS або DDoS, зловмисники намагаються переповнити мережу запитами, призначеними для одного або кількох пристроїв, з метою перевантаження їх ресурсів або знищення їхнього функціонування.

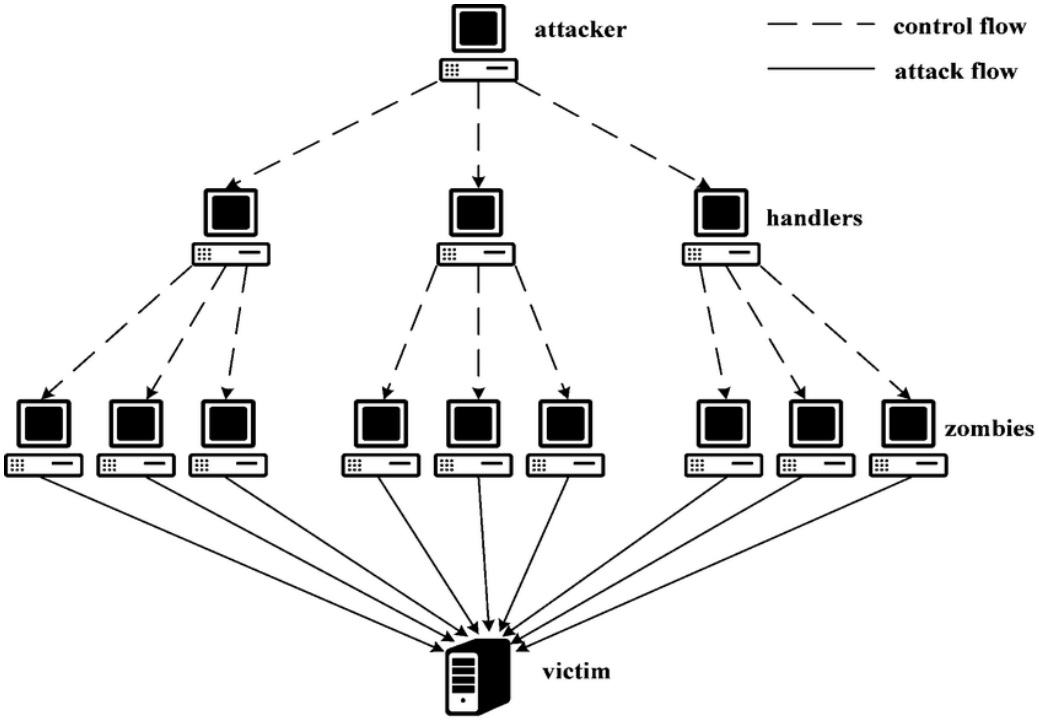


Рис. 2.1 Схема потенційної атаки на мережу(DDoS)

Однією з найбільш поширених є DDoS-атаки. DDoS-атака: трапляється, коли мережа заражених комп'ютерів, ботнет, постійно надсилає кілька запитів до системи. Незвично висока активність може призвести до значних затримок в роботі або відключення системи. Правильно налаштована та налаштована DDoS-атака може призвести до помилок системи компонентів безпеки та приховати фактичні шкідливі дії. Крім того, заражені пристрої Інтернету речей стають частиною

ботнету, допомагаючи зловмисникам проводити ще більш руйнівні атаки в локальних мережах, які часто мають високий ступінь довіри до систем інформаційної безпеки.

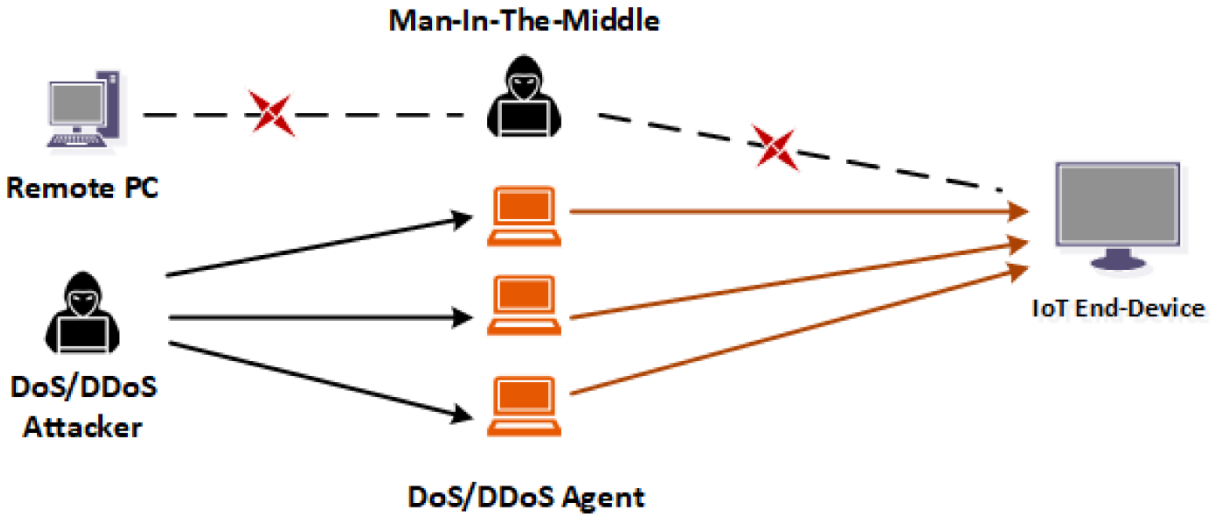


Рис. 2.2 Схема DDoS атаки на мережу

Dos-атаку можна здійснити за допомогою спеціально створеного додатка під назвою "бот", який контролюється зловмисником. Ці програми можуть надсилати велику кількість запитів на цільовий пристрій, що призводить до перевантаження ресурсу та втрати доступності.

У випадку DDoS атаки, зловмисники використовують ботнет - мережу компрометованих пристроїв, щоб спільно надсилати запити до цільового пристрою чи сервісу. Це робить атаку більш складною для виявлення та обмеження, оскільки запити надходять з різних джерел, а не з одного.

2.1.2 Викрадення даних

Ще однією з доволі типових атак на мережі IoT є викрадення даних. Зловмисники можуть використовувати різні методи для отримання доступу до

конфіденційної інформації, що передається через мережу IoT. Наприклад, зловмисники можуть перехоплювати бездротовий трафік між пристроями IoT та інтернетом за допомогою спеціального обладнання, такого як WiFi адаптери. Іншим методом може бути використання різних програмних уразливостей пристроїв або мережевих протоколів для здійснення атаки "людський посередник" або "перехоплення".

Одразу як зловмисники отрмали доступ до даних, вони можуть використати їх проти вас, наприклад для шантажу, крадіжки ідентичності, розповсюдження шкідливого ПО у мережу, забезпечення або просто видалення персональних інформаційних даних.

2.1.3 Відмова в обслуговуванні через вразливості

Ще однією загрозою для мереж IoT є використання вразливостей у програмному забезпеченні чи у апаратній частині пристроїв для здійснення атаки відмови в обслуговуванні (DoS). Зловмисники можуть використовувати різні методи, такі як використання програмних уразливостей, переповнення буфера, або атаки з використанням хитроманіпуляції, щоб заблокувати доступ до пристроїв або мережі.

Відмова в обслуговуванні може бути використана для завдання шкоди інфраструктурі, перешкоджаючи роботі пристроїв або послуг. Наприклад, атака DoS може призвести до тимчасової втрати доступу до системи моніторингу відео або віддаленого керування, що може бути критичним у важливих ситуаціях, таких як безпека будинку або бізнесу.

2.1.4 Використання пристроїв IoT для ботнетів

Зловмисники можуть використовувати мережі інтернет речей для створення ботнетів – це мережі комп'ютерів або пристроїв, які керуються зловмисниками та

використовуються для виконання різних кібератак, включаючи DDoS, розсилання спаму або викрадення даних.

Такі ботнети можуть бути створені шляхом інфікування пристроїв IoT шкідливим програмним забезпеченням або використанням стандартних аутентифікаційних уразливостей. Через велику кількість підключених пристроїв, ботнети IoT можуть стати дуже потужними та складними для виявлення та припинення їхньої діяльності.

Атаки на мережу інтернет речей можуть мати серйозні наслідки як для особистих даних користувачів так і доя бізнесу та фінансів в цілому. Тому важливо важливо вжити певних засобів захисту. Що зможе перешкодити атакам або мати можливість їх швидко ідентифікувати. Навчання користувачів є не меншш важливим кроком для захисту. Тому варто підійти до цього питання серйозно і врахувати усі аспекти які можуть вплинути на неправильне функціонування вашої мережі.

2.2 Огляд типових атак на мережі IoT

Звичайно самі по собі пристрої інтернет речей мають доволі великий потенціал для нашого розвитку та полегшення життя, проте вони є загрозою для усієї мережі. Один лише прилад може стати дверями до зламу усієї мережі У цьому підрозділі я проаналізував вплив вразливостей на мережу IoT, іхні наслідки та методи безпеки.

2.2.1 Відомі вразливості та їх потенційні наслідки

Важливо зрозуміти які є вразливості та їх можливі наслідки перед тим як перед тим як досліджувати методи захисту. До основних вразливостей входять незашифроване з'єднання, погана аутентифікація, використання застарілих або

небезпечних протоколів. Також мають місце недоліки у апаратних та програмних компонентах дека. Ди них відносяться недоліки в управлінні життєвим циклом пристрою

Важливо зрозуміти які є вразливості та їх можливі наслідки перед тим як перед тим як досліджувати методи захисту. До основних вразливостей входять незашифроване з'єднання, погана аутентифікація, використання застарілих або небезпечних протоколів. Також мають місце недоліки у апаратних та програмних компонентах дека. Ди них відносяться недоліки в управлінні життєвим циклом пристрою.

Рис. 2.3 Схема кібератаки

Атаки призводять до неприємних наслідків які є досить серйозними та руйнівними. Наприклад зловмисники можуть скомпрометувати безпеку мережі шляхом перехоплення конфіденційних даних, таких як паролі або особиста інформація користувачів, заблокування доступу до пристроїв або послуг, або навіть використання пристроїв для створення ботнетів для масштабних кібератак.

2.2.2 Розповсюдженість вразливостей у пристроях IoT

Вразливість, яка поширюється в пристроях Інтернету речей, є значною проблемою для мережевої безпеки. Багато виробників не приділяють достатньої уваги безпеці пристроїв Інтернету речей, коли вони розробляють і виробляють їх. Це призвлдить до того що є багато пристроїв вже з відомими проблемними місцями

Ще одна важлива проблема полягає в тому, що багато пристроїв IoT мають тривалий термін служби і рідко отримують оновлення програмного забезпечення. Це означає, що вразливості, виявлені в пристроях, можуть залишатися незахищеними протягом тривалого часу, збільшуючи ризик злочинного використання.

2.2.2 Потенційні наслідки для безпеки мережі

Вразливі пристрої у мережі можуть поставити під загрозу усю мережу. Наприклад, одне враження від пристрою може дозволити зловмисникам проникнути в мережу та отримати доступ до інших систем і пристроїв.Крім того, велика кількість пошкоджених пристроїв може бути використана для створення великих кібератак, таких як DDoS, які можуть призвести до відмови в обслуговуванні людини. велика кількість клієнтів. Це чудова ідея.

2.2.3 Стратегії захисту від вразливостей пристроїв IoT

Для того, щоб захистити пристрої IoT від вразливостей, важливо вжити ефективних стратегій безпеки:

- Основними заходами є оновлення програмного забезпечення.
- Виробники повинні регулярно випускати оновлення програмного забезпечення, щоб виправити вразливості, які були виявлені.

- Захист мережі від несанкціонованого доступу, важливо використовувати захищені паролі та шифрування.
- Постійний моніторинг мережі може допомогти виявити аномальну активність і реагувати на потенційні загрози.
- Використання безпечних мережевих протоколів і стандартів допоможе запобігти багатьом типам атак.

Вразливості в пристроях Інтернету речей можуть мати серйозний вплив на мережеву безпеку, включаючи ряд можливих наслідків, таких як кібератаки, втрата конфіденційності даних і відмова в обслуговуванні. Для захисту від цих загроз важливо приділяти достатньо уваги заходам безпеки, включаючи оновлення програмного забезпечення, мережеву безпеку і використання захищених протоколів.

2.3 Перспективні методи атак на системи IoT

Мережі Інтернету речей (IoT) надають безліч можливостей для підключення та автоматизації різних пристроїв, але разом з цими перевагами вони також стають об'єктом для нових та еволюціонних методів кібератак. У цьому розділі ми розглянемо деякі перспективні методи атак на системи IoT, їхні принципи роботи та потенційні наслідки для безпеки мереж.

2.3.1 Атаки на апаратний рівень

Одна з найбільш популярних способів атаки на системи Інтернету речей є атака на апаратному рівні. Зловмисник може спробувати скомпрометувати пристрій, використовуючи різні методи, такі як фізичний доступ до пристрою, модифікація або підробка пристрою, або представляючи хакерський пристрій або "троянського коня".

Атаки на апаратному рівні особливо небезпечні, оскільки їх важко виявити та усунути. Це також може призвести до серйозних проблем безпеки мережі, таких як крадіжка конфіденційних даних, перехоплення повідомлень та віддалене управління пристроями.

2.3.2 Атаки на основі штучного інтелекту і машинного навчання

Ще однією перспективною сферою атак на системи Інтернету речей є використання штучного інтелекту (ШІ) та машинного навчання (MN). Зловмисники можуть навчати алгоритми вводу-виводу та ML виявляти та використовувати вразливості в мережах IOT, а також виконувати різні атаки.

Наприклад, алгоритм ML можна навчити розпізнавати моделі поведінки користувачів і пристроїв і виявляти ненормальні або підозрілі дії. Зловмисник може використовувати цю інформацію для здійснення цільових атак, таких як фішинг або віруси.

2.3.3 Атаки з використанням розподілених технологій

Варто також відзначити, що зростає інтерес до атак на системи IoT з використанням децентралізованих технологій, таких як блокчейн і розподілені обчислення. Зловмисники можуть використовувати ці технології для побудови децентралізованих мереж, що ускладнює виявлення та запобігання їхньої діяльності.

Наприклад, блокчейн можна використовувати для забезпечення безпеки та конфіденційності даних, що передаються через мережі IoT. Однак зловмисники можуть спробувати використати блокчейн для створення анонімних або

невідстежуваних транзакцій і використовувати його для фінансових махінацій або інших видів шахрайства.

2.3.4 Атаки на додатки та сервіси хмарних платформ

Зростаюче використання хмарних платформ для зберігання та обробки даних створює нові можливості для атак на системи IoT. Атаки на додатки і сервіси хмарних платформ можуть мати серйозні наслідки для мережевої безпеки, такі як втрата конфіденційності даних, відмова в обслуговуванні або крадіжка інтелектуальної власності.

На малюнку зображено аналіз потенційної атаки на мережу IoT.

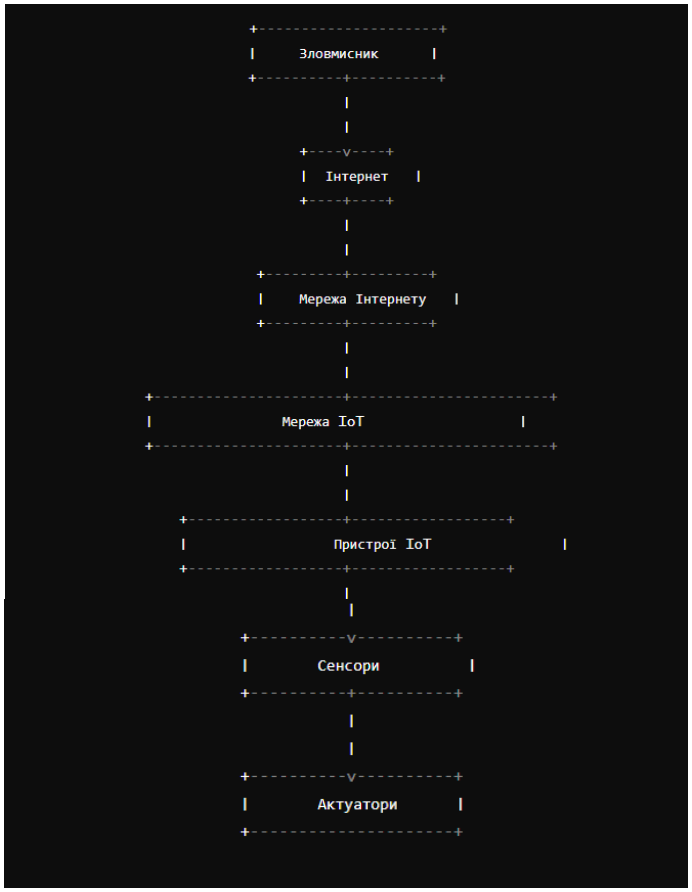


Рис. 2.4 Аналіз потенційної атаки на мережу IoT

Сучасні методи атак на системи Інтернету речей створюють нові виклики для безпеки мереж і пристроїв. Для захисту від цих загроз важливо завжди бути в курсі і вживати ефективних заходів безпеки, таких як оновлення програмного забезпечення, моніторинг мережі і використання безпечних протоколів. Також важливо вдосконалити способи виявлення потенційних загроз і реагування на них, щоб запобігти серйозному впливу на безпеку мережі.

2.4 Інструменти та техніки, використовувані зловмисниками для атак на мережі IoT

Рис. 2.5 Класифікація атак на мережу IoT

У цьому розділі ми розглянемо різноманітні інструменти та техніки, які злов мисники використовують для здійснення атак на мережі IoT, їхні принципи роботи та наслідки для безпеки систем.

2.4.1 Сканування мережі та виявлення пристроїв

Одним з перших кроків, які зловмисник робить перед атакою на мережу IOT, є ідентифікація підключених пристроїв та виявлення їх функцій та вразливостей за допомогою різних інструментів, включаючи Nmap, Shodan та Masscan.

Ці інструменти дозволяють зловмиснику виявляти пристрої IoT, що працюють у мережі, та налаштовувати такі властивості, як IP-адреса, порт, використовуваний протокол та Версія програмного забезпечення. Ця інформація є основою для подальших атак та зловживань.

2.4.2 Використання збройкітів

Виявивши пристрій та його вразливості, зловмисник використовує коваля, щоб скористатися цими вразливими місцями та здійснити атаку. Gunsmith може використовувати програмні або апаратні вразливості для отримання несанкціонованого доступу до систем або пристроїв, що використовують програмне забезпечення або програмний код.

Зловмисники можуть використовувати відому зброю або розробляти власну зброю, щоб використовувати унікальні вразливості, які виробники пристроїв ще не виявили та не виправили.Ці атаки можуть призвести до крадіжки даних, віддаленого управління пристроями або їх знищення.

2.4.3 Використання ботнетів

Ботнет- це комп'ютер або пристрій, який контролюється зловмисником і використовується для виконання різних кібератак, включаючи атаки Інтернету речей networks.An зловмисник може використовувати ботнет для проведення великомасштабних кібератак, таких як DDoS, спам і майнінг криптовалют.

Зловмисники створюють ботнети різними способами, включаючи використання вразливостей в пристроях Інтернету речей і зараження пристроїв за допомогою шкідливих програм і атак соціальної інженерії. Як тільки пристрій стає частиною ботнету, зловмисник може використовувати його для виконання різних типів атак у мережі.

2.4.4 Фішинг та соціальні інженерні атаки

Фішингові атаки та атаки соціальної інженерії також є поширеними способами нападу на мережі Інтернету речей. Зловмисники використовують ці методи для маніпулювання користувачами та адміністраторами з метою отримання несанкціонованого доступу до конфіденційної інформації та пристроїв.

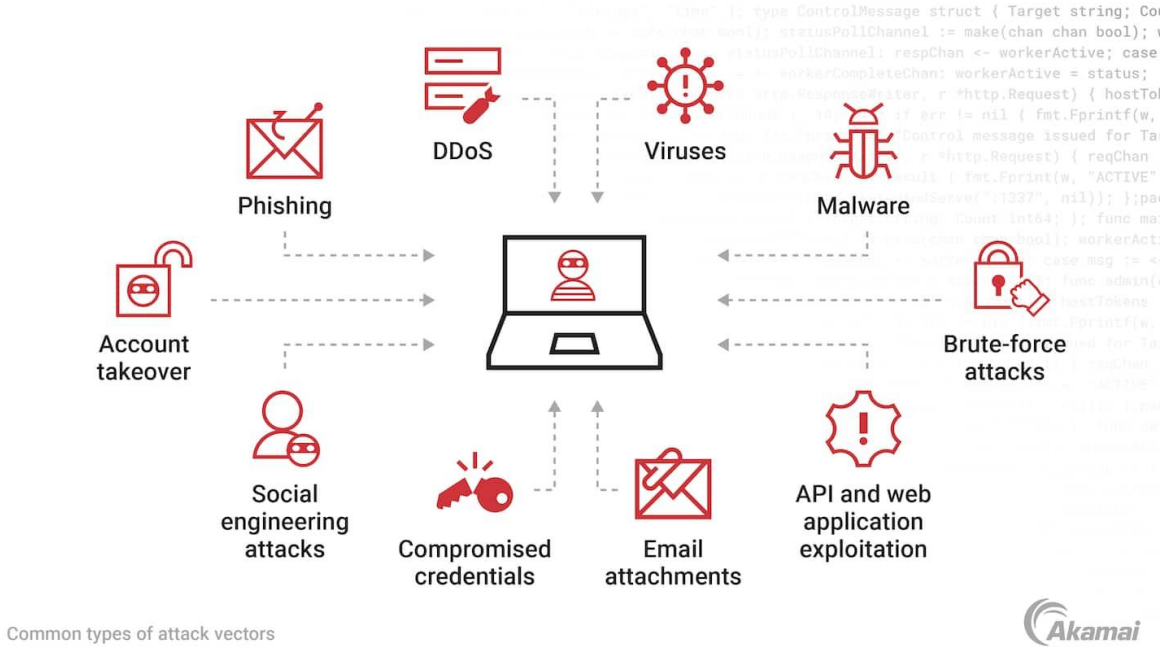


Рис. 2.6 Види кібератак

Розглянемо ситуацію: зловмисник надіслав фішинговий електронний лист або повідомлення із посиланням на шкідливий сайт який одразу заражає ПК. Досить полулярною атакою є так звана соціальна інженерія за допомогою цієї атаки він може відвернути користувачів від своїх притроїв та отримати доступ до облікових даних та особистої інформації.

Звичайно з розвитком інтернет речей розвиваються і інструменти які зловмисники використовують. Тому важливо вжити ефективних заходів безпеки моніторинг мережі та інформування користувачів може бути початковим рівнем захисту.

2.5 Аналіз відомих випадків успішних атак на системи IoT

Одні з найвідоміших кібератак відображають низку проблем взагалом у кібербезпеці, що становить велику загрозу для безпеки користувачів та інфраструктури у цілому. Тому у цьому підрозділі я розглянув декілька типових атак на мережу.

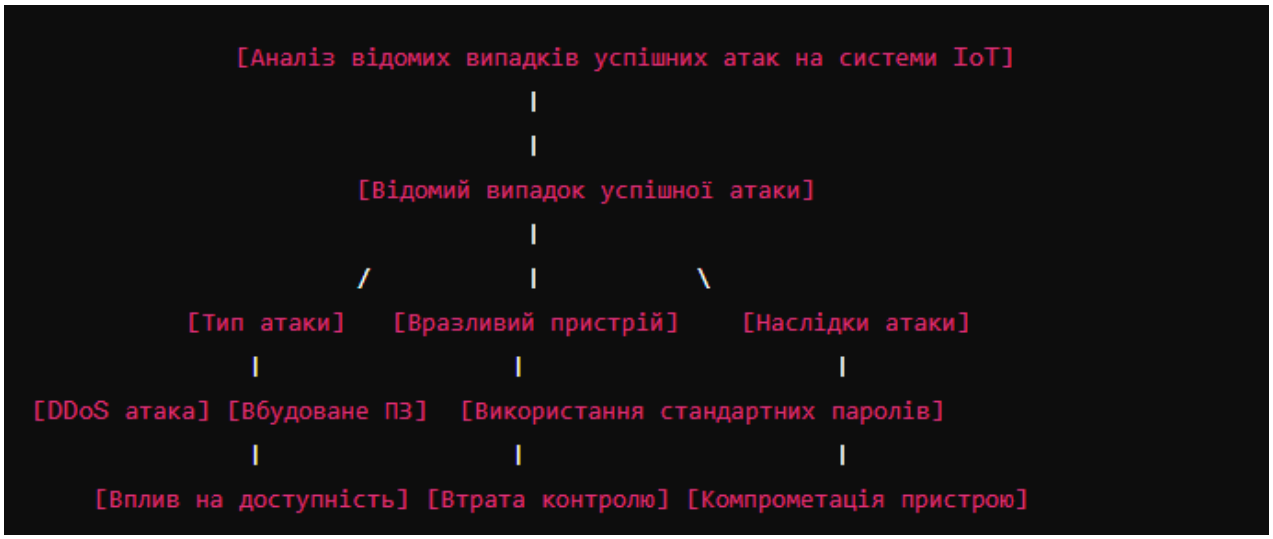


Рис. 2.7 Аналіз успішної кібератаки

2.5.1 Випадок: Mirai Botnet

Метод: Mirai Botnet використовував вразливості в безпеці багатьох пристроїв IoT, таких як маршрутизатори, веб-камери та підключені термостати, для створення великої мережі зброї, яка використовувалася для відправлення великих обсягів трафіку на цільові сервери.

Наслідки: Кібератака залишила тисячі користувачів без доступу до популярних веб-сайтів та послуг протягом кількох годин. Вона також привернула увагу до проблем безпеки систем IoT та підкреслила необхідність покращення захисту цих пристроїв.

Вивчені уроки: Важливо виявити та виправити вразливості в пристроях IoT, а також вжити заходів для запобігання їх використанню для створення ботнетів. Крім того, провідні постачальники послуг Інтернету повинні бути готові до великих кібератак та мати відповідні заходи для зменшення їх впливу.

2.5.2 Випадок: Stuxnet

Інший відомий випадок успішної атаки на систему IoT - це Stuxnet, вірус, який вплинув на ядерну програму Ірану. Stuxnet був розроблений для використання в індустріальних системах контролю, таких як програмовані контролери логіки (PLC), і вперше був виявлений у 2010 році.

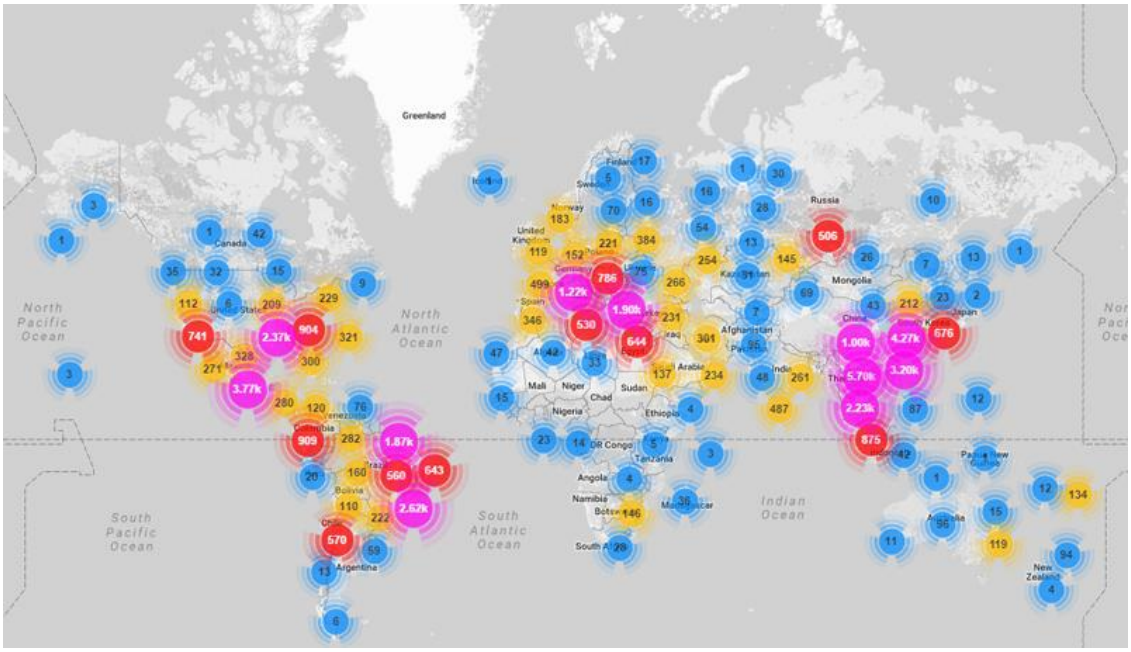


Рис. 2.8 Відомий випадок кібератаки

Метод: Stuxnet використовував ряд вразливостей у програмних продуктах Microsoft Windows та Siemens Step7, що використовувалися в іранській ядерній

програмі, для інфікування PLC, використовуваних для керування центрифугами з обогащенням урану

Наслідки: Вірус призвів до руйнування багатьох центрифуг та значною затримкою в ядерній програмі Ірану. Крім того, він підняв питання про безпеку промислових систем та підкреслив необхідність захисту критичних інфраструктур від кібератак.

Вивчені уроки: Stuxnet підкреслив важливість захисту критичних інфраструктур від кібератак та наголосив на потребі підвищення свідомості про цю проблему серед різних секторів промисловості.

2.5.3 Випадок: IoT мініатюрні атаки

Останнім часом стали популярні атаки, спрямовані на мініатюрні пристрої IoT, такі як підключені датчики, реле або мікроконтролери. Ці пристрої, як правило, мають обмежені ресурси та властивості безпеки, що робить їх вразливими до атак.

Метод: Зловмисники використовують різноманітні методи для атаки на мініатюрні пристрої IoT, такі як перехоплення комунікацій, використання вразливостей безпеки або впровадження шкідливого програмного забезпечення через віддалений доступ.

Наслідки: Атаки на мініатюрні пристрої IoT можуть призвести до втрати конфіденційності даних, віддаленого керування пристроями або навіть їхнього знищення. Крім того, вони можуть бути використані для створення ботнетів або для здійснення інших видів кібератак.

Розглягнуті кібератаки та проблеми безпеки у мережі, дають зрозуміти серйозність загрози, які вони становлять для безпека мереж та пристроїв. Для захисту від таких атак важливо розуміти їх структуру, методи та наслідки, щоб розробити систему захисту. Тому варто навчитися та зрозуміти як проводяться успішні кібератаки щоб уникнути їх у майбутньому.

Включаючи різні типи атак, вразливості в пристроях Інтернету речей, необхідність усунення слабких місць і необхідність постійного моніторингу та оновлення заходів захисту, які важливі для розуміння загроз і загроз. уразливості цих мереж. Ці результати відображають складність та серйозність проблем мережевої безпеки IOT та підкреслюють важливість розробки ефективних стратегій захисту для запобігання подібним атакам у майбутньому.

3. Захист від атак на мережі IoT

3.1 Як захистити мережі IoT на рівні пристроїв

В першу чергу варто звернути увагу на захист мережі інтернет речей на рівні пристрою, адже пристрої це приймають на себе перший удар, саме вони стають мішенню для кіберзлочинців. У третьому розділі кваліфікаційної роботи я описав різні методи та стратегії захисту які допоможуть захистити як окремі пристрої так і усю мережу.

3.1.1 використання захищених з'єднань і шифрування даних

Одним з найважливіших аспектів безпеки пристроїв IoT є використання захищених з'єднань та шифрування даних для забезпечення конфіденційності та цілісності інформації, що передається через мережу. Протоколи шифрування, такі як SSL / TLS, можуть використовуватися для захисту зв'язку між пристроями і серверами, а також для запобігання перехоплення і підробки даних. Шифрування

може використовуватися для захисту зв'язку між пристроями і серверами, а також для запобігання перехоплення і підробки даних. Шифрування також можна використовувати для захисту локальних даних на пристроях IOT та забезпечення безпеки у разі втрати або крадіжки пристрою.

3.1.2 Використання автентифікації та авторизації

Двофакторна автентифікація або складні паролі можуть дозволити лише довіреним користувачам отримати доступ до пристрою та його функцій, що дуже важливо для захисту пристроїв.

Впровадження механізмів автентифікації також має вирішальне значення, оскільки вони обмежують доступ до різних функцій і ресурсів пристрою на основі ступеня автентифікації користувача. Це може допомогти пристрою не використовуватися для несанкціонованих дій.

3.1.3 Оновлення програмного забезпечення та усунення вразливостей безпеки.

Для стратегії безпеки оновлення прошивки IoT є важливим компонентом. Постачальники постійно знаходять нові вразливості та розробляють патчі для захисту пристроїв від атак.

Доволі важливим є використання механізмів зменшення вразливостей, такі як блокування з'єднань, фільтрація вхідних даних та обмеження доступу до системних ресурсів, ви будете впевнені шо вразливості не будуть використанні після їх виявлення

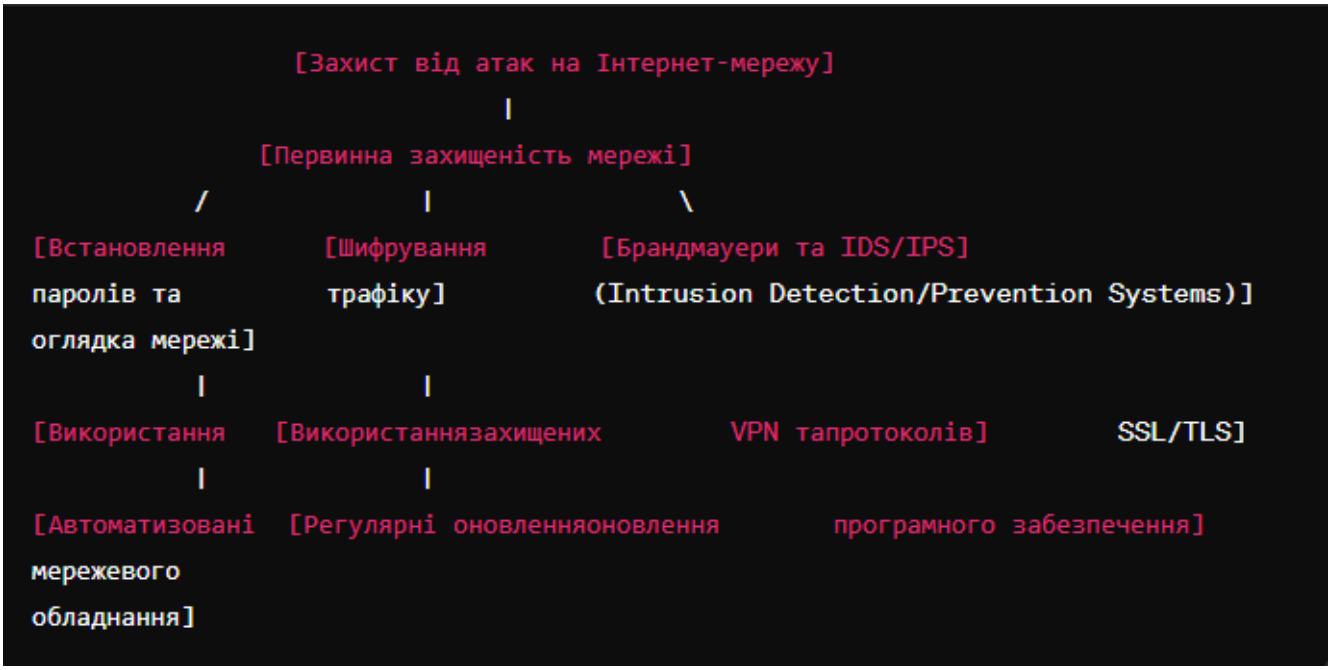


Рис. 3.1 Приклад схеми захисту від атак на IoT.

У цій схемі показано основні кроки захисту від атак на Інтернет-мережу. Вони включають встановлення захищених паролів і оглядку мережі, шифрування трафіку, використання брандмауерів і систем виявлення/попередження вторгнень, використання VPN та SSL/TLS, а також регулярне оновлення програмного забезпечення.

3.1.4 Фізична безпека та захист від фізичного доступу

Фізична безпека Інтернету речей також є важливою частиною загальної стратегії безпеки. Пристрої повинні бути розташовані в безпечних місцях і захищені від несанкціонованого доступу.

Захисні чохли, замки та інші фізичні засоби можуть бути використані для запобігання крадіжкам або фізичним втручанням, які можуть поставити під загрозу безпеку пристрою

3.1.5 Використання безпечних протоколів і стандартів

Застосування протоколів шифрування, таких як HTTPS, MQTT з TLS і CoAP з DTLS, може захистити зв’язок між пристроями та серверами від підслуховування та перехоплення.

Крім того, стандарти безпеки, такі як FIPS, ISO/IEC 27001 і NIST SP 800-63, дають основу для впровадження ефективних стратегій безпеки для пристроїв IoT.

На малюнку 10 зображена схема захищеної мережі. У цій схемі:

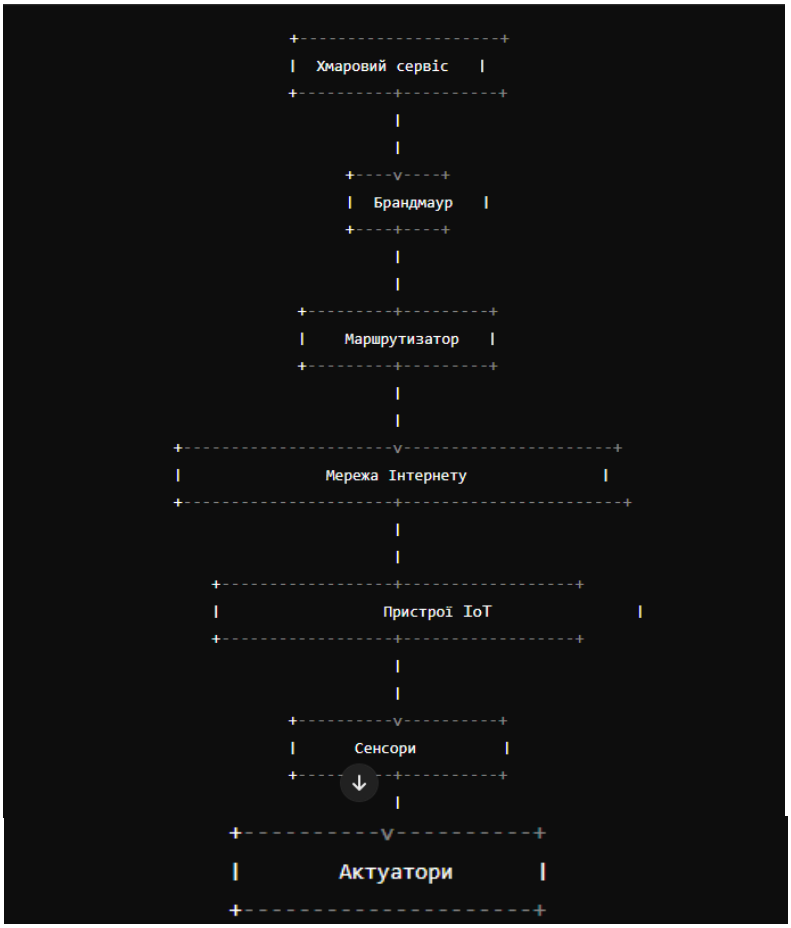


Рис. 3.2 Схема захищеної мережі IoT

Хмаровий сервіс забезпечує централізоване управління та зберігання даних, а також надає доступ до мережі IoT через Інтернет:

- Брандмаур служить першим рівнем захисту, що фільтрує та контролює трафік, що входить та виходить з мережі IoT.
- Маршрутизатор використовується для передачі даних між мережею IoT та мережею Інтернет.
- Пристрої IoT, такі як сенсори та актуатори, з'єднуються з мережею через маршрутизатор.
- Сенсори вимірюють дані та передають їх до хмарового сервісу або інших пристроїв IoT.
- Актуатори отримують команди з хмарового сервісу або інших пристроїв IoT та виконують відповідні дії.

Для захисту мережі Інтернету речей необхідні кілька підходів і методів безпеки. Безпечне з’єднання, аутентифікація, оновлення програмного забезпечення, фізична безпека та використання захищених протоколів можуть допомогти захистити мережі Інтернету речей від різних типів атак і небезпек.

3.2 Захист мережевого з'єднання для забезпечення безпеки IoT

Безпека мережевого підключення є важливим компонентом інфраструктури Інтернету речей (IoT), щоб захистити дані від кіберзагроз і зберегти конфіденційність, цілісність і доступність. У цьому розділі розглядаються різні підходи до захисту мережевих з’єднань для забезпечення безпеки систем Інтернету речей.

3.2.1 Використання безпечних протоколів зв'язку

Протоколи безпеки Secure Sockets Layer/Transport Layer (SSL/TLS), безпеки Internet Protocol (IPS декомунізація) і віртуальної приватної мережі (VPN) шифрують і аутентифицирують дані між пристроями та іншими вузлами мережі.

Шифровка даних зберігає конфіденційність і цілісність даних, запобігаючи перехопленню або підробці даних під час передачі. Аутентифікація обмежує доступ до мережі до авторизованих пристроїв.

3.2.2 Використання мережевих зон і віртуальних локальних мереж

Можна розділити мережу на окремі мережеві зони або віртуальні локальні мережі (VLAN), щоб підвищити безпеку мережевих з'єднань Інтернету речей. Це дозволяє розділити пристрої на різні групи та обмежити зв'язок між ними. Наприклад, пристрої, які обробляють конфіденційні дані або пристрої, які контролюють важливі системи, можуть бути розміщені в окремій зоні мережі з обмеженим доступом, що зменшує ймовірність компрометації.

3.2.3 Використання брандмауерів та інших заходів фільтрації трафіку

Одним із найкращих способів контролю трафіку в мережах Інтернету речей є брандмауери. Брандмауери застосовують правила доступу для контролю зв'язку між пристроями, фільтрують вхідний і вихідний трафік і блокують небажані з'єднання. Крім того, небажані атаки та несанкціонований доступ до мережі можуть бути виявлені за допомогою інструментів фільтрації трафіку, таких як системи виявлення вторгнень і системи запобігання вторгненню.

3.2.4 Моніторинг та аналіз трафіку

Моніторинг і аналіз трафіку є доволі важливими аспектами захисту мереж інтернет речей. Це дозволяє виявити аномальні або підозрілі дії в мережі, такі як несподівані підключення до пристроїв, надмірне використання ресурсів або спроби несанкціонованого доступу. Можливі загрози для мережевої безпеки можна виявити за допомогою моніторингу та аналізу трафіку, щоб запобігти їх поширенню та мінімізувати ризики.

3.2.5 Захист від DDoS-атак

DDoS-атаки є серйозною загрозою для мереж IoT, оскільки вони призводять до перевантаження мережевих ресурсів і недоступності пристроїв. Для захисту від DDoS-атак можна використовувати спеціалізовані рішення, такі як хмарні сервіси захисту від DDoS, які фільтрують трафік до того, як він досягне цільового пристрою.

Ця схема показує основні кроки захисту від DDoS-атак:

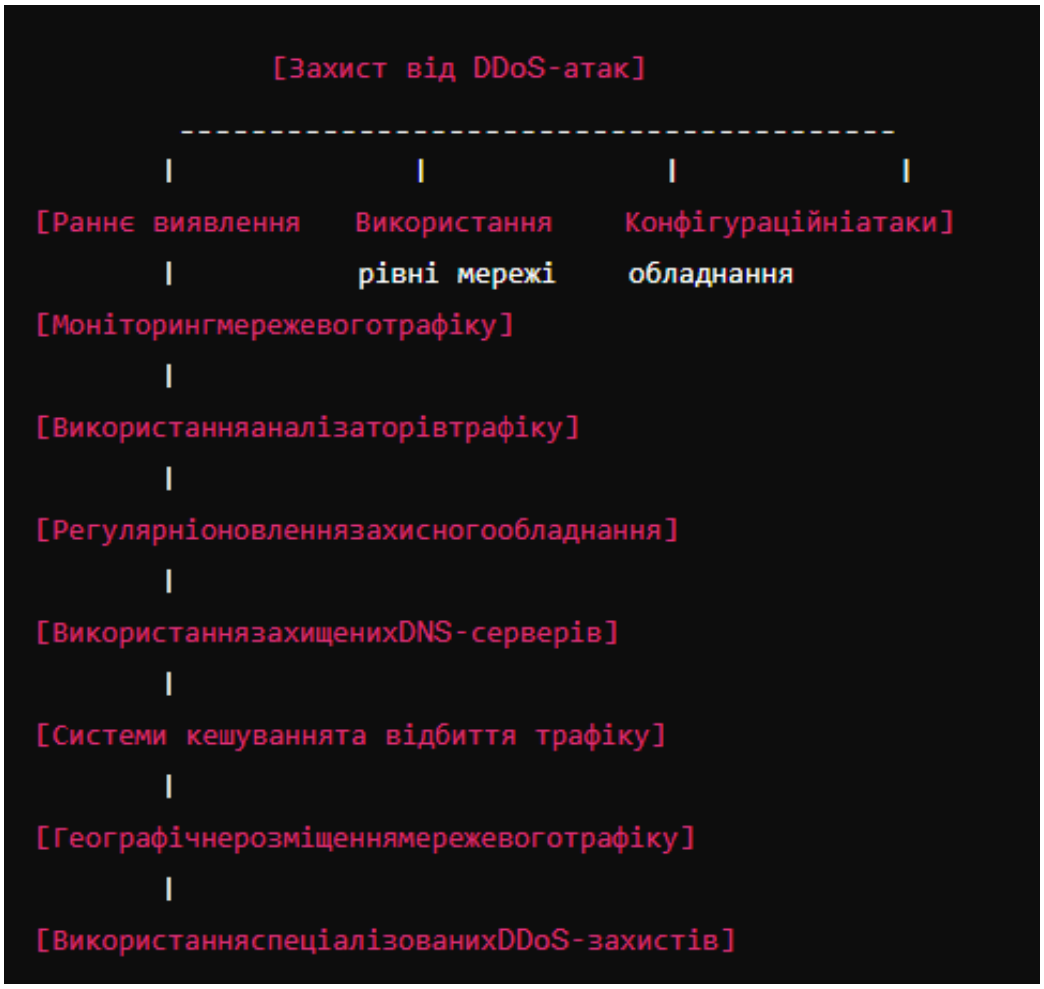


Рис. 3.3 Схема захитсту від DDoS-атак

- Раннє виявлення атаки: Моніторинг мережевого трафіку для раннього виявлення DDoS-атаки.
- Налаштування захисту на рівні мережевого обладнання для блокування атак.
- Налаштування мережевого обладнання для оптимального захисту від DDoS-атак.
- Використання аналізаторів трафіку: Використання спеціалізованих аналізаторів трафіку для виявлення та аналізу DDoS-атак.
- Регулярні оновлення захисного обладнання: Регулярне оновлення програмного та апаратного забезпечення для забезпечення ефективного захисту.
- Використання захищених DNS-серверів: Використання DNS-серверів, які мають захист від DDoS-атак.
- Системи кешування та відбиття трафіку: Використання систем кешування та відбиття трафіку для розподілення навантаження та зменшення впливу атак.
- Географічне розміщення мережевого трафіку: Розміщення мережевого трафіку у різних географічних регіонах для зменшення впливу DDoS-атак.
- Використання спеціалізованих DDoS-захистів: Використання спеціалізованих рішень для захисту від DDoS-атак.

Захист мережевих з'єднань в Інтернеті речей вимагає комплексного підходу і використання різних методів і стратегій. Використання безпечних протоколів зв'язку, мережевих зон, брандмауерів, моніторингу трафіку і захисту від DDoS може допомогти убезпечити мережі IoT і захистити їх від широкого спектру кіберзагроз.

3.3 Використання шифрування та аутентифікації для захисту даних у мережах IoT

Забезпечення безпеки даних у мережах Інтернету речей (IoT) вимагає ефективного застосування шифрування та механізмів аутентифікації. У цьому

розділі ми розглянемо різні методи та стратегії використання шифрування та аутентифікації для захисту даних у мережах IoT.

3.3.1 Використання шифрування даних у мережах IoT

Шифрування даних є ключовим елементом в захисті конфіденційності та цілісності інформації, що передається у мережах IoT. Використання захищених протоколів шифрування, таких як SSL/TLS, AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), дозволяє забезпечити безпеку комунікації між пристроями та іншими вузлами мережі.

Застосування шифрування даних у мережах IoT між пристроями, мережевими вузлами та хмарними сервісами забезпечує захист від перехоплення та модифікації даних, що передаються через мережу.

3.3.2 Використання аутентифікації пристроїв у мережах IoT

Аутентифікація пристроїв є важливим аспектом в захисті мереж IoT від несанкціонованого доступу. Вимога до складних паролів, використання механізмів двофакторної аутентифікації та використання цифрових сертифікатів можуть забезпечити, що лише довірені пристрої матимуть доступ до мережі.

Застосування аутентифікації пристроїв дозволяє ідентифікувати та автентифікувати пристрої перед тим, як вони отримають доступ до мережі, тим самим запобігаючи несанкціонованому доступу та використанню мережевих ресурсів.

3.3.3 Використання електронного підпису для підтвердження автентичності даних

Використання електронного підпису є ще одним способом забезпечення цілісності та автентичності даних у мережах IoT. Електронний підпис дозволяє підтверджувати, що дані були створені або змінені вповноваженим пристроєм та не були піддані модифікації під час передачі.

Застосування електронного підпису дозволяє забезпечити, що дані, які передаються між пристроями у мережі IoT, залишаються цілими та недоступними для модифікації або підробки третіми сторонами.

3.3.4 Реалізація механізмів керування ключами

Механізми керування ключами є важливими для ефективного використання шифрування та аутентифікації у мережах IoT. Вони дозволяють генерувати, зберігати, обмінюватися та керувати ключами шифрування та аутентифікації між пристроями та іншими вузлами мережі.

Ефективне керування ключами забезпечує безпеку даних у мережах IoT, дозволяючи вчасно оновлювати, відкликати та реагувати на будь-які випадки компрометації ключів.

3.3.5 Застосування блокчейн-технологій для забезпечення безпеки даних

Застосування блокчейн-технологій може стати ефективним рішенням для забезпечення безпеки даних у мережах IoT. Блокчейн дозволяє створювати розподілену, недоступну для зміни базу даних, яка забезпечує неперевершену цілісність та автентичність даних.

Застосування блокчейн-технологій може забезпечити безпеку та конфіденційність даних у мережах IoT, зменшуючи ризик компрометації та підробки даних.

Багато великих компаній застосовують блокчейни для аналізу та захисту від небезпек які можуть виникнути з їх мережами.

Рис. 3.4 Схема надійної та захищеної мережі від кібератак.

На малюнку 18 зображено схему надійної та захищеної мережі від кібератак з використанням брендмауера та шифрування даних. Шифрування даних є одним з основних методів захисту інформації в мережі Інтернету речей (IoT). Воно дозволяє захищати дані від несанкціонованого доступу, перехоплення та читання зловмисниками.

Використання шифрування та аутентифікації є важливими стратегіями для захисту даних у мережах IoT. Застосування цих методів дозволяє забезпечити конфіденційність, цілісність та доступність даних, зменшуючи ризик несанкціонованого доступу та компрометації даних у мережах IoT.

3.4 Розвиток технологій виявлення та відновлення після атак для систем IoT

Захист мереж Інтернету речей (IoT) від кібератак вимагає не лише передбачення можливих загроз та захисту від них, але й швидке реагування після виникнення атак та відновлення нормального функціонування мережі. У цьому розділі ми розглянемо різні технології обнаруження та відновлення після атак, які використовуються для захисту систем IoT.

3.4.1 Системи виявлення вторгнень (IDS)

Системи виявлення вторгнень (IDS) є ключовим елементом в захисті мереж IoT. IDS аналізують мережевий трафік та виявляють незвичайні чи підозрілі активності, які можуть свідчити про можливу кібератаку.

Сучасні IDS використовують різноманітні методи аналізу трафіку, такі як виявлення аномального збору даних, виявлення атак на основі сигнатур та

машинне навчання для виявлення нових видів загроз. Це дозволяє швидко виявляти та реагувати на кібератаки в мережах IoT.

3.4.2 Системи відновлення після інцидентів

Системи реагування на інциденти допомагають організаціям відновлювати роботу мережі після кібератак. Вони складаються з набору процедур і методик, що забезпечують ефективне виявлення, реагування та відновлення після інциденту.

Ці системи включають резервне копіювання даних, відновлення заблокованих або пошкоджених файлів, ізоляцію заражених пристроїв і мережевих вузлів, а також аналіз причин та наслідків кібератак для запобігання подібним інцидентам у майбутньому.

3.4.3 Моніторинг та аналіз журналів подій

Моніторинг та аналіз журналів подій є важливою складовою вашої стратегії виявлення та запобігання кібератак у ваших системах Інтернету речей. Журнал подій фіксує всі дії та дії в Інтернеті, включаючи підозрілі та незвичні дії, які можуть свідчити про кібератаку.

Завдяки моніторингу та аналізу журналу подій ви можете швидко виявляти та реагувати на кібератаки, аналізувати результати та вживати необхідних заходів для відновлення нормальної роботи мережі.

3.4.4 Використання штучного інтелекту та машинного навчання

Застосування штучного інтелекту та машинного навчання в системах обнаруження та відновлення після атак може значно полегшити процес виявлення та реагування на кіберзагрози.

Алгоритми штучного інтелекту та машинного навчання можуть аналізувати великі обсяги даних та виявляти відмінності та закономірності, що вказують на кібератаки. Крім того, ці дані можуть бути використані для прогнозування майбутніх загроз та рекомендації заходів безпеки.

3.4.5 Розвиток інтегрованих платформ безпеки

Розвиток інтегрованих платформ безпеки, які поєднують в собі різні методи та технології обнаруження та відновлення після атак, стає все більш важливим для захисту систем IoT.

Ці платформи можуть об'єднувати в собі функціонал IDS, систем відновлення після інцидентів, моніторингу журналів подій, а також інтегрувати штучний інтелект та машинне навчання для автоматизації процесів виявлення та реагування на кібератаки.

Розвиток технологій обнаруження та відновлення після атак для систем IoT є важливим етапом в забезпеченні безпеки та надійності мереж. Використання систем виявлення вторгнень, відновлення після інцидентів, моніторингу та аналізу журналів подій, а також інтеграція штучного інтелекту та машинного навчання допомагає виявляти, реагувати та відновлювати мережі після кібератак, забезпечуючи їхню надійність та безпеку.

3.5 Використання віртуальної приватної мережі (VPN) для захисту інтернет-мереж від кібератак

3.5.1 Опис віртуальної мережі

Використання віртуальної приватної мережі (VPN) є ефективним методом захисту інтернет-мереж від кібератак. Ось кілька способів, які віртуальна приватна мережа допомагає забезпечити безпеку:

Шифрування трафіку: VPN шифрує весь інтернет-трафік між вашим пристроєм та сервером VPN. Це ускладнює процес перехоплення чи зчитування даних зловмисниками.

Приховування IP-адреси: VPN приховує вашу справжню IP-адресу, замінюючи її на IP-адресу сервера VPN. Це ускладнює ідентифікацію вашого місцезнаходження та захищає вашу приватність.

Захист від вимогливих атак: VPN може захистити вас від різних видів кібератак, включаючи вимогливі атаки, захоплення даних та перехоплення паролів.

Блокування шкідливого контенту: Деякі VPN-провайдери використовують фільтрацію шкідливого контенту, щоб блокувати доступ до веб-сайтів з відомою шкідливою активністю.

Безпечний доступ до внутрішньої мережі: VPN дозволяє працювати в безпечній мережі, навіть якщо ви підключені до ненадійної або ненадійної мережі, наприклад, публічного Wi-Fi.

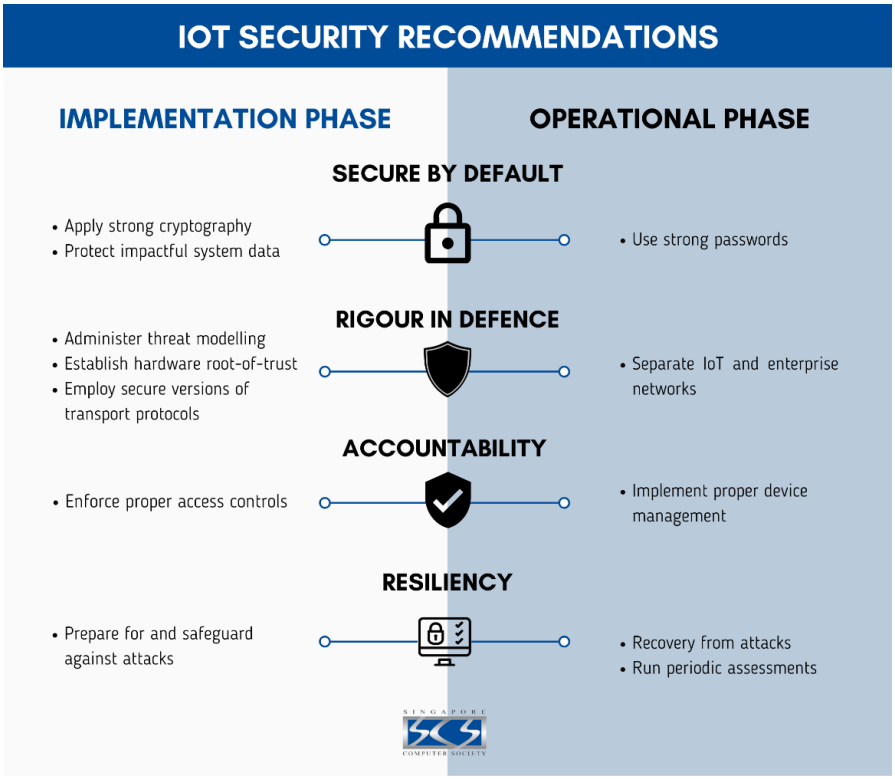


Рис. 3.5 IoT рекомендації щодо зажисту

Захист від ретельного аналізу трафіку: VPN ускладнює або навіть унеможливлює аналіз вашого трафіку зловмисниками, що використовується для виявлення вразливостей та створення атак.

Отже, використання VPN дозволяє ефективно захищати інтернет-мережі від кібератак, забезпечуючи шифрування трафіку, приховування вашої IP-адреси та забезпечуючи безпечний доступ до мережі навіть у вразливих середовищах, таких як публічні Wi-Fi мережі.

3.5.2 Захист мережі від потенційної атаки за допомогою VPN

Використання віртуальної приватної мережі (VPN) іноді, але не завжди, може захистити від DDoS-атак. Ось кілька способів використання VPN для захисту від DDoS-атак:

- Приховування вашої IP-адреси: При використанні VPN ваша реальна IP-адреса приховується, а замість неї використовується IP-адреса VPN-сервера. Це ускладнює зловмисникам визначення вашої реальної IP-адреси та проведення атаки.

- Фільтрація трафіку: деякі провайдери використовують фільтрацію трафіку для виявлення та блокування DDoS-атак до того, як вони потраплять на ваш пристрій.

- Розподіл серверів: багато провайдерів мають сервери в різних країнах. Якщо один сервер зазнає DDoS-атаки, ви можете легко переключитися на інший.

- Шифрування трафіку: шифрування VPN-трафіку може ускладнити зловмисникам перехоплення та підробку трафіку.

Однак слід зазначити, що VPN не є універсальним рішенням для запобігання кібератакам. Деякі типи атак можуть проходити через VPN і досягати серверів і мереж напряму. Якщо ви зіткнулися з серйозною кібератакою, краще покластися на спеціалізовану службу захисту від таких атак.

3.6 Важливість навчання користувачів та адміністраторів щодо безпеки у мережах IoT

Мережі Інтернету речей (IoT) надають безліч можливостей для покращення зручності та ефективності життя, але одночасно вони стають потенційною мішенню для кіберзлочинців. Тому важливо, щоб користувачі та адміністратори були освіченими щодо безпеки у мережах IoT. У цьому розділі розглянемо важливість навчання користувачів та адміністраторів у цій області та шляхи досягнення цієї мети.

3.5.1 Розуміння загроз та ризиків

Розуміння потенційних загроз і ризиків є першим кроком у навчанні користувачів і адміністраторів безпеки мереж IoT. Користувачі повинні знати, що підключення до Інтернету багатьох пристроїв може призвести до кіберзагроз, таких як витік особистих даних, атаки на конфіденційність та інші.

Особлива увага має бути приділена небезпекам, пов’язаним із недостатньою захищеністю пристроїв IoT від несанкціонованого доступу. Наприклад, зловмисники, які використовують слабкі паролі, незахищену мережу Wi-Fi або вразливості в програмному забезпеченні, можуть завдати непоправних збитків.

3.5.2 Правила безпеки та кращі практики

Навчання користувачів і адміністраторів також включає вивчення основних правил безпеки та кращих практик використання мереж IoT. Це може контролювати такі частини, як встановлення складних паролів, регулярне оновлення програмного забезпечення, встановлення захисту від несанкціонованого доступу до мережі та пристроїв, а також відключення непотрібних функцій або служб.

Правила безпеки та кращі практики забезпечують безпеку та захист особистих даних, уникаючи багатьох загроз і ризиків, пов’язаних з використанням мереж IoT.

3.5.3 Реагування на інциденти безпеки

Важливо навчити адміністраторів і користувачів, як реагувати на інциденти безпеки. Важливо швидко вжити заходів для зменшення шкоди та відновлення безпеки мережі в разі кібератаки або порушення безпеки. Це може включати відключення атакованих пристроїв від мережі, зміну паролів, оновлення програмного забезпечення або навіть отримання допомоги фахівців з кібербезпеки.

Правильне реагування на інциденти безпеки допомагає зберегти надійність і цілісність мережі та запобігти таким інцидентам у майбутньому.

3.5.4 Систематичне навчання та оновлення знань

Оскільки сфера кібербезпеки постійно змінюється, важливо, щоб користувачі та адміністратори мереж IoT регулярно отримували навчання та оновлення. Це може включати регулярне навчання, відвідування вебінарів і семінарів, читання спеціалізованої літератури та моніторинг останніх тенденцій у кібербезпеці.

Систематичне навчання та оновлення знань допомагає користувачам та адміністраторам відчувати впевненість у своїх знаннях і навичках, що є важливим фактором для забезпечення безпеки мереж IoT.

3.5.5 Усвідомлення відповідальності

Навчання адміністраторів і користувачів також має підвищити усвідомлення відповідальності за безпеку мереж IoT. Вони повинні знати, що їхні дії або бездіяльність можуть мати значний вплив на безпеку та захист мережі, а також на конфіденційність і цілісність особистих даних.

Усвідомлення відповідальності сприяє створенню культури безпеки серед адміністраторів і користувачів мереж IoT, що є важливим для їхнього захисту та безпеки.

Для забезпечення цілісності та безпеки мереж IoT критично важливо навчати користувачів і адміністраторів безпеці. Створення безпечного середовища для використання мереж IoT можна досягти шляхом розуміння загроз і ризиків, дотримання правил безпеки та кращих практик, ефективного реагування на інциденти безпеки, систематичного навчання та оновлення знань, усвідомлення відповідальності.

Під час дослідження було виявлено, що системи виявлення вторгнень (IDS) і відновлення після інциденту (IR) є критично важливими компонентами безпеки мереж Інтернету речей (IoT). Вони не тільки дозволяють виявляти та реагувати на кібератаки, але й дозволяють відновлювати мережу після їх виникнення.

Використання штучного інтелекту та машинного навчання, моніторинг і аналіз журналів подій і розробка інтегрованих платформ безпеки також є важливими компонентами забезпечення безпеки мереж IoT. Забезпечуючи надійність і безпеку мереж, ці технології допомагають виявляти та вирішувати потенційні загрози.

Загалом, щоб захистити мережі Інтернету речей (IoT) від атак, необхідно використовувати комплексний підхід і широкий спектр методів і технологій. Це єдине, що може забезпечити ефективний захист від кіберзагроз і зберегти надійність і цілісність мереж Інтернету речей.

ВИСНОВКИ

В кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

– Дослідив виявило низку загроз та ризиків, які можуть вплинути на безпеку мереж IoT. Це включає аналіз типових атак, виявлення вразливостей пристроїв та можливих наслідків успішної атаки.

– Проаналізував усе, були розроблені стратегії та методи безпеки для запобігання і виявлення кібератак на мережі IoT. Вони охоплюють використання технічних заходів безпеки, як-от шифрування й автентифікація, розроблення політик безпеки та програм навчання користувачів і адміністраторів.

– Після дослідження я отримав оцінку ефективності різних заходів і методів захисту від кіберзагроз у мережах Інтернету речей. Це допомагає нам визначити найбільш ефективні стратегії захисту для конкретних випадків використання.

– Результати дослідження є основою для розробки навчальних програм та інформаційних матеріалів для користувачів та адміністраторів мереж IoT. Це піднімить компетентність та знизить ризик загрози.

– Загалом, наукові та практичні результати цього дослідження роблять значний внесок у розвиток безпеки мереж IoT і сприяють створенню більш безпечного та надійного середовища IT.

ПЕРЕЛІК ПОСИЛАНЬ

1. IoT Інтернет речей - conf.ztu.URL:https://conf.ztu.edu.ua/wpcontent/uploads/2022/12/164.pdf (датазвернення 06.04.2024)
2. IoT and web-developing – Bdut. URL:https://bdut.co.ua/pro-nas/internet-rechey-iot/ (датазвернення 06.04.2024)
3. Top 10 trends in IoT technology and their impact on the world - proit. URL: https://proit.org.ua/kliuchovi-rozrobki-ta-tiendientsiyi-v-intiernieti-riechiei-iot-d/ (датазвернення 06.04.2024)
4. 7 Benefits of the Internet of Things (IoT) for Business fron - Stfalcon URL: https://stfalcon.com/uk/blog/post/iot-in-healthcare-benefits-challenges (датазвернення 07.04.2024)
5. Bruce Montgomery, PhD, PMP Sr. Instructor A Case History – coursera. URL: https://www.coursera.org/lecture/m2m-iot-interface-design-embedded-systems/iot-security-jbkAW (датазвернення 07.04.2024)
6. 10 IoT Security Challenges and Solutions To Protect Your Devices – linkedin URL: https://www.linkedin.com/pulse/10-iot-security-challenges-solutions-protect-your-2023-jansasoy- (датазвернення 07.04.2024)
7. How to Write the Rationale of the Study in Research - blog.wordvice. URL: https://blog.wordvice.com/rationaleofthestudy/#:~:text=It%20explains%20the%20reason%20the,%E2%80%9Cjustification%E2%80%9D%20of%20a%20study. (датазвернення 08.04.2024)
8. Internet of Things (IoT) typical attacks – internetsociety. URL: https://www.internetsociety.org/iot/?gad_source=1&gclid=Cj0KCQjwq86wBhDiARIsAJhuphl5FOTWWSCR4WBoDSI1ltKBTmWItqW8G1TExGxYGzp7TlTF_mZxoaAsamEALw_wcB (датазвернення 08.04.2024)
9. HowtosecureIoTdevicesinbusiness - nordlayer. URL :https://nordlayer.com /blog/how to secure iot devices in- business/?gad_source=1&gclid=Cj0KCQjwq86wBh

DiARIsAJhuphltPmlOFfRqlCriTXZE3BtFTQxKo6uw8lzYjx81qIfStryGDrMAaAgx3EALw_wcB (датазвернення 08.04.2024)

10. SECURITY PROBLEMS AND THREATS OF IoT DEVICES – csecurity. URL : https://csecurity.kubg.edu.ua/index.php/journal/article/view/231 (датазвернення 11.04.2024)

11. The Role Of Cyber Security In The IoT [Електронний ресурс] – wizardcyber. URL : https://wizardcyber.com/the-role-of-cyber-security-in-the-iot/ (датазвернення 11.04.2024)

12. A Framework for IP Based Virtual Private Networks. – ietf. URL : http://www.ietf.org/rfc/rfc2764.txt (датазвернення 22.04.2024)

13. Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects – mdpi. URL : https://www.mdpi.com/2079-9292/11/9/1502 (датазвернення 26.04.2024)

14. Манько А. В. Сучасні тенденції застосування інтернет-технологій – repository. URL: http://repository.hneu.edu.ua/ (датазвернення 16.04.2024)

15. Tools and Techniques for Collection and Analysis of Internet-of-Things malware: A systematic state-of-art review – sciencedirect. URL: https://www.sciencedirect.com/science/article/pii/S1319157821003621 (датазвернення 28.04.2024)

16. Analysis of cyber-attacks in IoT-based critical infrastructures – researchgate URL : https://www.researchgate.net/publication/350374715_Analysis_of_cyber-attacks_in_IoT-based_critical_infrastructures (датазвернення 29.04.2024)

17. How to ensure IoT security across system levels: a comprehensive guide – n-ix. URL : https://www.n-ix.com/how-to-ensureiotsecurity/ (датазвернення 29.04.2024)

18. Best Practices for Securing IoT Systems– dig8ital. URL :https://dig8ital.com/post/iot-network-security/#:~:text=To%20ensure%20Network%20Security%20in,devices%20for%20any%20suspicious%20activities. (датазвернення 29.04.2024)

19. Посібник із впровадження IoT – mokosmart. URL : https://www.mokosmart.com/uk/iotimplementationguide/ (датазвернення 03.05.202

20. Methods for Detection and Prevention of Vulnerabilities in the IoT (Internet of Things) Systems– intechopen. URL : https://www.intechopen.com/chapters/88775

21. Detection of DoS Attacks for IoT in Information-Centric[Research gate] – https://www.researchgate.net/publication/378881807_Detection_of_DoS_Attacks_for_IoT (датазвернення 03.05.2024)

22. How vpns can help protect against cyber attacks - le-vpn. URL: https://www.le-vpn.com/how-vpns-can-help-protect-against-cyber-attacks/
(датазвернення 06.05.2024)

23. Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques [MDPI] - URL:https://www.mdpi.com/1424-8220/23/3/1708

(датазвернення 08.05.2024)

24. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches [SienceDirect] - URL:https://www.sciencedirect.com/science/article/pii/S2542660519300241 (датазвернення 11.05.2024)

25. Tips For Safeguarding Your Smart Devices and Networks [sennovate] - URL:https://sennovate.com/iot-security-101-tips-for-safeguarding-your-smart-devices-and-networks/ (датазвернення 07.05.2024)

26.Protection for IoT security [Deviceauthority] - https://deviceauthority.com/security-issues-of-iot-securing-your-iot-device-in-2023/ (датазвернення 03.05.2024)

27. IoT Security: How an IoT VPN can benefit your solution [onomondo] - URL: https://onomondo.com/blog/iot-vpn-network-security-explained/
(датазвернення 08.05.2024)

28. Top Five IoT Security Risks For Businesses [Cybersecurity centre of excellence] - URL:https://ccoe.dsci.in/blog/top-five-iot-security-risks-for-businesses (датазвернення 03.05.2024)

29. What Is IoT Security? Challenges and Requirements [FORTINET] - URL:https://www.fortinet.com/resources/cyberglossary/iot-security (датазвернення 07.05.2024)

30. IoT Security: Safeguarding Critical Networks Against Digital Assaults[SECURITY EXCHANGE] - URL:https://www.eccouncil.org/cybersecurity-exchange/network-security/guide-to-iot-security-protecting-critical-networks/ (датазвернення 0.05.2024

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

БАКАЛАВРСЬКА РОБОТА

НА ТЕМУ: «АНАЛІЗ ТА ЗАХИСТ ВІД АТАК НА МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ (IOT))»

Керівник:
Сосновий В. С.

Виконав:
Студент 4-го курсу
Групи КІД-42
Кліменченко Ігор Сергійович

МЕТА, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

1. Об'єкт дослідження - безпечне функціонування мережі інтернет речей(IoT).

2. Предмет дослідження – аналіз та способи захисту від атак на мережі інтернет речей.

3. Мета роботи – дослідити та розробити рекомендації для підвищення захисту та функціонування інтернет речей.

Для досягнення поставленої в роботі мети вирішено наступні наукові завдання:

- Досліджено поняття безпечного функціонування мережі інтернет речей та особливості їх роботи.
- Проаналізовано різні типи вразливостей та рекомендовано контрзаходи.
- Перераховано методи та впроваджені технології для захисту та підвищення ефективності функціонування.

3

СТРУКТУРА ТА ОСНОВНІ ХАРАКТЕРИСТИКИ НЕЗАХИЩЕНИХ МЕРЕЖ IoT.

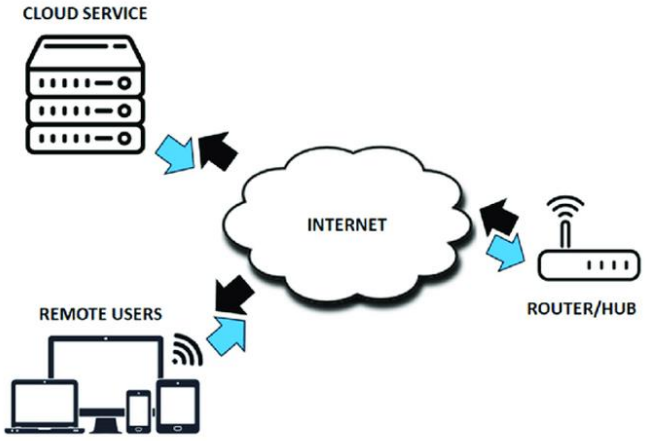


Рис. 1 Принципова схема незахищеної автоматизованої системи локальної мережі

4

РІЗНОМАНІТНІСТЬ ТА КОНЦЕПЦІЇ КІБЕРАТАК

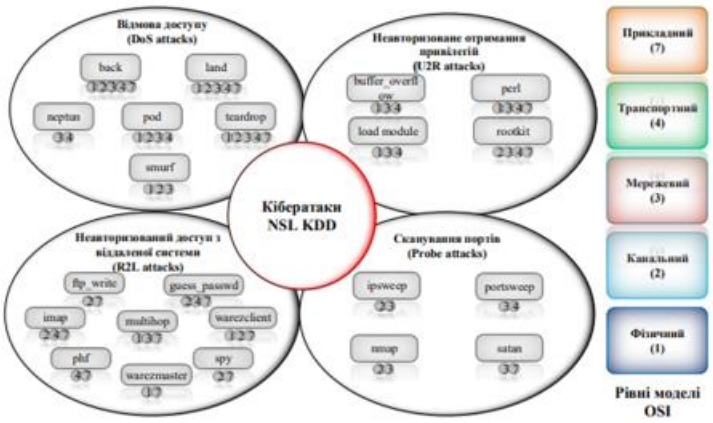


Рис. 2 Класифікація кібератак

5

РІЗНОМАНІТНІСТЬ ТА КОНЦЕПЦІЇ КІБЕРАТАК

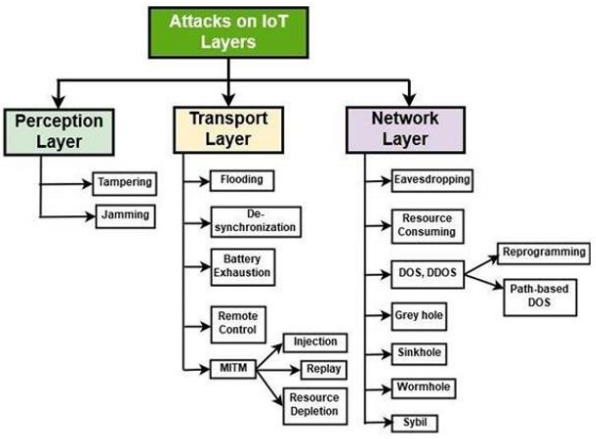


Рис. 3 Атаки на шари мережі IoT.

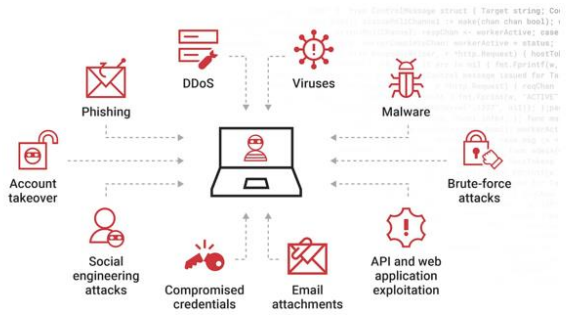


Рис. 4 Види атак на мережі IoT.

6

АНАЛІЗ ПОТЕНЦІЙНОЇ АТАКИ НА МЕРЕЖІ IOT

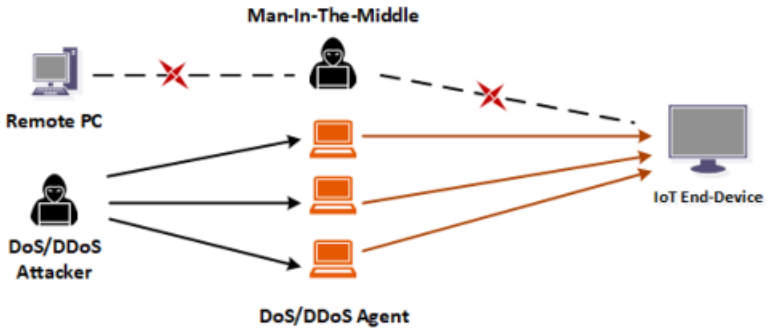


Рис. 5 Приклад потенційної DDoS атаки

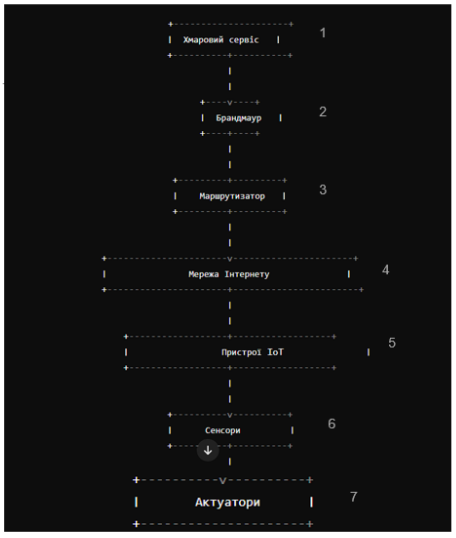
7

СХЕМА ЗАХИЩЕНОЇ МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ(IOT)

У цій схемі:
Хмаровий сервіс забезпечує централізоване управління та зберігання даних, а також надає доступ до мережі IoT через Інтернет.

Брандмаур служить першим рівнем захисту, що фільтрує та контролює трафік, що входить та виходить з мережі IoT.
Маршрутизатор використовується для передачі даних між мережею IoT та мережею Інтернет.

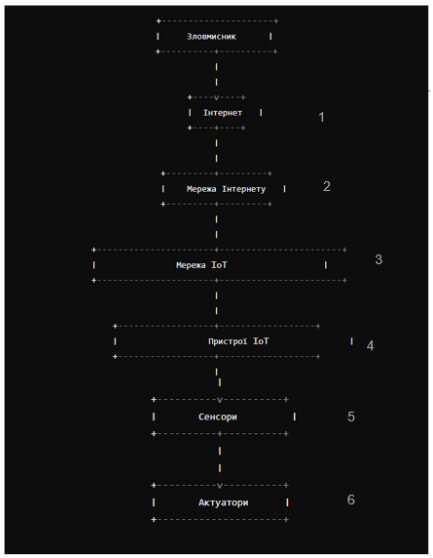
Пристрої IoT, такі як сенсори та актуатори, з'єднуються з мережею через маршрутизатор.
Сенсори вимірюють дані та передають їх до хмарового сервісу або інших пристроїв IoT.
Актуатори отримують команди з хмарового сервісу або інших пристроїв IoT та виконують відповідні дії.
Ця схема показує основні компоненти та зв'язки у захищеній мережі Інтернету речей.



IOT

8

АНАЛІЗ КІБЕРАТАКИ НА МЕРЕЖУ IoT



У цій схемі:
•Зловмисник використовує Інтернет для доступу до мережі IoT.
•Мережа дозволяє зловмисникові взаємодіяти з мережею IoT через Інтернет.
•Пристрої IoT, такі як сенсори та актуатори, можуть бути скомпрометовані зловмисником через мережу Інтернету.
•Сенсори та актуатори можуть бути використані зловмисником для втручання у нормальну роботу системи або для збору конфіденційної інформації.
Ця схема ілюструє загальний принцип атаки на мережу IoT через Інтернет та можливі наслідки для пристроїв і сенсорів у мережі:

- Перевантаження або навіть знищення обладнання.
- Крадіжка конфіденційної інформації
- Доступом для подальших атак

9

СХЕМА НАДІЙНОЇ ТА ЗАХИЩЕНОЇ МЕРЕЖІ, ВІД КІБЕРАТАК

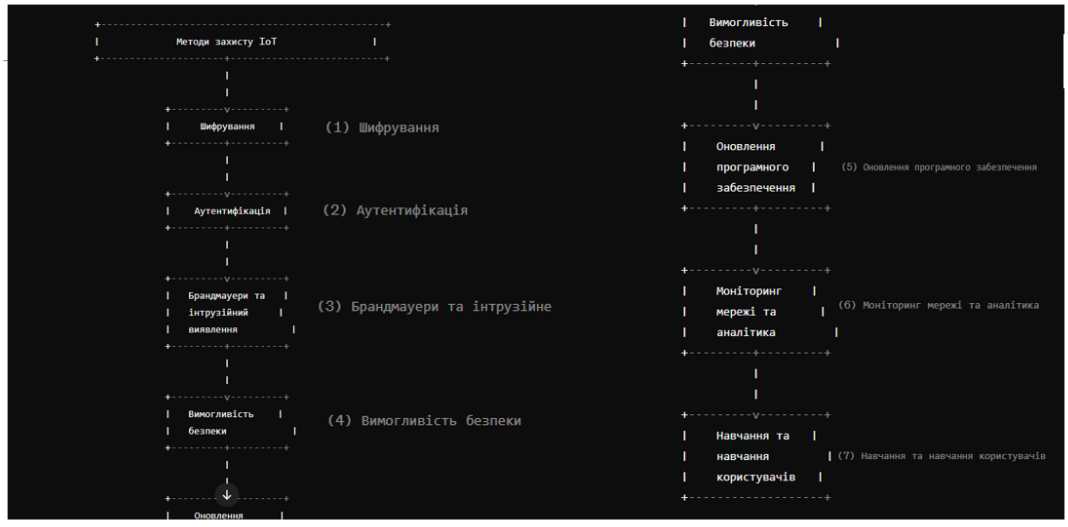


Рис. 8 Схема надійної мережі IoT

10

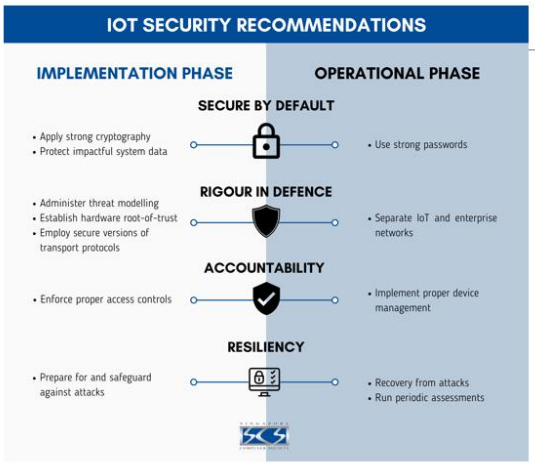


Рис. 9 Рекомендації щодо захисту мережі IOT

Рис. 10 Віртуальна приватна мережа(VPN)

Використання віртуальної приватної мережі (VPN) може забезпечити додатковий рівень безпеки для мереж Інтернету речей (IoT). В цілому, використання VPN може покращити безпеку мережі IoT, забезпечуючи шифрування трафіку, ізоляцію мереж, аутентифікацію та авторизацію, моніторинг та контроль доступу.

ВИСНОВКИ

В бакалаврській роботі отримано наступні науково-теоретичні та науково-практична навички:

- Дослідження виявило низку загроз та ризиків, які можуть вплинути на безпеку мереж IoT. Це включає аналіз типових атак, виявлення вразливостей пристроїв та можливих наслідків успішної атаки.
- Проаналізувавши все, були розроблені стратегії та методи безпеки для запобігання і виявлення кібератак на мережі IoT. Вони охоплюють використання технічних заходів безпеки, як-от шифрування й автентифікація, розроблення політик безпеки та програм навчання користувачів і адміністраторів.
- Після дослідження ми отримали оцінку ефективності різних заходів і методів захисту від кіберзагроз у мережах Інтернету речей. Це допомагає нам визначити найбільш ефективні стратегії захисту для конкретних випадків використання.
- Результати дослідження є основою для розробки навчальних програм та інформаційних матеріалів для користувачів та адміністраторів мереж IoT. Це піднімить компетентність та знизить ризик загрози.