МІНІСТЕРСТВО ОСВІТИ І НАУКИ
УКРАЇНИНАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ
УНІВЕРСИТЕТФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Вдосконалені методи підвищення кібербезпеки системи розумний будинок»

Виконавець: _____ Іван МИРСЬКИЙ
(підпис)

Керівник: _____ Олександр ПУЗИРЕНКО
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультантрозділу«Охоронапраці»_____ БатирХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»_____
_____ Андріан ЯВНЮК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра телекомунікаційних та радіоелектронних систем

Спеціальність 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма«Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Віктор ГНАТЮК
«_____» _____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Мирського Івана Ігоровича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Вдосконалені методи підвищення кібербезпеки системи розумний будинок»затверджена наказом ректора від«28»вересня2023р.№1965/ст
2. Термін виконання роботи: з 02.10.2023 р. по 31.12.2023 р.
3. Вихідні дані до роботи:.проаналізувати сучасні рішення для побудови інтелектуалізованих систем та вдосконалити системи та засоби кібербезпеки на базі "Розумний Будинок" провести експеримент з вдосконалення захисту баз данних.
4. Зміст пояснювальної записки:.аналіз існуючих рішень, систем та засобів захисту кібербезпеки та безпеки дому, вдосконалення захисту данних через внесення протоколу Kerberos на базі "Розумного Будинку".
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: презентація, слайди.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	29.09.2023-11.10.2023	Виконано
2	Вступ	11.10.2023-12.10.2023	Виконано
3	Аналіз існуючих рішень для побудови розумного будинку	12.10.2023-18.10.2023	Виконано
4	Аналіз сучасних методів підвищення кібербезпеки розумного будинку	20.10.2023-25.10.2023	Виконано
5	Удосконалення існуючих методів підвищення кібербезпеки розумного будинку	26.10.2023-31.10.2023	Виконано
6	Експериментальне дослідження існуючих методів підвищення кібербезпеки розумного будинку	01.11.2023-10.11.2023	Виконано
7	Охорона праці	13.11.2023-17.11.2023	Виконано
8	Охорона навколишнього середовища	20.11.2023-27.11.2023	Виконано
9	Усунення недоліків та захистккваліфікаційної роботи	01.12.2023-15.12.2023	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант(посада,П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., професорБатир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.б.н., доц. Андріан ЯВНЮК		

8. Дата видачі завдання: “29" вересня 2023 р.

Керівник кваліфікаційної роботи _____ Олександр ПУЗИРЕНКО
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Іван МИРСЬКИЙ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Вдосконалені методи підвищення кібербезпеки системи розумний будинок» містить

____сторінок,29 рисунків,12 таблиці,25 використаних джерел.

SMART HOME, Ajax, Xiaomi, Google, Blockchain.

Об’єкт дослідження:різні системи кібербезпеки такі як Ajax, Google, Xiaomi та протоколів захисту Zigbee, 2AF.

Предмет дослідження:система «Розумний будинок», «SMARTHOUSE» та різні захисні пристрої.

Мета кваліфікаційної роботи:метою даної роботи є порівняння кращої системи забезпечення захисту SMARTHOUSE та вдосконалення певних видів кіберзахисту програмного забезпечення, обладнання, будинку та насамперед фізичного споживача таких послуг.

Метод дослідження: використання методів обробки даних, аналізу даних, синтезу даних та методи об’єктно-орієнтованого програмування різними мовами та використанням різних програм, протоколів та електронних пристроїв.

Матеріали кваліфікаційної роботи рекомендується використовувати при проектуванні та розробці чи вдосконаленні старих методів(рішень) захисту «SMART» винаходів, автівок, будинків та інше.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

DHCP – Dynamic Host Configuration Protocol

IDE – Integrated development environment

IoT – Internet of Things

IP- address – Internet Protocol address

LED – light-emitting diode

MAC- address – Media Access Control

MQTT – Message Queue Telemetry Transport

PIR – Passive infrared sensor

QoS – quality of service

RGB – Red, Green, Blue

RGBW – Red, Green, Blue, White

SRAM – static random access memory

USB – Universal Serial Bus

WEP – Wired Equivalent Privacy

Wi-Fi – Wireless Fidelity

WPA – Wi-Fi Protected Access

2FA - Two-factor authentication

ВСТУП

Актуальність теми. Сьогодні ми спостерігаємо стрімкий розвиток інформаційних телекомунікаційних, комп’ютерних систем, що зумовлено запитами сучасної людини та рівнем розвитку країни. Поруч із розвитком цих систем розвивається яінабуваєвеликогозначення сучасна концепція Інтернету речей (IoT), яка представляє сукупність заємозв'язаних фізичних пристроїв, які мають вбудовані приймачі та давачі, а також програмне забезпечення, що здійснює передачу та обмін даними між фізичним світом і комп'ютерними, теле-радіосистемами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку. Крім сенсорів, мережа має виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через різні типи сполучень мережі.

Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів, штучних інтелектів.

Разом з розвитком IoT змінюється життялюдей, з’являються «розумні університети», «розумніавтомобілі» (SMARTAUTO), «розумні пристрої» які почали використовуватись набагато частіше у житті людей.

Неоминув розвиток і будівну галузь, яскравими представниками якої є сучасні будинки «SMARTHOUSE» (багатоповерхові, таунхауси, приватні будинки), при початку використання яких, сьогодні виникає дуже багато проблем пов’язаних з недостатньою автоматизацією операційних процесів.

Серед основних проблем можемо виділити такі: погана захищенність інформації, проблеми з фізичною безпекою, забезпечення доступу до приміщень (гараж, бомбосховище, комора) лише легітимним відвідувачам,застаріла та дорога протипожежна безпека, велика кількість рутинних процесів у роботібудинку, складність у керуванні процесами та

надлишкова участь людей у процесі керування рутинними справами будинком тощо.

Метою і завдання дослідження: Дивлячись на всі ці проблеми які існують та утворюються нові метою даної роботи є порівняння кращої системи забезпечення захисту SMARTHOUSE та вдосконалення певних видів кіберзахисту програмного забезпечення, обладнання, будинку та насамперед фізичного споживача таких послуг.

Для досягнення нашої мети перед нами постають такі задачі які ми повинні вирішити:

– проаналізувати існуючі рішення для побудови інтелектуалізованих систем для будинків;

– вдосконалити різні розробки систем «Розумний університет»;

– провести експериментальне дослідження існуючих методів підвищення кібербезпеки розумного будинку.

Об’єктом дослідження – різні системи кібербезпеки такі як Ajax, Google, Xiaomi та протоколів захисту Zigbee, 2AF.

Предметом дослідження – система «Розумний будинок», «SMARTHOUSE» та різні захисні пристрої.

Методидосліджень. Використовувалися методи обробки даних, аналізу даних, синтезу даних та методи об’єктно-орієнтованого програмування різними мовами та використанням різних програм.

РОЗДІЛ 1: АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ПОБУДОВИ РОЗУМНОГО БУДИНКУ

1.1 Огляд сучасних технологій при розробці розумного будинку

Розумний будинок - це житло, в якому використовуються передові технології для автоматизації та оптимізації різних аспектів життя, таких як енергоефективність, безпека, зручність і розваги.

«Розумний будинок» — це сучасний житловий будинок, створений для проживання людей за допомогою автоматизації та сучасних технологій. Термін слід розуміти як систему, яка гарантує безпеку та збереження ресурсів, а також комфорт для всіх користувачів. Інститут інтелектуальної будівлі у Вашингтоні (округ Колумбія) запропонував концепцію в 1970-х роках: це дім, який дозволяє використовувати робочий простір ефективно та продуктивно. Зі збільшенням обчислювальної здатності гаджетів концепція «розумний будинок» отримала своє логічне продовження – систему «Інтернет речей», згідно з якою була проведена первинна стандартизація та визначені основні правила та рекомендації до побудови готового продукту на рівні як системи загалом, так і окремих компонентів. Незважаючи на відносну новизну, вже зараз існує декілька десятків різних рішень.

«Розумний будинок» повинен вміти розпізнавати конкретні ситуації, що відбуваються в будівлі, і відповідним чином на них реагувати. Одна з систем може управляти поведінкою інших по заздалегідь виробленим алгоритмам. Основною особливістю інтелектуальної будівлі є об'єднання окремих підсистем в єдиний керований комплекс (див. рис. 1.1).

Важливою особливістю і властивістю «розумного будинку», яка відрізняє його від інших способів організації життєвогопростору, є те, що це найбільш прогресивна концепція взаємодії людини з житловим простором, коли людина однією командою задає бажану обстановку, а вже автоматика відстежує режими роботи всіх інженерних систем і електроприладів.

У цьому випадку виключається необхідність користуватися кількома пультами при перегляді телебачення, десятками вимикачів при управлінні освітленням, окремими блоками при управлінні вентиляційними і опалювальними системами, системами відеоспостереження та сигналізації, воротами і іншим. У smart-будинку достатньо одним натисканням на настінній клавіші або пульті дистанційного керування (ДК) чи сенсорній панелі, вибрати один зі сценаріїв, і будинок сам налаштує роботу всіх систем, відповідно до побажань господаря, часу доби, погоди, зовнішньої освітленості.

Концепція інтелектуальної будівлі містить в собі такі положення:

- Створення інтегрованої системи управління будівлею - системи з можливістю забезпечення комплексної роботи всіх інженерних систем будівлі: освітлення, опалення, вентиляції, кондиціонування, водопостачання, контролю доступу та багатьох інших.
- Відсутність обслуговуючого персоналу і передача функцій контролю і прийняття рішень підсистемам інтегрованої системи управління будівлею. У ці підсистеми і закладається «інтелект» – алгоритм дій у відповідь на зміну параметрів датчиків системи та інші події типу позаштатних ситуацій.
- Реалізація механізму негайного відключення і передачі, при необхідності, управління людині будь-якою підсистемою інтелектуальної будівлі. Разом з цим людині повинен надаватися зручний і однаковий доступ до управління і відображення всіх підсистем і частин «розумного будинку».
- Забезпечення коректної роботи окремих підсистем в разі відмови загальної керуючої системи або інших частин системи.
- Мінімізація вартості обслуговування і модернізації систем будівлі, що має забезпечуватися застосуванням загальних стандартів у побудові підсистем,автоматичне конфігурування і виявлення нових пристроїв і модулів при їх додаванні в систему.

• Наявність в будівлі прокладеною комунікаційного середовища для підключення до неї пристроїв і модулів. Поряд з цим, можливість використання в якості комунікаційного середовища в системі управління різних типів фізичних каналів: слабкострумові лінії, силові лінії, радіоканал.

Система «розумний дім» включає в себе наступні об'єкти автоматизації:

• управління освітленням;

• управління електроприводами;

• клімат-контроль;

• управління системою вентиляції;

• централізоване управління системами на кшталт домашнього кінотеатру;

• мультирум;

• системи відеоспостереження;

• охоронно-пожежна сигналізація (ОПС);

• системи контролю доступу;

• контроль електричних навантажень і аварійних станів;

• управління інженерним обладнанням з сенсорних панелей;

• сервер управління.

Дещо зображено на рисунку 1.1.

Рис.1.1 Датчики та взаємопоїднання їх

Сучасні технології значно розширюють можливості розумного будинку. Ось деякі з них:

Інтернет речей (IoT) — це технологія, яка дозволяє використовувати смартфони або голосові асистенти, щоб керувати різними пристроями та датчиками через Інтернет. Це може включати камери безпеки, домофони, освітлення та багато іншого.

Голосові асистенти: велика популярність голосових асистентів, таких як Amazon Alexa, Google Assistant та Apple Siri, дозволяє керувати різними функціями вдома за допомогою голосу. Ви можете регулювати освітлення, температуру або навіть замовляти продукти через голосові команди.

Системи безпеки - вдосконалені системи безпеки включають в себе відеоспостереження, сенсори диму, газу і води, системи контролю доступу та централізоване керування. За допомогою додатків ви можете отримувати сповіщення і керувати системою безпеки в будь-якому місці.

Смарт-термостати - вони дозволяють вам віддалено керувати температурою в будинку через смартфон або автоматично регулювати її залежно від вашої присутності в будинку, що допомагає зекономити енергію.

Спрощені інтерфейси - Мобільні додатки та голосові помічники дозволяють користувачам керувати розумним будинком зі смартфона або через голосові команди. Це робить управління будинком легким і доступним для кожного.

Енергоефективність- сучасні розумні будинки використовують енергоефективні технології, такі як LED-освітлення, сонячні панелі, енергоефективні системи опалення та кондиціонування повітря для зменшення споживання енергії.

Розумна кухня- кухні можуть бути оснащені смарт-пристроями, такими як холодильники, духовки, кавоварки та плити, які можна керувати з допомогою смартфона або голосових асистентів.

Розваги - розумний будинок може мати домашній кінотеатр з автоматичним керуванням аудіо та відео, аудіосистеми, які забезпечують звук у всьому будинку, та ігрові системи, підключені до мережі.

Розумний сад та полив - технології IoT дозволяють вам віддалено керувати поливом, контролювати рост рослин та отримувати інформацію про стан ґрунту.

Системи очищення повітря та води - розумний будинок може включати системи фільтрації повітря та води для забезпечення здорового середовища для вас і вашої сім'ї.

Автоматизація заходів в будинку - розумний будинок може виконувати автоматичні дії, такі як вимкнення світла або регулювання температури, коли ви покидаєте будинок або йдете спати.

Системи аналітики та штучного інтелекту - деякі розумні будинки використовують системи аналітики та штучного інтелекту для прогнозування потреби в енергії, планування розходу ресурсів та оптимізації дому для максимальної зручності.

Сучасні технології роблять розумний будинок більш безпечним, зручним і ефективним. Вони дозволяють власникам будинку ефективно

керувати його функціями і отримувати більше контролю над своїм життям рисунок 1.2

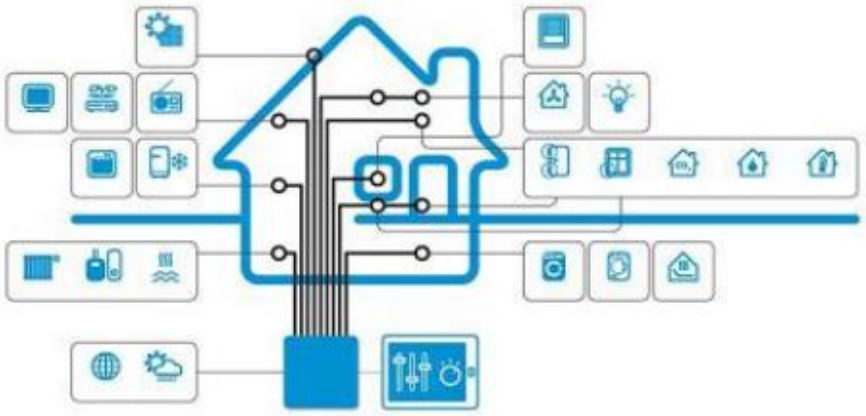


Рис. 1.2 Концептуальне зображення як працює система «розумний будинок»

Система «розумний дім» забезпечує механізм централізованого контролю та інтелектуального управління в житлових, офісних або громадських приміщеннях.

Загальна схема системи управління виглядає наступним чином:

1. центральний процесор управління/головний блок управління;
2. датчики (температури, освітленості, задимленості, руху та ін.);
3. керуючі пристрої (димери, реле, інфрачервоні (ІЧ) емітери та ін.);
4. інтерфейси управління (кнопкові вимикачі, пульти ІЧ, радіопульт, сенсорні панелі, web/wap інтерфейс);
5. власна мережа управління, що об'єднує вищевказані елементи;
6. керовані пристрої (світильники, кондиціонери, компоненти домашнього кінотеатру та ін.);
7. допоміжні мережі (Ethernet, телефонна мережа, дистрибуція аудіо і відеосигналу);
8. програмне забезпечення проекту.

Основна функція центрального процесора – управління підпорядкованими йому пристроями з використанням наступних інтерфейсів: Ethernet, RS-232, RS- 485, IR, аналогових і цифровихта ін. Також

центральний процесор управління містить багатозадачну операційну систему, інструментальні засоби програмування і, в деяких випадках, web-сервер.

Датчики розташовуються в певних місцях квартири, які безпосередньо або через проміжні пристрої зв'язані єдиною мережею. Інтерфейси управління здійснюють загальне управління системами «розумного будинку».

Загальний алгоритм роботи системи «розумний будинок»:

• По власній мережі управління інформація від датчиків або інтерфейсів надходить до центрального процесора управління.

• Програмне забезпечення центрального процесора обробляє отриману інформацію і генерує команди для керуючих пристроїв.

1.2 Оцінка існуючих розумних пристроїв та платформ

Оскільки ринок постійно зростає, а нові продукти та технології постійно виходять на ринок, оцінка існуючих розумних пристроїв і платформ для розумного будинку може бути складною. Коли ви оцінюєте розумні пристрої та платформи для розумного будинку, слід враховувати наступні елементи:

- Сумісність; переконатися, що розумні пристрої підтримують платформу, яку ви використовуєте.
- Зручність і інтуїтивність: оцініти, наскільки просто і легко ви можете керувати пристроями і налаштовувати автоматизацію.
- Безпека: звернути увагу на заходи безпеки, які надає платформа або виробник пристрою.
- Вартість: розглянути вартість як самого пристрою, так і можливі витрати на додаткове обладнання або платні підписки.
- Розширюваність: продумати які системи можна розширити у майбутньому, коли ви захочете додати нові пристрої або функції.

У кожного користувача можуть бути власні потреби та вимоги, тому важливо ретельно дослідити різні пристрої та платформи перед прийняттям рішення.

Однак деякі з найпопулярніших та найбільш рекомендованих пристроїв і платформ можуть включати наступне:

Платформи для розумних будинків:

1. Amazon Alexa - Користувачі можуть керувати різними розумними пристроями за допомогою платформи голосового управління Alexa від Amazon, яка інтегрується з багатьма сторонніми пристроями та службами. Основними технічними характеристиками цього помічника є наступні: Amazon Echo пристрої мають вбудовані мікрофони, які мають функції шумозниження та детектора голосу. Вбудований динамік для відтворення музики та голосу Alexa Підтримка мережі Wi-Fi для підключення до Інтернету. Amazon Alexa розуміє та виконує голосові команди за допомогою розширених технологій штучного

інтелекту та обробки природної мови.Можливість отримання оновлень програмного забезпечення через Інтернет для вдосконалення функцій та безпеки. Заходи безпеки та захисту конфіденційності для збереження особистої інформації користувача. Див. рисунок 1.3

Рисунок 1.3 Amazon Alexa Echo

2. Google Assistant - Google Assistant - цеіншаплатформаголосовогоуправління, якадозволяєкеруватирозумнимипристроямитаінтегруєтьсязекосистемою Google.Рисунок 1.4

Рис. 1.4 GoogleAssistant«Увімкнення світла користувачем»

3. AppleHomeKit - Платформа HomeKit надає користувачам пристроїв Apple можливість керувати розумними пристроями за допомогою додатку Apple Home або голосових команд Siri.

Крім того, трохи про технічні функції: HomeKit використовує безпечний стандартний протокол, який називається HomeKit Accessory Protocol (HAP), для зв'язку між пристроями. Цей протокол може працювати за допомогою Wi-Fi або Bluetooth. HomeKit шифрує дані між пристроями та пристроями iOS за допомогою шифрування end-to-end. Всі пристрої, які можуть працювати з HomeKit, повинні бути сертифіковані Apple. Навіть коли ви не вдома, ви можете отримати віддалений доступ до свого розумного будинку через мобільний пристрій за допомогою iCloud. HomeKit дозволяє створювати різноманітні сценарії та автоматизації на основі подій і умов. Ви можете, наприклад, налаштувати вмикач світла ввімкнутися, коли ви входите в будинок.

HomeKit може інтегруватися з іншими платформами та службами, такими як Homeapp в iOS, що робить керування розумним будинком більш уніфікованим.

4. SamsungSmartThings -Платформа SmartThings від Samsung є відкритою, що дозволяє створювати автоматизовані сценарії та інтегрувати кілька розумних пристроїв. Для підключення до різних розумних пристроїв SamsungSmartThings використовує протоколи Zigbee та Z-Wave, а також Wi-Fi та Bluetooth. Латформа працює з великою кількістю розумних пристроїв, таких як термостати, лампи, датчики руху, розумні розетки та інші. Користувачі можуть використовувати попередні голосові команди для керування розумним будинком, оскільки SmartThings сумісний з голосовими асистентами, такими як AmazonAlexa та GoogleAssistant. З іншими популярними платформами та додатками для розумного дому, такими як Ring, PhilipsHue та GoogleHome, SamsungSmartThings може взаємодіяти.

5. AjaxStarterKit (рис. 1.2). Український бренд Ajax представляє систему свого смарт будинку, із забезпеченням контролю безпеки. AjaxStarterKit попередить власника про несанкціоноване проникнення, спалах, затоплення. У комплект входять: центральний контролер; сирена; брелок з функцією пульта; сенсори положення дверей і вікон (відкрито/закрито); розбитого скла; протікання води; руху (розрізняє людей і тварин). Зображені на рисунку певні датчики та контрольна панель Ajax рис. 1.5

Рисунок 1.5 – Система «розумного будинку» Ajax StarterKit

Переваги та недоліки висвітлено в таблиці 1.1.

Переваги:	Недоліки:
Захищений радіоканал	Виключно охоронні функції;
Простота налаштування;	Відсутність голосового інтерфейсу;
Простота управління;	
Швидке оповіщення;	
Резервне живлення контролера;	
Середня ціна: 4600 грн.	

Табл. 1.1. Переваги та недоліки системи Ajax

Розумні пристрої

Розумне освітлення (Philips Hue, LIFX,AJAX): Ці бренди пропонують розумні лампи та лампочки, які можна керувати за допомогою мобільного додатка або голосових помічників.

Розумний термостат (Nest,Ecobee, AJAX): Розумні термостати дозволяють оптимізувати систему опалення та охолодження в будинку для зменшення енергоспоживання.

Розумні дверні замки (August, Schlage, AJAX): З розумними дверними замками можна віддалено керувати доступом до будинку, ділитися кодами доступу та відслідковувати активність.

Камери відеоспостереження (Nest Cam,Arlo, AJAX): Розумні камери надають можливість віддалено переглядати відео та сповіщати про події, що відбуваються в будинку.

Розумні датчики (Samsung SmartThings, Wyze, AJAX): Датчики руху, диму, витоку води та інші можуть попереджати про небезпеки та автоматизувати деякі функції.

Аудіо- та відеосистеми (Sonos, Bose, Samsung, AJAX): Розумні аудіо- та відеосистеми дозволяють стрімити музику та відео в будинку з різних джерел.

Роботи-пилососи (Roomba, Xiaomi): Роботи-пилососи автоматично прибирають підлогу та можуть бути програмовані для роботи в певний час.

Розумні системи безпеки (Ring, SimpliSafe, AJAX): Системи відеоспостереження, датчики та сигналізація для забезпечення безпеки в будинку.

Розумний голосовий асистент (Amazon Echo, Google Nest): Голосові асистенти можуть керувати розумними пристроями та надавати інформацію за допомогою голосу.

Розумні кухонні пристрої (Instant Pot Smart, Anova Precision Cooker): Ці пристрої дозволяють керувати приготуванням їжі через мобільний додаток.

Розглянемо певні технічні характеристики деяких пристроїв таких як AJAXNestPhilips.

LED лампи різних форм та кольорів, ьездротове керування через різні додатки, які підтримують різні платформи такі як IOS та Android, також сумісність різних платформ AppleHomeKit, GoogleAssistant та AmazonAlexa.

Використання протоколів зв'язку, таких як Zigbee для взаємодії з іншими пристроями. Забезпечення віддаленого керування освітленням через Інтернет. Центральна блокада (Hub): Бездротова технологія: Jeweller (868/433 МГц). Забезпечує зв'язок з різними датчиками та пристроями AJAX.

Датчики та Девайси:

- Датчики руху (MotionProtect, MotionProtect Plus).
- Відкриття дверей/вікон (DoorProtect, DoorProtect Plus).
- Датчики витоку (LeakProtect).
- Камери (CamProtect, CamOutdoor).
- Детектори диму (FireProtect, FireProtect Plus).
- Детектори вуглекислого газу (FireProtect Plus).
- Сирени (StreetSiren, HomeSiren).
- Пульт дистанційного керування (SpaceControl).

Можливість співпрацювати з IFTTT та іншими платформами. Можливість віддаленого керування та звітів через Wi-Fi відео у високій якості 1080p. автоматизація графіків опалення та охолодження та оптимізація споживання енергії.

При виборі розумних пристроїв і платформ для розумного будинку важливо враховувати сумісність з іншими пристроями в будинку, а також довіру виробникам, які мають хорошу репутацію в галузі безпеки та приватності. Зверніть увагу на функції та вартість пристроїв, а також на те, наскільки легко вони поєднуються з вашим домашнім середовищем. Вибір і встановлення певних пристроїв і платформ у домі — це складне завдання.

Наприкладі розгялнемо декілька найпопулярніших функцій розумного будинку – це системи безпеки та витоку газу, води.

Почнемо з системи безпеки, відеонагляду Постановка і зняття квартири з охорони виконується за допомогою кодової панелі при вході. При відкритті вхідних дверей у людини є декілька секунд на введення коду. Якщо ж код не буде введений, розумний будинок включить сирени і відправить СМС-повідомлення на кілька номерів. Датчики руху, розташовані на кухні, спальні і вітальні дозволять виявити проникнення через вікна. Схема застосування датчиків руху в квартирі з інтелектуальною системою «розумний будинок» показана на рис. 1.6.

Рис. 1.6 Схема застосування датчиків охорони

Введення кода на охоронній панелі дозволить «розумному будинку» включити сигналізацію та відключити освітлення, а також перевести систему опалення в режим енергозбереження.

Якщо виникає витоок газу або води, відповідний датчик вмить повідомить центральний контролер. Він потім перекриває газ або воду в будинку електроклапаном. Власники та аварійні служби будуть негайно проінформовані. «Розумний будинок» також допоможе виявити та запобігти витоку води.

Схема використання датчиків протікання води показана на рис. 1.7. Контрольованими зонами є санвузли та кухня, тобто ті приміщення, де проходять труби водопостачання та газу або де встановлені лічильники. Прорив труби або перелив води через краї раковини фіксується за допомогою спеціальних датчиків. У випадку протікання розумний будинок перекроїть доступ води в квартиру і відправить СМС-повідомлення на телефон.

Рис. 1.7 Схема використання датчиків ГАЗу Води

Отже, порівняймо всі системи(датчики) в таблиці 1.2

Система	**Ajax**	**Xiaomi**	**Google**	**Amazon**
Простота налаштування	+	+	+	+
Відкритість	-	+	+	+
Мобільний додаток	+	+	+	+
Інтерфейс ВЕБ	+	+	+	+
Голосовий помічник	+	-	+	+
Вартість,	**6000**	**2500**	**10000**	**15000**

ГРН				

Табл. 1.1 Порівняння цін та характеристик

Висновки до РОЗДІЛУ 1

Системи «розумного будинку» були розглянуті та проаналізовані. Незважаючи на те, що їх розробка почалася нещодавно, основні принципи були розроблені давно, оскільки створити системи такого рівня було неможливо за відсутності відповідного програмного забезпечення та апаратного забезпечення.

«Розумний будинок» складається з таких компонентів: сервер, канали передачі даних, хмара, датчики, мікроконтролери та пристрої. Користувач керує системою «розумного будинку» через сервер.

Проаналізовано певні групи контролю:

Освітлення – відповідає за контроль над освітленістю дому, взаємодіє з групою знаходження.

Енергозбереження – оптимізує роботу пристроїв.

Клімат-контроль – регулює системи встановлення температури та вологості в залежності з потребами користувача.

Безпеки – підсистема захисту від фізичного несанкціонованого вторгнення в дім та аварійних ситуацій.

Протікання води – система визначення та усунення проблем з протіканням води та, відповідно, оповіщуванням користувача. • Штучного інтелекту – система, що на основі статистичних даних сама від імені користувача підлагоджує роботи всіх інших систем.

Недостатній захист паролів, використання слабких або стандартних паролів для розумних пристроїв та систем може зробити їх вразливими до атак перебору паролів.

Неоновлене програмне забезпечення, брак регулярних оновлень програмного забезпечення може залишити системи розумного будинку вразливими до вже відомих атак та експлойтів.

Небезпека віддаленого доступу: віддалені функції керування розумним будинком через Інтернет можуть стати об'єктом атак, якщо не застосовані належні заходи безпеки, такі як двофакторна аутентифікація.

Несправжні чи неадекватно захищені мережі можуть дозволити несанкціонований доступ до розумних пристроїв.

Атаки на датчики та пристрої:Датчики руху, камери та інші пристрої можуть бути піддані атакам, якщо не використовуються шифрування та захист від вторгнень.

Розумні пристрої та платформи можуть збирати та використовувати персональні дані користувачів, що може призвести до проблем із безпекою та приватністю. Брак стандартів безпеки: багато розумних пристроїв виробляються різними виробниками і можуть не мати спільних протоколів безпеки. Це робить складніше створити єдину систему безпеки.

Атаки через Інтернет речей, оскільки взломані розумні пристрої можуть створювати ботнети або атакувати інші системи.

Атаки спаму та фішінгу через розумні пристрої можуть використовувати шляхи атаки, щоб шахрайським чином отримати доступ до систем.Недостатній фізичний захист пристроїв, таких як камери чи датчики, може зробити їх доступними для фізичного вторгнення.

Отже, як ми зрозуміли ми маємо дуже велику кількість різних платформ, пристроїв та програмних забезпечень для регулювання різних типів будинків та на певний бюджет який матимемо. Створювати Розумний будинок на базі однієї екосистеми зовсім не обов'язково. Поєднуючи різні відкриті рішення або розширюючи закриті за допомогою спеціальних мостів і шлюзів, можна домогтися синергетичного ефекту, отримавши, припустимо, українськомовного або іноземномовного голосового помічника і найширший асортимент недорогих датчиків та інших приладів. Але такій варіант підійде лише тим, хто досконально вивчив принципи роботи хоча б однієї екосистеми.

В іншому випадку ризики розчарування та зайвих витрат зростають, а не ефективність і економія коштів. Для того, щоб розумний будинок був безпечним, важливо використовувати надійні паролі, оновлювати програмне

забезпечення, застосовувати заходи безпеки мережі та використовувати тільки відомі та надійні виробники та платформи.

РОЗДІЛ 2: АНАЛІЗ СУЧАСНИХ МЕТОДІВ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ РОЗУМНОГО БУДИНКУ

2.1. Ідентифікація загроз та вразливостей у розумних будинках

Зростаюча зацікавленість людей у використанні підключених до Інтернету пристроїв у своїх домівках вимагає аналізу сучасних методів підвищення кібербезпеки розумного будинку. Оскільки багато пристроїв у таких системах можуть не мати достатнього кіберзахисту, розумні будинки можуть бути більш вразливими до кібератак.

Ідентифікація загроз і вразливостей розумного будинку — це процес виявлення потенційних ризиків і слабких місць у системі розумного будинку, які можуть бути використані кіберзлочинцями для несанкціонованого доступу, втрати даних або порушення приватності користувачів.

Для розумних будинків необхідний комплексний аналіз для виявлення загроз і вразливостей. Нижче наведено короткий опис цих етапів:

1) **Ідентифікація пристроїв і систем:**

Першим кроком є створення списку всіх підключених до мережі пристроїв та систем в розумному будинку. Це можуть бути смартфони, планшети, смарт-телевізори, камери, термостати, домофони, освітлення, розетки, дверні замки, системи відеоспостереження та багато інших пристроїв. На рисунку 2.1 зображено індетифікацію певних пристроїв та підключених систем.

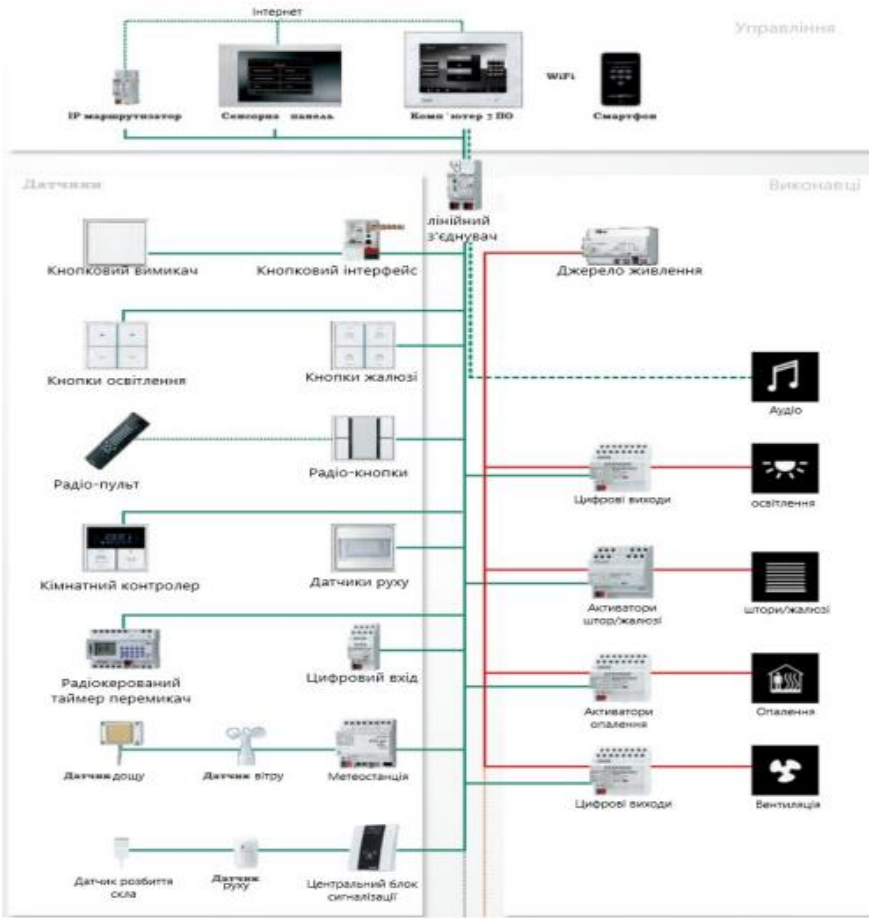


Рис. 2.1 Індетифікація підключених пристроїв та систем

2) **Збір інформації про кожен пристрій:**

Інформація, яка включає модель, виробник, версію програмного забезпечення, серійний номер, IP-адресу (якщо вони підключені до мережі) та інші важливі параметри, потрібна для кожного ідентифікованого пристрою. Ця інформація необхідна для управління та аналізу.

Ось деякі з ключових параметрів, які слід зібрати для кожного пристрою:

- Модель: Інформація про модель пристрою допомагає ідентифікувати його тип та призначення. Це може бути корисним для подальшого аналізу та визначення можливих загроз.

- Виробник: Зазначення виробника пристрою дозволяє визначити, хто виробив пристрій та чи він має добру репутацію в галузі кібербезпеки.
- Версія програмного забезпечення: Інформація про версію програмного забезпечення пристрою є важливою, оскільки оновлення програмного забезпечення часто містять виправлення безпеки. Важливо перевіряти, чи встановлено останні версії програмного забезпечення на всіх пристроях.
- IP-адреса: Якщо пристрій підключений до мережі, важливо знати його IP-адресу. Це допомагає в ідентифікації та моніторингу пристроїв у мережі, а також для виявлення можливих вторгнень.
- Серійний номер: Серійний номер пристрою є унікальним ідентифікатором, який дозволяє однозначно відокремити пристрій від інших. Він може бути корисним для ведення журналів та відстеження пристроїв.
- Параметри конфігурації: Деякі пристрої мають різні конфігураційні параметри, такі як налаштування мережі, паролі та інші параметри безпеки. Збір цих параметрів допомагає переконатися, що пристрої налаштовані безпечно.
- Заводські налаштування: Інформація про заводські налаштування пристрою може бути корисною для відновлення до заводського стану у випадку проблем або відновлення до заводських налаштувань після можливих атак.
- Доступність оновлень та патчів: Перевірка, чи є доступними оновлення та патчі для пристрою, є важливою для забезпечення безпеки. Збирайте інформацію про наявність оновлень та частоту їх випуску.

Збір цих параметрів для кожного пристрою допомагає створити повний інвентар розумного будинку, що є важливим для подальшого аналізу, аудиту безпеки та вживання заходів для запобігання загрозам та вразливостям. Як це показано на рисунку 2.2.

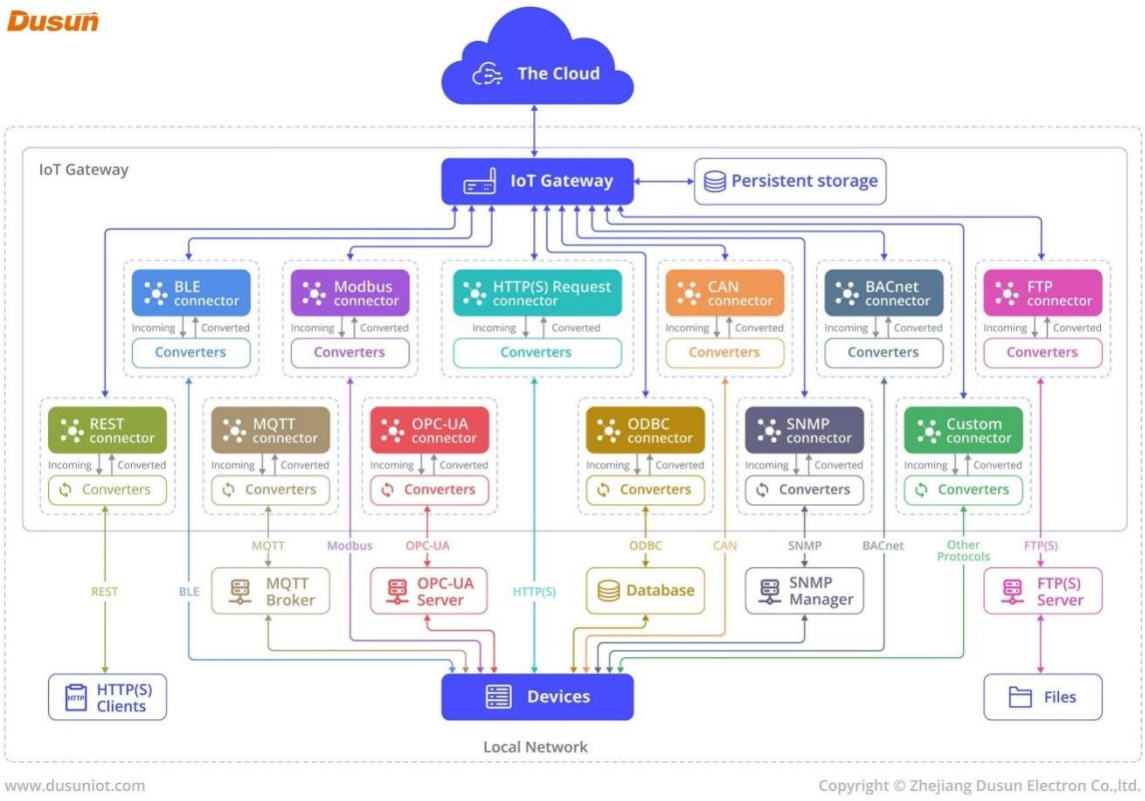


Рис.2.2 Збір інформації про кожен пристрій, приєднання та співпрацю

3) **Пошук документації і налаштувань:**

Перевірте інструкції, документацію, гарантійні картки та налаштування кожного пристрою. Це може містити важливі інструкції щодо безпеки, а також інші аспекти, які необхідно враховувати. Пошук інструкцій і документації щодо кожного пристрою розумного будинку є важливим етапом у забезпеченні кібербезпеки та правильній конфігурації цих пристроїв. З цієї інформації користувачі можуть краще зрозуміти пристрій, встановити правильні параметри безпеки та ефективно ним керувати.

Ось кілька кроків, які варто виконати під час пошуку документації та налаштувань для кожного пристрою:

– Почніть з перегляду коробки, в якій поставлявся пристрій, та будь-яких включених документів. Багато виробників додають короткі інструкції та посібники із загальними вказівками.
– Відвідайте офіційний веб-сайт виробника пристрою та пошукайте додаткову інформацію та документацію. Більшість виробників надають

інструкції та підтримку для своїх продуктів. Також деякі користувачі можуть ділитися своїми досвідами та порадами на інтернет-форумах та спільнотах, які присвячені конкретним пристроям. Це може бути корисним для знаходження додаткових вказівок та рекомендацій.

- Пошукайте та завантажте офіційну документацію виробника. Це може включати інструкції з налаштування, безпеки та технічні характеристики.
- Перевірте, чи в коробці з пристроєм є посібники користувача та гарантійні картки. Вони можуть містити важливі контактні дані для підтримки та рекомендації щодо безпеки.
- Перевірте налаштування самого пристрою. Деякі пристрої мають вбудовані інструкції та рекомендації щодо безпеки. Окремі пристрої мають компоненти додаткової безпеки, такі як паролі, антивірусне програмне забезпечення чи системи моніторингу.
- Вивчіть, як вони працюють та як їх налаштовувати. Пошукайте інформацію про журнали подій та збережені дані про безпеку пристрою.Це може допомогти виявити незвичайну активність та потенційні загрози.
- Перевірте, чи виробник надає оновлення програмного забезпечення та патчі для пристрою. Інформація про ці оновлення та процес їх встановлення може бути важливою для забезпечення безпеки.

4) **Перевірка оновлень:**

Переконайтеся, що всі системи та пристрої мають найновіші фірмові оновлення та версії програмного забезпечення. Усі оновлення, які включають виправлення безпеки, повинні бути встановлені вчасно. У розумному будинку дуже важливо регулярно перевіряти, чи всі підключені пристрої та системи оновлені. В залежності від можливостей вашого пристрою та рівня кібербезпеки він може бути щоденним, щотижневим або щомісячним.

Багато пристроїв мають функцію автоматичних оновлень, що дозволяє їм самостійно завантажувати та встановлювати доступні оновлення. Якщо

вона доступна, активуйте цю функцію для забезпечення постійної безпеки. Багато виробників надають фірмові оновлення для своїх пристроїв; ці оновлення можуть включати виправлення безпеки, а також нові функції та поліпшення.

Слід перевірити наявність цих оновлень і, якщо вони доступні, встановити їх. Пом’ятайте, що оновлення повинні завантажуватися з офіційних джерел виробників.

Оскільки завантаження програмного забезпечення або оновлень з ненадійних джерел може призвести до введення шкідливого програмного забезпечення, не завантажуйте їх. Перед встановленням оновлень вкрай важливо зробити резервне копіювання налаштувань і даних, які є критичними.

Це запобігає втрати даних у випадку проблем під час оновлення. Після встановлення оновлень слід ретельно перевірити пристрій на наявність проблем або змін у його роботі. Після оновлення слід негайно зв’язатися з виробником для допомоги.

Правильний процес перевірки та встановлення оновлень допомагає підтримувати високий рівень кібербезпеки в розумному будинку та захищати його від потенційних загроз.

5) **Перевірка паролів та аутентифікації:**

Переконайтеся, що для кожного пристрою створені сильні та унікальні паролі. Впевніться, що кожен пароль для розумних пристроїв у вашому домі є унікальним і сильним. Вони повинні містити як великі, так і малі літери, цифри та спеціальні символи. Уникайте використання простих паролів, таких як «пароль» або «123456». У розумному будинку необхідно регулярно змінювати паролі для всіх пристроїв. Зловмисники, які намагаються отримати несанкційний доступ, можуть зіткнутися з труднощами через це. Активуйте двофакторну аутентифікацію для своїх пристроїв і облікових записів, якщо це можливо. Цей додатковий шар захисту потребує додаткових компонентів, крім пароля, наприклад мобільного телефонного кода.

Використовуйте унікальні імена користувачів для кожного облікового запису.

Уникайте використання загальних або стандартних імен користувачів, які можуть стати легкою мішенню для атак. Також регулярно перевіряйте журнали доступу до своїх пристроїв, щоб виявити будь-яку незвичайну активність чи можливі спроби несанкційного доступу. Це дозволяє швидко реагувати на потенційні загрози. Багато розумних пристроїв поставляються зі стандартними паролями, які можна легко вгадати. Змініть їх негайно після встановлення пристрою, щоб уникнути вразливостей. Навчайте всіх членів сім'ї або користувачів про важливість безпечного використання паролів та методів аутентифікації. Усвідомленість щодо кібербезпеки може значно покращити загальний рівень захисту.

Використання сильних паролів та ефективних методів аутентифікації грає ключову роль у забезпеченні безпеки розумного будинку, допомагаючи уникнути можливих загроз та вторгнень. На рисунках 2.3 і 2.4 зображено створення та встановлення 2FAзахисту.

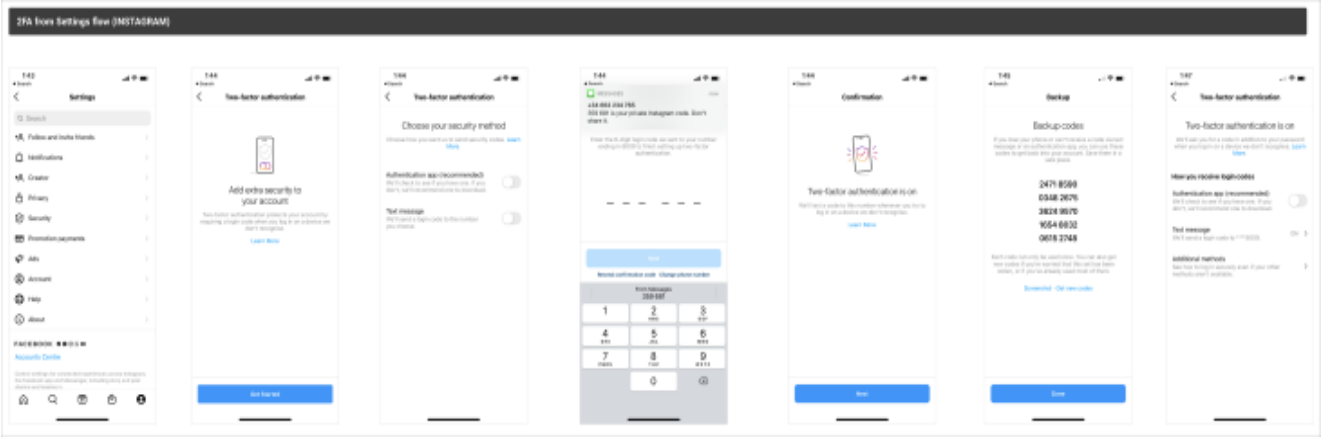


Рис.2.3

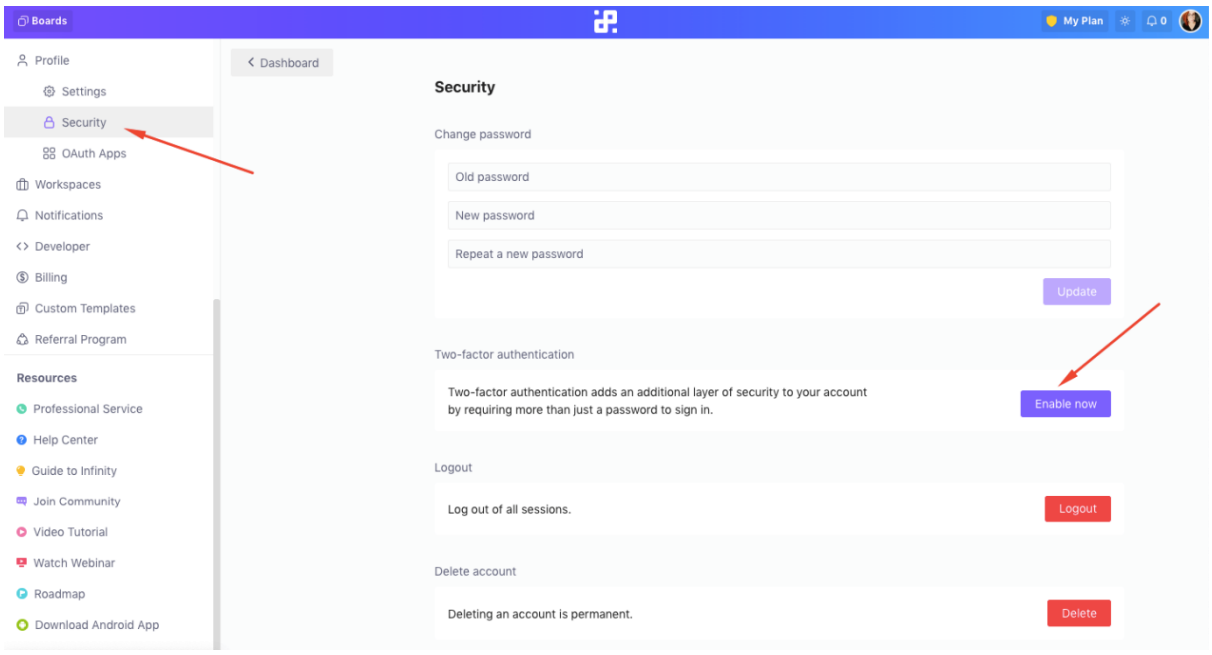


Рис 2.4

6) **Розділення мережі:**

Розгляньте можливість розділення мережі розумного будинку на дві частини: одну для пристроїв, які потребують доступу до Інтернету, і іншу для основних комп'ютерів та пристроїв з доступом до важливої інформації.

Розподіл мережі розумного будинку на дві частини для пристроїв з доступом до Інтернету та важливих комп’ютерів є розумним і ефективним способом забезпечення кібербезпеки. Це може забезпечити додатковий захист і зменшити ймовірність нападів. Розподіл мережі полегшує виявлення та обмеження потенційних небезпек. Одна частина мережі може бути атакована, але інша частина може залишатися безпечною та відокремленою. За допомогою сегментації можна точно регулювати правила доступу до пристроїв у кожному сегменті. Це означає, що пристрої, які мають доступ до важливих даних, можуть мати обмежений доступ до Інтернету та інших пристроїв, що зменшує ймовірність атак.

Пристрої, які не потребують прямого доступу до даних, залишаються віддаленими від основної мережі, де зберігаються комп’ютери та важливі дані. Це захищає важливі ресурси. Оскільки не кожен пристрій може отримати прямий доступ до всіх частин мережі, розділення мережі допомагає

зменшити поверхню атаки. Це може ускладнити зловмисникам атаку. Зменшення кількості пристроїв у кожній частині може призвести до більш ефективного управління та моніторингу мережі. Це полегшує виявлення аномалій і відповідь.

У разі атаки або компрометації одного сегменту мережі, інший сегмент може залишитися непорушеним. Це дає можливість використовувати резервне копіювання та відновлення для швидкого відновлення важливих даних.

Загально кажучи, розділення мережі є розумним стратегічним рішенням для підвищення кібербезпеки у розумних будинках, забезпечуючи більший контроль та захист важливих ресурсів.

7) **Встановлення мережевих фаєрволів:**

Встановіть мережеві фаєрволи для контролю трафіку та захисту від небажаних вторгнень. Вони допомагають заборонити небажаним особам доступ до мережі розумного будинку. Встановлення мережевих фаєрволів є ефективним заходом для контролю трафіку та захисту від потенційних небажаних вторгнень у розумному будинку.

Мережеві фаєрволи дозволяють забезпечувати загальний рівень безпеки, контролювати доступ до мережі та змінювати правила фільтрації пакетів даних. Мережевий фаєрвол може визначати, які з’єднання приймаються або відхиляються, щоб керувати як вхідним, так і вихідним трафіком. Це забезпечує фільтрацію небажаного трафіку та блокування потенційно небезпечних підключень. Мережевий фаєрвол може керувати доступом до мережі, фільтруючи порти та протоколи. Це має вирішальне значення для блокування певних типів трафіку та захисту від атак. Упровадження правил у мережевому фаєрволі дозволяє обмежувати доступ до певних програм і служб.Це зменшує вразливості та ризики.

Мережевий фаєрвол може дозволяти чи блокувати доступ до мережі в залежності від довіреності пристроїв чи мереж. Це дозволяє створити більш індивідуалізовані та безпечні налаштування. Важливим аспектом є

моніторинг роботи мережевого фаєрволу та ведення журналів подій. Це дозволяє виявляти аномалії, атаки та інші потенційно небезпечні події. Періодично оновлюйте програмне забезпечення мережевого фаєрволу та перевіряйте конфігурацію для виявлення можливих слабких місць або помилок. Мережевий фаєрвол допомагає захищати мережу від зовнішніх атак з Інтернету, а також від можливих загроз всередині мережі. Встановлення такиї фаєрволів в розумному будинку є критично важливим елементом для створення безпечного середовища та захисту ваших пристроїв від потенційних загроз.

8) **Моніторинг мережі:**

Використовуйте системи моніторингу мережі для виявлення аномальної активності та потенційних загроз на мережі розумного будинку. Використання систем моніторингу мережі є важливим елементом забезпечення кібербезпеки в розумному будинку. Ці системи дозволяють виявляти аномальну активність та потенційні загрози, що може вказувати на можливі атаки чи невірну роботу пристроїв. Системи моніторингу можуть аналізувати патерни трафіку та виявляти незвичайну чи аномальну активність, яка може бути ознакою атаки.

Моніторинг дозволяє виявити зміни в мережі, такі як додавання нових пристроїв, зміни в трафіку чи несподівані з’єднання. Такі системи можуть виявити потенційно небезпечні події, відстежуючи та аналізуючи журнали подій пристроїв і мережевих компонентів. Система моніторингу може автоматично сповістити адміністратора чи користувача про підозрілу активність, що дозволяє швидко реагувати на потенційні загрози. Крім того, моніторинг сприяє виявленню та вирішенню технічних проблем мережі, таких як збої в роботі пристроїв або втрата з’єднання. Відповідно до своїх потреб, користувачі можуть самостійно встановлювати параметри моніторингу, включаючи типові дії, які вважаються підозрілими. Раніше виявлення аномалій дозволяє швидше реагувати та ізолювати проблемні частини мережі, щоб мінімізувати наслідки.

Загально кажучи, системи моніторингу мережі є важливим інструментом для забезпечення безпеки в розумному будинку, дозволяючи вчасно виявляти та вирішувати потенційні загрози та проблеми.

9) **Використання віртуальних приватних мереж (VPN):**

Розгляньте використання віртуальної приватної мережі (VPN) для шифрування з'єднань у розумному будинку для додаткового забезпечення з'єднань і захисту приватності. Використання віртуальної приватної мережі (VPN) є хорошим способом захистити приватність і безпеку розумного будинку. Використання віртуального приватного протоколу (VPN) дозволяє шифрувати з'єднання та захистити конфіденційність даних, що передаються через Інтернет. Це особливо важливо для розумних пристроїв, які обмінюються чутливими даними. Обладнання віртуальної приватної мережі (VPN) запобігає перехопленню та відстеженню даних, які передаються через відкриті мережі.

Це особливо актуально для віддаленого керування розумними пристроями за межами дому. Використання VPN дозволяє залишати анонімними та захищеними ваший інтернет-трафік і особисту інформацію, забезпечуючи додатковий рівень конфіденційності. Якщо ви віддалено керуєте своїм розумним будинком, VPN забезпечить безпеку та шифрування підключення, запобігаючи можливі атаки чи перехоплення даних. Такі мережі дозволяють обходити обмеження географічного доступу до деяких ресурсів чи послуг, що може бути корисним для отримання доступу до контенту з будь-якої точки світу.

При використанні розумних пристроїв у відкритих мережах, таких як кав'ярні чи готелі, VPN допомагає захистити ваші дані від можливих атак та небажаних вторгнень. Використання VPN дозволяє зберігати контроль над інтернет-трафіком, що входить та виходить з вашого розумного будинку рисунок 2.5. Загалом, використання VPN у розумному будинку є додатковим заходом для забезпечення безпеки та захисту приватності в сучасному цифровому середовищі.

Рис. 2.5 VPN система для захисту ваших данних

10) **Навчання користувачів:**

Навчайте користувачів правилам кібербезпеки та як визначити підозрілі дії або повідомлення, що можуть вказувати на потенційні загрози.

Ключовим кроком у забезпеченні безпеки розумного будинку є навчання користувачів основам кібербезпеки. Існує менша ймовірність того, що користувачі стануть жертвами кіберзлочинців, чим більш освічені вони. Навчіть користувачів створювати надійні та унікальні паролі для своїх облікових записів. Поясніть, чому важливо використовувати різні паролі для різних сервісів і уникати поєднань, які легко впізнати. Навчіть людей ідентифікувати незвичайні або підозрілі дії в розумному будинку. Непередбачені повідомлення, неочікувані зміни в роботі пристроїв або інші аномалії можуть бути частиною цього.

Поясніть ризики соціальної інженерії та навчіть користувачів уникаєти розголошення особистої інформації чи відповіді на сумнівні повідомлення. Поясніть користувачам можливі ризики та переваги використання розумних функцій. Заохочуйте до обміркованого використання та обрання налаштувань, які максимально забезпечують безпеку. Навчіть розпізнавати фішингові атаки та уникати натискання на сумнівні посилання чи надсилання

особистої інформації через ненадійні канали. Підтримуйте постійну усвідомленість кібербезпеки через регулярні нагадування та оновлення щодо нових загроз та заходів безпеки. Навчання користувачів стає ключовим елементом створення безпечного середовища у розумному будинку, сприяючи зменшенню ризиків та підвищенню захищеності.

11) **Регулярний аудит безпеки:**

Проводьте регулярний аудит безпеки розумного будинку. Незалежні фахівці з кібербезпеки проводять детальний огляд систем та мережі розумного будинку. Вони визначають наявні ризики та перевіряють відповідність встановленим стандартам безпеки. Аудитори перевіряють версії програмного забезпечення та фірмове оновлення для всіх підключених пристроїв. Вони визначають, чи є актуальні оновлення, які містять виправлення безпеки. Фахівці перевіряють налаштування безпеки розумних пристроїв, роутерів та інфраструктури мережі. Вони визначають потенційні слабкі місця та рекомендують необхідні зміни. Здійснюється тестування на проникнення для виявлення слабких місць у системі безпеки.

Це включає в себе спроби вторгнення та перевірку ефективності заходів безпеки. Аудитори перевіряють системи автентифікації та керування доступом, визначаючи, чи вони відповідають вимогам безпеки та чи використовуються сильні паролі. Фахівці також аналізують журнали подій систем та пристроїв для виявлення підозрілих або аномальних активностей.

Це допомагає реагувати на можливі загрози вчасно. Після аудиту експерти надають детальні рекомендації щодо усунення виявлених вразливостей та покращення загальної безпеки системи. Аудитори повинні бути орієнтовані на останні кіберзагрози та тенденції, щоб враховувати їх при визначенні ризиків та розробці стратегій безпеки. Регулярний аудит безпеки допомагає розпізнавати та усувати потенційні загрози, забезпечуючи стійкий рівень кібербезпеки в розумному будинку.

Ці кроки створюють основу для детального аналізу ідентифікації загроз та вразливостей у розумних будинках та допомагають забезпечити їх

кібербезпеку та приватність користувачів. Усі ці етапи та заходи мають на меті створити надійне та безпечне середовище для користувачів розумних пристроїв, зменшуючи ризики кібератак та забезпечуючи конфіденційність та цілісність даних. Важливо постійно вдосконалювати стратегії кібербезпеки відповідно до зростаючих загроз та технологічних змін, щоб ефективно захищати розумний будинок в сучасному цифровому світі.

2.2. Аналіз сучасних методів кібербезпеки

Аналіз сучасних методів кібербезпеки свідчить про те, що цей сегмент технологій постійно розвивається для боротьби зі зростаючими загрозами та викликами в цифровому просторі. Нижче розглянуті деякі сучасні методи кібербезпеки:

Штучний інтелект та машинне навчання: Використання штучного інтелекту (ШІ) та машинного навчання (МН) дозволяє системам аналізувати величезні обсяги даних для виявлення аномалій та патернів.

Системи мають здатність самостійно реагувати на нові загрози та адаптуватися до змін, які відбуваються в кіберпросторі. Машинне навчання та штучний інтелект відіграють важливу роль у сучасних стратегіях кібербезпеки, оскільки вони пропонують ефективні методи виявлення та запобігання кіберзагрозам. МН і ШІ ефективно обробляють і аналізують великі кількості даних, знаходячи навіть дрібні аномалії, які можуть вказувати на потенційні кіберзагрози. Нові дані дозволяють цим системам навчатися та адаптуватися до змін у кіберпросторі. Це підвищує їхню ефективність у режимі реального часу, надаючи їм здатність ідентифікувати нові небезпеки та такі, що розвиваються.

Алгоритми штучного інтелекту та МН можуть виявити навіть тіньові патерни та зв’язки між даними, які людський аналіз може не помітити. ШІ допомагає виявляти нормальну та аномальну активність, передбачаючи

поведінку систем і користувачів. ШІ дозволяє системам швидко реагувати на потенційні загрози та мінімізувати збитки. Автоматизовані системи, які використовують ШІ та МН, можуть змінювати умови та контекст, щоб зменшити кількість помилкових спрацювань. Загалом, у кібербезпеці використання ШІ та МН робить захист від кіберзагроз більш інтелектуальним, гнучким і ефективним. Однак важливо пам’ятати, що ці технології потребують ретельного нагляду та конфігурації, щоб запобігти викривленням і зловживанню.

Zero Trust архітектура:На основі ідеї, що "ніщо і ніхто не повинен автоматично довіряти, навіть якщо він вже знаходиться всередині мережі", Zero Trust Architecture є інноваційним підходом до забезпечення кібербезпеки. Ця стратегія вирішує проблему традиційних мережевих методів, які ґрунтуються на створенні довіри до внутрішніх ресурсів. Важливість перевірки автентичності залишається високою, навіть для внутрішніх користувачів і пристроїв, серед основних елементів Zero Trust архітектури. Навіть якщо запит на доступ здійснюється в межах внутрішньої мережі, він повинен бути активно перевірений. Zero Trust базується на принципі найменших привілеїв, що означає, що користувачам і пристроям надаються лише ті права, необхідні для виконання певних завдань. Це допомагає зменшити ймовірність небажаного або шкідливого використання привілеїв. Мережа розділена на менші сегменти або зони, і між ними жорстко контролюється доступ. Це допомагає уникнути розповсюдження атак та обмежити їх вплив. Системи Zero Trust активно моніторять активність користувачів та пристроїв для виявлення аномалій або підозрілих дій. При виявленні незвичайної активності може застосовуватися автоматизована реакція або генерація сповіщень. Архітектура Zero Trust дозволяє динамічно змінювати політики безпеки в залежності від контексту, такого як місцезнаходження, тип пристрою чи стан безпеки для кожного юзера індивідуально, рисунок 2.6

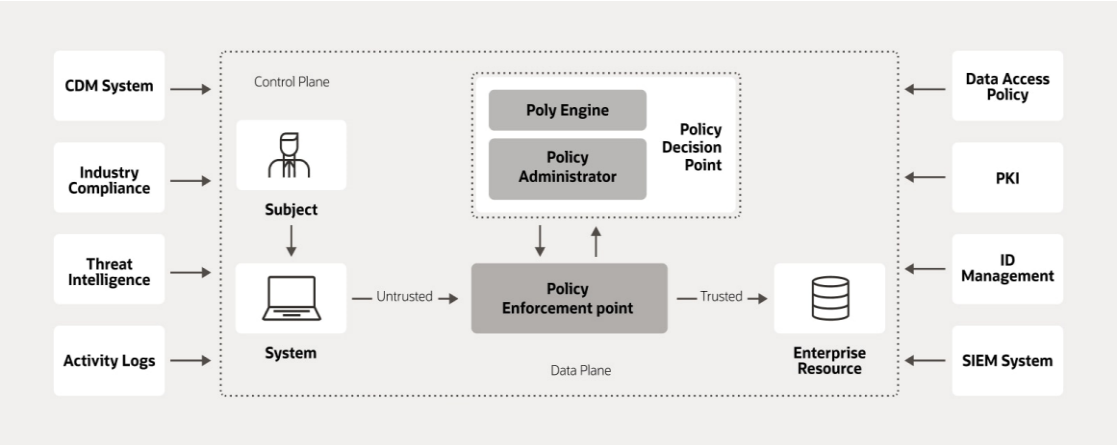


Рис. 2.6 ZeroTrust архітектура в системі розумний будинок

Впровадження ZeroTrust архітектури дозволяє створити дуже захищене кіберпросторове середовище, де кожен елемент є потенційною точкою входу для кіберзагроз, і кожен запит на доступ ретельно перевіряється та автоматизовано контролюється. Цей підхід є основоположним для сучасних стратегій кібербезпеки, спрямованих на забезпечення найвищого рівня захисту.

Багаторівнева аутентифікація:Використання багаторівневої аутентифікації, такої як введення паролю, у поєднанні з використанням біометричних даних або одноразових кодів, підвищує безпеку та робить більш складним спроби несанкціонованого доступу. Багаторівнева аутентифікація підвищує загальний рівень безпеки та створює додаткові перешкоди для несанкціонованого доступу, що робить її ефективним заходом кібербезпеки. Система, яка використовує кілька аутентифікаційних факторів, стає більш надійною, оскільки вона враховує різні елементи ідентифікації користувача. Під час використання одноразових кодів або токенів можна створити нетривалий елемент для ідентифікації, який стає недійсним після використання, що ускладнює несанкціонований доступ. Багаторівнева аутентифікація часто використовується для важливих або конфіденційних операцій, таких як фінансові транзакції або доступ до критичних систем.

Загалом, багаторівнева аутентифікація є корисним інструментом для підвищення рівня безпеки в цифровому світі. Вона є важливою частиною стратегій кібербезпеки, оскільки дозволяє забезпечити надійний захист від потенційних кіберзагроз.

Блокчейн для кібербезпеки:Дані охороняються та недоступні завдяки використанню технології блокчейн. Це особливо важливо для захисту даних і попередження кібератак на централізовані системи. Використовуючи систему розподіленого реєстру, блокчейн зберігає інформацію в блоках, кожен з яких містить хеш попереднього блоку. Це гарантує, що дані залишаються цілісними, оскільки будь-яка спроба змінити один блок призведе до змін у всіх наступних блоках. Зломщики блокчейну повинні атакувати багато комп’ютерів одночасно, щоб змінити інформацію. Це робить блокчейн складним для них, оскільки дані розподілені між кількома комп’ютерами, а не зберігаються в централізованому репозитарії.Блокчейн може використовуватися для створення безпечних систем автентифікації та авторизації, де доступ до даних або ресурсів контролюється за допомогою криптографічних ключів рисунок 2.7 показує можливості керування смарт будинком.

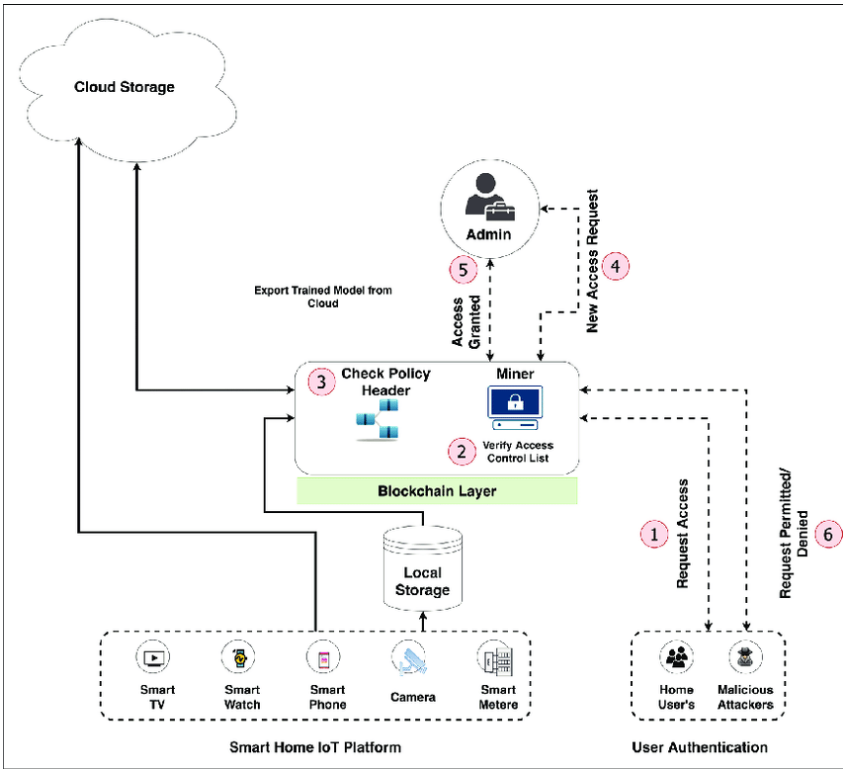


Рис.2.7 Блокчейн: від Юзера до Датчику

Блокчейн забезпечує можливість аудиту та відстеження кожної транзакції, що дозволяє виявити будь-які неправомірні або підозрілі дії. У випадку кібератаки, деякі блокчейн мережі можуть використовувати концепцію резервних копій для швидкого відновлення системи. В цілому, використання блокчейну в кібербезпеці сприяє створенню надійних та стійких до атак систем, де захист даних базується на розподіленому підході та криптографії. Наразі система Blockchain розповсюджується стрімкими кроками і це поки що один з найкращих варіантів для будинків та любих інших проектувань рисунок 2.8.

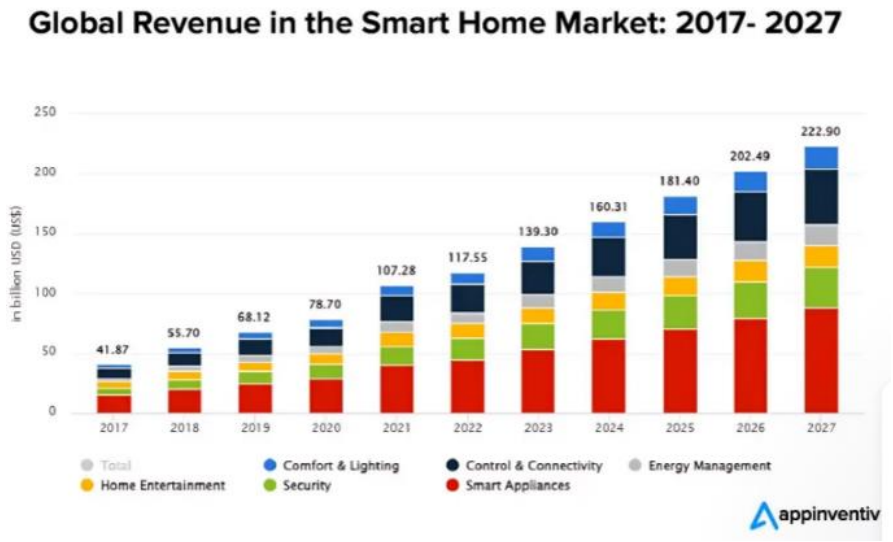


Рис. 2.8 Розповсюдження системи Blockchain

Інцидентний відгук та відновлення:Плани інцидентного відгуку та відновлення організації можуть швидко реагувати на кібератаки, відновлювати роботу та мінімізувати збитки. Щоб план був ефективним, він повинен містити чіткі правила та обов'язки для швидкого виявлення, класифікації та відповіді на кіберінциденти. Команда повинна бути готовою негайно взяти під контроль ситуацію. План повинен включати аналіз інциденту, який включає визначення причин, розміру та впливу. Це допоможе вирішити проблему на корені та запобігти подальшим подібним ситуаціям.

Хмарна безпека: Застосування спеціальних засобів безпеки для хмарних сервісів, які враховують унікальні аспекти обчислення в хмарі та забезпечують захист даних, які зберігаються та обробляються в хмарі як показано на рисунках 2.9-2.10. Хмарна безпека може бути важливим методом кібербезпеки для систем розумного будинку. Особливості використання хмарної безпеки в системах розумного будинку включають:

- Хмарні сервіси дозволяють централізовано зберігати дані, зібрані від різних пристроїв у розумному будинку. Це спрощує управління та забезпечує однаковий рівень безпеки для всіх інформаційних активів.

- Застосування механізмів шифрування для забезпечення конфіденційності даних, які зберігаються в хмарі та передаються між системою розумного будинку та хмарними серверами.
- Застосування ефективного контролю доступу, який обмежує права користувачів до конкретних функцій та пристроїв у розумному будинку. Ідентифікація та авторизація користувачів використовуються для підтвердження їхньої легітимності.
- Використання заходів для запобігання мережевим атакам та захисту від кіберзагроз, що можуть впливати на пристрої та системи у розумному будинку.
- Забезпечення високого рівня фізичної безпеки серверів та обладнання, яке обробляє дані розумного будинку в хмарі.
- Захист мережевих з'єднань між пристроями у розумному будинку для запобігання несанкційованому доступу та перехопленню комунікацій.

Використання хмарної безпеки у системах розумного будинку допомагає покращити загальний рівень захисту, спрощує управління та забезпечує доступ до передових засобів кібербезпеки.

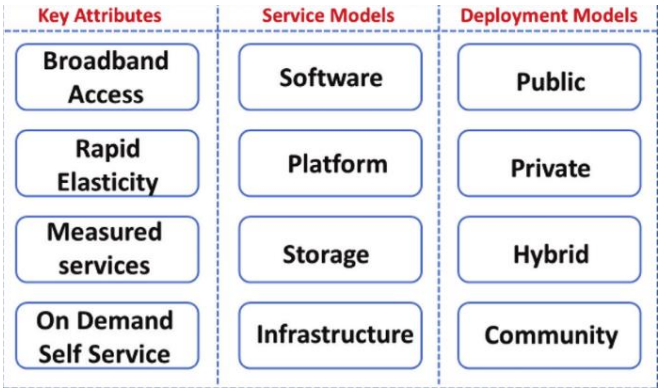


Табл. 2.9 Таблиця хмарних сховищ

KeyAttributes- ключові атрибути; DeploymentModels – Моделі розгортання.

ServiceModels – Сервісні моделі

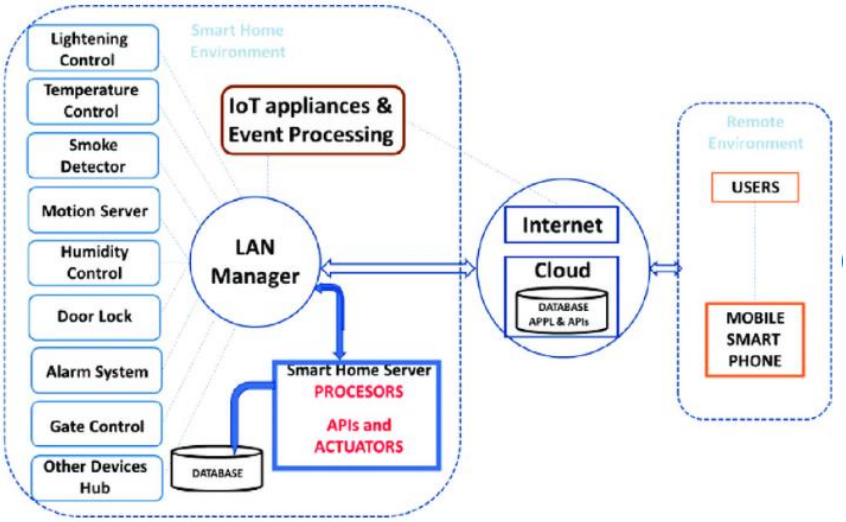


Рис. 2.10 Схема роботи хмарного сховища

Захист Інтернету речей (IoT): Розробка спеціалізованих рішень для захисту великої кількості підключених пристроїв, що складають Інтернет речей, від кіберзагроз. Захист Інтернету речей (IoT) виступає як ключовий метод забезпечення кібербезпеки в системах розумного будинку. Основні аспекти цього заходу включають:

- Шифрування даних: Використання шифрування для захисту передачі та зберігання даних між підключеними пристроями у розумному будинку. Шифрування забезпечує конфіденційність інформації та унеможливлює несанкціонований доступ.
- Управління аутентифікацією: Встановлення ефективних механізмів аутентифікації для всіх підключених пристроїв, щоб гарантувати, що лише легітимні пристрої мають доступ до системи розумного будинку. Це допомагає уникнути атак ідентифікації та забезпечує безпеку користувачів.
- Моніторинг активності пристроїв: Встановлення систем моніторингу, які слідкують за активністю підключених пристроїв. Вчасне виявлення аномальної поведінки дозволяє швидко реагувати на потенційні загрози.

- Регулярні оновлення програмного забезпечення: Забезпечення можливості регулярного оновлення власного програмного забезпечення та вбудованих систем кожного підключеного пристрою. Оновлення часто включають патчі безпеки, які виправляють виявлені вразливості.
- Власне програмне забезпечення (Firmware) та програмні оновлення: Забезпечення безпечної та ефективної процедури для оновлення власного програмного забезпечення підключених пристроїв. Це важливо для виправлення потенційних вразливостей та підтримання надійності системи.
- Фізична безпека пристроїв: Захист фізичного доступу до підключених пристроїв, щоб уникнути можливостей фізичних атак та несанкціонованого доступу.
- Захист від мережевих атак: Застосування заходів для виявлення та захисту від мережевих атак, таких як атаки відмови в обслуговуванні (DDoS) чи атаки на мережеві протоколи.

Загальна мета заходів з захисту Інтернету речей у системі розумного будинку полягає в забезпеченні конфіденційності, цілісності та доступності даних, а також уникненні потенційних кіберзагроз.

Сучасні методи кібербезпеки прагнуть до комплексності та адаптивності, щоб ефективно протистояти загрозам у цифровому середовищі, які постійно змінюються. Ці методи враховують високий рівень інтелектуалізації та глобалізації кіберпростору, забезпечуючи високий рівень захисту та відповідь на потенційні атаки.

2.3. Висновки до 2 розділу

Забезпечення кібербезпеки приватного будинку вимагає використання широкого спектру методів і стратегій. Щоб гарантувати захист від потенційних кіберзагроз, необхідно починати з виявлення небезпек і вразливостей.

Ідентифікація систем і пристроїв є важливим етапом. Важливо скласти повний список підключених пристроїв і зібрати важливу інформацію про кожен з них. Це створює основу для подальшого аналізу та управління безпекою.

Збір інформації про пристрій, пошук інструкцій і налаштувань, перевірка оновлень програмного забезпечення, перевірка паролів і аутентифікації, розділення мережі та встановлення мережевих фаєрволів є частиною детального аналізу загроз і вразливостей.

Додаткові дії, такі як використання віртуальної приватної мережі (VPN), навчання користувачів правилам кібербезпеки та регулярний аудит безпеки, доповнюють стратегію та сприяють підвищенню рівня захисту розумного будинку.

Ці кроки та заходи мають на меті створити безпечне та надійне середовище для користувачів розумних пристроїв, зменшуючи ймовірність кібератак і гарантуючи конфіденційність і цілісність даних. Щоб ефективно захистити розумний будинок у сучасному цифровому світі, важливо постійно вдосконалювати стратегії кібербезпеки, щоб реагувати на зростаючі загрози та зміни в технологіях.

Після перегляду сучасних стратегій кібербезпеки стає очевидним, що захист систем розумного будинку вимагає комплексного та детального підходу. Ідентифікація загроз і вразливостей починається з ідентифікації систем і пристроїв, а також перевірки та ідентифікації їхньої документації.

Збір інформації про кожен пристрій дозволяє створити основу для управління безпекою та аналізу.

Перевірка паролів і використання аутентифікації для забезпечення надійних і унікальних доступів є важливим етапом. Встановлення мережевих фаєрволів і розділення мережі збільшують безпеку мережі розумного будинку та обмежують ризики атак.

Використання методів Zero Trust і багаторівневої аутентифікації, а також технологій, таких як машинне навчання та штучний інтелект, підвищує рівень детекції та захисту. Регулярний аудит безпеки та використання блокчейну дозволяють ефективно протистояти постійно зростаючим кіберзагрозам.

Хмарна безпека визначається як важлива частина стратегії безпеки, зокрема використання шифрування даних і управління доступом у хмарі. Розроблені методи захисту необхідні враховуючи вимоги систем розумного будинку, таких як Інтернет речей.

Загалом можна сказати, що безпека систем розумного будинку вимагає поєднання новітніх технологій і традиційних методів. Захист розумного будинку від загроз шляхом постійного моніторингу та навчання користувачів є важливою частиною ефективної стратегії кібербезпеки.

РОЗДІЛ 3: УДОСКОНАЛЕННЯ ІСНУЮЧИХ МЕТОДІВ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ РОЗУМНОГО БУДИНКУ

3.1. Розробка та вдосконалення алгоритмів шифрування та автентифікації

Розробка та вдосконалення алгоритмів шифрування та автентифікації є ключовими елементами у забезпеченні кібербезпеки розумного будинку.Головне завдання шифрування полягає в збереженні данних та забезпеченні захисту від їх взламування приклад зображений на рисунку 3.1

Рис.3.1 Приклад шифрування данних

Ось кілька напрямків для розробки та вдосконалення цих алгоритмів:

1. **Шифрування:**

-Квантова криптографія:

Вивчайте можливість використання квантової криптографії для створення шифрування, яке стійке навіть перед квантовими обчисленнями.

Основна ідея полягає в тому, щоб використовувати властивості квантових частинок (квантових бітів або кубітів) для створення безпечних комунікаційних каналів, які неможливо скомпрометувати без зміни фізичних властивостей самого каналу. Квантовий ключовий обмін використовує принципи квантової необоротності. За допомогою квантових бітів, дві сторони можуть обмінювати ключі таким чином, що будь-яке спостереження чи спроба взлому ключа стає виявленою. Використовуючи квантовий ентанглемент, сторони можуть забезпечити стан кубітів, який буде взаємозалежним. Зміна одного кубіту негайно відобразиться на стані іншого,

що дозволяє виявити будь-яку спробу зміни інформації. Неклонові теореми квантової механіки стверджують, що неможливо створити точну копію невідомого квантового стану. Це дає можливість виявити будь-яку спробу перехоплення квантового ключа. Деякі криптографічні схеми, використовуючи квантові принципи, можуть бути стійкими до атак, заснованих на швидкому розширенні обчислювальних можливостей, таких як квантові обчислення. Дивитись на рисунок 3.2.

Рис. 3.2 Класифікація квантової криптографії

-Мультифакторна шифрація:

Розглядайте використання більше одного методу шифрування для кожного підключення, що забезпечить додатковий рівень безпеки.

Мультифакторна аутентифікація (MFA) - це метод аутентифікації, який використовує два або більше незалежних методів для підтвердження ідентичності користувача. У контексті шифрування та безпеки, MFA може бути використана для захисту від несанкціонованого доступу до розумного будинку та його пристроїв. Основні елементи MFA включають:

- Щось, що ви знаєте: Це може бути традиційний пароль або PIN-код.

- Щось, що ви маєте: Це може бути фізичний об'єкт, такий як токен, смарт-карта або USB-ключ.
- Щось, що ви - біометричний параметр: Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя, сканування очей, для підтвердження ідентичності.

Принцип MFA полягає в тому, що, навіть якщо один фактор доступу стає відомим чи компромітованим, інші фактори залишаються для забезпечення безпеки. Такий підхід ускладнює завдання несанкціонованого доступу, оскільки зловмиснику необхідно зламати не тільки один, а кілька різних захистів.

При впровадженні MFA для шифрування та безпеки розумного будинку важливо: обирати різноманітні фактори для максимальної ефективності, забезпечувати можливість легкої і безпечної реєстрації та керування факторами аутентифікації, використовувати стандарти протоколів безпеки для взаємодії між пристроями та платформами.

MFA є ефективним інструментом для усунення багатьох загроз безпеці в розумних будинках та інших системах, де забезпечення безпеки даних є пріоритетом.

-Диференційована шифрація для певних пристроїв.

Диференційована шифрація для конкретних пристроїв - це підхід до застосування різних методів шифрування для різних пристроїв у розумному будинку. Замість того, щоб використовувати один загальний алгоритм шифрування для всіх пристроїв, можна вибрати та налаштувати різні методи шифрування для кожного конкретного пристрою, залежно від його функціональності та рівня чутливості даних.

Основні переваги диференційованої шифрації для конкретних пристроїв:

- Дозволяє вибирати алгоритми шифрування відповідно до особливостей та потреб кожного конкретного пристрою. Наприклад, пристрої, що зберігають чутливі особисті дані, можуть використовувати більш стійкі алгоритми, ніж ті, які просто управляють освітленням.
- Забезпечує можливість використовувати потужніші алгоритми для пристроїв, які вимагають вищого рівня безпеки, тим самим зменшуючи ризик компрометації.
- Дозволяє використовувати менш ресурсоємні алгоритми для пристроїв з обмеженими обчислювальними ресурсами, що дозволяє зберігати ефективність роботи системи.
- Спрощує процес управління та обслуговування системи безпеки, оскільки кожен пристрій може мати свій власний набір шифрувань та ключів.

В разі компрометації одного пристрою, решта системи може залишитися безпечною, оскільки шифрування та ключі для кожного пристрою відрізняються.

2. Аутентифікація:

а. Біометричні технології:

Біометричні технології використовують унікальні фізіологічні або поведінкові характеристики особи для ідентифікації та аутентифікації. Основні біометричні характеристики включають відбитки пальців, розпізнавання обличчя, розпізнавання рис, сканування очей, голосові та пальцеві геометричні характеристики.

Переваги використання біометричних технологій включають високий рівень точності та унікальність, важливість в спрощенні процесу аутентифікації для користувачів та виключення можливості втрати або забування аутентифікаційних засобів. Однак такі технології також можуть стикатися із питаннями приватності та можливістю обхідних методів атак.

b. Двоетапна аутентифікація (2FA) про яку я розповідав у 2 розділі та багатофакторна аутентифікація (MFA) рисунок 3.3

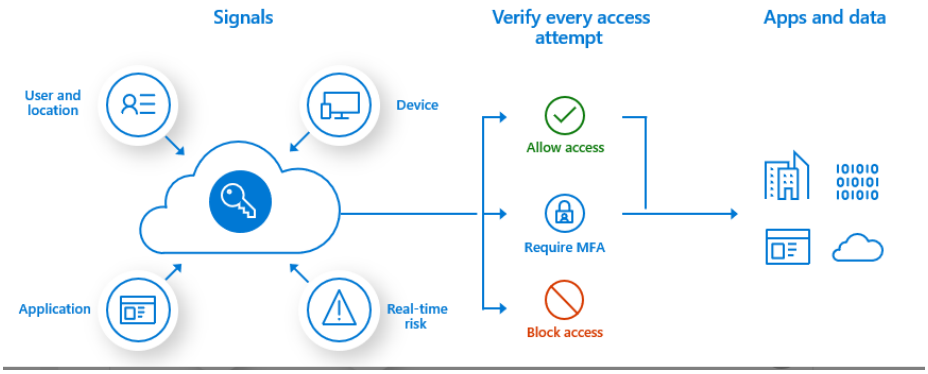


Рис.3.3 Система MFA

Застосовуйте 2FA та MFA для створення додаткових бар'єрів для несанкціонованого доступу. Використання двоетапної аутентифікації (2FA) та багатофакторної аутентифікації (MFA) є ефективними заходами для забезпечення додаткового рівня безпеки та ускладнення несанкціонованого доступу. Ось, як ці методи можуть бути застосовані у контексті кібербезпеки розумного будинку:

- 2FA для входу:

Користувачі, які намагаються отримати доступ до системи розумного будинку, повинні вводити не лише пароль, але й додатковий елемент аутентифікації. Це може бути одноразовий код, який відправляється на мобільний телефон користувача або генерується за допомогою аутентифікаційного додатку.

- MFA для різних пристроїв:

Враховуючи, що розумний будинок може містити різні пристрої (камери, термостати, розетки, тощо), важливо застосовувати різні методи аутентифікації для кожного пристрою. Наприклад, для камер може використовуватися аутентифікація на основі обличчя, а для управління температурою - аутентифікація за допомогою біометричних даних.

- Фактори аутентифікації:

Використовуйте різні фактори для 2FA або MFA. Наприклад, можна комбінувати щось, що користувач знає (пароль), і щось, що він має (одноразовий код або біометричні дані).

- Системи моніторингу та аналізу:

Застосовуйте системи моніторингу та аналізу для виявлення аномальних дій та можливих атак. Наприклад, велика кількість невдалих спроб входу може спричинити вимогу до додаткового підтвердження.

Застосування 2FA та MFA дозволяє ускладнити завдання несанкціонованого доступу та підвищити рівень безпеки розумного будинку.

c. Застосування блокчейну для аутентифікації:

Розглядайте можливість використання технології блокчейн для забезпечення довірливості і безпеки аутентифікаційних процесів. Застосування блокчейну для аутентифікації може внести значний внесок у покращення безпеки та надійності процесів аутентифікації. Ось декілька способів, які блокчейн може бути використаний для підвищення безпеки аутентифікації:

- Блокчейн може слугувати основою для децентралізованих систем аутентифікації. Користувачі можуть мати унікальний цифровий ідентифікатор, який зберігається в блокчейні, а доступ до нього контролюється за допомогою приватних ключів.
- Кожен користувач може мати свій цифровий ідентифікатор, який зберігається в блокчейні і підтверджує його ідентичність. Цей ідентифікатор може бути самоуправляється, і користувач може контролювати, які конкретні атрибути своєї ідентичності він дозволяє іншим сторонам переглядати.
- Застосування блокчейну дозволяє створити безпечний простір для обміну аутентифікаційною інформацією між різними довіреними

сторонами. Система може використовувати розподілений реєстр для відстеження та підтвердження аутентифікаційних подій.

- Інформація про аутентифікацію може бути збережена в блокчейні як імутабельний запис. Це зменшує ризик фальсифікації чи зміни аутентифікаційних даних.
- Блокчейн може дозволяти користувачам надавати доступ до свого ідентифікатора або аутентифікаційних атрибутів в обмін на певні послуги чи функції.
- Використання блокчейну для створення систем віртуальних ідентичностей дозволяє користувачам управляти своєю ідентичністю в цифровому просторі та використовувати її для аутентифікації в різних сервісах.
- Блокчейн може слугувати централізованою точкою аутентифікації для різних систем і додатків, забезпечуючи консистентність та високий рівень безпеки.

Використання блокчейну для аутентифікації може покращити безпеку та прозорість процесів ідентифікації, а також надати користувачам більший контроль над своєю особистою інформацією.

3. Загальні заходи:

a. Стійкість до квантових обчислень:

Стійкість до квантових обчислень — це важливий аспект при розробці криптографічних систем, оскільки квантові комп'ютери можуть представляти загрозу для багатьох традиційних криптографічних алгоритмів. Квантові обчислення можуть ефективно вирішувати проблеми, які зараз важко або навіть неможливо розв'язати за допомогою класичних обчислень, зокрема, факторизація чисел та розв'язання дискретного логарифму. Розглядайте використання алгоритмів, стійких до квантових обчислень, для забезпечення тривалої ефективності шифрування.

b. Стійкість до атаки перебором:

Стійкість до атаки перебором є ключовим аспектом криптографічної безпеки. Атака перебором полягає в спробах визначити секретний ключ, пароль чи іншу конфіденційну інформацію, шляхом спроб усіх можливих комбінацій. Щоб забезпечити стійкість до таких атак, використовуються різні стратегії та методи: збільшення довжини секретного ключа чи пароля ускладнює атаку перебором, використання криптографічних алгоритмів, які вважаються сильними, зменшує ймовірність успішної атаки перебором, введення обмежень на кількість невдалих спроб введення пароля чи ключа може знизити ефективність атаки перебором, застосування механізмів захисту, таких як капча, які ускладнюють виконання автоматизованих атак перебором, системи повинні бути налаштовані для моніторингу невдалих спроб та своєчасного реагування на аномальну активність, наприклад, блокування облікового запису після певної кількості невдалих спроб.

Всі ці заходи спрямовані на ускладнення процесу атаки перебором та підвищення вартості та часу, необхідного для успішного злому криптографічної системи.

c. Машинне навчання для виявлення загроз:

Використання машинного навчання для виявлення загроз у сфері кібербезпеки є актуальним та ефективним підходом. Машинне навчання може виявляти аномалії, визначати вразливості та реагувати на потенційні загрози в реальному часі.

d. Стандарти безпеки:

Дотримуйтеся останніх стандартів безпеки та активно взаємодійте з галузевими організаціями.

Регулярні аудити та тестування на проникнення також є важливою частиною процесу вдосконалення кібербезпеки. Важливо надавати пристроям оновлення для виправлення виявлених вразливостей.

3.2. Оптимізація контролю доступу та визначення прав доступу

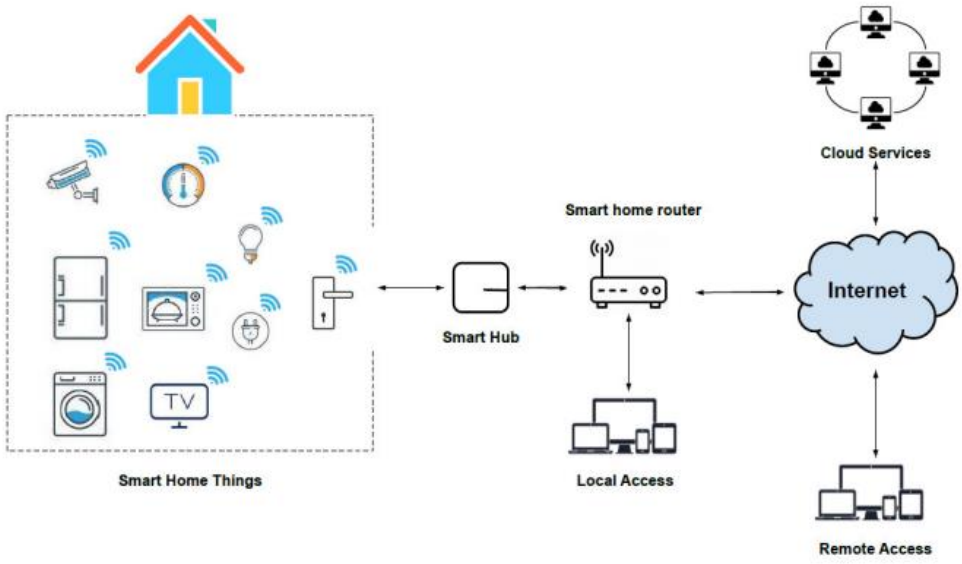
Оптимізація контролю доступу та визначення прав доступу важлива для ефективного та безпечного управління ресурсами інформаційних систем. Нижче подано кілька стратегій та практик, які можуть бути використані для цих цілей:

1. Розумний рольовий контроль доступу (RBAC):

Розумний рольовий контроль доступу (RBAC) — це метод управління правами доступу, який базується на присвоєнні ролей користувачам і наданні прав доступу на основі цих ролей. Це ефективний спосіб забезпечити безпеку та визначення прав в інформаційних системах. Основні елементи RBAC включають:

- Ролі: Роль представляє собою набір прав доступу, які пов'язані з конкретною функцією чи позицією в організації. Наприклад, адміністратор, менеджер, користувач, тощо.
- Користувачі: Користувачі в системі призначаються для виконання конкретних ролей. Один користувач може мати багато ролей, а роль може бути призначена багатьом користувачам.
- Права доступу: Права доступу визначають ті дії, які користувач може виконати в межах своєї ролі. Це може включати доступ до конкретних функцій системи, перегляд чи редагування певних даних, тощо.
- Політики безпеки: RBAC може включати в себе встановлення політик безпеки, що визначають, які комбінації ролей та користувачів можуть виконувати певні дії.
- Управління життєвим циклом ролей (RLCM): RLCM визначає процеси додавання, зміни та видалення ролей у системі з часом. Це важливо для забезпечення актуальності та відповідності системи змінюючимся умовам.

- Централізоване управління: Зазвичай використовується централізована адміністративна консоль чи інші інструменти для централізованого керування ролями та правами доступу.
- Диференціація завдань: Забезпечення того, що ролі визначаються чітко та відповідають функціональним обов'язкам конкретних користувачів.
- Аудит та звітність: Забезпечення можливості ведення журналів подій для відстеження, які користувачі мають які права доступу, і аналізу цих даних для виявлення аномалій.



- **Рис.3.4 Запровадження системи RBAC в SmartHouse**

Для визначення моделі RBAC визначаються наступні умови:

- S = Суб'єкт = Людина або автоматизований агент (множина користувачів);
- R = Роль = Робоча функція або назва, яка визначається на рівні авторизації (множина ролей);
- P = Дозволи = Затвердження режиму доступу до ресурсу (множина прав доступу на об'єкти системи);
- SE = Сесія = Відповідність між S, R та / або P
- SA = Призначення суб'єкта

- PA: R → 2p — функція, що визначає для кожної ролі множину прав доступу; при цьому для кожного p ∈ P існує r ∈ R така, що p ∈ PA (r);
- RH = Частково впорядкована ієрархія ролей. RH може бути ще записана так:
    - Один суб'єкт може мати кілька ролей.
    - Одну роль можуть мати декілька суб'єктів.
    - Одна роль може мати кілька дозволів.
    - Один дозвіл може належати кільком ролям.

Ролі призначаються суб'єктам, внаслідок чого суб'єкти отримують ті чи інші дозволи через ролі. RBAC вимагає саме такого призначення, а не прямого призначення дозволів суб'єктам, інакше це призводить до складно контрольованих відносин між суб'єктами і дозволами.

На можливість успадкування дозволів від протилежних ролей накладається обмежувальна норма, яка дозволяє досягти належного поділу режимів. Наприклад, одній і тій же особі може бути не дозволено створити обліковий запис для когось, а потім авторизуватися під цим обліковим записом.

Використовуючи нотацію теорії множин:

- $PA \subseteq P \times R$, при цьому дозволи призначаються зв'язкам ролей у відношенні «багато до багатьох».
- $SA \subseteq S \times R$, при цьому суб'єкти призначаються зв'язкам ролей і суб'єктів у відношенні «багато до багатьох».
- $RH \subseteq R \times R$

Позначення: x ≥ y означає, що x успадковує дозволи y.

Суб'єкт може мати множину одночасних сесій з різними дозволами.

Розумний рольовий контроль доступу є ефективним механізмом для керування доступом до ресурсів та забезпечення безпеки в інформаційних системах, де важливо контролювати доступ користувачів на основі їх ролей та відповідальностей.

2. Принципнайменшихпривілеїв (Principle of Least Privilege, PoLP):

Принципнайменшихпривілеїв (Principle of Least Privilege, PoLP) — цеконцепція, згіднозякоюкожнийкористуваччисистемнийпроцесповиненматилишетіправад оступу, якінеобхіднідлявиконаннясвоїхфункційчизавдань. Іншими словами, користувачеві надаються мінімально необхідні привілеї для виконання його роботи. Це зменшує ризик вразливостей та злому, оскільки навіть якщо облікові дані користувача будуть компрометовані, атакуючий не матиме повного доступу до системи чи інших важливих ресурсів.

Кожен користувач або системний процес має отримувати лише ті привілеї, які необхідні для виконання конкретної роботи. Доступ до ресурсів повинен обмежуватися тільки необхідними діями. Наприклад, користувачеві може бути надано право на читання файлу, але не на його зміну. Призначайте привілеї та доступ лише на той час, коли вони є фактично необхідними. Після закінчення роботи доступ може бути відкликаний. Ведіть журнали подій, щоб виявити аномальні чи неправомірні дії та вчасно реагувати на них. Користувачі та системні процеси повинні втрачати надлишкові привілеї після закінчення необхідної роботи. Розділіть завдання та обов'язки між різними користувачами або процесами для зменшення можливості розповсюдження зловмисного коду чи вразливостей. У випадку невизначеності або сумніву надавайте менше привілеїв, а не більше. Тобто, встановлюйте більш суворі політики безпеки.

Принцип найменших привілеїв є ключовим елементом стратегії безпеки та важливим компонентом забезпечення конфіденційності, цілісності та

доступності систем та інформації ось як відбувається принцип PoLP рисунок 3.5-3.8.

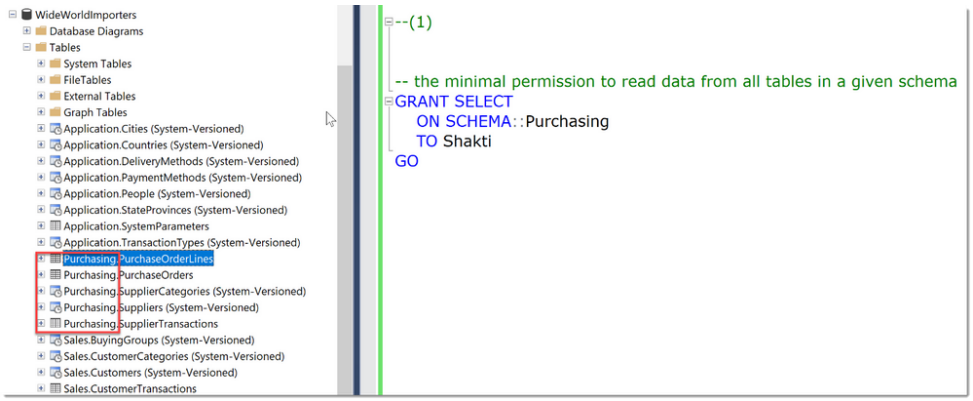


Рис.3.5 PoLP

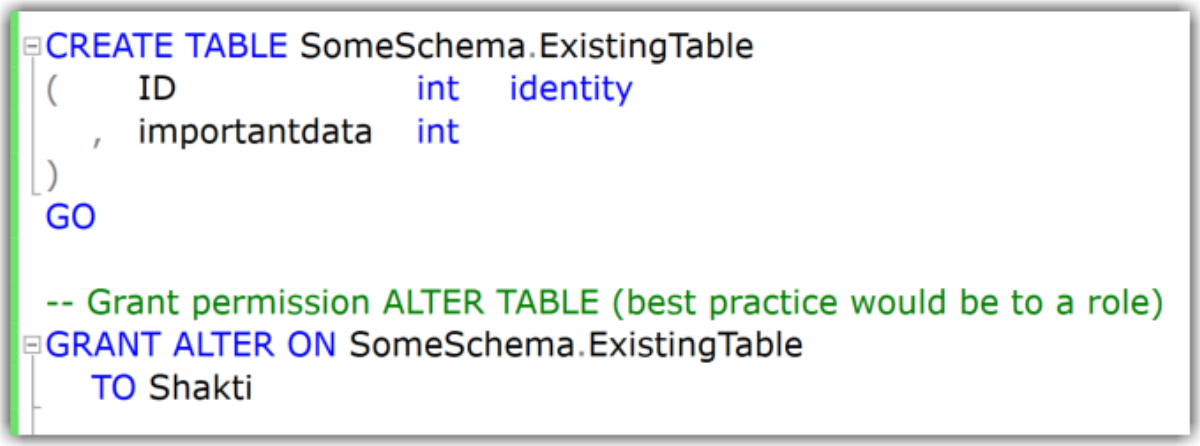


Рис.3.6 PoLP

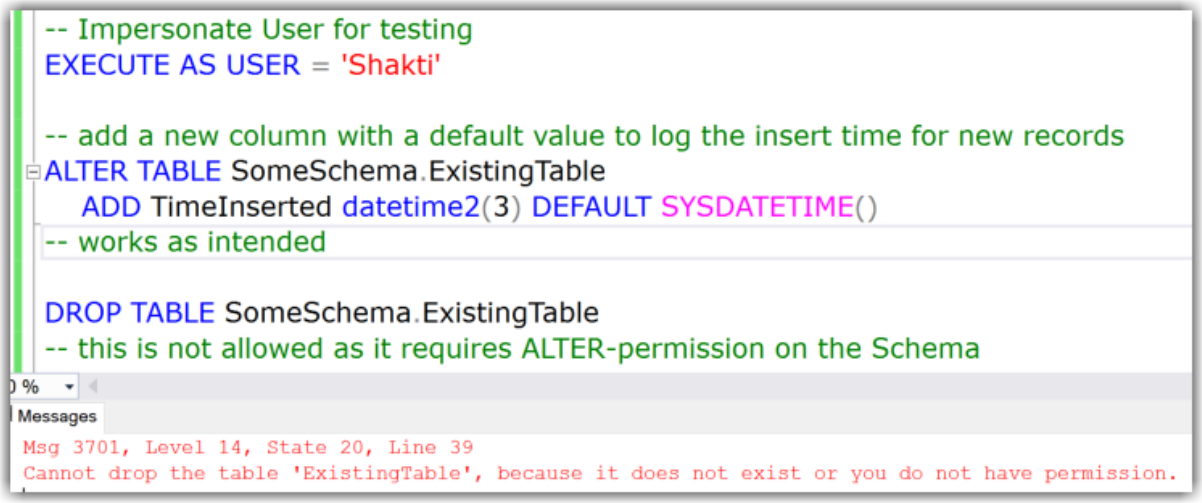


Рис.3.7 PoLP

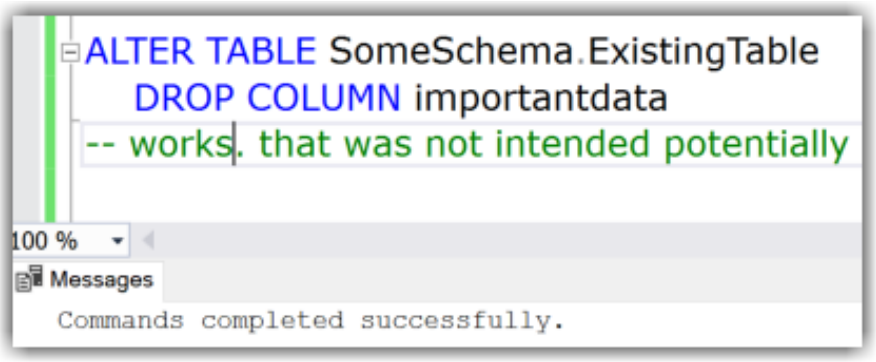


Рис.3.8 PoLP

3. Аудит та моніторинг:

Аудит та моніторинг є важливими елементами стратегії кібербезпеки, які дозволяють виявляти та реагувати на потенційні загрози та аномалії в інформаційній системі.

Система повинна вести журнали подій, реєструючи дії користувачів, події безпеки та зміни в системі. Ці журнали можуть бути використані для виявлення потенційних загроз і слідування діяльності користувачів. Використовуйте системи виявлення вторгнень (Intrusion Detection Systems, IDS) та системи виявлення аномальної поведінки (Anomaly Detection Systems), щоб виявляти незвичайні чи підозрілі активності, які можуть бути індикаторами атаки.

Слідкуйте за трафіком у мережі для виявлення підозрілих або нормальних патернів, які можуть свідчити про атаку чи компрометацію системи. Розробіть процедури реагування на події, щоб вчасно та ефективно реагувати на виявлені загрози. Це може включати автоматизовані відповіді та плани відновлення.

Слідкуйте за змінами у конфігурації системи та програмного забезпечення для виявлення можливих вразливостей та аномалій. Регулярно переглядайте журнали безпеки для виявлення надмірної активності, аномалій

чи будь-яких підозрілих дій. Забезпечте надійне збереження журналів подій для можливості подальшого аналізу та слідування подій з часом.

Проводьте регулярні тести та сценарії для перевірки ефективності систем аудиту та моніторингу, а також тренування персоналу на випадок кібератак. Використовуйте розвинуті алгоритми штучного інтелекту та машинного навчання для виявлення патернів та аномалій, які можуть бути невидимими для традиційних методів.

Моніторинг та аудит - це проактивні підходи до забезпечення безпеки, які дозволяють виявляти та реагувати на загрози у реальному часі, забезпечуючи таким чином ефективний контроль та захист інформаційних систем.

Централізоване управління правами:

Централізоване управління правами (Centralized Rights Management) відноситься до методології, в якій усі права доступу до ресурсів або функцій у системі контролюються та керуються з одного центрального пункту управління. Цей підхід спрощує адміністрування та полегшує забезпечення безпеки в інформаційних системах. Централізоване управління правами дозволяє ефективно керувати та забезпечувати безпеку прав доступу до інформаційних ресурсів, особливо в масштабних та складних системах.

Автоматизація:

Автоматизація в контексті кібербезпеки розумного будинку означає використання автоматизованих інструментів та технологій для управління та забезпечення безпеки системи. Автоматизація може полегшити ряд аспектів кібербезпеки, включаючи виявлення загроз, реагування на події та управління доступом. Основні аспекти автоматизації в кібербезпеці розумного будинку включають:

- Системи виявлення вторгнень (IDS): Використовуйте автоматизовані системи виявлення вторгнень для моніторингу мережі та системи на

предмет підозрілої активності. Системи IDS можуть автоматично виявляти аномалії та сповіщати адміністратора про потенційні загрози.

- Автоматизована реакція на події (Automated Incident Response): Налаштуйте автоматизовані процедури реагування на інциденти для виявлення, ізоляції та виправлення вразливостей чи атак. Це може включати автоматичне відключення вражених пристроїв чи блокування небезпечних мережевих з'єднань.
- Автоматизована система аналізу журналів: Використовуйте інструменти машинного навчання для автоматизованої аналітики журналів подій. Це дозволяє виявляти неочікувані патерни та аномалії у великих обсягах даних.
- Автоматизована управління патчами та оновленнями: Налаштуйте систему автоматичного оновлення для всіх пристроїв та програмного забезпечення в розумному будинку. Це допомагає уникнути вразливостей, пов'язаних із застарілим програмним забезпеченням.
- Автоматизована реакція на атаки: Використовуйте системи, що дозволяють автоматично виявляти та реагувати на конкретні види кібератак. Це може включати блокування IP-адрес, зміну прав доступу чи ізоляцію підозрілих пристроїв.
- Автоматизоване виявлення збоїв: Використовуйте системи, які автоматично виявляють аномалії у роботі пристроїв чи системи, що може свідчити про проблеми безпеки чи виробничі збої.
- Автоматизоване резервне копіювання та відновлення: Налаштуйте автоматизовані системи резервного копіювання та відновлення для забезпечення безпеки ваших даних в разі втрати чи пошкодження.

Автоматизація в кібербезпеці розумного будинку дозволяє покращити ефективність та швидкість реакції на потенційні загрози, зменшити ризики та забезпечити безпеку системи.

4. Доступ до ресурсів на основі контексту:

Доступ до ресурсів на основі контексту (Context-Based Access Control, CBAC) - це підхід до управління правами доступу, де рішення про надання чи обмеження доступу залежить від специфічного контексту, пов'язаного з користувачем, ресурсом, середовищем або іншими факторами. Цей метод дозволяє гнучко налаштовувати права доступу в залежності від конкретних обставин. Рішення про доступ може враховувати особисті уподобання користувача, такі як мови, теми чи налаштування інтерфейсу.

CBAC дозволяє створювати більш адаптовані та інтелектуальні системи керування доступом, що допомагають збільшити безпеку та ефективність управління правами доступу.Рисунок 3.9 CBAC

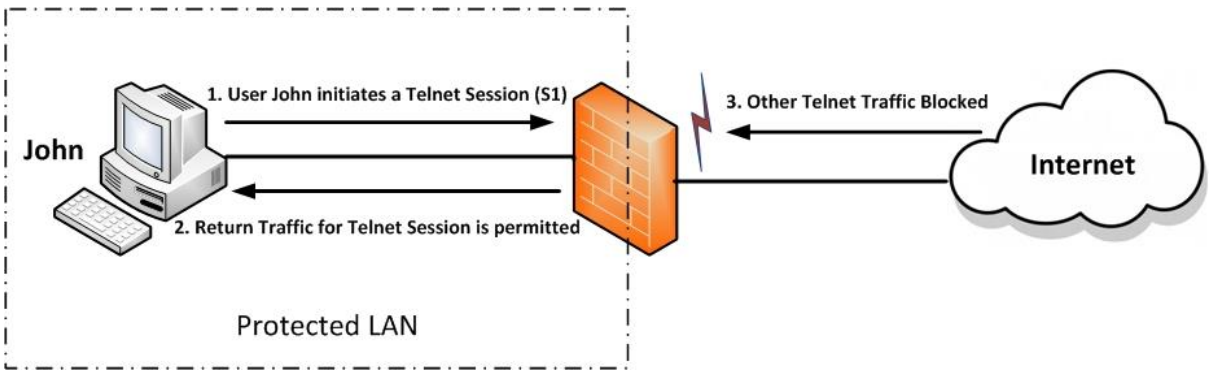


Рисунок 3.9CBAC

Регулярне оновлення та аудит системи:

Регулярне оновлення та аудит системи є ключовими складовими стратегії кібербезпеки, оскільки вони дозволяють виявляти, виправляти вразливості та моніторити безпеку системи з часом. Все це сприяє зменшенню ризиків інцидентів та покращенню загальної безпеки інформаційної системи.

Регулярно оновлюйте всі встановлені на системі програми та операційні системи. Це включає в себе патчі безпеки, виправлення багів та нові версії програм. Забезпечте вчасне встановлення всіх патчів та виправлень для операційних систем, програмного забезпечення та пристроїв. Періодично оновлюйте бази даних антивірусних програм та проводьте регулярні

сканування системи для виявлення та видалення потенційно шкідливого програмного забезпечення. Переглядайте та оновлюйте конфігурації системи, включаючи фаєрволи, правила безпеки та налаштування аутентифікації.

Проводьте періодичні аудити безпеки для виявлення потенційних загроз, вразливостей та незвичайної активності. Ведіть журнали подій для виявлення та аналізу аномальної активності, спрощуючи виявлення можливих загроз. Проводьте регулярні тести на проникнення, щоб перевірити стійкість системи до потенційних атак та вразливостей. Використовуйте інструменти для аудиту безпеки мережі та виявлення можливих атак або незвичайної мережевої активності. Змінюйте паролі та інші облікові дані регулярно, та переглядайте права доступу користувачів для забезпечення принципу найменших привілеїв. Використовуйте системи аналізу аномалій для виявлення непередбачених патернів та потенційно шкідливої активності. Забезпечте регулярне створення резервних копій важливої інформації та перевіряйте можливість їх відновлення.

Регулярне оновлення та аудит системи допомагає не лише уникати вразливостей, але й забезпечує швидке виявлення та реагування на потенційні загрози.

Ці практики можуть бути використані в поєднанні для оптимізації контролю доступу та визначення прав в інформаційних системах та забезпечення їхньої кібербезпеки.

3.3. Висновки до 3 розділу

Для забезпечення високого рівня кібербезпеки та приватності користувачів розробка та вдосконалення алгоритмів шифрування та автентифікації в сучасних розумних будинках є життєво важливими. Застосування сучасних методів шифрування, таких як квантова криптографія, є життєво важливим для вирішення завдань, пов’язаних із захистом конфіденційності даних від поточних і майбутніх кіберзагроз.

Мультифакторна аутентифікація гарантує високу безпеку доступу до ресурсів розумного будинку та відіграє важливу роль у підвищенні надійності процесу ідентифікації користувачів. Використання біометричних технологій робить процес аутентифікації не тільки безпечним, але й зручним для користувачів.

Щоб оптимізувати контроль доступу та визначення прав, використовуються принципи найменших привілеїв і розумний рольовий контроль. Це дозволяє ефективно контролювати права користувачів, зменшуючи ризики несанкціонованого доступу та створюючи прозорий і адаптивний механізм управління доступом.

Цей комплексний підхід інтегрує технології та стратегії кібербезпеки. Він враховує технічні та інтерфейсні аспекти. Підтримка високих стандартів безпеки та адаптація до нових викликів кібербезпеки залежить від регулярного оновлення алгоритмів, системного аудиту та впровадження сучасних практик безпеки.

У значній мірі успіх у розробці та вдосконаленні цих елементів кібербезпеки визначає якість захисту, так і продовження розвитку інтелектуальних систем. Забезпечення безпеки розумних будинків є важливим фактором у формуванні довіри до сучасних технологій і визначає, наскільки вони придатні для широкого використання в сучасному світі.

РОЗДІЛ 4: ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ РОЗУМНОГО БУДИНКУ

4.1 Постановка експерименту та методологія

У цьому розділі будуть розглянуті та розглянуті основні загрози та вразливості системи розумного будинку, які можуть порушити К, Ц і Д. На основі результатів аналізу будуть визначені найбільш небезпечні небезпеки.

Таблиця 4.1 - Аналіз основних вразливостей та загроз

Об'єкт вразливості	Точки атаки(вразливості)	Наслідки	Що виходить зладу(порушує)
Всі системи та пристрої які підключені до Інтернету	Права та доступи пристроїв Смарт Будинку мають доступ до даних	ПЗ пристроїв можуть створювати повідомлення до реальних сигналів від фіз.пристроїв чим і дає можливість передавати недостовірну інформацію	К Ц
Датчики	Дешеві , поганої якості	Затримка реагування	К Ц Д
Програмне забезпечення	Старе та неліцінзійне	Помилки ПЗ	Д
Головний сервер	Відправка конфідеційної інформації на сервери компаній що займаються підтримкою систем та пристроїв будинку	Стеження про дії власника, надсилання інформаціїї про взаємодії з пристроями на сервер, атаки на ЦС	К Ц Д
Розумна розетка	Використання однакових тільки логінів та паролів	Можливо прочитати повідомлення або перехопити	К Ц Д

		керування для підклч. DDoS атак	
Відеокамери	Застарілий механізм, слабкий пароль відсутність шифрування при передачі данних до відеокамери через «cloud»	Взлом для створення ботнет та використання для DDoSатак	К Ц Д
Файли під захистом	Механізм розмежування доступу застарів або слабий	Доступ до файлів які захищені з використанням обхідного шляху	К Ц
Носій інформц. та пристрої системи апаратура	Незахищене зберігання, перепади напруги, відсутність автономного електроживлення	Знищення носіїв інформц. та апаратури	К Ц Д

У таблиці 2.1 присутні такі скорочення: К-конфіденційність, Ц-цілісність, Д-доступність

Згідно аналізу, найбільшу загрозу представляють собою ті, що порушують К, Ц та Д:

Неякісні та недорогі датчики;

Слабкий захист мережі;

Недостатній захист при взаємодії лампочок у локальній мережі (наприклад, коли виробник обмежений використанням шифрованого бездротового протоколу);

Для захисту сторінки з налаштуваннями використовується лише логін і пароль; неможливо змінювати авторизаційні дані, оскільки більшість пристроїв компанії використовують однакові паролі;

Слабкий незмінений пароль від постачальника систем та пристроїв;

Передача данних через USB, тощо.

З таблиці 4.1 можна знайти основні загрози для кожного об’єкту атаки, а також оцінити їх за допомогою методу оцінки ризиків:

-виходячи з ймовірності реалізації загрози, висока ймовірність її реалізації протягом одного року, середня ймовірність її реалізації протягом 2-3 років, а низька ймовірність є малоймовірною;

-вплив високого, середнього або низького, якщо загроза буде реалізована;

Також, дивлячись з аналізу рівня загроз який я описував в 3 Розділі, можемо виділити такі основні загрози:

-атаки на центральний сервер;

-фішингові атаки;

-нелегитимний доступ до облікових даних для входу та персональних даних;

-перехоплення сигналу та передача недостовірної інформації в мережу;

-впровадження шкідливого коду або програми;

-використання пристроїв у ботнет.

Фізичні загрози включають пожежі, протікання, проникнення в будинок без дозволу власника, відключення електроенергії та багато іншого.

На основі проведеного аналізу необхідно вжити наступних заходів безпеки:

встановлення паролю високої складності на профіль адміністратора системи;

оновлення програмного забезпечення для всіх пристроїв системи розумний будинок до найновішої версії;

використання системи, яка контролює несанкціонований доступ до розумного дому;

налаштування VPN-мережі системи;

встановлення файрвола або екрану міжмережевого зв’язку між локальною мережею розумного дому;

використання антивірусних вакцин;

встановити систему моніторингу для управління доступом;

регулярна перевірка роботи всіх розумних пристроїв у домі;

використання запасного джерела енергії

Згідно з попередніми розділами, забезпечення конфіденційності даних є найважливішим для систем розумного дому. Таким чином, у цьому розділі буде розглянуто, як захистити додаток для керування розумним домом.

Захист сховища даних, яке може забезпечити безпечне читання та запис файлів, необхідний для захисту даних на пристрої.

Для підвищення безпеки необхідно шифрувати файли «на льоту», наприклад, коли вони отримуються з сервера. Протоколи передачі даних через мережу відомі тим, що розділяють файли на пакети та передають їх.

Принцип полягає в тому, щоб файли отримували по частинах. У результаті кожен наступний блок шифрується та зберігається в пам’яті пристрою. Це робиться для того, щоб дані не затримувалися на довго в пам’яті пристрою, і вони шифруються відразу після надходження. Схожий алгоритм використовується для розшифрування файлу, щоб він міг бути прочитаний.

Блокове шифрування має бути послідовним, оскільки відтворення медіа-контенту вимагає постійного розшифровування даних. . Таким чином, файл, зашифрований, має зберігатися на носії перед використанням.

Розшифрувати в оперативну пам'ять. Далі файл буде прочитаний і видалений з оперативної пам'яті.

Такий алгоритм використовується для шифрування файлів: після отримання файлу він спочатку записується в оперативну пам'ять, потім шифрується і записується в основну пам'ять. У Бому після шифрування файл видаляється з оперативної пам'яті.

AE38 і PE3 є двома найбільш поширеними симетричними 0 алгоритмами для блокового шифрування даних.

Щоб пристрій міг розшифровувати дані без доступу до каналу передачі даних, необхідно розглянути симетричні алгоритми попереднього розподілу ключів, оскільки однією з умов є можливість зберігання даних на пристрої та

їх використання без наявності інтернету. Схема розподілу ключі Блома може зменшити цю вразливість.

Суть схеми розподілу ключів Блома наступна: довірена сторона роздає кожному учаснику відкритий та закритий ключ. Далі всі учасники, обмінюються між собою тільки відкритими ключами по каналах зв'язку (які можуть бути незахищеними), а також можуть згенерувати секретний сеансовий ключ для спілкування між собою. Спочатку відбувається ініціалізація - довірена сторона вибирає симетричну матрицю D розмірності k на k над кінцевим полем GF(p). Потім коли добавляється новий учасник до системи управління SmartHouse довірена особа(юзер) обирає для нього новий довірений ключ. В якості довіреної сторони буде використан сервер зберігання даних клієнт-серверної архітектури.

Далі перевірена сторона обчислює закритий ключ g = D * I. Після цього відкритий і закритий ключ надсилаються учаснику по надійному каналу, який не може бути прослуховований.

Якщо один клієнт сервер хоче створити секретний канал між собою, вони передають один одному свої відкриті ключі через відкритий канал. Далі кожен з них множить свій закритий ключ на відкритий ключ того, хто стоїть з іншого боку (1).

$$S_A = (g^t_A I_B)^t = (I^t_A D I_B)t = I^t_B D I_A$$

$$S_B = (g^t_B I_A)^t = (I^t_B D I_A)t = I^t_A D I_B$$

$$S_A = S_B \tag{1}$$

Вони отримають одне і те ж число, оскільки матриця P симетрична. Це число буде використовуватися як загальний сеансовий ключ. Далі сервер використає сеансовий ключ для шифрування та розшифровки, зроблені клієнтом. Іншими словами, одна сторона завжди буде сервером зберігання даних, а інша сторона буде клієнтом.

Надійність схеми безпосередньо залежить від розміру секретної матриці. Щоб відновити секретну матрицю (або будь-яку матрицю, яка виконує аналогічну функцію) потрібно кількість ключів, що дорівнює кількості рядків матриці.

Алгоритм шифрування був вибраний AE85-CBC із довжиною ключа 256 біт.Вразливість цього алгоритму полягає в тому, що для передачі відкритого та закритого ключа необхідний секретний канал передачі.

Тепере розгялнемо аналізи симетричних протоколів розподілу ключів.

Протокол WideMouthFrog - найпростіший протокол керування ключами. Він дозволяє двом абонентам встановити загальний сесійний ключ для захищеного спілкування між собою. У протоколі бере участь довірений центр. Анжела хоче встановити сесійний ключ із Богданом. Вона починає, формуючи: К - випадковий сеансовий ключ, ТА - мітку часу та відправляє Тарасу (довіреному центру), додавши своє ім'я (2):

$$M0 = A.EA\left(TA, B, K\right) \tag{2}$$

Тарас розшифровує повідомлення, використовуючи секретний ключ, який він отримав від Анжели, і перевіряє, чи правильна мітка часу ТА та ідентифікатор Богдана. Якщо все гаразд, він створює:

ТВ- нова мітка часу також вона може відрізнятись від ТА та робить відправку Богдану, формула (3).

$$M1 = EB\left(TA, B, K\right) \tag{3}$$

Богдан отримує повідомлення, розшифровує його за допомогою спільного ключу з Тарасом і перевіряє мітку часу ТА, а також ідентифікатор Анжели. Якщо повідомлення пройшло перевірку, Богдан тепер має ключ від Анжели.

Недоліком цього протоколу є те, що він досить простий і може бути нестійким.

Інший протокол який можливо запропонувати це протокол Отвея-Рііса.

Протокол Отвея-Ріїса використовує симетричні ключі, що дозволяє розподіляти ключі без позначок часу.

Перед запуском протоколу були присутні Тарас, довірений центр, і два користувача, Анжела та Богдан, які отримали ЕА та ЕВ. Анжела вибирає числа N і NA, тоді як Боогдан вибирає числа NB.

Анжела створює повідомлення для Богдана, у якому відкритим текстом передається N, A, B, а також ті ж самі N, A, B з NA, які зашифровані спільним ключем ЕА з Тарасом (4)

$$M0 = N, A, B, EA(NA, N, A, B) \quad (4)$$

Богдан отримує повідомлення, друга частина якого для нього не розшифровується, додає ще один рядок, який шифрує ключем ЕВ та відправляє Тарасу (5).

$$M1 = N, A, B, EA(NA, N, A, B), EB(NB, N, A, B) \quad (5)$$

Тарас знаючи обидва ключі, може розшифрувати повідомлення Анжели та Богдана. Тепер його мета - підтверджувати, що він - Тарас і сформувати ключ К для подальшого спілкування Анжели та Богдана.

Тарас генерує ключ К та посилає Богдану зі спілкування формула (6).

$$M3 = EA(NA, K), EB(NB, K) \quad (6)$$

Богдана не зміг розшифрувати першу частину за допомогою ключу Анжели, але коли зміг розшифрувати другу частину NB, він зрозумів, що повідомлення прийшло від Тараса. Далі отримує ключ К, який був

створений. Тепер Богдан готовий спілкуватись з Анжелою , Богдан відправляє першу частину ключа Анжелі від Тараса (7).

$$M4 = EA(NA, K) \tag{7}$$

Анжела приймає повідомлення, засвідчується, що воно від Тараса (NA), та зчитує ключ К. Анжела та Богдан готові до спілкування. В результаті Богдан впевнений, що поговорив із Тарасом: Богдан відправив йому число NB, шифроване секретним ключем ЕВ, і отримав інше повідомлення, що містить те саме число і шифроване тим самим ключем.

Анжела також переконана, що Богдан поговорив із Тарасом, бо вона послала своє число NA, шифроване ключем ЕА, і отримала назад інше повідомлення, що при цьому теж містить NA і шифроване ЕА. У Анжели та Богдана з'явився спільний ключ К.

Недолік цього протоколу полягає в тому, що Аліса ніяк не може бути впевнена, що Богдан є Богданом. Вона впевнена лише в тому, що спілкується з кимось, хто може листуватись з Тарасом.

Щоб вирішити цю проблему за чотири кроки, Богдан може відправити Анжелі не тільки ЕА(NA, K), але й ЕК (NA, NB), що вказує на те, що він знає ключ К. Анжела також може довести, що знає ключ К, відповівши Богдану ЕК (NB).

Проаналізувавши протоколи розподілу ключів, протокол Kerberos був обраний, оскільки він може одночасно забезпечити конфіденційність і цілісність, не маючи недоліків, як у попередніх протоколів. Таким чином, Kerberos використовуватиметься для аутентифікації на довіреній стороні сервера рисунок 4.1.

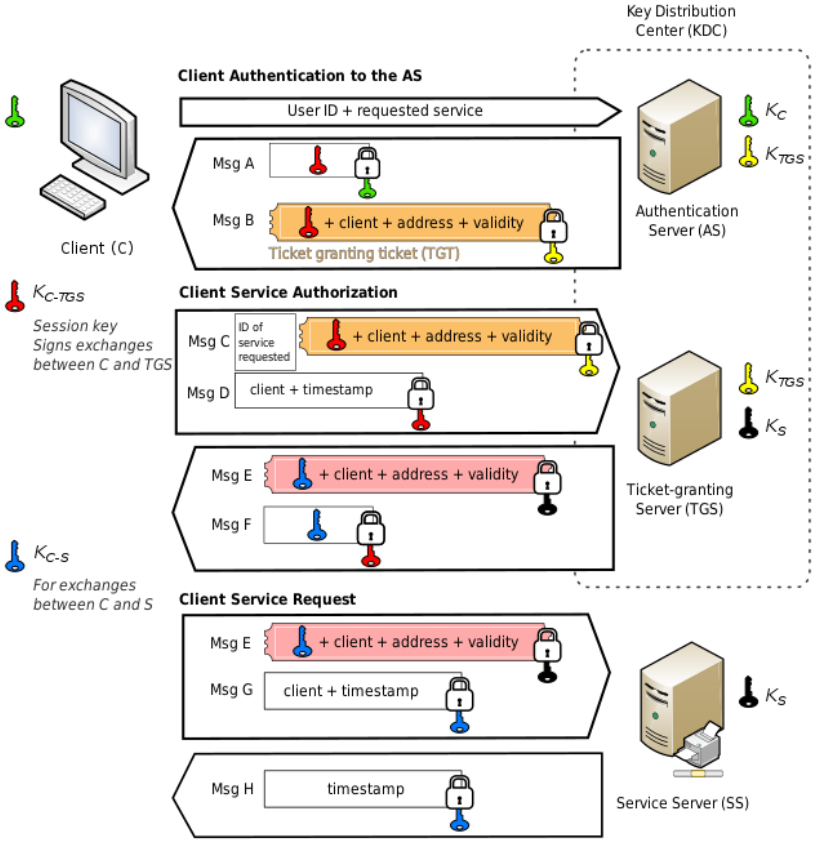


Рис.4.1 СистемапротоколуKerberos

Протокол Керберос - це розподілена система аутентифікації, яка дозволяє клієнту довести свою особистість серверу без надсилання даних по мережі. Керберос гарантує, що дані, які передаються клієнтом і сервером, є безпечними та конфіденційними.

Перед запуском протоколу три дійові особи (ідентифікатори) повинні бути визначені: Анжела — клієнт, Богдан — сервер, якому Анжела хоче довести свою справжність, і Тарас — довірений центр.

Анжела та Богдан мають секретні ключі EA та EB, щоб спілкуватися з Тарасом. Анжела вибирає число NA і встановлює маркер часу TA на своєму годиннику. Тарас обирає період валідності (lifetime).

Згодом Анжела, запускаючи протокол, у відкритому вигляді, передає Тарасу свій ідентифікатор, ідентифікатор Боба iNA (8).

$$M0 = A, B, NA \tag{8}$$

Тарас, отримавши повідомлення від Анжели, генерує ключ K для подальшого спілкування Анжели та Богдана і передає назад Анжелі

повідомлення з двох частин: перша частина зашифрована секретним ключем Анжели і містить К, NA, період валідності t та ідентифікатор Богдана; друга частина невідома Анжелі - вона зашифрована секретним ключем Богдана, і в ній міститься К, t та ідентифікатор Анжели (9)

$$M1 = EA\left(K, NA, t, B\right), EB\left(K, A, t\right) \tag{9}$$

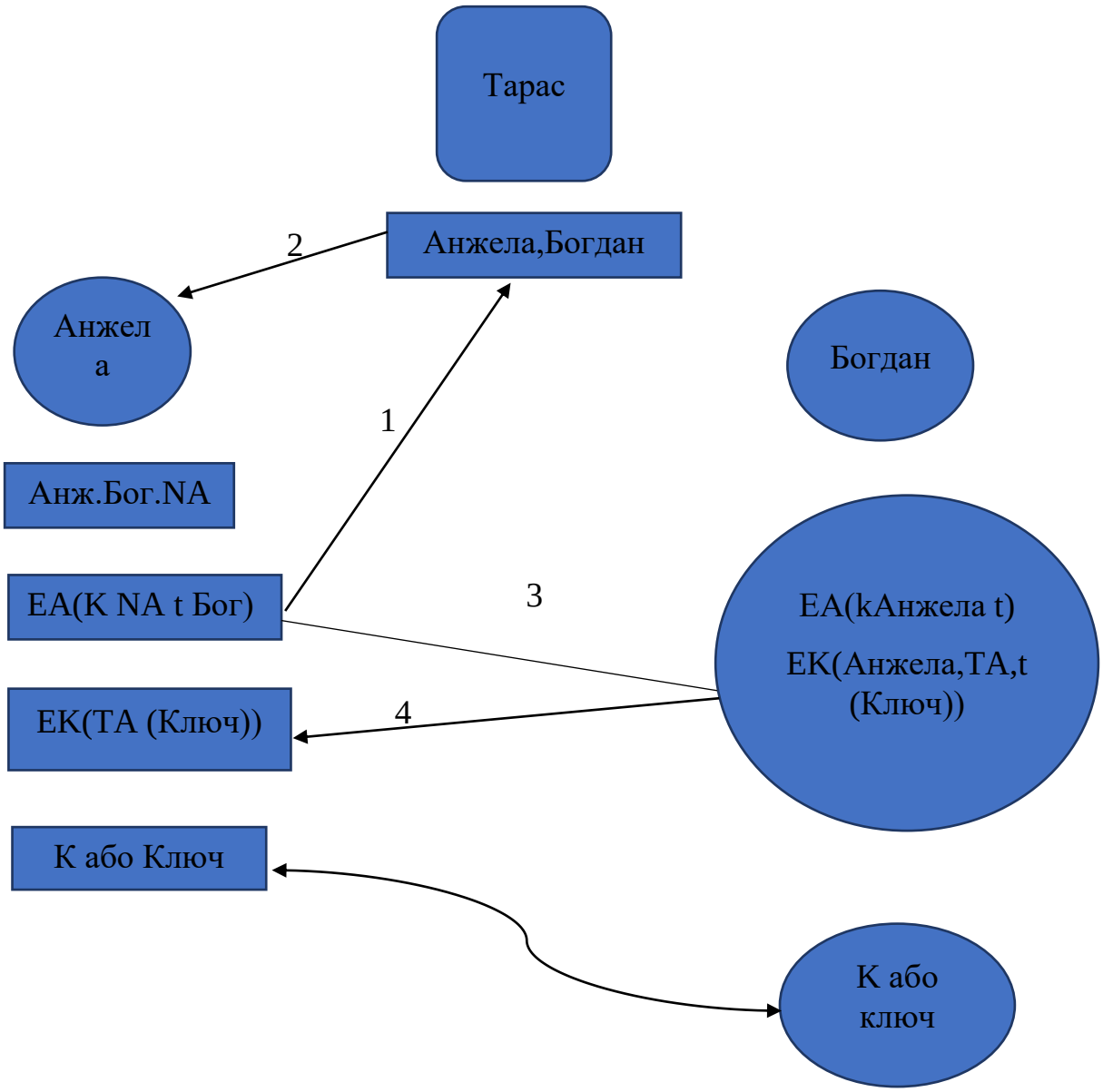
Анжела розшифровує першу частину прийнявши того від Тараса повідомлення, і отримавши ключ К, створює новий пакет для відправки Богдану, в який входять ідентифікатор Аліси, t та мітка часу ТА. Після цього Анжела надсилає Богдану повідомлення з двох частин: перша частина - це та, що прийшла від Тараса, а друга - створена Анжелою (10)

$$M2 = EB\left(K, A, t\right), EK\left(A, TA, t\right) \tag{10}$$

Богдан приймає повідомлення. Розшифрувавши першу частину, він дістає новий ключ К, а потім, використовуючи його, розшифровує другу частину. Щоб підтвердити Анжелі, що він знає новий ключ К, Богдан надсилає їй повідомлення з позначкою часу, зашифроване новим ключем К (11)

$$M3 = EK\left(TA\right) \tag{11}$$

Анжела засвідчується, що Богдан - це Богдан. Тут застосовні такі міркування: Богдан міг розшифрувати повідомлення від Анжели з позначкою часу, тільки якщо він знав ключ К. А ключ К він міг дізнатися тільки якщо знає ЕВ. А оскільки це секретний ключ Богдана і Тараса, то надіслав повідомлення Анжелі - Богдан. Потім використовуючи схеми Блома відкритий та закритий ключі передаються з використанням ключа К. Таблиця 4.2.



Таблиця 4.2 Робота протоколу Kerberos

4.2 Результати експерименту та аналіз

Бібліотека CryptoCommon буде використана для шифрування та розшифрування.

Наприклад, алгоритм AES-256 був обраний. алгоритм AES, довжина ключа якого становить 256 бітів. Крім того, використання змінних шифрування, які змінюються час від часу, замість «жорстко зашитих» у код чисел, може зробити алгоритм більш гнучким.

Можливість взлому підвищується, коли привілейовані облікові записи поєднуються з атаками на аутентифікацію Kerberos в доменах. Такі атаки націлені на права адміністратора домену, які дають їм необмежений доступ і контроль над системою. Зловмисники можуть приховано маніпулювати контролерами домену та створювати квитки Kerberos для отримання несанкціонованого доступу, використовуючи привілеї адміністратора.

Доступність, неясність і постійність є основними недоліками протоколу Kerberos.

Доступ: якщо зловмисник отримає привілеї локального адміністратора, він може отримати додаткові облікові дані. Це дозволить зловмиснику переміщатися по мережі, підвищувати привілеї та отримати несанкціонований доступ до цінних активів, якщо вони залишать їх на зламаних комп’ютерах.

Неясність: зловмисник може повторно використовувати квитки Kerberos, щоб видавати себе за авторизованих користувачів і обійти процеси аутентифікації, маскуючи активність і уникаючи слідів журналу аутентифікації, щоб уникнути виявлення.

Постійність: зловмисники часто поступово відправляють інформацію, щоб залишатися в мережі невиявленими протягом тривалого періоду часу.

Атаки Kerberos дають зловмисникам час, що їм найбільше потрібно. Квитки Kerberos забезпечують стабільність, навіть якщо облікові дані змінюються.

Хоча існує кілька типів атак на протоколи аутентифікації, включаючи PasstheHash, PasstheTicket, OverpasstheTicket, найбільш руйнівною є «ЗОЛОТИЙ КВИТОК».

Ця атака полягає в тому, що зловмисник може отримати несанкціонований доступ до домену Active Director за допомогою квитків Kerberos, якщо у нього є доступ адміністратора або локального адміністратора. Атака «золотий квиток» — це тип атаки, під час якої зловмисник створює квиток Kerberos, який працює протягом десяти років. Зловмисник може бути ким завгодно, за умови, що він має хеш, додати будь-який обліковий запис до будь-якої групи (включаючи групи з високими привілеями) і використовувати всі можливості автентифікації Kerberos.

Зловмисник може створити КВИТКИ Kerberos, придатні для використання для облікових записів користувачів, комп’ютерів і служб, які не знаходяться в Active Directory. Золотий квиток — це підроблений центр розповсюдження ключів Kerberos, який порушує конфіденційність і цілісність одночасно.

Як ми можемо поліпшити цю систему та запровадити в Розумні будинки.

У той час як протокол Kerberos використовується для генерації та розподілу ключової інформації в комп’ютерній мережі, сервери TGS (Ticket Granting Server) обчислюють пакети ключової інформації, які надсилаються клієнтам із сервера додатків у складі посилок TGS.

Нехай є принаймні одна кількість серверів видачі квитків (TGS) і один або більше серверів автентифікації (AS).

Кожен сервер TGS пов’язаний з одним сервером AS. Коли кожен домен мережі зв’язується з сервером TGS, усі абоненти домену прив’язуються до TGS.

Якщо сервер програм NAS розташований у кількох доменах, він прив’язується до кожного TGS, що належить даним доменам. Служба одноразових паролів OTPS (One Time Password Service) підтримує кілька AS, до яких прив'язані відповідні TGS.

Сервер програм NAS підтримує функцію одноразових паролів для кількох OTPS. Як сервер автентифікації ASj, так і абонент Ai мають один пароль.

На етапі ініціалізації (рис. 4) кожен сервер ASj обчислює ключі для зв’язку з TGSt, абонентів Ai та NASp. Припустимо, що кожен ASj має ключ зв’язку з TGSt, і кожен TGS має KDP(P.F)-схему для відповідного домену мережі. Кожному абоненту Ai чи NASp цього домену обчислюються пакети Si, Ss.

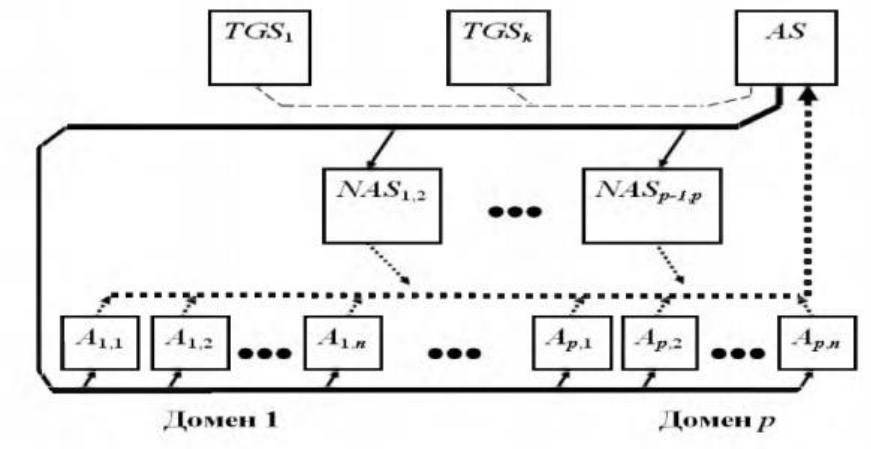


Рис.4.2 Протокол обміну з сервером автентифікації з метою отримання дозволу на видачу ключової інформації

Тепер кожен учасник Ai, який використовує послугу одноразового пароля з відповідним сервером аутентифікації ASj, може ініціалізувати та виконувати протоколи, щоб отримати свій пакет Ki ключової інформації:

-протокол обміну з сервером аутентифікації для отримання дозволу TGT на отримання ключової інформації (Рисунок 4.2);

-протокол обміну з сервером TGS для отримання ключової інформації (Рисунок 4.3);

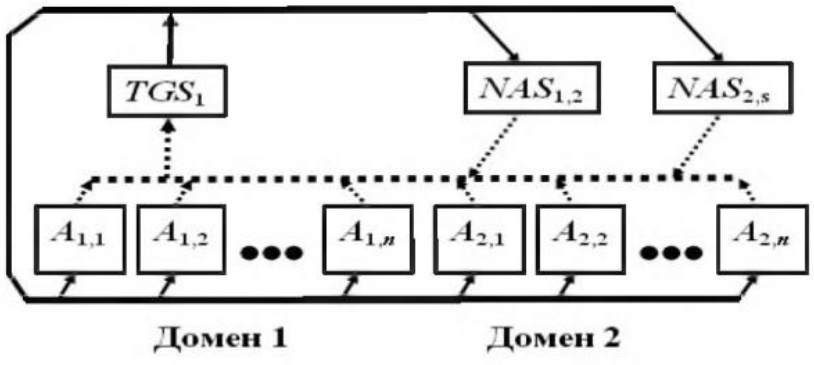


Рис.4.3 Протокол обміну із сервером ТО5 з метою отримання ключового матеріалу абонентами мережі А та серверами додатків NAS

Для безпечного обміну інформацією між абонентами мережі використовується протокол комунікації абонентів мережі, зокрема через сервер додатків NAS (Рисунок 4.4).

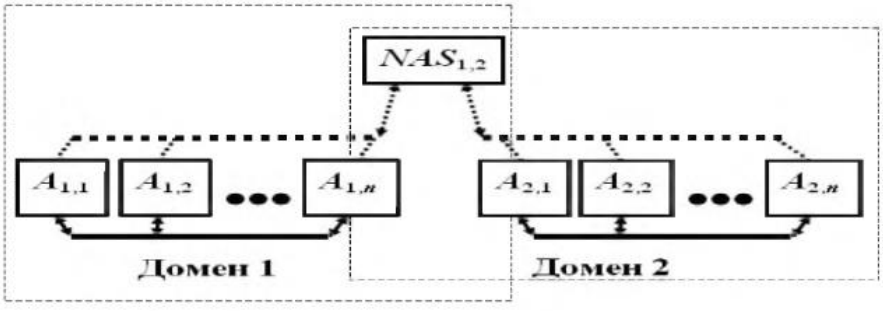


Рис. 4.4. Протокол комунікацій абонентів мереж

Дано оцінки ключової інформації, необхідної для організації захищених комунікацій, для мереж різних типів.

Дані, представлені в Таблиці 4.3 показують переваги використання нецентралізованих 10КІОР(1002, 56) та ТОНАКІОР(1002, 56, 10)-схем.

	Без поперд. Розподілу	10KDP(1002,56)	10HAKDP(1002,56,10)
Довжина пакета	1001	27	38
Число переданих ключів	10030020	370740	280560

Таб. 4.3 - Порівняльна таблиця нецентралізованих 10KDP(1002, 56) та централізованих 10HAKDP(1002, 56, 10)-схем

Ця таблиця показує, що у нецентралізованій мережі (KDP) менше ключів, що надсилаються учасникам ТА, ніж у централізованій мережі (HAKDP). Схеми хешування скорочують загальну довжину пакетів ключової інформації та кількість ключової інформації, що передається від довіреного центру ТА.

4.3 Висновок до 4 розділу

У цьому розділі розглядаються основні проблеми та загрози системи розумного будинку. Було проведено дослідження системи розумного будинку щодо рівнів загроз і методів підвищення кібербезпеки.

Було розглянуто та створено масштабовану систему для забезпечення конфіденційності, цілісності та доступності даних для великої кількості користувачів Smart Home. Було запропоновано змінити відомий алгоритм Kerberos, щоб підвищити ефективність захисту. Крім того, у цьому розділі детально описано процедури шифрування, ідентифікації та валідації розробленої системи безпеки розумного будинку, яка використовує різні протоколи.Зокрема, було проведено дослідження функцій системи, які можуть вплинути на її функціонування та безпеку.

Крім того, були проведені експерименти з метою перевірки ефективності розробленої системи; це допомогло визначити потенційні слабкі сторони та вразливості системи. Результати дозволили зробити висновки щодо ступеня безпеки та стабільності системи в реальних умовах. Також можливе запровадження такого принципу захисту в новітніх будинках

РОЗДІЛ 5 ОХОРОНА ПРАЦІ

5.1 Аналіз потенційно небезпечних виробничих факторів

Метою дипломної роботи є кіберзахист системи «Розумного будинку». Об’єктом дослідження є процес взаємодії різних плат, мікросистем, програм, датчиків та сенсорів, які використовуються в системі «SMARTHOUSE». Таким чином, важливо звернути увагу на умови праці фахівця, який займається розробкою програмно-апаратного забезпечення.

Такі шкідливі та небезпечні виробничі фактори, як електромагнітне та інфрачервоне випромінювання, шум, іонізуюче випромінювання та електричне випромінювання, пожежна небезпека та інші, можуть впливати на фахівців. Зважаючи на це, заходи з охорони праці є важливою частиною комплексного підходу до вдосконалення умов праці. Охорона праці на робочому місці повинна забезпечувати технічну підготовку працівників і необхідні умови для правильної організації трудової діяльності людини як інженера телекомунікацій.

Корисна площа та корисний об’єм робочого місця відповідають стандартам (ДСанПіН 3.3.2.007-98). Немає потреби в додаткових процедурах нормалізації.

Небезпека ураження людини електричним струмом вважається потенційно небезпечним фактором на робочому місці. Пожежа під час аварії є важливим, але менш ймовірним фактором.

Хімічні табіологічні джерела майже не впливають.

Таблиця 5.1.Параметри робочої кімнати

Найменування	Основні характеристики
Довжина приміщення	5 м
Ширина приміщення	4 м
Висота приміщення	2,9 м
Загальна площа (S)	20 $м^2$
Загальний об’єм (V)	77 $м^3$
Кількість робочих місць	2
Кількість вікон	1

Таблиця 5.2.Реальні та нормативні характеристики приміщення

Назва параметра	Реальне значення	Нормативне значення
Площа на 1 працюючого	10 $м^2$	6 $м^2$
Об’єм на 1 працюючого	29 $м^3$	20 $м^3$

Перелік небезпечних та шкідливих виробничих факторів наведено у таблиці 5.3.

Таблиця 5.3.Небезпечні та шкідливі виробничі фактори

Фізичні	Електронебезпека, пожежа, шум, мікроклімат
Хімічні	Відсутні
Біологічні	Відсутні
Психофізіологічні	монотонність, статична робоча поза, підвищена відповідальність за рішення що приймаються

В приміщенні присутні небезпечні фактори, та за умов дотримання заходів безпеки, вони не є критичним.

Обчислювальна техніка генерує тепло, що може викликати гіпертермію (підвищення температури тіла), збільшення потовиділення та фізіологічні проблеми з роботою організму. Комп'ютери повинні мати певні мікрокліматичні умови. Санітарні норми ДСН 3.3.6.042-99 визначають параметри мікроклімату, які створюють комфортні умови. Цей тип роботи відноситься до категорії 1а, що означає, що він виконується сидячи і не вимагає фізичного напруження. Рабоче місце залишається постійним.

Таблиця 5.4.Фактичні та нормативні значення мікроклімату приміщення

Період року	Нормативні значення		Фактичні значення	
	Температура, °С	Відносна вологість, %	Температура, °С	Відносна вологість, %
Холодний	20...23	40...60	22	50
Теплий	23...25	40...60	23-24	50-60

Застосування систем вентиляції, кондиціонування повітря та встановлення світловідбиваючої плівки на вікна є основним методом забезпечення необхідних параметрів мікроклімату і складу повітряного середовища.

Відповідно до відповідного санітарно-гігієнічного стандарту ДСН 3.3.6.042-99, основні характеристики мікроклімату в приміщенні відповідають встановленим нормам.

Зміни природного освітлення залежать від часу дня, пори року, характеру місця та багатьох інших факторів. Коли нормовані значення коефіцієнта природного освітлення не досягаються (похмура погода,

короткий світловий день), штучне освітлення використовується для роботи в темний час доби та вдень.

Відповідно до ДБН.В.2.5-28-2018 «Природне і штучне освітлення», КПО має бути не нижче 0,9%. Розряд зорової роботи фахівця IV (в) (середньої точності — найменший розмір об’єкта розрізнення 0,5–1,0 мм). Люмінесцентні лампи часто використовуються як джерела штучного освітлення, і вони попарно об’єднуються в світильники, розташовані рівномірно над робочою поверхнею. При виконанні робіт вимоги до освітленості в приміщеннях, де встановлені комп’ютери, становлять 200 і 400 лк відповідно. Бокова система природного освітлення. Загальна система штучного освітлення.

Робочий кабінет не відноситься до приміщень з підвищеною небезпекою. Обладнання не завдає великого навантаження на мережу. Джерела небезпеки наведено у табл. 5.5.

Таблиця 5.5. Джерела небезпеки

№	Найменування	Джерело небезпеки	Причини небезпеки	Наслідки небезпеки
1	Персональний комп’ютер	Блок живлення	Пошкодження блоку живлення, кабеля живлення.	Ураження струмом
2	Роутер	Блок живлення	Пошкодження блоку живлення, кабеля живлення	Ураження струмом
3	Джерело безперебійного живлення	Блок вхідного живлення, деталі, що знаходяться під напругою	Пошкодження блоку живлення, вхідного кабеля живлення.	Ураження струмом

5.2. Розробка заходів з поліпшення умов праці

Для забезпечення відповідних мікрокліматичних умов у приміщенні передбачені кондиціонери, які регулюють температуру та відносну вологість повітря.

Вибір кондиціонера за потужністю (охолодження) ґрунтується на теплі, що надходить із зовнішнього середовища, а також теплі, що надходить від працівників і обладнання. Розрахунок потрібної потужності (Qk) кондиціонера можна приблизно зробити за допомогою формули

$$Q_к = Q_з + Q_о + Q_р \qquad (4.1)$$

де $Q_з$ – надходження тепла зовні.

Орієнтовно $Q_з = q \cdot V$, де q=30 Вт/м^3 для вікон північної орієнтації

V – об'єм приміщення, м^3;

$Q_о$ – виділення тепла від обладнання, кВт орієнтовно для персонального комп’ютера $Q_о$=0,3 кВт;

$Q_р$ – виділення тепла від робітників (при спокійній роботі Qp=0,1 кВт).

Остаточний розрахунок потужності кондиціонера виглядає так:

$Q_к = 1{,}74 + 0{,}3 + 0{,}1 = 2{,}14$ кВт.

Далі вибирають ближчу за потужністю марку кондиціонера. Для нашого варіанту виберемо кондиціонер Inverter GWH07AAB-K3DNA5A/A4A потужність якого 2,2 кВт.

Розрахунок освітленості робочого місця включає вибір системи освітлення, визначення необхідного числа світильників, їхнього типу та місця розташування. Розрахуємо параметри штучного освітлення на основі цього. Штучне освітлення зазвичай створюється за допомогою електричних

джерел світла, як-от ламп розжарювання або люмінесцентних ламп. Будемо використовувати люмінесцентні лампи, оскільки вони мають багато переваг порівняно з лампами розжарювання. Зокрема, їхній спектральний склад подібний до денного, природного світла; їхній ККД більший (у 1,5–2 рази вище, ніж у ламп розжарювання); їхня світловіддача більша (3–4%), ніж у ламп розжарювання; і вони мають більший термін служби. Для обраного для аналізу прміщення проводиться розрахунок освітлення.

Для визначення кількості світильників визначимо світловий потік, за формулою:

$$F = \frac{E \cdot S \cdot Z \cdot K}{\eta} \qquad (4.2)$$

де F - розрахунковий світловий потік освітлювальної установки, лм;

E - нормована мінімальна освітленість, лк (визначається за таблицею, відповідно до якої роботу розробника, можна віднести до розряду точних робіт, отже, мінімальна освітленість буде E = 300 лк);

S - площа освітлюваного приміщення (S = 20 м^2);

Z - відношення середньої освітленості до мінімальної (для люмінесцентних ламп приймається рівним 1,1);

K - коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення залежить від типу приміщення і характеру проведених в ньому робіт, у випадку даного приміщення та функціонального призначення K = 1,3);

η - коефіцієнт використання світлового потоку, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп, і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{ст.}$) і стелі ($\rho_{стелі}$)), значення коефіцієнтів дорівнюють $\rho_{ст}$ = 40% і $\rho_{стелі}$=60%.

Для цього обчислимо індекс приміщення по формулі:

$$I = \frac{S}{h(A+B)} \quad (4.3)$$

де h - розрахункова висота підвісу ламп над робочою поверхнею, h = 2,9-0,8=2,1 м;

А - ширина приміщення, А = 4 м;

В - довжина приміщення, В = 5 м.

Підставивши значення отримаємо:

$$I = \frac{20}{2,1*(4+5)} = 1,06.$$

Знаючи індекс приміщення I, за таблицею знаходимо n = 0,22.

Підставивши всі значення в формулу (4.2) для визначення світлового потоку

F, отримуємо:

$$F = \frac{300 \cdot 1,3 \cdot 20 \cdot 1,1}{0,48} = 17875 \text{ Лм.}$$

Для освітлення вибираємо люмінесцентні лампи типу ЛБ 40-1, світловий потік яких F = 4320 Лм. Розрахуємо необхідну кількість ламп по формулі:

$$N = \frac{F}{F_л}, \quad (4.4)$$

де N - розрахункова кількість ламп;

F - світловий потік, F = 17875 лм;

$F_л$- світловий потік лампи,

$$N = \frac{17875}{4320} = 4.$$

Розрахунок показав, що чотири люмінесцентні лампи цього типу необхідні для ідеального освітлення робочого приміщення. Ці лампи можуть забезпечити рівномірне освітлення по всій площині приміщення залежно від обраної системи освітлення.

5.3 Пожежна безпека

Відповідно до ДБН В.2.5-56:2014, приміщення відноситься до категорії В за наявності важко горючих твердих і волокнистих матеріалів і речовин, таких як комп'ютери, монітори, периферійні пристрої та канцелярські товари. При аналізі приміщення короткі замикання та перевантаження в електрообладнанні та електропроводці можуть бути потенційними джерелами загоряння, які можуть призвести до пожежі. Перевантаження електричної мережі через несправності комп'ютерного обладнання також може бути причиною займання. Характеристика джерел небезпеки наведена в таблиці 5.6.

Таблиця 5.6Джерела пожежної небезпеки

№	Найменування	Джерело небезпеки	Причини небезпек	Наслідки небезпеки
1	Персональний комп'ютер	Блок живлення, деталі під напругою	Коротке замикання	Виникнення пожежі
2	Матеріали і речовини, що схильні до займання	Загоряння матеріалів	Зовнішнє загорання	

3	Щільність проводки	Оплавлення ізоляції	Коротке замикання	

Засоби протипожежного захисту включають системи пожежної сигналізації, пожежогасіння, оповіщення про пожежу та управління евакуацією людей, пожежне спостерігання, основні засоби пожежогасіння та пристрої, які запобігають розрядам будинків і споруд.

На стінах приміщення та коридору обов’язково має бути план евакуації людей у випадку пожежі. Двері в бік аварійного виходу повинні бути відчинені. Немає перешкод для персоналу рухатися до дверей. Як зазначено вище, приміщення повинно бути оснащене димовими оптико електронними автономними сповіщувачами, які монтуються в стелю приміщення. Ці сповіщувачі повинні мати можливість ідентифікувати пожежі. Спрацювання сигналу пожежної небезпеки передає його до пульту управління, який знаходиться в приміщенні черговим персоналом.

Для забезпечення пожежної та вибухової безпеки приміщення необхідно створити комплекс організаційно-технічних заходів, які включають перші кроки включають загальне навчання кожного працівника перед початком роботи на підприємстві; щорічний інструктаж, який записується в відповідному журналі; чіткі правила та інструкції, з якими кожен працівник повинен бути ознайомлений; і визначення особи, відповідальної за безпеку пожежі.

Таким чином, запобігання впливу небезпечних і шкідливих виробничих факторів на працівників досягається шляхом забезпечення відповідності виробничих приміщень санітарним і будівельним нормам, розумної організації робочого місця, дотримання проектних технологічних процесів, використання засобів індивідуального захисту відповідно до діючих норм, навчання працівників і перевірки їхнього розуміння вимог безпеки. Для забезпечення пожежної безпеки у приміщенні використовують порошковий вогнегасник ОПУ-10, та протипожежний тепловий сповіщувач FT-B.

ВИСНОВКИ ДО 5 РОЗДІЛУ

Фахівці, які розробляють програмне забезпечення для системи «розумного університету» на базі Arduino, виявили, що такі шкідливі та небезпечні виробничі фактори, як електромагнітне та інфрачервоне випромінювання, шум і пожежна небезпека, були визначені під час проведеного аналізу виробничих факторів у приміщенні на робочому місці. Для зменшення негативного впливу на працівників, які працюють на розробці та під час подальшої експлуатації будівлі та виробничих приміщень, де розташовані ці робочі місця, розроблено заходи з покращення шкідливих показників, такі як використання систем вентиляції, опалення та кондиціонування повітря, щоб забезпечити необхідні параметри мікроклімату та складу повітряного середовища. Щоб зменшити вплив випромінювання моніторів, рекоменд Крім того, було проведено проектний розрахунок, щоб визначити ідеальне штучне освітлення для приміщення. Запропоновані дії зменшать ризик виникнення професійних захворювань і травм на цьому об’єкті дослідження.

РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРИДОВИЩА

6.1 Забруднення навколишнього середовища

Охорона навколишнього середовища – це політика, яка регулює відносини, пов’язані з охороною, використанням і відтворенням природних ресурсів, забезпеченням екологічної безпеки та запобіганням і ліквідацією шкідливих впливів, спричинених господарською та іншою діяльністю. Охорона навколишнього середовища також включає збереження природних ресурсів, генетичного фонду живої природи, ландшафтів, інших природних комплексів, унікальних

Сучасні програми, розроблені фахівцями з комп’ютерної техніки, повинні враховувати охорону та збереження навколишнього середовища.

Забруднення навколишнього середовища означає внесення в екологічну систему фізичних або структурних змін, живих або неживих елементів або відтоків енергії, що порушує процеси круговороту і обміну речовин і призводить до зниження продуктивності або руйнування екосистеми. Забруднюючі речовини зазвичай класифікуються залежно від їх природи.

-фізичні забруднення включають шумове та низькочастотне забруднення, електромагнітне забруднення та радіоактивні елементи.

-хімічні та біологічні забруднення включають синтетичні органічні речовини, важкі метали та фтористі з’єднання.

-механічні, включають пил і тверді частки.

Для вирішення проблем, пов’язаних з охороною навколишнього середовища, існує наука, відома як екологія.

Екологія – це економіка природи та вивчення всіх взаємодій живих істот з органічними та неорганічними компонентами навколишнього середовища.

Забруднення навколишнього середовища — це зміна властивостей середовища (хімічних, механічних, фізичних, біологічних і інформаційних), яка відбувається в результаті природних або штучних процесів і призводить до погіршення функцій середовища по відношенню до будь-якого біологічного або технологічного об’єкту. У процесі діяльності людина змінює якість свого навколишнього середовища. Часто ці зміни проявляються через забруднення.

Без комп’ютерів, телевізорів та інших електронних пристроїв сьогоднішній день, а, можливо, і завтрашній, важко уявити себе.

Інформаційне суспільство — концепція, яка базується на інформаційних та телекомунікаційних технологіях, які включають екологію як гуманну основу розвитку, — стало способом життя людства і забезпечує новий цикл розвитку цивілізації та планети.

Сьогодні інформаційні технології менш шкідливі для навколишнього середовища, ніж більшість інших видів активної людської діяльності, але вони все ще не можуть бути повністю екологічно чистими. Скажімо, інформаційна мережа безпосередньо залежить від кількості користувачів, тобто від кількості комп’ютерів у ній. Виготовлення одного звичайного персонального комп’ютера, однак, потребує від п’ятнадцяти до дев’ятнадцяти тонн матеріалів. Це порівняно з 25 тоннами матеріалу, необхідних для виготовлення автомобіля. 1,5 комп’ютера виготовлено на кожен функціонуючий комп’ютер протягом 4 років. Крім того, через те, що комп’ютери перестають бути технологічно актуальними, приблизно третина комп’ютерів ніколи не продається. Це вказує на те, що споживання ресурсів наближається до рівня автомобіля.

Електронні пристрої містять надзвичайно токсичні з’єднання, які, коли потрапляють у навколишнє середовище, представляють значну небезпеку для життя людей. Наприклад, електронна промисловість, зокрема мобільні телефони, споживає 22 відсотки ртуті, що виробляється

щорічно в усьому світі. Практично всі напівпровідникові пристрої використовують кадмій, який є канцерогеном. Екрани моніторів і батареї містять свинець, який особливо шкідливий для нервової системи. Діоксин та інші високотоксичні речовини виділяється в навколишнє середовище, коли захисні покриття електронних пристроїв розкладаються.

Великі виробники устаткування змушені створювати мережі по збору техніки, яка вийшла з обігу, і заводи з її утилізації через стурбованість громадськості проблемами екології та нові, більш жорсткі закони про навколишнє середовище. Конструкція обладнання також допомагає максимізувати частку матеріалів, придатних для переробки. Місцеві та регіональні закони визначають розміри мережі з утилізації «електронного брухту».

Все, що використовується в оргтехнікі, складається з органічних компонентів, таких як пластик різних видів, матеріали на основі полівінілхлориду та фенолформальдегіда, а також майже повного набору металів.

Отже, звичайні комп’ютери містять як цінні метали (наприклад, золото, срібло, алюміній, мідь) так і небезпечні метали (наприклад, кадмій, свинець, цинк, нікель тощо). Тому керівнику необхідно дотримуватися законодавства про охорону навколишнього середовища під час списання та утилізації обладнання.

6.2 Заходи щодо запобігання забруднення навколишнього середовища

Персональні комп’ютери, ноутбуки та інша інформаційна техніка широко використовується як у промисловості, у наукових дослідженнях, так і в повсякденному житті. Але будь-яка техніка стрімко застаріває, і нові, більш потужні, більш сучасні комп’ютери та комп’ютерна техніка замінюють їх. Поступово виникає проблема, що робити зі застарілою

технікою, яка є морально застарілою або вийшла з ладу, захаращуючи підсобні приміщення та склади. Утилізація комп’ютерів і оргтехніки — це процес, який виконується в кілька етапів. Найпершим кроком є зняття обладнання безпосередньо з компанії. Розбір методів і сортування отриманих матеріалів є наступним кроком. Деталі, в яких містяться дорогоцінні метали, відправляються на очищення, якщо вони можуть використовуватися як вихідна сировина, наприклад, кінескоп.

Як нам відомо, комп’ютери складаються з різних металів, таких як золото, срібло, алюміній, мідь та інші. Вторинна переробка є ще одним кроком до утилізації персональних комп’ютерів.

Цей процес полягає в тому, щоб витягти частину корисних і рідких матеріалів, таких як мідь, іридія та інші, з цієї сировини. Відтворення цього процесу набагато складніше, ніж видобути тонну міді, яка міститься в тисячотонних гірських породах.

Співробітники Національної фізичної лабораторії Великобританії придумали можливість використання спеціального розчину, який розчиняють у гарячій воді. Це було одним із нововведень для утилізації друкованих плат. який призводить до відшарування електронних компонентів.

Таким чином, у порівнянні з двома відсотками компонентів, які можна використовувати за традиційними методами, дев’яносто відсотків компонентів нових друкованих плат можна повторно використовувати.

Утилізація комп’ютерів і оргтехніки — це складний процес, який вимагає спеціальних знань і сучасного обладнання. Практично жодне підприємство не може зробити це самостійно. Таким чином, таку роботу можна довірити лише спеціалістам, які мають значний досвід у цій галузі.

З кожним роком зростає проблема утилізації використаних комп’ютерів і периферійного обладнання. Компанії стикаються з

проблемою біодеградації через зростання виробництва продуктів інформаційно-телекомунікаційних технологій і частоту заміни їх на нові моделі. Успіхи в цій галузі допоможуть виробникам зменшити податки, які вони зараз сплачують за утилізацію застарілих моделей. Останнє стає ще важливішим, оскільки економічні переваги екологізації стимулюють більшу кількість досліджень і довгострокових капіталовкладень у цю галузь. Таким чином, подальше поширення інформаційних технологій не збільшить навантаження на довкілля, а навпаки, зменшить його.

ВИСНОВКИ ДО 6 РОЗДІЛУ

Коли використовуються сучасні програми, розроблені фахівцями з комп’ютерної техніки, важливо пам’ятати про охорону та збереження навколишнього середовища. Розвиток і вдосконалення сучасних інформаційних технологій повинні бути спрямовані на те, щоб максимально покращити умови життя людей, а також забезпечити безвідходну утилізацію відпрацьованої техніки, не завдаючи шкоди навколишньому середовищу.

ВИСНОВКИ

В ході виконання роботи було проаналізовано систему «Розумний будинок» на рахунок кіберюезпеки та шляхи вдосконалення захису данних. Розроблена система протоколу дає можливість покращити енергоефективність використовуваних приміщень будинку, підвищити рівень фізичної безпеки (зменшити крадіжки), здешевити протипожежну безпеку шляхом обрання оптимальних рішень, забезпечити зручне керування процесами у будинку.

Для досягнення мети було вирішено такі наукові завдання: проведено аналіз сучасних рішень для захисту як самого будинку так і данних про господарів: платформа Інтернету речей INTERACT; платформа AjaxSystems та XiaomiSmartHomeSuite, GoogleAssistance, AppleHomeKit, AmazonAlexa та інші. Розглянуті рішення мають багато спільних характеристик, проте у них і є відмінності, зокрема технічні характеристики, особливості експлуатації та вартість.

Тому проаналізувавши деякі з систем безпеки , було розроблене експерементальне рішення щодо вбудови протоколу Kerberosв систему «Розумного Будинк» та вдосконалення її. Це сприятиме більшій захищенності данних, нормальній роботі систем і пристроїв та захист фізичного споживача і його будинку в цілому. Зроблено експерементальне дослідження в якому було показано сам процес роботи протоколу Kerberos у звичаній роботі, у порівнянні з іншими протоколами та процес удосконалення його і використання у «Розумному будинку».

У результаті аналізу небезпечних та шкідливих виробничих факторів на робочому місці фахівець, який розробляє програмне забезпечення для системи «розумного будинку», виявив, що електромагнітне та інфрачервоне випромінювання, шум і пожежна небезпека є небезпечними факторами. Для

зменшення негативного впливу на працівників, які працюють на розробці та під час подальшої експлуатації будівлі та виробничих приміщень, де розташовані ці робочі місця, розроблено заходи з покращення шкідливих показників, такі як використання систем вентиляції, опалення та кондиціонування повітря, щоб забезпечити необхідні параметри мікроклімату та складу повітряного середовища. Щоб зменшити вплив випромінювання моніторів, рекоменд Крім того, було проведено проектний розрахунок, щоб визначити ідеальне штучне освітлення для приміщення.Запропоновані дії зменшать ризик професійних захворювань і травм на цьому об’єкті дослідження.

Сучасні програми, розроблені фахівцями з комп’ютерної техніки, повинні враховувати охорону та збереження навколишнього середовища. Розвиток і вдосконалення сучасних інформаційних технологій повинні бути спрямовані на те, щоб максимально покращити умови життя людей, а також забезпечити безвідходну утилізацію відпрацьованої техніки, не завдаючи шкоди навколишньому середовищу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Платформа Інтернету речей Interact [Електронний ресурс]: https://www.interact-lighting.com/uk-ua
2. Комплект для інтелектуалізованих приміщень FIBARO PREMIUM KIT [Електронний ресурс]: https://secur.ua/komplekt-dlja-umnogo-doma-fibaro-premium-kit.html
3. Ajax Systems [Електроннийресурс]: https://uk.wikipedia.org/wiki/ Ajax_Systems
4. Бездротова система безпеки Ajax [Електронний ресурс]: https://ajax.systems
5. Bardaji, Raul; Sánchez, Albert-Miquel; Simon, Carine; Wernand, Marcel R.; Piera, Jaume (2016-03-15). "Estimating the Underwater Diffuse Attenuation Coefficient with a Low-Cost Instrument: The KdUINO DIY Buoy". Sensors. 16 (3): 373. doi:10.3390/s16030373. PMC 4813948. PMID 26999132.
6. Що таке крозумний будинок» і навіщо він потрібен? [Електронний ресурс] - Режим доступу до ресурсу: https://stylus.ua/uk/articles/528.html
7. loT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process [Електронний ресурс] - Режим доступу до ресурсу: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635- 020-00111-0
8. CYBERSECURITY CONSIDERATIONS FOR CONNECTED SMART HOME SYSTEMS AND DEVICES [Електронний ресурс] Режим доступу до ресурсу: https://industrie-4-0.ul.com/wp-content/uploads/2018/02/UL_Cybersecurity_ SmartHome_White_Pap er en.pdf
9. Методика аналізу ризиків Microsoft [Електронний ресурс] - Режим доступу до ресурсу: http://ni.biz.ua/3/3 5/3 52705 metodika-analiza-riskov-Microsoft. Html

10. НД-Т31-2.5-005-99 [Електронний ресурс - Режим доступу до ресурсу https://tzi.ua/assets/files/6D0%9D%D0%94%D0%A2%D0%97%D0%86-2.5-005_99 pdf
11. Weakness Within: Kerberos Delegation (Електронний ресурс| Режим доступу до ресурсу: https://www.eyberark.com/resources/threat-research-blog/weakness-within-kerberos-delegation
12. CYBERSECURITY CONSIDERATIONS FOR CONNECTED SMART HOME SYSTEMS AND DEVICES [Електронний ресурс] - Режим доступу до ресурс: https://industrie-4-0.ul.com/wp-content/uploads/2018/02/UL_Cybersecurity_ SmartHome White_ Pap er en.odf
13. МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗЛЕКИ РОЗУМНОГО БУДИНКУ [Електронний ресурс] - Режим доСТУПУ До ресурсу: https://oaji.net/articles/2020/8096-1594973817.pdf
14. Privacy Preserving Data Analytics for Smart Homes [Електронний ресурс] - Режим доступу до ресурсу: https://www.i eee-security.org/TC/SPW2013/papers/data/5017a023.pdf
15. Kerberos: An Authentication Service for Computer Networks [Електронний ресурс] - Режим доступу до ресурсу: https://courses.cs.vt.edu/~cs5204/fall09-kafura/Papers/Security/Kerberos-Paper.pdf
16. Електронний ресурс https://ajax.systems/ua/blog/cyber-safety-essentials/
17. A. Tilley, “How a few words to Apple’s Siri unlocked a man’s front door,” http://www.forbes.com/sites/aarontilley/2016/09/21/ apple-homekit-siri-security, 2016
18. S. Bandara et al., “Access control framework for api-enabled devices in smart buildings,” in APCC. IEEE, 2016.
19. Електронний ресур Опис протоколу Kerberos 5 і його архітектурна реалізація у WindowsServer 2003.

20. Kerberos Weaknesses: Pass the Ticket Is a Real Threat [Електронний ресурс] - Режим доступу ДО ресурсу: https://www.varonis.com/blog/kerberos-loopholes-pass-ticket
21. Kerberos Attack: How to Stop _[Електронний ресурс| Режим доступу Golden до Tickets? ресурсу: https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets
22. Поляков О. І. Розумний будинок: технології та системи керування. - К.: НТ Україна, 2017. - 256 с.
23. Кучеренко О. М. Ефективне використання технологій розумного будинку для підвищення безпеки. - Дніпро: Видавництво ДНУ, 2022. - 128 с.
24. Санітарні норми виробничого шуму, ультразвуку та інфразвуку: ДСН 3.3.6.037-99-2000.
25. Розумне освітлення [Електронний ресурс]. – Режим доступу до ресурсу: https://milight.com.ua/ua/umnoe-osveshchenie/
26. Технологія розумного будинку: як AI створює простір, комфортний для життя [Електронний ресурс]. – Режим доступу до ресурсу: https://www.everest.ua/tehnologiya-rozumnogo-budynku-yak-ai-stvoryuye-prostirkomfortnyj-dlya-zhyttya/
27. Granzer W. P. Security in Building Automation Systems / Wolfgang Praus Granzer. Munich: Appress, 2018. – 578 с
28. Dickson B. How to prevent your IoT devices from being forced into botnet bondage [Електроннийресурс] / Dickson. – 2015. – Режимдоступудоресурсу: https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devices-from-being- forcedinto-botnet-slavery/.