КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій
(факультет)

інформаційних технологій
(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: «Розробка підсистеми захисту "розумного" дому»

ШИМЧУК ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ
(прізвище, ім’я та по батькові студента повністю)

Київ 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

(факультет)

інформаційних технологій

(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ
д.т.н., професор Цюцюра С.В.

«___» _____20___ року

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: «Розробка підсистеми захисту "розумного" дому»

Виконав:студент 4-го курсу, групи КН-41

Спеціальності: 122 «Комп`ютерні науки»

Спеціалізація: _«Інформаційні управляючі системи та технології»
(шифр і назва напряму підготовки, спеціальності)

Шимчук О.О.
(прізвище та ініціали)

Керівник к.т.н., доц. Горда О.В.
(прізвище та ініціали)

Рецензент к.т.н., доц. Шутовський О.М.
(прізвище та ініціали)

Київ, 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: __автоматизації і інформаційних технологій
Кафедра:__ __інформаційних технологій
Освітній рівень: «бакалавр» за ОПП
Спеціальність:_122 «Комп`ютерні науки»
Спеціалізація:__Інформаційні управляючі системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ
д.т.н., професор Цюцюра С.В.
_____
„___” _____2023 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

_____Шимчук Олександр Олександрович_____
(прізвище, ім’я, по батькові)

1. Тема роботи: Розробка підсистеми захисту "розумного" дому
керівник роботи: Горда Олена Володимирівна, д.т.н,
затверджені наказом ректора КНУБА № 1811/2 від « 17» листопада 2022 р.

2. Термін подачі студентом роботи до захисту: 01 червня 2023 .
3. Вихідні дані до роботи _____
4. Зміст пояснювальної записки: Вступ 1. Аналіз та дослідження проблеми. 2. Проєктування програмного забезпечення. 3. Розробка програмного забезпечення. 4. Техніко-економічне обґрунтування розробки підсистеми (Бізнес-план)
5. Перелік презентаційно-інформаційних слайдів: 1. Розробка підсистем захисту розумного будинку. 2. Вступ. 3. Дерево цілей . 4. Загрози та контрзаходи. 5. Три основних методики шифрування. 6. Постановка основних задач. 7. Перспективи подальшого дослідження. 8. Функціональні та нефункціональні вимоги . 9. Сутність клієнт-серверної архітектури. 10. Розподіл функцій та компонентів між модулями ПЗ. 11. Симетричне та асиметричне шифрування. 12. Бізнес план. 13. Висновок.

6. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис
Техніко-економічне обґрунтування розробки підсистеми (Бізнес-план)	д.т.н. проф. Цюцюра С.В.		
Прийом програмного продукту	к.т.н., доц. Єрукаєв А.В.		

7. Дата видачі завдання: 15 лютого 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Види робіт та їх зміст	Дата виконання
Р. 1. Аналіз та дослідження проблеми	14.04.2023-22.04.2023
Р. 2. Проєктування інформаційного забезпечення	22.04.2023-01.05.2023
Р. 3. Практична реалізація	02.05.2023-12.05.2023
Р. 4. Бізнес план	05.04.2023-12.04.2023
Остаточне оформлення роботи	23.05.2023–24.05.2023
Направлення роботи на рецензування	24.05.2023-28.05.2023
Попередній захист роботи на кафедрі	13.06.2023–14.06.2023

Бакалавр _____ Шимчук О.О.
(підпис) (прізвище та ініціали)

Керівник _____ Горда О.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Шимчук О.О. Розробка підсистем захисту «розумного» дому

Дипломна бакалаврська робота за спеціальністю – «Комп’ютерні науки» - Київський національний університет будівництва та архітектури, Київ, 2023 рік.

Бакалаврську роботу присвячено дослідженню основних тенденцій, принципів та реалізацій підсистем захисту «розумних» будинків.

У роботі досліджено основні принципи та технології розробки систем захисту "розумного" будинку, створені та проаналізовані, основні методи забезпечення безпеки більшості підключених пристрої.

Ключовими словами є: "Безпека", "розумний будинок", "системи захисту", "шифрування", "функціональні можливості".

ABSTRACT

Shymchuk O.O. Development of "smart" home protection subsystems

Bachelor's diploma work in the specialty - "Computer Science" - Kyiv National University of Construction and Architecture, Kyiv, 2023.

The bachelor's work is devoted to the study of the main trends, principles and realizations of the protection subsystems of "smart" buildings.

The work explores the basic principles and technologies of developing "smart" home protection systems, creates and analyzes the main methods of ensuring the security of most connected devices.

Key words are: "Security", "smart home", "protection systems", "encryption", "functionality".

ЗМІСТ

ВСТУП 9

1. АНАЛІЗ ТА ДОСЛІДЖЕННЯ ПРОБЛЕМИ 11

1.1. Огляд ринку, концепції розумних домівок та їх захисту 11

1.1.1 Тенденції та перспективи ринку розумних домівок 12

1.1.2 Аналіз існуючих систем захисту розумних домівок..... 12

1.1.3 Інноваційні рішення в галузі захисту розумних домівок 14

1.2. Опис загроз та вразливостей систем розумного дому 14

1.2.1. Типові загрози для розумного дому 15

1.2.2. Аналіз вразливостей існуючих систем розумного дому 16

1.2.3. Шляхи реалізації атак на розумний дім 19

1.3. Огляд шифрування розумного дому. 21

1.4. Розробка дерева цілей..... 23

1.5. Постановка задачі 26

1.6. Заключні рекомендації 26

1.6.1. Визначення основних висновків та результатів дослідження. 27

1.6.2. Рекомендації щодо покращення захисту розумного дому……. 27

1.6.3. Перспективи подальшого дослідження..... 28

2. ПРОЕКТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ..... 30

2.1. Опис необхідних функціональних та нефункціональних вимог до програмного забезпечення..... 30

2.2. Опис вимог до забезпечення безпеки, доступності, надійності та інших аспектів програмного забезпечення..... 33

2.3. Архітектурні особливості..... 36

2.3.1. Вибір архітектурного стилю 36

2.3.2. Опис загальної архітектури системи захисту розумного дому…….. 38

2.3.3. Розподіл функцій та компонентів між модулями програмного забезпечення 41

2.4. Огляд основних алгоритмів та методів захисту, що використовуються в системах розумного дому 44

3. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 48

3.1. Вибір програмного інструментарію 48

3.1.1. Вибір мови програмування 48

3.1.2. Вибір програмного середовища 50

3.2. Програмування основних захисних елементів розумного дому……. 52

3.2.1. Встановлення захищеного підключення Wi-Fi з використанням WPA2 52

3.2.2. Програмування процесу аутентифікації та авторизації .. 53

3.2.3. Програмування методу шифрування комунікації 55

3.2.4. Оновлення програмного забезпечення 56

3.2.5. Програмування методу відстеження активності 57

3.2.6. Метод захисту від перехоплення даних 60

3.2.7. Метод захисту від фізичного доступу 61

3.2.8. Метод симетричного шифрування 63

3.2.9. Метод асиметричного шифрування 64

3.2.10. Хешування паролів 65

4. БІЗНЕС-ПЛАН 67

4.1. Основні питання сутності власного та конкурентного продукту…….. 67

4.1.1. Фінансові відомості проєкту 68
4.2. Проектований продукт або вид послуг 70
4.2.1. Опис продукту проєкту 70
4.3. Оцінка ринку збуту 72
4.3.1. Дослідження відношення продукту до ринку 72
4.3.2. Інформаційні джерела 73
4.3.3. Аналіз даних 74
4.4. Конкуренція 75
4.5. Умови та план виробництва 78
4.6. Організаційний план 80
4.6.1. Працівники та їх кваліфікація 80
4.7. Юридичний план. Приватна власність розроблюємого продукту 81
4.8. Оцінка ризику і страхування 82
4.8.1. Ризики і конфлікти 82
4.8.2. Зменшення витрат 83
4.9. Стратегія фінансування 85
4.9.1. Засоби реалізації продукту 85
4.9.2. Джерела фінансування ресурсів 87
ВИСНОВОК 90
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 92
Додаток А 94

ВСТУП

Актуальність дослідження. Дослідження систем захисту систем розумного будинку полягає в необхідності забезпечення безпеки та конфіденційності в умовах швидкого розвитку технологій та зростаючого застосування розумних будинків. Злочинні елементи стають все більш винахідливими в шляхах проникнення до системи розумного будинку, тому необхідно розробляти ефективні підсистеми захисту, що відповідають сучасним вимогам та стандартам безпеки.

Мета дослідження. Розробка підсистеми захисту систем розумного будинку, яка забезпечує високий рівень безпеки, виявлення та запобігання можливим загрозам та вразливостям. Подолання цих викликів сприятиме створенню надійних та безпечних систем розумного будинку, що забезпечує затишок та захист для користувачів.

Об’єкт дослідження. Системи розумного будинку, які включають різноманітні елементи та пристрої, що забезпечують комфорт та автоматизацію функцій в будинку. Проте, ці системи також стикаються з ризиками та загрозами, що вимагає належного захисту.

Предмет дослідження. Підсистема захисту систем розумного будинку, яка включає в себе архітектуру, методи та інструменти для виявлення, запобігання та реагування на можливі загрози. Розробка цієї підсистеми має на меті забезпечити цілісну безпеку системи розумного будинку.

Методика дослідження. Включає аналіз існуючих рішень та стандартів, дослідження потенційних загроз та вразливостей, проектування архітектури та функціонаналу підсистеми захисту, програмування програмного продукту та розробку бізнес-плану. Були використані науково-дослідницькі методи, а також практичні експерименти та тестування для перевірки ефективності розроблених рішень.

Завдання дослідження. Аналіз існуючих технологій та методів захисту, ідентифікацію потенційних загроз та вразливостей систем

розумного будинку, розробку концептуальної моделі та архітектури підсистеми захисту, реалізацію програмного продукту з використанням сучасних інструментів програмування, а також оцінку комерційної придатності розробленої системи та розробку бізнес-плану.

Практична значимість. Полягає в тому, що розроблена підсистема захисту систем розумного будинку забезпечує надійний рівень безпеки та захисту користувачів. Це сприяє популяризації та впровадженню розумних будинків, забезпечує конфіденційність та захищеність особистих даних, а також зменшує ризик несанкціонованого доступу та злочинних дій.

Результат дослідження. Розроблена підсистемаа захисту систем розумного будинку, яка ефективно виявляє та запобігає можливим загрозам та вразливостям. Крім того, був розроблений програмний продукт, який втілює розроблену архітектуру та функціонал підсистеми захисту. Також було розроблено бізнес-план, що демонструє комерційну придатність розробленої системи та її можливість успішного впровадження на ринку розумних будинків.

1. АНАЛІЗ ТА ДОСЛІДЖЕННЯ ПРОБЛЕМИ

1.1. Огляд ринку, концепції розумних домівок та їх захисту

Розумний будинок - це будинок, обладнаний різноманітними пристроями та системами, які автоматизують та оптимізують його функціонування з метою підвищення комфорту, безпеки та енергоефективності.

У розумному будинку використовуються різні технології та системи автоматизації, такі як система освітлення, опалення та кондиціонування повітря, система безпеки, система керування енергоспоживанням, система домашнього кінотеатру, система домашньої автоматизації тощо. Тож за допомогою різних сенсорів, контролерів та програмного забезпечення, розумний будинок може відслідковувати та аналізувати поведінку та потреби мешканців, що дозволяє оптимізувати роботу різних систем будинку з метою забезпечення максимальної ефективності та зручності для мешканців.

Розумний будинок може керуватися за допомогою голосових команд, мобільного додатку, дистанційного керування або автоматично, залежно від налаштувань системи. Всі ці функції дозволяють мешканцям контролювати та керувати будинком з будь-якого місця та в будь-який час, що робить життя в розумному будинку більш комфортним та безпечним. Але, як ми знаємо, у л

За останні кілька років розумні домівки стали все популярнішими серед споживачів. За даними досліджень, глобальний ринок розумних домівок очікується зрости з 76 мільярдів доларів у 2022 році до 135 мільярдів доларів у 2025 році [1]. Такі тенденції росту пов'язані зі збільшенням інтересу до автоматизації будинків, зручності та збільшенням збереження енергії. Однак разом з цим зростає і загроза кібератак на розумні домівки, що може привести до втечі конфіденційної інформації, порушення приватності, або навіть фізичних пошкоджень.

1.1.1 Тенденції та перспективи ринку розумних домівок

Розумні домівки є однією з найшвидше зростаючих галузей в світі IoT (Internet of Things). Споживачі все більше зацікавлені в зручності та практичності, які забезпечує автоматизація будинку. Однак, в той же час, з'являється більше загроз та ризиків з приводу безпеки і приватності.

Загалом, ринок розумних домівок тенденції зростання, і, згідно з дослідженнями, очікується, що він буде зростати зі стабільною темпом у майбутньому. Більше того, з'являться нові можливості і технології, що дають змогу розширювати можливості розумних домівок та покращувати їх функціональність. Наприклад, додатки для голосового керування, інтеграція з різними девайсами, такими як розумні двері, вікна, системи вентиляції тощо.

Проте, разом з цими можливостями з'являється і більше потенційних точок входу для кібератак. Тому, бізнеси, що працюють у цій галузі, мають велику відповідальність забезпечити належний рівень захисту розумних домівок та даних користувачів.

1.1.2 *Аналіз існуючих систем захисту розумних домівок*

На даний момент існує багато різних систем захисту розумних домівок, що використовують різні методи захисту та критерії безпеки. Наприклад, деякі системи використовують паролі та шифрування даних, інші пропонують біометричну аутентифікацію, а деякі використовують мережеві заходи безпеки, такі як брандмауери та системи виявлення вторгнень. Приклад найпопулярніших з них:

1. Ring Alarm: Ring Alarm є системою безпеки, яка включає в себе різні компоненти, такі як сенсори дверей/вікон, рухові датчики, камери спостереження тощо. Вона підключається до Інтернету та надсилає

повідомлення на ваш телефон у разі виявлення підозрілого руху або інших потенційних проблем.

2. ADT Smart Home Security: ADT є відомим постачальником систем безпеки, який також пропонує розумні рішення для будинків. Їх система включає в себе різноманітні сенсори, камери спостереження, детектори витоку газу та вуглекислого газу, систему пожежної сигналізації тощо. ADT також має сервіс моніторингу, який може надсилати повідомлення на місцеву поліцію або пожежну службу у разі виявлення небезпеки.

3. SimpliSafe: SimpliSafe є ще однією популярною системою безпеки для розумного будинку. Вона має бездротові сенсори, рухові датчики, камери, датчики диму та інші компоненти. SimpliSafe також пропонує моніторингові плани, які дозволяють вам забезпечити постійний нагляд за вашим будинком.

4. Nest Secure: Nest Secure є системою безпеки, розробленою компанією Nest, яка спеціалізується на розумних продуктах для будинку. Вона включає в себе датчики дверей/вікон, рухові датчики, клавіатуру для введення коду доступу та інші компоненти. Nest Secure може бути інтегрована з іншими розумними пристроями Nest, наприклад, камерами спостереження або термостатами.

5. Honeywell Home Security: Honeywell також пропонує системи безпеки для розумних будинків. Вони включають в себе сенсори дверей/вікон, рухові датчики, витяжку вуглекислого газу та інші компоненти. Honeywell також надає можливість керувати системою захисту з використанням мобільного додатку, що дає вам дистанційний доступ до вашої системи безпеки.

Однак, незважаючи на наявність багатьох систем захисту, багато з них не забезпечують достатнього рівня захисту від кібератак. Наприклад, в деяких системах біометрична аутентифікація може бути обманута з використанням фейкових даних, а інші системи можуть бути зламані шляхом використання підроблених сертифікатів.

1.1.3 Інноваційні рішення в галузі захисту розумних домівок

Інноваційні технології та рішення можуть допомогти покращити захист розумних домівок та даних користувачів. Наприклад, однією з них є використання блокчейн технології для забезпечення безпеки даних та ідентифікації користувачів. Блокчейн дозволяє зберігати дані у розподіленій мережі, що робить їх більш стійкими до зламів та крадіжок. Крім того, блокчейн може бути використаний для створення системи ідентифікації користувачів, що дозволить уникнути проблем з фальшивими обліковими записами та зберігати дані про користувачів у безпечному місці.

Іншим інноваційним рішенням є використання штучного інтелекту для виявлення підозрілих дій у системі розумного дому. Завдяки цьому розробники можуть швидко виявляти та реагувати на кібератаки та інші загрози безпеці.

Також, до інноваційних рішень в галузі захисту розумних домівок можна віднести розвиток нових методів аутентифікації, таких як розпізнавання обличчя та відбитків пальців з використанням машинного навчання, що дозволяє покращити стійкість систем захисту до шахрайства.

Отже, розробка підсистем захисту розумного дому є важливою задачею, оскільки безпека користувачів та їхніх даних є однією з найважливіших складових розумного дому. Для досягнення належного рівня захисту від кібератак необхідно постійно вдосконалювати існуючі системи та застосовувати нові інноваційні технології.

1.2. Опис загроз та вразливостей систем розумного дому

Так як системи IoT мають значні плюси, в концепції яких вони є технологіями, які дозволяють автоматизувати багато рутинних процесів в

повсякденному житті, так і мають свої недоліки. В основному, з використанням цієї технології пов'язуються певні загрози. Наприклад, можливість зламу системи, яка керує всім домом, може призвести до ризику безпеки жителів та їх майна. Також, відсутність стандартів безпеки може призвести до використання пристроїв у кібератаках та крадіжках даних. У цьому контексті, важливо розуміти потенційні загрози та приймати заходи для захисту від них.

1.2.1. *Типові загрози для розумного дому*

З технологічного погляду, розумний дім є мережевою системою, що підключає до мережі різні смарт-пристрої, такі як телефони, планшети, ноутбуки та інші гаджети. Тож, як і в усіх мережевих системах, існують ризики і загрози для безпеки. Ось найсуттєвіші з них:

1. Кібератаки: Розумний дім містить велику кількість електронних пристроїв, які підключені до мережі Інтернет. Це може стати предметом кібератак, які можуть призвести до порушення конфіденційності даних, втрати контролю над пристроями або навіть можуть стати загрозою для життя та здоров'я власників будинку.
2. Зламання паролів: Розумний дім містить велику кількість пристроїв, які потребують авторизації за допомогою паролів. Якщо паролі занадто прості або якщо вони були зламані, це може стати загрозою безпеки.
3. Фізичний доступ: Якщо зловмисники можуть отримати фізичний доступ до розумного дому, вони можуть зламати систему захисту або виконати шкідливі дії, такі як встановлення шпигунського програмного забезпечення або викрадення даних.
4. Відсутність оновлень: Більшість розумних пристроїв мають програмне забезпечення, яке потребує регулярного оновлення. Якщо власники не оновлюють програмне забезпечення своїх розумних пристроїв, це може стати причиною вразливості і непродуктивності

системи, що може призвести до збоїв і порушення роботи всієї мережі. Також, застаріле програмне забезпечення може містити вразливості, які можуть бути використані для кібератак.

5. Віддалений доступ: Багато розумних пристроїв дозволяють власникам віддалений доступ до своїх систем через Інтернет. Однак, якщо цей доступ не захищений від зламу, то це може стати загрозою для конфіденційності та безпеки даних.
6. Недостатня захищеність мережі: Розумний дім містить велику кількість електронних пристроїв, які підключені до мережі Інтернет. Якщо мережа не захищена від зламу, то це може стати загрозою для безпеки всієї мережі, включаючи розумний дім.
7. Недостатня захист від шпигунського програмного забезпечення: Розумний дім може бути піддається атакам шпигунського програмного забезпечення, яке може збирати конфіденційну інформацію та навіть віддалено контролювати пристрої.

Усі ці загрози, і не тільки, можуть призвести до порушення безпеки розумного дому та залишити його власників без контролю над системою, що може бути дуже небезпечним. Для захисту від цих загроз, важливо використовувати сильні паролі, оновлювати програмне забезпечення, використовувати захист мережі та використовувати антивірусне програмне забезпечення, тощо.

1.2.2. Аналіз вразливостей існуючих систем розумного дому

З більшим застосуванням даних систем з'являються нові виклики щодо забезпечення безпеки та конфіденційності власників будинку. Аналіз вразливостей існуючих систем розумного дому показує, що деякі з них можуть бути піддаються атакам та злому. Ось кілька вразливостей, які можуть бути присутні в існуючих системах розумного дому:

1. Відкриті порти і слабкі паролі: Це може бути найбільш поширеною вразливістю в системах розумного дому. Якщо використовується

слабкий пароль, зловмисник може використати його для доступу до системи. Крім того, відкриті порти можуть бути використані для атаки на систему ззовні.

2. Вразливості програмного забезпечення: В системах розумного дому, як і в будь-якому іншому програмному забезпеченні, можуть бути виявлені вразливості, які можуть бути використані для злому системи.
3. Незашифровані з'єднання: Якщо з'єднання між пристроями та центральною системою не зашифровані, то зловмисники можуть отримати доступ до інформації, що передається між ними.
4. Фізичний доступ до пристроїв: Якщо зловмисники мають фізичний доступ до пристроїв, вони можуть мати можливість змінити їх налаштування або взагалі зламати їх.
5. Неоглядна підключення до Інтернету: Якщо підключення до Інтернету не належним чином налаштоване, то можуть бути відкриті додаткові порти, які зловмисники можуть використовувати для злому системи.
6. Відсутність засобів аутентифікації: Якщо система розумного дому не має адекватних засобів аутентифікації, то зловмисники можуть отримати доступ до системи, використовуючи підроблені дані.
7. Використання старих протоколів: Якщо система розумного дому використовує застарілі протоколи зв'язку, то це може стати вразливістю, оскільки такі протоколи можуть бути піддані атакам.
8. Проблеми з безпекою веб-інтерфейсу: Якщо система розумного дому має веб-інтерфейс для керування, то це може стати вразливістю, якщо веб-інтерфейс не захищений належним чином.
9. Недостатнє оновлення системи: Якщо система розумного дому не отримує регулярних оновлень з метою виправлення вразливостей, то це може стати проблемою, оскільки зловмисники можуть використовувати відомі вразливості для злому системи.

10. Відсутність захисту від злому: Якщо система розумного дому не має захисту від злому, то зловмисники можуть використовувати різні методи злому, такі як внесення змін до програмного забезпечення або використання вразливостей для злому системи.

Загалом, системи розумного дому можуть бути вразливі для атак, якщо не будуть вжиті відповідні заходи забезпечення безпеки та конфіденційності. Для захисту від атак необхідно забезпечити достатній рівень безпеки та конфіденційності системи розумного дому.

1. Заходи безпеки, які можна вжити для захисту системи розумного дому включають:
2. Використання сильних паролів та двофакторної аутентифікації для забезпечення безпеки входу в систему.
3. Шифрування даних, що передаються через Інтернет.
4. Використання надійних протоколів зв'язку та їх належна конфігурація.
5. Перевірка налаштувань системи розумного дому для виявлення можливих вразливостей та їх виправлення.
6. Регулярне оновлення програмного забезпечення та компонентів системи розумного дому для забезпечення їхньої безпеки та стійкості.
7. Встановлення мережевого брандмауера та інших захисних заходів для запобігання вторгненням в систему розумного дому.
8. Використання захищеного веб-інтерфейсу з достатньою аутентифікацією та шифруванням даних.
9. Обмеження доступу до системи розумного дому тільки для авторизованих користувачів та пристроїв.
10. Відключення непотрібних функцій та послуг, які можуть збільшити поверхню атаки.
11. Періодичний аудит системи розумного дому для виявлення вразливостей та інших проблем.

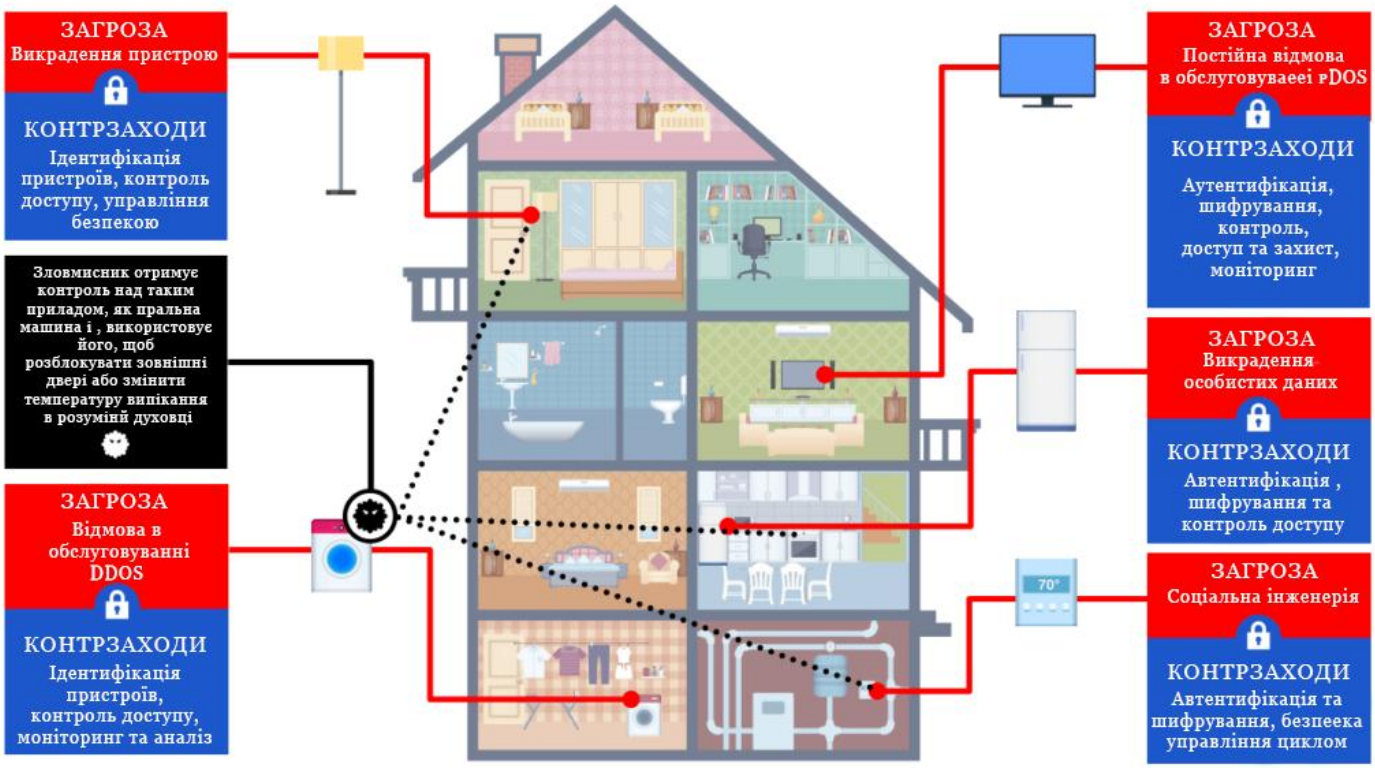


Рисунок 1.1 – Загрози і контрзаходи в розумних речах

Загалом, забезпечення безпеки та конфіденційності систем розумного дому є важливим завданням для забезпечення надійного та безпечного функціонування системи. Це допоможе уникнути можливих атак та захистити особисті дані користувачів від зловмисників.

1.2.3. Шляхи реалізації атак на розумний дім

Ось декілька шляхів реалізації атак на розумний дім:

Атака на мережу Wi-Fi: Атакувач може використати слабкі місця в мережі Wi-Fi, щоб отримати доступ до системи розумного дому. Для цього він може скористатися різними техніками, такими як перехоплення трафіку, ман-в-середньому атаки та інші.

Атака на хмарне сховище: Багато розумних домів зберігають дані в хмарних сховищах. Атакувач може спробувати отримати доступ до цих сховищ, використовуючи різні методи, такі як підбір паролів або використання вразливостей.

Атака на додатки розумного дому: Багато розумних домів мають свої додатки, які дозволяють керувати системою з мобільних пристроїв. Атакувач може спробувати використати вразливості у цих додатках, щоб отримати доступ до системи розумного дому.

Атака на роутер: Атакувач може спробувати отримати доступ до роутера, який забезпечує зв'язок між різними пристроями у розумному домі. Він може використати вразливості роутера або спробувати зламати його пароль.

Атака на підключені пристрої: Атакувач може спробувати отримати доступ до будь-якого з пристроїв, підключених до системи розумного дому. Він може використати зламати пароль на пристрої, використати вразливість у програмному забезпеченні, яке використовується на пристрої, або використовувати інші методи атак.

Атака на систему голосового керування: Багато систем розумного дому мають функцію голосового керування, таку як Amazon Alexa або Google Home. Атакувач може спробувати використати цю функцію для керування системою розумного дому або отримання конфіденційної інформації.

Атака на систему автоматизації: Багато систем розумного дому мають функцію автоматизації, яка дозволяє налаштувати різні сценарії для пристроїв у домі. Атакувач може спробувати використати цю функцію, щоб налаштувати небезпечні сценарії, такі як вмикання світла в середині ночі або відкриття дверей під час відсутності мешканців.

Атака на систему відеоспостереження: Багато систем розумного дому мають камери відеоспостереження, які дозволяють віддалено переглядати те, що відбувається в домі. Атакувач може спробувати отримати доступ до цих камер, щоб вивчити розташування пристроїв, розміщення дверей та вікон або використовувати цю інформацію для злочинних цілей. Атака на систему звукового спостереження: Деякі системи розумного дому мають мікрофони, які дозволяють записувати

звук у приміщенні. Атакувач може спробувати отримати доступ до цих мікрофонів, щоб отримати конфіденційну інформацію.

Соціальна інженерія: Один з найпростіших, але ефективних способів атак на розумний дім - це соціальна інженерія. Атакувач може спробувати отримати доступ до системи розумного дому, використовуючи ім'я користувача та пароль, які він отримав шляхом обману або шахрайства. Наприклад, він може надіслати електронний лист, який виглядає, як повідомлення від компанії-виробника пристрою розумного дому, з проханням надати інформацію про свої облікові дані.

Крім того, атакувач може спробувати використовувати соціальні мережі, фішингові атаки або інші методи маніпулювання користувачем, щоб отримати доступ до системи розумного дому. Наприклад, він може створити фальшивий профіль на соціальній мережі та запропонувати співпрацю чи допомогу користувачеві з проблемами в системі розумного дому, або надіслати фішингове повідомлення з проханням надати облікові дані для входу до системи.

Загалом, атаки на розумний дім можуть бути досить складними та різноманітними, і важливо пам'ятати про заходи безпеки та захисту пристроїв розумного дому. Деякі рекомендації щодо захисту системи розумного дому можуть включати в себе використання сильних паролів, зміну паролів регулярно, оновлення програмного забезпечення на пристроях, використання антивірусного програмного забезпечення та захист мережі Wi-Fi від несанкціонованого доступу.

1.3. Огляд шифрування розумного дому.

Системи захисту розумного дому складаються з різних компонентів, таких як шифрування даних, відеокамери, датчики руху, системи контролю доступу та інші. Хоча основна концепція захисту знаходиться в ключовому елементі, а саме – шифруванні.

Шифрування даних – це процес перетворення звичайного тексту в зашифрований вигляд, що забезпечує конфіденційність даних. Існує багато алгоритмів шифрування, що застосовуються в системах розумного дому. Основні алгоритми шифрування, які використовуються в системах розумного дому, включають в себе:

1. AES (Advanced Encryption Standard): це симетричний алгоритм шифрування, який використовується для захисту конфіденційної інформації, такої як паролі та ключі. Цей алгоритм шифрує дані блоками розміром 128 біт, 192 біт або 256 біт.
2. RSA (Rivest–Shamir–Adleman): це асиметричний алгоритм шифрування, який використовується для шифрування та розшифрування повідомлень та для цифрового підпису. Цей алгоритм використовує ключі розміром 1024 біт, 2048 біт або 4096 біт.
3. Blowfish: це симетричний алгоритм шифрування, який використовується для захисту даних та паролів. Цей алгоритм шифрує дані блоками розміром 64 біта.
4. ChaCha20: це симетричний алгоритм шифрування, який використовується для шифрування даних та забезпечення безпеки передачі даних в мережі. Цей алгоритм шифрує дані блоками розміром 512 біт.

Простий порівняльний аналіз описано в таблиці 1.1 – опис алгоритмів шифрування, які використовуються в системах «розумного» дому.

Таблиця 1.1 – простий опис алгоритмів шифрування розумного дому

Алгоритм шифрування	Використання в системах захисту	Рівень захисту
AES	Контроль доступу, шифрування даних	Високий
Blowfish	Захист паролів та даних	Середній

RSA	Шифрування даних, цифровий підпис	Високий

Продовження таблиці 1.1 – простий опис алгоритмів шифрування розумного дому

Алгоритм шифрування	Використання в системах захисту	Рівень захисту
ChaCha20	Захист передачі даних в мережі	Високий

У цій таблиці представлені основні алгоритми шифрування, що використовуються в системах захисту розумного дому. Рівень захисту залежить від алгоритму шифрування, який використовується. AES та RSA забезпечують високий рівень захисту, тоді як Blowfish та ChaCha20 забезпечують середній та високий рівень захисту відповідно.

Шифрування даних є важливою складовою будь-якої системи захисту розумного дому, яка забезпечує конфіденційність даних та захист від несанкціонованого доступу. Різні алгоритми шифрування мають різний рівень захисту, і використання правильного алгоритму шифрування допоможе забезпечити максимальний рівень захисту.

1.4.Розробка дерева цілей

Захист від несанкціонованого доступу до систем розумного будинку є необхідністю, оскільки це може призвести до небезпеки для життя та здоров'я людей, а також до втрати майна. Для досягнення цієї мети розроблений комплексний підхід до захисту розумного будинку, що включає в себе програмні та апаратні засоби захисту, методи реагування на загрози та процедури взаємодії з користувачами, який описаний нижче.

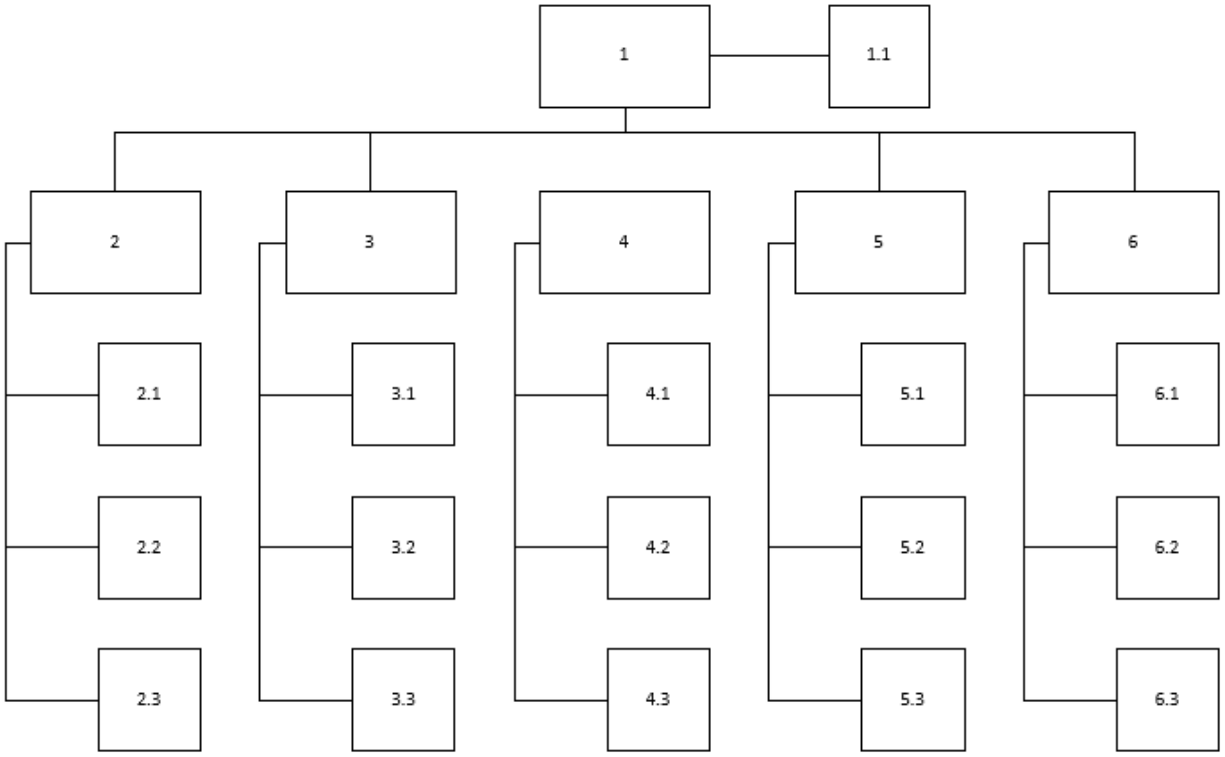


Рисунок 1.1 – Дерево цілей розроблюваного проекту

Опис розробленого дерева цілей:

1. Загальна мета:
   1.1. Розробити ефективну підсистему захисту розумного будинку.
2. Цілі першого рівня:
   2.1. Дослідити основні загрози та вразливості розумних будинків.
   2.2. Розробити стратегію захисту розумного будинку.
   2.3. Розробити програмні та апаратні засоби захисту розумного будинку.
3. Цілі другого рівня:
   3.1. Дослідити основні загрози, що можуть виникнути при використанні розумних будинків, включаючи атаки зловмисників, некоректну роботу програмного забезпечення та несправності апаратного забезпечення.
   3.2. Визначити найбільш ефективні методи захисту від основних загроз, включаючи захист мережі, захист апаратного забезпечення та захист програмного забезпечення.
   3.3. Розробити програмні та апаратні засоби захисту розумного будинку, що забезпечать ефективний захист від визначених загроз.

4. Цілі третього рівня:
   4.1. Дослідити методи захисту мережі, що використовуються в розумних будинках, включаючи файрволи, віртуальні приватні мережі та інші.
   4.2. Визначити найбільш ефективні методи захисту апаратного забезпечення розумного будинку, що забезпечать захист від фізичних впливів, таких як зламування, крадіжки та інших негативних дій.
   4.3. Розробити програмні засоби захисту розумного будинку, що забезпечать захист від різноманітних атак, включаючи захист від вірусів, шкідливих скриптів та інших шкідливих програм.
5. Цілі четвертого рівня:
   5.1. Дослідити технології, що використовуються в розумних будинках, та визначити загрози, що можуть виникнути при їх використанні.
   5.2. Розробити методи захисту від специфічних загроз, що виникають при використанні різних технологій, таких як голосові асистенти, датчики руху та інші.
   5.3. Розробити програмні та апаратні засоби захисту, що забезпечать захист від виявлених загроз та забезпечать безпеку при використанні розумного будинку.
6. Цілі п'ятого рівня:
   6.1. Розробити протоколи та процедури реагування на виявлені загрози та атаки.
   6.2. Перевірити ефективність розроблених програмних та апаратних засобів захисту на практиці.
   6.3. Провести аналіз можливих підходів до подальшого вдосконалення підсистеми захисту розумного будинку.

Дерево цілей, розроблене для даної дипломної роботи, дозволило систематизувати та усвідомити всі складові процесу розробки підсистем захисту розумного будинку. Однак, не всі цілі повинні бути обов'язково виконані. Залежно від ресурсів та обмежень, можуть бути виконані лише

окремі частини дерева цілей. Головною метою є створення ефективної підсистеми захисту розумного будинку, яка забезпечить безпеку жителів та їх майна. Результати дослідження та розробки підсистем захисту можуть бути використані для подальшого покращення безпеки та захисту від несанкціонованого доступу до систем розумного будинку.

1.5.Постановка задачі

Мета даної роботи – дослідження та розробка підсистем захисту розумного будинку з метою зменшення ризику кібератак та збільшення рівня приватності користувачів.

Для досягнення цієї мети, необхідно частково, або в повній мірі, вирішити наступні завдання:

1. Розглянути існуючі підходи до захисту розумних будинків від кібератак та порушень приватності користувачів.
2. Розробити архітектуру підсистем захисту розумного будинку. Розробити методи та алгоритми захисту, які забезпечать високий рівень безпеки та приватності користувачів.
3. Реалізувати розроблену архітектуру та методи захисту у вигляді прототипу підсистеми захисту розумного будинку.
4. Провести експериментальне дослідження розробленої підсистеми захисту розумного будинку для оцінки її ефективності та рівня захисту.

Основні вимоги:

- Забезпечення безпеки даних
- В міру, простий алгоритм захисту
- Можливість розширення, тестування та підтримка

1.6.Заключні рекомендації

У даному дослідженні розглянуто питання розробки підсистем захисту розумного дому. У процесі роботи було проведено аналіз існуючих систем захисту, визначено їх недоліки та пропоновано рішення для покращення їх ефективності. На основі цього дослідження зроблені наступні висновки та рекомендації:

1.6.1. Визначення основних висновків та результатів дослідження

В процесі дослідження виявлено, що більшість існуючих систем захисту розумного дому мають недоліки, які можуть стати причиною порушення безпеки житла. Найбільш поширеним недоліком є недостатня захищеність мережі зв'язку між компонентами системи захисту. Це може призвести до можливості зламування системи та отримання незаконного доступу до даних власника.

Окрім того, виявлено, що більшість систем захисту не враховують можливості новітніх технологій, таких як штучний інтелект та машинне навчання. Використання цих технологій може значно підвищити ефективність систем захисту та знизити кількість помилок.

1.6.2. Рекомендації щодо покращення захисту розумного дому

На основі проведеного дослідження запропоновані наступні рекомендації щодо покращення захисту розумного дому:

1. Використовуйте сучасні технології: штучний інтелект та машинне навчання можуть допомогти знизити кількість помилок та збільшити ефективність систем захисту.
2. Забезпечте захист мережі зв'язку: важливо враховувати можливість зламування мережі зв'язку та вживати заходи для підвищення захисту цієї мережі. Наприклад, можна використовувати шифрування даних, використовувати паролі та двофакторну аутентифікацію.

3. Проводьте регулярні аудити безпеки: важливо періодично перевіряти стан системи захисту та виявляти можливі недоліки. Це допоможе попередити можливі атаки та забезпечити високий рівень безпеки розумного дому.

1.6.3. Перспективи подальшого дослідження

У майбутньому можна проводити дослідження у таких напрямках:

1. Вдосконалення систем захисту: проведення досліджень щодо створення більш ефективних систем захисту розумного дому з використанням новітніх технологій.
2. Вивчення проблем безпеки Інтернету речей: дослідження проблем безпеки, пов'язаних із використанням різноманітних пристроїв, що підключені до Інтернету, у складі розумного дому.
3. Вивчення соціальної інженерії: дослідження можливостей використання соціальної інженерії у процесі зламування систем захисту розумного дому та розробка заходів для запобігання таким атакам.
4. Розробка більш точних інструментів для виявлення вразливостей систем захисту розумного дому та проведення регулярного аналізу стану безпеки.
5. Розробка стандартів та протоколів безпеки: розробка стандартів, що враховують специфіку розумного дому та рекомендацій щодо використання певних протоколів безпеки.
6. Вивчення можливості застосування штучного інтелекту: дослідження можливостей застосування методів машинного навчання та штучного інтелекту для виявлення вразливостей та вдосконалення систем захисту розумного дому.
7. Розробка аналітичних моделей: використання аналітичних моделей та інструментів для прогнозування можливих загроз безпеці розумного дому та вдосконалення систем захисту.

8. Розробка та підтримка глобальних мереж безпеки розумного дому: створення мережі, що об'єднує фахівців та організації для обміну досвідом та вдосконалення заходів безпеки розумного дому.

Отже, розробка підсистем захисту розумного дому є важливою проблемою, яка потребує досліджень та вдосконалення існуючих систем. Проведене дослідження дає можливість запропонувати рекомендації для покращення захисту розумного дому та вказує на перспективи подальшого дослідження в цій області.

2. ПРОЕКТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Опис необхідних функціональних та нефункціональних вимог до програмного забезпечення

Функціональні вимоги включають в себе:

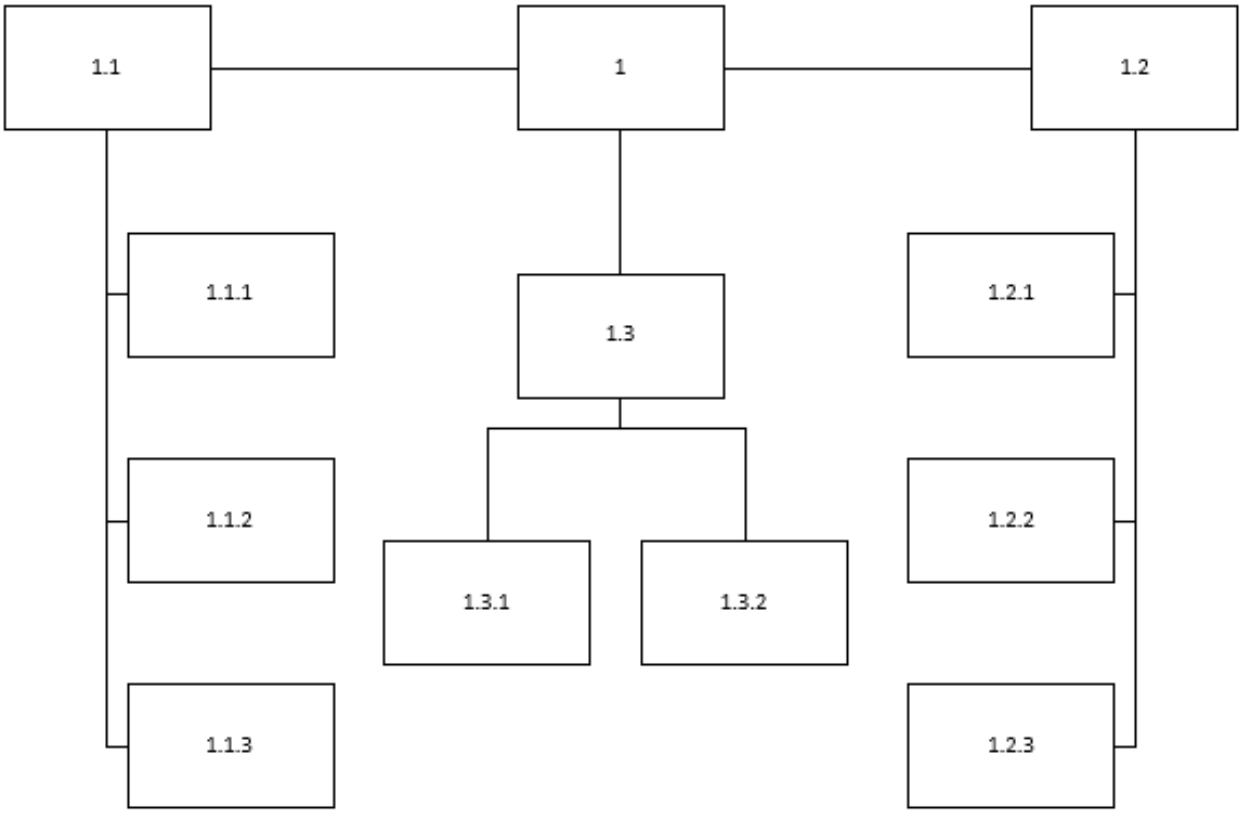


Рисунок 2.1 – функціональні вимоги

1. Функціональні вимоги
   1.1. Керування доступом
      1.1.1. Наявність в системі можливості керування доступом до будинку або окремих його частин.
      1.1.2. Наявність можливості встановлювати різних рівні доступу для різних користувачів (наприклад, членів родини, друзів, гостей, співробітників служби безпеки).
      1.1.3. Можливість надання тимчасового доступу, який автоматично відключатиметься після закінчення строку.

1.2. Моніторинг

1.2.1. Система з можливостями моніторингу будинка, приміщення, тощо; та модулями збирання даних про зміни в стані помешкання (відкриті двері, вікна, рух в помешканні тощо).

1.2.2. Забезпечення можливості аналізу отриманих дані та сповіщення користувача про потенційні загрози безпеці.

1.2.3. Можливість записувати дані та зберігати їх для подальшого використання.

1.3. Управління системою

1.3.1. Система володіє і має інтуїтивно зрозумілий інтерфейс для користувача, який дозволить керувати всіма функціями системи.

1.3.2. Наявні налаштування параметрів системи, зокрема, часу спрацювання сигналізації, чутливості датчиків тощо.

Нефункціональні вимоги:

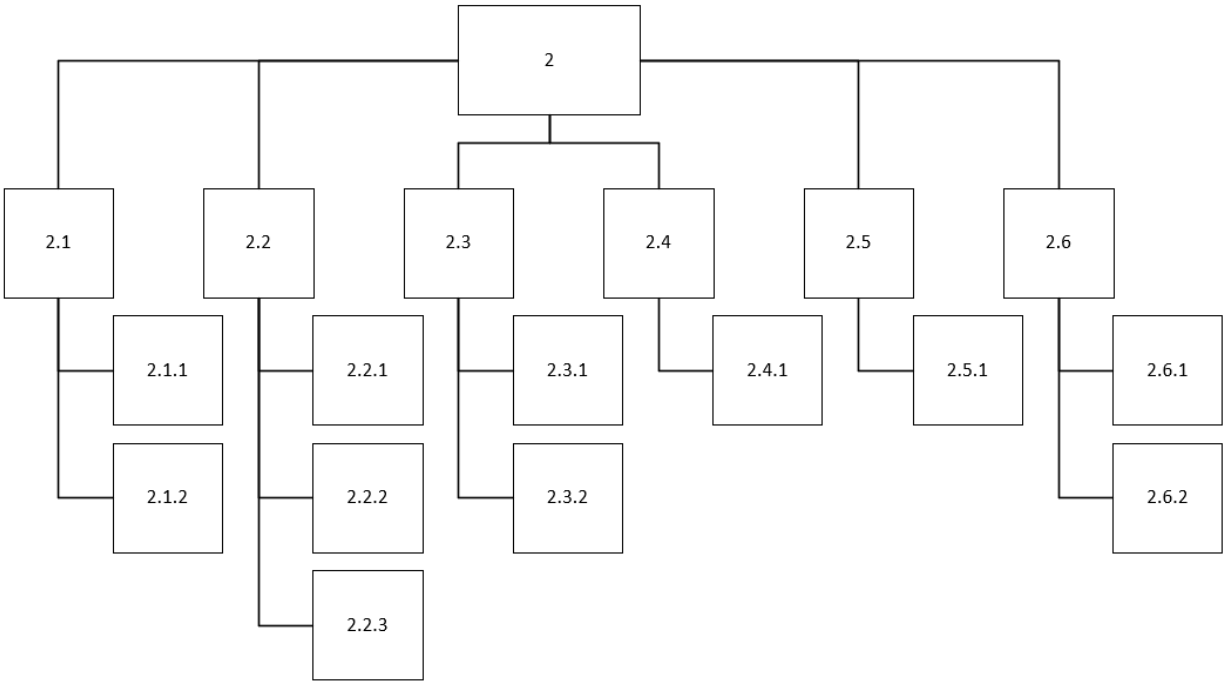


Рисунок 2.2 – Нефункціональні вимоги

1. Нефункціональні вимоги

1.1. Надійність

1.1.1. Система володіє можливістю працювати безперебійно та надійно.

1.1.2. Система володіє можливістю резервного копіювання даних.

1.2. Безпека

1.2.1. Система володіє можливістю захисту від несанкціонованого доступу та зберігання даних в зашифрованому вигляді.

1.2.2. Наявність в системі захисту від хакерських атак та вірусів.

1.2.3. Наявність в системі миттєвого сповіщення про загрози безпеці.

1.3. Ефективність

1.3.1. Система обладнана та працює швидко та ефективно.

1.3.2. Система забезпечує оптимальну роботу системи при великому обсязі даних.

1.4. Сумісність

1.4.1. Система сумісна з іншими пристроями, що використовуються в розумному домі (наприклад, з освітленням, системою опалення, відеокамерами тощо).

1.5. Масштабованість

1.5.1. Система готова до масштабування при збільшенні кількості підключених до неї пристроїв.

1.6. Легкість використання

1.6.1. Система інтуїтивно зрозуміла та легка у використанні.

1.6.2. Має швидке орієнтування в системі та виконання необхідних налаштування.

Розумний дім забезпечує безпеку й комфорт життя власників. Надійне та безпечне програмне забезпечення є однією з ключових складових системи безпеки. З метою запобігання загрозам безпеці розумного дому, необхідно враховувати функціональні та нефункціональні вимоги до програмного забезпечення, які були описані в даному розділі. Їх виконання дозволить забезпечити надійну та безпечну роботу системи в будь-який момент.

2.2. Опис вимог до забезпечення безпеки, доступності, надійності та інших аспектів програмного забезпечення

Опис вимог до забезпечення безпеки, доступності, надійності та інших аспектів програмного забезпечення є важливим етапом розробки будь-якої системи, включаючи підсистеми захисту розумного дому. У даній дипломній роботі, ви працюєте над розробкою підсистеми захисту розумного дому, тому докладний опис вимог до забезпечення безпеки, доступності, надійності та інших аспектів програмного забезпечення є критичним завданням.

1. Безпека:
   1.1. Аутентифікація та авторизація: Система повинна мати механізми перевірки та ідентифікації користувачів, а також забезпечити контроль доступу до різних функцій та ресурсів системи.
   1.2. Конфіденційність: Всі дані, що передаються та зберігаються в системі, повинні бути захищені від несанкціонованого доступу та витоку інформації.
   1.3. Цілісність: Система має гарантувати, що дані не піддаються несанкціонованій модифікації або порушенню цілісності.
   1.4. Відновлення та резервне копіювання: Передбачення механізмів для резервного копіювання та відновлення даних, щоб уникнути втрати інформації у випадку аварійних ситуацій.
2. Доступність:
   2.1. Управління помилками: Система повинна забезпечувати ефективне управління помилками та відмовами, щоб запобігти недоступності та забезпечити швидке відновлення роботи після помилок.
   2.2. Масштабованість: Програмне забезпечення повинно бути гнучким та масштабованим, здатним працювати з більшим обсягом даних та збільшеним навантаженням без значного погіршення продуктивності та доступності.

3. Надійність:
   3.1. Забезпечення стійкості: Система має бути стійкою до помилок, збоїв та аварій, здатною швидко відновлюватися після них та забезпечувати неперервну роботу.
   3.2. Відновлення після збоїв: Програмне забезпечення повинно мати механізми автоматичного відновлення після збоїв та забезпечувати цілісність даних після таких ситуацій.
   3.3. Тестування та верифікація: Система повинна пройти відповідні тести та верифікацію, щоб гарантувати правильну роботу та надійність функцій.
4. Інші аспекти програмного забезпечення:
   4.1. Ефективність: Система має працювати ефективно, забезпечуючи швидку відповідь на запити та оптимальне використання ресурсів.
   4.2. Легкість використання: Програмне забезпечення повинно мати інтуїтивно зрозумілий інтерфейс та надавати зручні інструменти для користувачів.
   4.3. Сумісність: Система має бути сумісною з іншими пристроями та платформами, що використовуються в розумних домах. Модульність: Програмне забезпечення повинно бути розбитим на модулі, що дозволяє зручно розширювати та модифікувати систему.

Ці вимоги до забезпечення безпеки, доступності, надійності та інших аспектів програмного забезпечення важливі для розробки підсистеми захисту розумного дому. Вони гарантують, що система буде функціонувати безпечно, надійно та ефективно, забезпечуючи задані функціональність та задоволення потреб користувачів. Для досягнення цих вимог рекомендується використовувати такі практики та методи:

Ретельний аналіз загроз безпеці: Проведення оцінки ризиків та визначення потенційних загроз безпеці допоможе ідентифікувати слабкі місця та розробити відповідні заходи для їх усунення.

Використання шифрування: Застосування сильного шифрування для захисту передачі та збереження конфіденційної інформації забезпечить її захист від несанкціонованого доступу.

Резервне копіювання та відновлення: Регулярне резервне копіювання даних та розробка плану відновлення допоможуть уникнути втрати даних та забезпечити швидке відновлення системи після збоїв.

Використання механізмів авторизації та контролю доступу: Розробка механізмів, які перевіряють ідентичність користувачів та контролюють їх доступ до різних функцій системи, забезпечить безпеку та обмежить ризик несанкціонованого використання.

Тестування та аудит безпеки: Регулярне проведення тестування безпеки та аудиту допоможе виявити можливі уразливості та вразливі точки в системі, що дозволить своєчасно вжити заходів для їх усунення.

Розробка інтуїтивного інтерфейсу: Забезпечення легкості використання системи та інтуїтивного інтерфейсу дозволить користувачам легко орієнтуватися в функціях та забезпечить правильне використання системи без помилок. Регулярні оновлення та підтримка: Забезпечення постійного оновлення програмного забезпечення та надання технічної підтримки дозволить виправляти помилки, виправляти виявлені уразливості та забезпечувати безпеку та надійність системи на протязі її експлуатації.

Використання стандартів та нормативних вимог: Розробка системи відповідно до встановлених стандартів та нормативних вимог забезпечить дотримання високих стандартів безпеки, доступності та надійності.

Врахування ризиків та потенційних загроз: У процесі розробки програмного забезпечення необхідно провести аналіз потенційних ризиків та загроз, що можуть вплинути на безпеку та доступність системи, та розробити відповідні заходи для їх запобігання або зменшення.

Перевірка та аудит коду: Проведення регулярної перевірки та аудиту коду програмного забезпечення допоможе виявити потенційні помилки,

уразливості та слабкі місця, що можуть вплинути на безпеку та надійність системи.

Коректне збереження та обробка даних: Дотримання вимог до обробки та збереження персональних даних, використання механізмів шифрування та інших заходів безпеки даних забезпечить конфіденційність та цілісність інформації.

Усі ці вимоги та практики допоможуть забезпечити безпеку, доступність, надійність та інші аспекти програмного забезпечення в розробці підсистеми захисту розумного дому. Враховуючи їх у процесі розробки та тестування, ви створите надійну та безпечну систему, яка відповідає потребам користувачів.

2.3.Архітектурні особливості

2.3.1. Вибір архітектурного стилю

Оглянувши різні архітектурні стилі, виявлено, що клієнт-серверна архітектура відповідає вимогам системи найкраще. Цей стиль базується на розділенні функцій між клієнтами та серверами, де клієнти виконують запити, а сервери забезпечують обробку та надання необхідної інформації. Це дозволяє забезпечити централізований контроль над системою та зручний доступ до різних функцій.

Мікросервісна архітектура також розглядалась, проте, враховуючи потреби системи розумного дому, виявлено, що вона менш підходить для даного проекту. Хоча мікросервіси забезпечують гнучкість та масштабованість, вони вимагають складнішого управління та координації між компонентами системи, що може бути проблематичним у розумному домі.

Таким чином, вибір клієнт-серверної архітектури був обґрунтований на основі її спроможності забезпечити централізований контроль, розподіленість функцій та легкий доступ до різних клієнтів. Цей

архітектурний стиль забезпечить зручну та ефективну реалізацію підсистеми захисту розумного дому.

Клієнт-серверна архітектура також дозволяє забезпечити безпеку та надійність системи. Централізований сервер може використовувати механізми аутентифікації, авторизації та шифрування для захисту доступу до системи і забезпечення конфіденційності даних. Крім того, розділення функцій між клієнтами та серверами дозволяє легко внести зміни або оновлення до системи без впливу на всю архітектуру.

У виборі архітектурного стилю також були враховані особливості розумного дому та його вимоги до доступності. Клієнт-серверна архітектура дозволяє підключати різні клієнтські пристрої, такі як смартфони, планшети, комп'ютери, до центрального сервера, що забезпечує доступ до функцій системи через різні інтерфейси. Це робить систему доступною для користувачів з різних пристроїв та забезпечує їх зручність у використанні.

З урахуванням всіх цих факторів та вимог до системи, було прийнято рішення про використання клієнт-серверної архітектури для реалізації підсистеми захисту розумного дому. Цей архітектурний стиль забезпечить централізований контроль, розділення функціональності, безпеку, надійність та доступність системи.

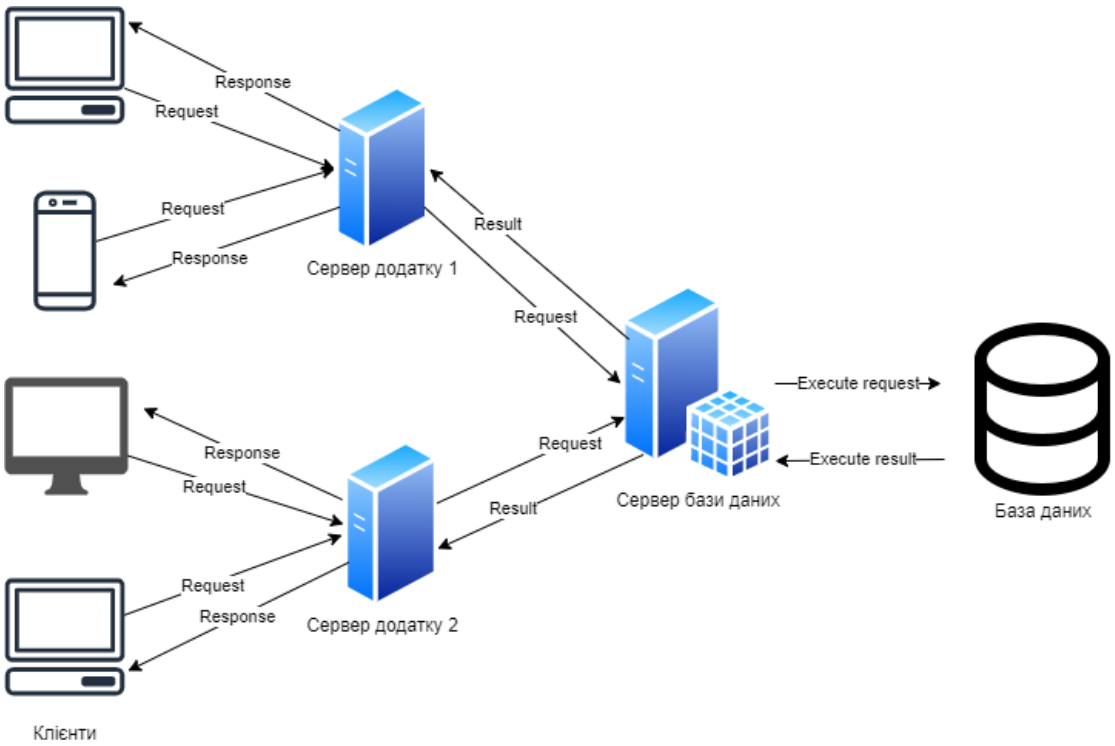


Рисунок 2.1 – Сутність клієнт-серверної архітектури

2.3.2. Опис загальної архітектури системи захисту розумного дому.

Загальна архітектура системи захисту розумного дому базується на принципах клієнт-серверної моделі. В системі існує центральний сервер, що відповідає за обробку запитів та забезпечення функцій безпеки, доступності та надійності. Клієнти системи можуть бути різними пристроями, такими як смартфони, планшети, комп'ютери, які взаємодіють з сервером через різні інтерфейси, такі як мобільні додатки або веб-інтерфейс.

Центральний сервер виконує ключові функції системи захисту розумного дому, зокрема:

1. Аутентифікація та авторизація: Сервер забезпечує механізми аутентифікації користувачів та пристроїв, що забезпечують доступ до системи. Він також визначає рівні доступу для кожного користувача чи пристрою, щоб контролювати їх можливості.
2. Керування пристроями: Сервер взаємодіє з різними пристроями розумного дому, такими як системи відеоспостереження, датчики

руху, замки, освітлення тощо. Він надає можливість керування цими пристроями з використанням відповідних команд та протоколів.

3. Моніторинг та спостереження: Сервер відстежує стан пристроїв та систем безпеки розумного дому. Він сповіщає користувачів про будь-які відхилення, спрацювання датчиків або подій, що відбуваються в системі, наприклад, спрацювання датчика руху або сповіщення про вторгнення. Це дозволяє забезпечити постійний моніторинг та контроль над безпекою розумного дому.
4. Зберігання та обробка даних: Сервер забезпечує зберігання та обробку даних, що стосуються системи захисту розумного дому. Це включає зберігання журналів подій, інформації про користувачів, налаштувань системи та іншої важливої інформації. Обробка даних може включати аналіз статистики, генерацію звітів та створення попереджень на основі зібраних даних.

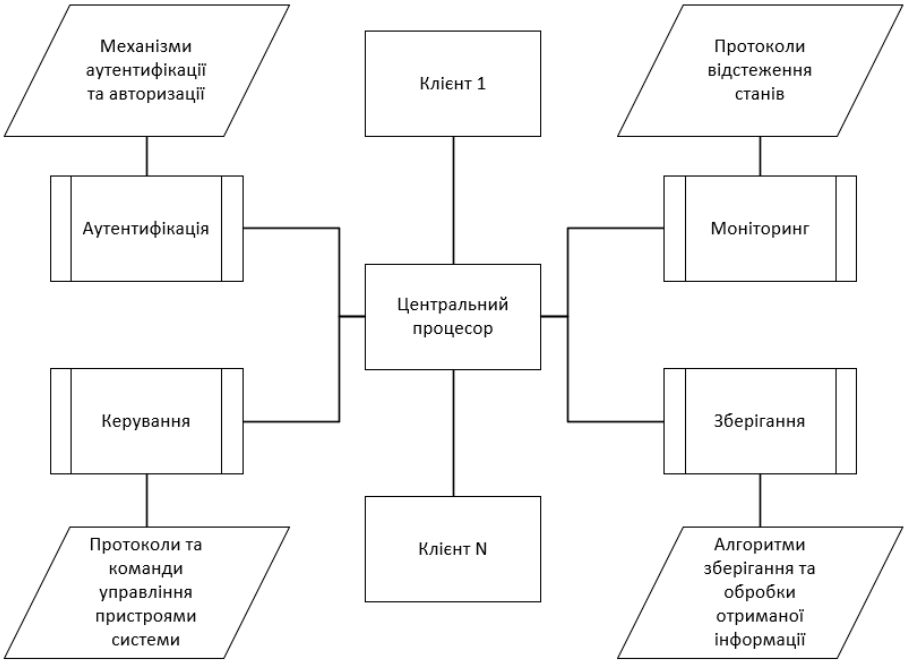


Рисунок 2.2 – ключові функції центрального пристрої в поєднанні з клієнт-серверною архітектурою

Ця клієнт-серверна архітектура дозволяє ефективно забезпечити безпеку, доступність та надійність системи захисту розумного дому. Централізований сервер забезпечує централізований контроль та керування, а також забезпечує зберігання та обробку даних. Клієнти

системи можуть взаємодіяти з сервером з різних пристроїв і використовувати різні інтерфейси, забезпечуючи доступ до функцій системи зручним способом.

Отже, загальна архітектура системи захисту розумного дому базується на клієнт-серверному архітектурному стилі. Цей вибір дозволяє забезпечити ефективне управління, безпеку, доступність та надійність системи. Центральний сервер виконує ключові функції системи, в той час як клієнти можуть взаємодіяти з системою з різних пристроїв. Така архітектура є оптимальним вибором для підсистеми захисту розумного дому, забезпечуюючи високу рівень безпеки, гнучкість, розширюваність та зручність використання.

Центральний сервер в системі захисту розумного дому виступає як головний мозок, який координує роботу всіх компонентів системи. Він взаємодіє з клієнтськими пристроями, приймає їх запити і надає відповіді згідно з встановленими правилами та налаштуваннями. Пристрої розумного дому передають дані про стан системи, події, зміни в реальному часі на сервер, що дозволяє оперативно реагувати на потенційні загрози та події.

Центральний сервер також виконує завдання аутентифікації та авторизації користувачів та пристроїв. Він перевіряє правильність ідентифікаційних даних, контролює рівні доступу і забезпечує, щоб кожен користувач чи пристрій отримував лише необхідну інформацію та функціональність відповідно до своїх прав.

Окрім цього, сервер забезпечує моніторинг та спостереження за станом системи захисту розумного дому. Він отримує дані від різних пристроїв та датчиків, аналізує їх, виявляє незвичайні або підозрілі активності та сповіщає користувачів про потенційні загрози або події. Це дозволяє забезпечити оперативну реакцію на небезпеку та запобігти можливим проблемам.

Клієнтські пристрої в системі захисту розумного дому виконують роль інтерфейсу між користувачем і системою. Вони надають зручну та

інтуїтивно зрозумілу взаємодію з системою через спеціальні додатки або веб-інтерфейси. Користувачі можуть залогінитися до системи, переглядати стан своєї розумної системи, керувати підключеними пристроями, налаштовувати правила безпеки та отримувати сповіщення про події.

Клієнтські пристрої можуть бути смартфонами, планшетами, комп'ютерами або іншими пристроями, які мають доступ до Інтернету та можуть встановлювати зв'язок з центральним сервером. Це дозволяє користувачам зручно керувати своєю розумною системою з будь-якого місця та в будь-який час.

Загальна архітектура системи захисту розумного дому, яка базується на клієнт-серверному архітектурному стилі, дозволяє забезпечити ефективну та безпечну взаємодію між користувачами, пристроями та системою захисту. Центральний сервер виконує ключові функції безпеки, керування та моніторингу, в той час як клієнтські пристрої забезпечують зручну взаємодію та керування системою з боку користувачів. Така архітектура допомагає створити надійну та доступну систему захисту розумного дому, яка забезпечує безпеку та спокій користувачів.

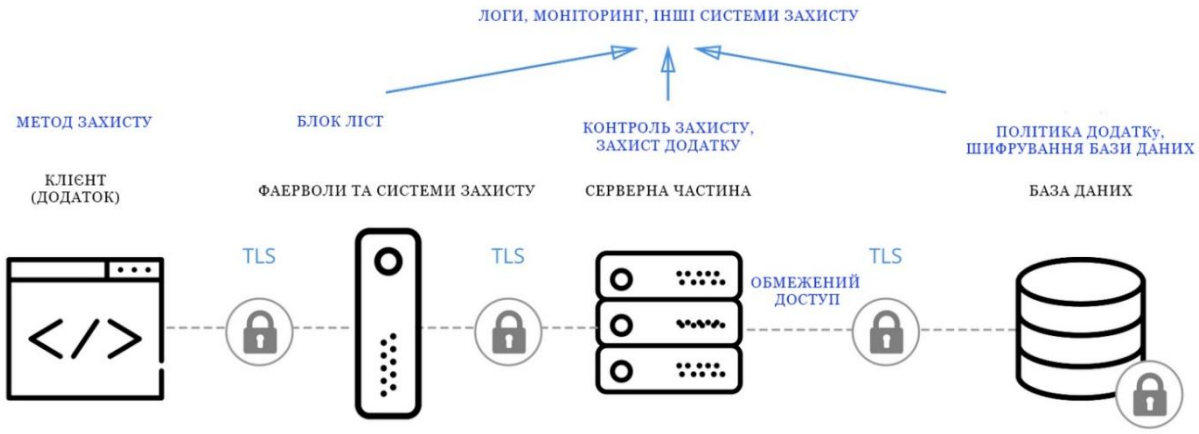


Рисунок 2.3 – Теоретично побудована схема системи на основі описаної архітектури та критеріїв забезпечення безпеки

2.3.3. Розподіл функцій та компонентів між модулями програмного забезпечення

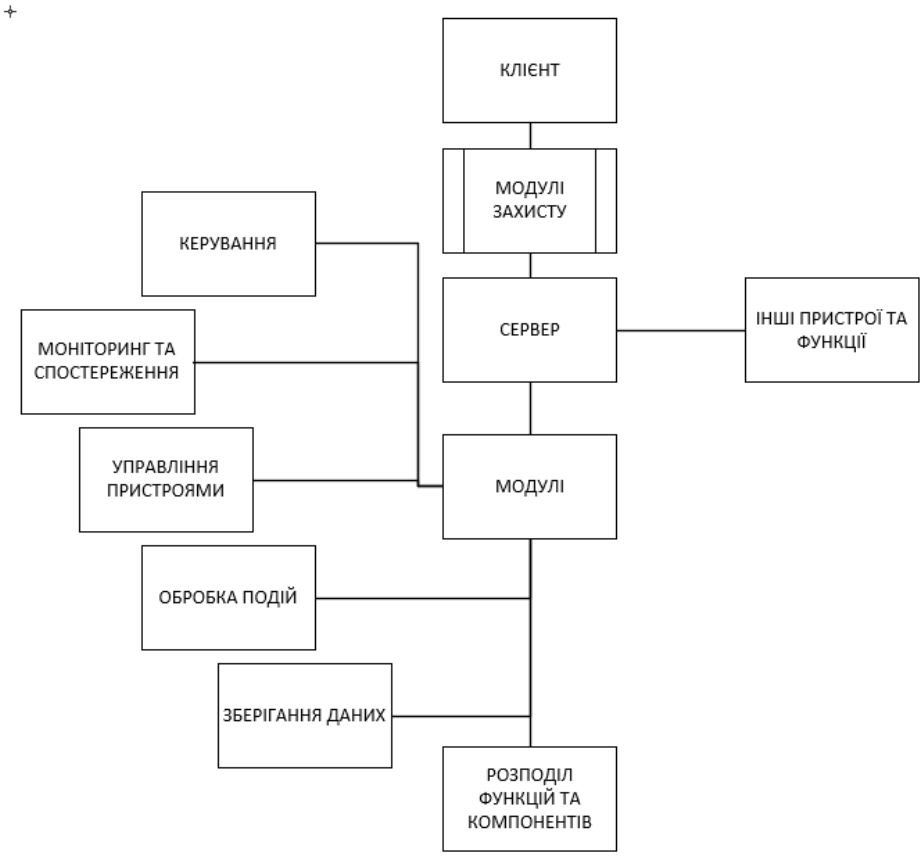


Рисунок 2.4 – Розподіл системи за модульними можливостями

У розумному домі система захисту виконує різноманітні функції, що вимагають чіткого розподілу функцій та компонентів між модулями програмного забезпечення. Цей розділ описує розподіл функцій та компонентів системи захисту розумного дому на окремі модулі для забезпечення ефективності, надійності та розширюваності.

1. Модуль керування: Цей модуль відповідає за керування всією системою захисту розумного дому. Він забезпечує інтерфейс для взаємодії з користувачами та клієнтськими пристроями. Модуль керування обробляє команди користувачів, встановлює налаштування системи, керує реакцією на події та сповіщення. Він також відповідає за автентифікацію та авторизацію користувачів.
2. Модуль моніторингу та спостереження: Цей модуль забезпечує постійний моніторинг та спостереження за станом системи захисту розумного дому. Він отримує дані від датчиків, пристроїв та інших компонентів системи, аналізує їх і реагує на небезпеку або підозрілу активність. Модуль моніторингу та спостереження генерує

сповіщення, створює журнали подій та забезпечує зберігання відповідної інформації.

3. Модуль управління пристроями: Цей модуль взаємодіє з різними пристроями в системі захисту розумного дому, такими як камери спостереження, датчики руху, сигналізаційні пристрої та інші. Він включає в себе функції керування, налаштування та моніторингу цих пристроїв. Модуль управління пристроями взаємодіє з ними через встановлені протоколи комунікації та забезпечує коректну роботу пристроїв згідно з встановленими налаштуваннями та правилами.
4. Модуль обробки подій: Цей модуль відповідає за обробку подій, що виникають в системі захисту розумного дому. Він аналізує отримані дані, визначає типи подій, виконує необхідні дії та генерує сповіщення для користувачів. Модуль обробки подій також може включати в себе функціонал автоматичної реакції на певні події, наприклад, активацію сигналізації або виклик служби безпеки.
5. Модуль зберігання даних: Цей модуль відповідає за зберігання та керування даними системи захисту розумного дому. Він забезпечує зберігання журналів подій, конфігураційні дані, налаштування правил безпеки та іншу важливу інформацію. Модуль зберігання даних також може включати в себе механізми резервного копіювання та відновлення даних для забезпечення безпеки та надійності.
6. Розподіл функцій та компонентів між модулями програмного забезпечення системи захисту розумного дому забезпечує чітку організацію та структуру системи. Він дозволяє забезпечити ефективне виконання різноманітних функцій, полегшує розробку та підтримку системи, а також забезпечує легкість розширення та модифікацікації системи. Кожен модуль відповідає за свої функціональні області, що сприяє зменшенню залежностей між компонентами та полегшує розвиток системи в майбутньому.

Розподіл функцій та компонентів між модулями програмного забезпечення системи захисту розумного дому дозволяє кожному модулю фокусуватись на своїй конкретній області відповідальності. Це сприяє зменшенню залежностей між модулями, полегшує розвиток, тестування та підтримку системи. Крім того, такий розподіл дозволяє легко розширювати та модифікувати систему, додавати нові функціональність і пристрої, не впливаючи на роботу інших компонентів.

В цьому розділі були описані основні модулі програмного забезпечення системи захисту розумного дому, які відповідають за розподіл функцій та компонентів системи. Однак, важливо зазначити, що розподіл модулів та їх функціональність може варіюватися залежно від конкретної системи захисту розумного дому та її вимог.

Наприклад, в деяких системах можуть бути додаткові модулі, які відповідають за інтеграцію з іншими додатками або зовнішніми системами, такими як системи безпеки, автоматизації будинку чи відеоспостереження. Ці модулі забезпечують взаємодію та обмін даними між системою захисту розумного дому та іншими системами, що розширює можливості та функціональність системи.

Загалом, розподіл функцій та компонентів між модулями програмного забезпечення системи захисту розумного дому є важливим кроком у розробці та реалізації системи. Він забезпечує чітку структуру, полегшує розширення та підтримку, а також забезпечує ефективну роботу системи захисту розумного дому з мінімальними залежностями між компонентами.

2.4. Огляд основних алгоритмів та методів захисту, що використовуються в системах розумного дому

У системах розумного дому, де забезпечення безпеки є пріоритетом, використовуються різні алгоритми та методи захисту для запобігання несанкціонованому доступу, виявлення аномалій та ефективного

реагування на потенційні загрози. Огляд основних алгоритмів та методів захисту надасть уявлення про те, як системи розумного дому забезпечують безпеку та надійність.

1. Аутентифікація та авторизація:
   1.1. Методи ідентифікації: Використання паролів, біометричних даних, карток доступу або інших методів для перевірки ідентичності користувачів та підтвердження їх прав доступу.
   1.2. Керування доступом: Встановлення рівнів доступу, обмежень та правил, щоб кожен користувач мав обмежений доступ до відповідних функцій та пристроїв.
2. Шифрування:
   2.1. Симетричне шифрування: Використання спільного ключа для шифрування та розшифрування інформації між взаємодіючими компонентами системи.
   2.2. Асиметричне шифрування: Використання пари ключів - публічного та приватного - для шифрування та розшифрування інформації та забезпечення цілісності та конфіденційності даних.

Таблиця 2.1 – порівняльна таблиця методів шифрувань

Основні характеристики	Симетричне шифрування	Асиметричне шифрування
Ключі	Використовується один ключ	Використовується пара ключів
Швидкодія	Швидше	Повільніше
Безпека	Нижча	Вища
Розмір ключів	Зазвичай менший	Зазвичай більший
Використання	Рекомендується для масового шифрування, де швидкодія важлива	Рекомендується для захисту комунікації між двома сторонами, де

		важлива безпека даних
Приклади алгоритмів	DES, AES, 3DES, Blowfish	RSA, DSA, ECC

3. Виявлення та запобігання вторгнень:
   3.1. Виявлення аномалій: Використання алгоритмів машинного навчання та аналізу великих обсягів даних для виявлення незвичайних та підозрілих активностей у системі.
   3.2. Брандмауери: Застосування спеціального програмного та/або апаратного забезпечення для контролю мережевого трафіку та фільтрації пакетів для запобігання несанкціонованому доступу до системи.
   3.3. Системи виявлення вторгнень (СВВ): Використання спеціалізованого програмного забезпечення для виявлення та сповіщення про спроби несанкціонованого доступу, атак або аномалій у системі.
4. Захист даних:
   4.1. Резервне копіювання та відновлення: Забезпечення регулярного резервного копіювання даних та можливості їх відновлення у випадку втрати або пошкодження.
   4.2. Шифрування даних: Застосування шифрування для захисту конфіденційності та цілісності збережених даних.
   4.3. Механізми контролю цілісності даних: Використання хеш-функцій або цифрових підписів для виявлення змін або порушень цілісності даних.
5. Моніторинг та журналювання:
6. Системи моніторингу: Використання спеціальних засобів для постійного моніторингу активності та стану системи з метою виявлення потенційних загроз або проблем.
7. Журналювання подій: Запис подій, дій та взаємодій в системі для подальшого аналізу та виявлення несанкціонованої активності.

Цей розділ надає огляд основних алгоритмів та методів захисту, які використовуються в системах розумного дому. Враховуючи унікальні вимоги та контекст системи, можна вибрати та налаштувати відповідні захисні методи, що допоможуть забезпечити безпеку, доступність та надійність системи захисту розумного дому.

3. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1. Вибір програмного інструментарію

3.1.1. Вибір мови програмування

У розробці підсистем захисту розумного дому вибір мови програмування відіграє важливу роль, оскільки від цього залежить ефективність, надійність та швидкість реалізації проекту. У даному підрозділі проведений порівняльний аналіз мов програмування C# та C++ з урахуванням їх характеристик і властивостей з метою обґрунтування вибору мови C# для реалізації підсистем захисту розумного дому.

Для початку розглянемо мову програмування C#. C# є об'єктно-орієнтованою мовою програмування, розробленою компанією Microsoft. Вона базується на мові C++, але має ряд вдосконалень та спрощень, що роблять її більш зручною для розробки додатків. C# має розширену підтримку бібліотек та фреймворків, зокрема .NET Framework, що дозволяє швидко та зручно реалізувати функціональність системи захисту розумного дому.

Таблиця 3.1 – Порівняльна таблиця мов C# та C++

Характеристика	C#	C++
Синтаксис	Легкий і зрозумілий	Складний і більш гнучкий
Об'єктно-орієнтованість	Повністю підтримується	Підтримується, але менш інтуїтивно
Ефективність	Менш ефективна за рахунок VM (.NET)	Вища ефективність за рахунок компіляції
Безпека	Висока	Залежить від програміста

Продовження таблиці 3.1 – Порівняльна таблиця мов C# та C++

Стандартні бібліотеки	Широкий вибір бібліотек та фреймворків для розробки різноманітних додатків	Широкий вибір бібліотек, але менше фреймворків для розробки
Мультиплатформеність	Можливість розробки на різних платформах (Windows, Linux, macOS) з використанням .NET Core	Можливість розробки на різних платформах, але вимагає додаткової налаштування та компіляції
Підтримка розробки	Інтегрована розробка засобами Visual Studio та іншими IDE, що спрощує розробку та налагодження	Багато різних IDE та засобів розробки, але менш інтегровані та зручні для розробки
Розширюваність	Легко розширювати функціональність за допомогою додаткових бібліотек та модулів	Гнучкість мови дозволяє розширити функціональність, але вимагає більше зусиль від програміста
Спільнота	Велика активна спільнота розробників, готових надати допомогу та документацію	Велика спільнота розробників, але менш активна у порівнянні з C#

Враховуючи вищевказані фактори, вибір мови програмування C# для реалізації підсистем захисту розумного дому є обґрунтованим. C# має зрозумілий синтаксис, повну підтримку об'єктно-орієнтованого програмування, високу безпеку та ефективність, а також широкий вибір бібліотек та фреймворків для розробки різноманітних додатків. Крім того, C# підтримує мультиплатформеність через .NET Core, що дозволяє розробляти на різних операційних системах.

Інтегрована розробка засобами Visual Studio та іншими IDE робить процес розробки зручним та ефективним. Крім того, наявність великої активної спільноти розробників C# забезпечує підтримку, документацію та готовність надати допомогу при необхідності.

Таким чином, обираючи мову програмування C# для реалізації підсистем захисту розумного дому, отримано зручний та швидкий спосіб розробки, високу безпеку, широкі можливості розширення функціональності та підтримку спільноти розробників.

3.1.2. Вибір програмного середовища

У розробці підсистем захисту розумного дому вибір правильного програмного середовища має велике значення для забезпечення ефективності та продуктивності процесу розробки. У даному підрозділі проведено порівняльний аналіз двох популярних середовищ: Microsoft Visual Studio та Builder C++, з метою обґрунтування вибору Microsoft Visual Studio для реалізації даного проекту.

Microsoft Visual Studio - це інтегроване середовище розробки (IDE), розроблене компанією Microsoft. Воно надає широкий спектр інструментів, можливостей та підтримку для розробки різних типів додатків. Visual Studio підтримує мови програмування, такі як C#, C++, і має багато вбудованих функцій та додатків, що полегшують процес розробки програмного та інформаційного забезпечення та налагодження системи в цілому.

Таблиця 3.2 – Порівняльна таблиця середовищ Microsoft Visual Studio та Builder C++:

Характеристика	Microsoft Visual Studio	Builder C++
Інтегрована розробка	Забезпечує повну інтеграцію розробки та налагодження	Обмежені можливості розробки, менша інтеграція
Підтримка мов	Підтримує різні мови програмування, включаючи C# та C++	Основна підтримка для C++
Інструменти розробки	Має багатий вибір інструментів та розширень для розробки	Обмежений вибір інструментів
Візуальне програмування	Має потужні засоби для розробки візуальних інтерфейсів	Обмежена підтримка візуального програмування
Підтримка платформ	Забезпечує підтримку різних платформ, включаючи Windows, Linux, та macOS	Обмежена підтримка платформ
Спільнота розробників	Має велику та активну спільноту розробників, яка надає підтримку, документацію та готовність надати допомогу	Менш активна та менш розгалужена спільнота розробників

3.2.Програмування основних захисних елементів розумного дому

3.2.1. Встановлення захищеного підключення Wi-Fi з використанням WPA2

Встановлення захищеного підключення Wi-Fi з використанням WPA2 є необхідним методом захисту розумного будинку від несанкціонованого доступу та злому. Оскільки розумні будинки зазвичай підключаються до Інтернету через бездротові мережі Wi-Fi, забезпечення безпеки цього з'єднання є критичним аспектом.

WPA2 (Wi-Fi Protected Access 2) є сучасним протоколом безпеки Wi-Fi, розробленим для забезпечення захисту від несанкціонованого доступу до мережі. Використання WPA2 забезпечує конфіденційність, цілісність та аутентифікацію даних, які передаються через Wi-Fi мережу.

```
void netConnectWPA2()
{
    string ssid = "назва_мережі"; // Замініть на свою назву мережі
    string password = "пароль"; // Замініть на свій пароль Wi-Fi мережі

    // Генерування команди для налаштування мережі Wi-Fi з використанням WPA2
    string command = $"netsh wlan set profileparameter name=\"{ssid}\" Authentication=WPA2PSK Encryption=AES UserAuth=MachineOnly";

    // Створення процесу для виконання команди
    ProcessStartInfo processInfo = new ProcessStartInfo("cmd.exe", "/c " + command);
    processInfo.RedirectStandardOutput = true;
    processInfo.UseShellExecute = false;
    processInfo.CreateNoWindow = true;

    // Запуск процесу
    Process process = new Process();
    process.StartInfo = processInfo;
    process.Start();

    // Очікування завершення процесу
    process.WaitForExit();

    // Перевірка статусу встановлення
    if (process.ExitCode == 0)
    {
        Console.WriteLine("Захищене підключення Wi-Fi розумного дому було успішно встановлене!");
    }
    else
    {
        Console.WriteLine("Під час встановлення захищеного підключення Wi-Fi розумного дому виникла помилка.");
    }

    Console.ReadLine();
}
```

Рисунок 3.1 – встановлення захищеного підключення WiFi WPA2 Smart Home

3.2.2. Програмування процесу аутентифікації та авторизації

Аутентифікація та авторизація є також важливими методами захисту розумного будинку. Аутентифікація перевіряє, чи є користувач дійсно тим, за кого себе видає, використовуючи ідентифікатори, паролі або біометричні дані. Авторизація визначає, які ресурси та функції можуть бути доступні користувачу після входу в систему. Це забезпечує контроль над доступом до пристроїв та функціональності розумного будинку.

```
7 references
public enum AccessLevel
{
    Guest,
    User,
    Admin
}

7 references
public class User
{
    5 references
    public string Username { get; set; }
    4 references
    public string Password { get; set; }
    4 references
    public AccessLevel AccessLevel { get; set; }
}
```

Рисунок 3.2 – Процес створення класу користувачів та їх рівню доступу

```
1 reference
public Authentication()
{
    // Ініціалізуємо користувачів системи
    users = new User[]
    {
        new User { Username = "guest", Password = "guest", AccessLevel = AccessLevel.Guest },
        new User { Username = "user", Password = "user", AccessLevel = AccessLevel.User },
        new User { Username = "admin", Password = "admin", AccessLevel = AccessLevel.Admin }
    };
}
```

Рисунок 3.3 – Процес ініціалізації користувачів в системі

```
1 reference
public bool Authenticate(string username, string password)
{
    // Перевіряємо, чи існує користувач з вказаними ім'ям та паролем
    User user = Array.Find(users, u => u.Username == username && u.Password == password);

    if (user != null)
    {
        Console.WriteLine("Authentication successful!");
        return true;
    }

    Console.WriteLine("Authentication failed!");
    return false;
}
```

Рисунок 3.4 – Процес перевірки наявності користувача

```
1 reference
public bool Authorize(string username, AccessLevel requiredAccessLevel)
{
    // Перевіряємо, чи користувач має необхідний рівень доступу
    User user = Array.Find(users, u => u.Username == username);

    if (user != null && user.AccessLevel >= requiredAccessLevel)
    {
        Console.WriteLine("Authorization successful!");
        return true;
    }

    Console.WriteLine("Authorization failed!");
    return false;
}
```

Рисунок 3.5 – Процес авторизації користувача

```
0 references
public class Program
{
    0 references
    public static void Main(string[] args)
    {
        Authentication authentication = new Authentication();

        // Приклад використання аутентифікації та авторизації
        string username = "admin";
        string password = "admin";
        AccessLevel requiredAccessLevel = AccessLevel.Admin;

        if (authentication.Authenticate(username, password))
        {
            if (authentication.Authorize(username, requiredAccessLevel))
            {
                // Виконання дій розумного дому з необхідним рівнем доступу
                Console.WriteLine("Access granted! Performing smart home actions...");
            }
        }

        Console.ReadLine();
    }
}
```

Рисунок 3.6 – Повний приклад використання методів авторизації та аутентифікації

3.2.3. Програмування методу шифрування комунікації

Шифрування комунікації є необхідним методом захисту розумного будинку. Воно дозволяє захистити передачу даних між пристроями та системами від несанкціонованого доступу та перехоплення. Шифрування перетворює дані у незрозумілу форму під час передачі, що робить їх некорисними для несанкціонованих осіб. Це забезпечує конфіденційність та цілісність даних, дозволяючи користувачам впевнено здійснювати комунікацію та керувати своїм розумним будинком, не хвилюючись про можливість зловмисного втручання.

```
private static readonly string serverIP = "ваш_сервер";
private static readonly int serverPort = 1122;
private static readonly string certificatePath = "шлях_до_сертифіката";
private static readonly string certificatePassword = "пароль_сертифіката";
```

Рисунок 3.7 – Підключення серверу та сертифікату

```
0 references
public static void Main()
{
    // Завантаження сертифіката
    X509Certificate2 certificate = new X509Certificate2(certificatePath, certificatePassword);

    // Встановлення з'єднання з сервером
    TcpClient client = new TcpClient(serverIP, serverPort);
    SslStream sslStream = new SslStream(client.GetStream(), false, ValidateServerCertificate);

    try
    {
        // Виконання SSL/TLS-рукостискання
        sslStream.AuthenticateAsClient(serverIP, new X509CertificateCollection() { certificate }, SslProtocols.Tls12, false);

        // Надсилання та отримання даних
        byte[] buffer = Encoding.UTF8.GetBytes("Дані для надсилання");
        sslStream.Write(buffer, 0, buffer.Length);
        sslStream.Flush();

        buffer = new byte[4096];
        int bytesRead = sslStream.Read(buffer, 0, buffer.Length);
        string response = Encoding.UTF8.GetString(buffer, 0, bytesRead);
        Console.WriteLine("Отримана відповідь: " + response);
    }
    finally
    {
        // Закриття з'єднання
        sslStream.Close();
        client.Close();
    }
}
```

Рисунок 3.8 – Процес з’єднання з сервером та завантаження сертифікату з подальшим надсиланням необхідних даних

```
// Метод для перевірки валідності серверного сертифіката
1 reference
private static bool ValidateServerCertificate(object sender, X509Certificate certificate, X509Chain chain, SslPolicyErrors sslPolicyErrors)
{
    // Ви можете налаштувати власну логіку перевірки сертифіката тут
    // Наприклад, перевірка на підпис або порівняння зі списком довірених сертифікатів
    // Повернути true, якщо сертифікат валідний, інакше - false
    return true;
}
```

Рисунок 3.9 – Процес валідації серверного сертифікату

3.2.4. Оновлення програмного забезпечення

Оновлення програмного забезпечення є необхідним методом захисту розумного будинку. Воно дозволяє попереджати та усувати вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу. Через регулярні оновлення, виробники можуть внести виправлення та покращення до програмного забезпечення, зміцнюючи безпеку системи розумного будинку. Це дозволяє користувачам мати актуальну й захищену версію програмного забезпечення, що знижує ризик зламу або зловживання системою.

```
static void Main(string[] args)
{
    // Перевірка доступності нових оновлень
    bool updatesAvailable = CheckForUpdates();

    if (updatesAvailable)
    {
        // Завантаження оновлень
        bool success = DownloadUpdates();

        if (success)
        {
            // Встановлення оновлень
            InstallUpdates();
        }
        else
        {
            Console.WriteLine("Помилка при завантаженні оновлень. Будь ласка, спробуйте ще раз пізніше.");
        }
    }
    else
    {
        Console.WriteLine("Нові оновлення не знайдені. Ваше програмне забезпечення розумного дому вже оновлене.");
    }

    Console.ReadLine();
}
```

Рисунок 3.10 – Загальний приклад системи оновлення

```
1 reference
static bool CheckForUpdates()
{
    // Логіка перевірки доступних оновлень

    // Припустимо, що оновлення доступні
    return true;
}
```

Рисунок 3.11 – Процес перевірки доступності нових оновлень системи

```
1 reference
static bool DownloadUpdates()
{
    // Логіка завантаження оновлень

    // Припустимо, що завантаження успішне
    return true;
}
```

Рисунок 3.12 – Процес логіки завантаження нових оновлень системи

```
1 reference
static void InstallUpdates()
{
    // Логіка встановлення оновлень

    Console.WriteLine("Встановлення оновлень розпочато...");
    Console.WriteLine("Оновлення встановлені успішно.");
}
```

Рисунок 3.13 – Процес логіки встановлення нових оновлень системи

3.2.5. Програмування методу відстеження активності

Відстеження активності є важливим методом захисту розумного будинку. Воно дозволяє системі виявляти та аналізувати активність в будинку, щоб вчасно реагувати на підозрілі дії або незвичайну поведінку. Цей метод допомагає виявити можливі зламання, незаконний доступ або інші небажані події, і вчасно сповіщати власника про потенційні загрози. Відстеження активності сприяє підвищенню рівня безпеки та захищеності розумного будинку та його мешканців.

```
0 references
static void Main(string[] args)
{
    // Створення списку пристроїв розумного дому
    List<SmartDevice> smartDevices = new List<SmartDevice>();

    // Додавання пристроїв до списку
    smartDevices.Add(new SmartLight("Living Room Light"));
    smartDevices.Add(new SmartThermostat("Bedroom Thermostat"));
    smartDevices.Add(new SmartCamera("Front Door Camera"));

    // Симуляція активності розумного дому
    foreach (SmartDevice device in smartDevices)
    {
        device.TurnOn();
        device.PerformAction();
        device.TurnOff();
        Console.WriteLine();
    }
}
```

Рисунок 3.14 – Метод створення списку пристроїв та їх додавання в хаб

```
// Базовий клас для пристроїв розумного дому
10 references
abstract class SmartDevice
{
    10 references
    public string Name { get; }

    3 references
    public SmartDevice(string name)
    {
        Name = name;
    }

    4 references
    public abstract void TurnOn();

    4 references
    public abstract void PerformAction();

    4 references
    public abstract void TurnOff();
}
```

Рисунок 3.15 – Абстракція класу пристроїв розумного дому

```
// Приклад класу для розумного світла
2 references
class SmartLight : SmartDevice
{
    1 reference
    public SmartLight(string name) : base(name)
    {
    }

    2 references
    public override void TurnOn()
    {
        Console.WriteLine($"Turning on {Name}...");
        // Додатковий код для управління світлом
    }

    2 references
    public override void PerformAction()
    {
        Console.WriteLine($"Changing brightness of {Name}...");
        // Додатковий код для виконання дії
    }

    2 references
    public override void TurnOff()
    {
        Console.WriteLine($"Turning off {Name}...");
        // Додатковий код для вимкнення світла
    }
}
```

Рисунок 3.16 – Унаслідуваний метод класу пристроїв розумного освітлення

```
// Приклад класу для розумного термостата
2 references
class SmartThermostat : SmartDevice
{
    1 reference
    public SmartThermostat(string name) : base(name)
    {
    }

    public override void TurnOn()
    {
        Console.WriteLine($"Turning on {Name}...");
        // Додатковий код для управління температурою
    }

    public override void PerformAction()
    {
        Console.WriteLine($"Adjusting temperature of {Name}...");
        // Додатковий код для виконання дії
    }

    public override void TurnOff()
    {
        Console.WriteLine($"Turning off {Name}...");
        // Додатковий код для вимкнення термостата
    }
}
```

Рисунок 3.17 – Унаслідуваний метод класу пристроїв розумного термостату

```
// Приклад класу для розумної камери
2 references
class SmartCamera : SmartDevice
{
    1 reference
    public SmartCamera(string name) : base(name)
    {
    }

    public override void TurnOn()
    {
        Console.WriteLine($"Turning on {Name}...");
        // Додатковий код для управління камерою
    }

    public override void PerformAction()
    {
        Console.WriteLine($"Capturing video with {Name}...");
        // Additional code for performing an action
    }

    public override void TurnOff()
    {
        Console.WriteLine($"Turning off {Name}...");
        // Additional code for turning off the camera
    }
}
```

Рисунок 3.18 – Унаслідуваний метод класу пристроїв розумного відео нагляду

3.2.6. Метод захисту від перехоплення даних

```
2 references
public class DataProtection
{
    private static readonly byte[] Key = { /* 16-byte secret key */ };
    private static readonly byte[] IV = { /* 16-byte initialization vector */ };

    1 reference
    public static byte[] EncryptData(byte[] data)
    {
        using (Aes aes = Aes.Create())
        {
            aes.Key = Key;
            aes.IV = IV;

            ICryptoTransform encryptor = aes.CreateEncryptor(aes.Key, aes.IV);

            using (MemoryStream memoryStream = new MemoryStream())
            {
                using (CryptoStream cryptoStream = new CryptoStream(memoryStream, encryptor, CryptoStreamMode.Write))
                {
                    cryptoStream.Write(data, 0, data.Length);
                    cryptoStream.FlushFinalBlock();
                    return memoryStream.ToArray();
                }
            }
        }
    }
```

Рисунок 3.19 – створення ключів та базових енкрипторів

```
1 reference
public static byte[] DecryptData(byte[] encryptedData)
{
    using (Aes aes = Aes.Create())
    {
        aes.Key = Key;
        aes.IV = IV;

        ICryptoTransform decryptor = aes.CreateDecryptor(aes.Key, aes.IV);

        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, decryptor, CryptoStreamMode.Write))
            {
                cryptoStream.Write(encryptedData, 0, encryptedData.Length);
                cryptoStream.FlushFinalBlock();
                return memoryStream.ToArray();
            }
        }
    }
}
```

Рисунок 3.20 – створення базових декрипторів

```
2 references
public class SmartHomeDevice
{
    1 reference
    public void SendData(byte[] data)
    {
        // Шифруємо дані перед відправкою
        byte[] encryptedData = DataProtection.EncryptData(data);

        // Відправка зашифрованих даних розумному дому
        // ...
    }

    1 reference
    public byte[] ReceiveData(byte[] encryptedData)
    {
        // Отримання зашифрованих даних від розумного дому
        // ...

        // Розшифровуємо отримані дані
        byte[] decryptedData = DataProtection.DecryptData(encryptedData);

        return decryptedData;
    }
}
```

Рисунок 3.21 – Приклад шифрування

```
0 references
public class Program
{
    0 references
    public static void Main(string[] args)
    {
        // Приклад використання
        byte[] data = { /* Дані, які потрібно зашифрувати і відправити */ };

        SmartHomeDevice device = new SmartHomeDevice();
        device.SendData(data);

        // ...

        byte[] encryptedData = { /* Отримані зашифровані дані */ };
        byte[] receivedData = device.ReceiveData(encryptedData);
        // Обробка отриманих розшифрованих даних
    }
}
```

Рисунок 3.22 – Приклад використання методу на основі шифровки/дешифровки

3.2.7. Метод захисту від фізичного доступу

Захист від фізичного доступу є невід'ємною складовою захисту розумного будинку. Цей метод спрямований на запобігання несанкціонованому фізичному доступу до пристроїв та систем розумного будинку. Включає в себе використання фізичних бар'єрів, таких як сигналізаційні системи, датчики руху та безпечні замки на дверях та вікнах. Захист від фізичного доступу дозволяє попереджати і виявляти

незаконний доступ до приміщень та забезпечує фізичну безпеку мешканців і їхнього майна у розумному будинку.

```
private bool isLocked;

1 reference
public SmartHomeSecurity_()
{
    isLocked = true; // Початково двері будуть заблоковані
}
```

Рисунок 3.23 – Встановлення початково блокування дверей

```
1 reference
public void Lock()
{
    if (!isLocked)
    {
        Console.WriteLine("Двері заблоковані.");
        isLocked = true;
    }
    else
    {
        Console.WriteLine("Двері вже заблоковані.");
    }
}
```

Рисунок 3.24 – Функція блокування датчику

```
1 reference
public void Unlock()
{
    if (isLocked)
    {
        Console.WriteLine("Двері розблоковані.");
        isLocked = false;
    }
    else
    {
        Console.WriteLine("Двері вже розблоковані.");
    }
}
```

Рисунок 3.25 – Функція розблокування датчику

```
0 references
class Program
{
    0 references
    static void Main(string[] args)
    {
        SmartHomeSecurity_ securitySystem = new SmartHomeSecurity_();

        Console.WriteLine("Введіть команду (lock/unlock/exit):");
        string command = Console.ReadLine();

        while (command != "exit")
        {
            if (command == "lock")
            {
                securitySystem.Lock();
            }
            else if (command == "unlock")
            {
                securitySystem.Unlock();
            }
            else
            {
                Console.WriteLine("Невідома команда. Спробуйте ще раз.");
            }

            Console.WriteLine("Введіть команду (lock/unlock/exit):");
            command = Console.ReadLine();
        }

        Console.WriteLine("Програма завершила роботу.");
    }
}
```

Рисунок 3.26 – Повний модуль блокування та розблокування заданого датчика

3.2.8. Метод симетричного шифрування

Симетричне шифрування є важливим методом захисту розумного будинку. Воно використовує спільний ключ для шифрування та дешифрування даних. Цей метод забезпечує конфіденційність і цілісність даних, зменшуючи ризик перехоплення та зламу. Симетричне шифрування дозволяє захистити комунікацію та передачу даних між пристроями розумного будинку, забезпечуючи безпеку та захищеність інформації в системі.

Рисунок 3.27 – Схема роботи симетричного шифрування

3.2.9. Метод асиметричного шифрування

Асиметричне шифрування є необхідним методом захисту розумного будинку. Воно використовує два взаємно пов'язаних ключі - публічний та приватний - для шифрування та розшифрування даних. Цей метод забезпечує конфіденційність, цілісність та автентичність даних, дозволяючи безпечно обмінюватись інформацією між пристроями розумного будинку. Асиметричне шифрування дозволяє впевнено захищати комунікацію та передачу даних, мінімізуючи ризик перехоплення та несанкціонованого доступу до інформації.

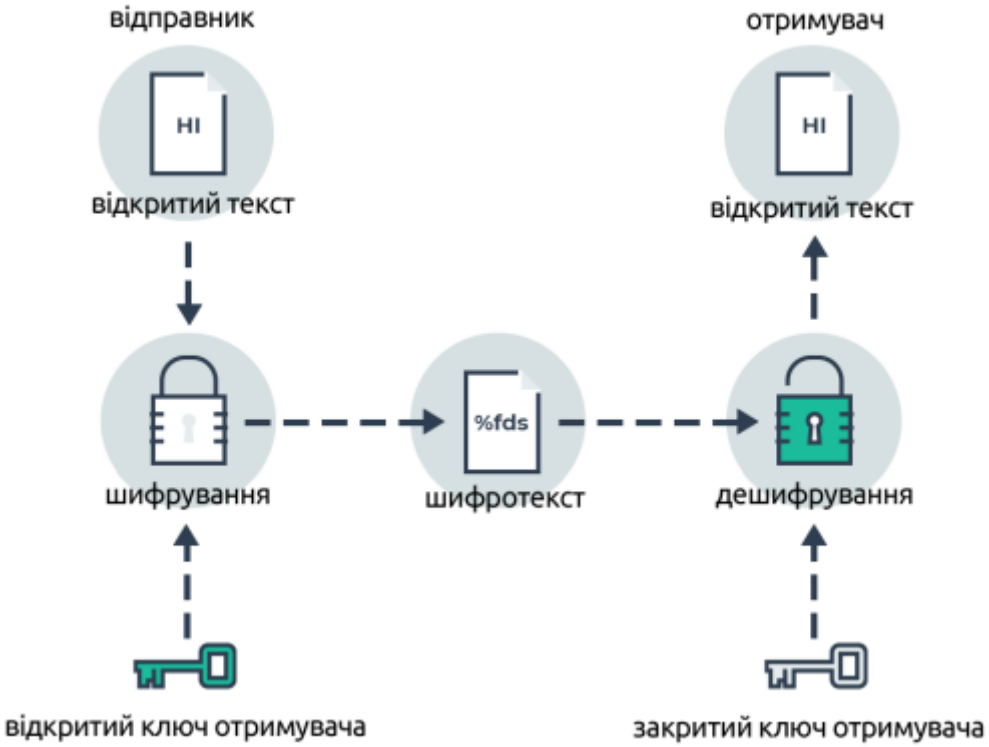


Рисунок 3.28 – Схема роботи асиметричного шифрування

3.2.10. Хешування паролів

Хешування паролів є важливим методом захисту розумного будинку. Воно використовує алгоритми для перетворення паролів на непередбачувані хеш-значення. Цей метод дозволяє зберігати паролі у захищеній формі, знижуючи ризик їхнього розкриття при можливому зламі. Хешування паролів покращує безпеку, оскільки навіть при отриманні хеш-значення зловмисник не може легко відновити оригінальний пароль. Це забезпечує захист від несанкціонованого доступу до системи розумного будинку через злам пароля.

Користувач	Значення солі	Рядок що хешується	Хешоване значення = SHA256 (Пароль + Значення солі)
user1	E1F53135E559C253	password123E1F53135E559C253	72AE25495A7981C40622D49F9A52E4F1565C90F048F59027BD9C8C8900D5C3D8
user2	84B03D034B409D4E	password12384B03D034B409D4E	B4B6603ABC670967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A

Рисунок 3.29 – Приклад шифрування завдяки хешу

```
static void Main()
{
    string password = "password123"; // Пароль, який потрібно зхешувати

    string hashedPassword = HashPassword(password);
    Console.WriteLine("Хешований пароль: " + hashedPassword);

    bool isMatch = VerifyPassword(password, hashedPassword);
    Console.WriteLine("Пароль співпадає: " + isMatch);
}
```

Рисунок 3.30 – Процес хешування паролю

```
2 references
static string HashPassword(string password)
{
    using (SHA256 sha256 = SHA256.Create())
    {
        byte[] passwordBytes = Encoding.UTF8.GetBytes(password);
        byte[] hashBytes = sha256.ComputeHash(passwordBytes);
        return Convert.ToBase64String(hashBytes);
    }
}
```

Рисунок 3.31 – Процес створення ключу хешу

```
1 reference
static bool VerifyPassword(string password, string hashedPassword)
{
    string hashedPasswordToVerify = HashPassword(password);
    return hashedPassword == hashedPasswordToVerify;
}
```

Рисунок 3.32 – Процес перевірки хешу

4. БІЗНЕС-ПЛАН

4.1. Основні питання сутності власного та конкурентного продукту

- як саме і за рахунок чому впроваджуватиметься продукт
- його визначні риси по відношенню до продукту конкурентів
- чому для споживача потрібен переважно саме цей продукт?

Розробка підсистеми захисту "розумного" дому впроваджується шляхом використання передових технологій і інноваційних рішень. Продукт базується на сучасних принципах кібербезпеки та забезпечує захист "розумного" дому від потенційних кіберзагроз, таких як несанкціонований доступ до системи, втручання в роботу підсистем та інших видів атак.

Визначні риси підсистеми захисту "розумного" дому відносно продуктів конкурентів включають:

1. Висока ефективність: продукт використовує передові алгоритми та технології для виявлення та блокування різноманітних кіберзагроз.
2. Широкий спектр захисту: продукт забезпечує захист на різних рівнях "розумного" дому, включаючи мережеві з'єднання, девайси, додатки та інтерфейси користувача.
3. Гнучкі налаштування: продукт має можливість налаштування рівня захисту в залежності від потреб та вимог користувача, забезпечуючи індивідуальний підхід до захисту "розумного" дому.

Для споживача цей продукт є важливим через такі причини:

1. Забезпечення кібербезпеки: "розумний" дім може містити велику кількість особистих даних та важливої інформації, таких як відеозаписи, фінансові дані, медичні дані тощо. Підсистема захисту допоможе забезпечити захист цих даних від несанкціонованого доступу.

2. Запобігання кіберзагрозам: зростання кількості кібератак на "розумні" доми стає загрозою для безпеки користувачів. Підсистема захист допоможе запобігти різноманітним кіберзагрозам, таким як вторгнення в систему, віруси, шкідливі програми та інші види атак, забезпечуючи безпеку системи "розумного" дому та знижуючи ризик втрати даних або пошкодження системи.
3. Зручність користування: підсистема захисту може бути легко налаштована та керована через зручний інтерфейс користувача, що дозволяє споживачам ефективно керувати рівнем захисту свого "розумного" дому без великого зусилля.
4. Інтеграція з існуючими системами: продукт може бути інтегрований з вже наявними системами "розумного" дому, що дозволяє споживачам додатково забезпечити захист своєї системи без необхідності встановлювати нову апаратну або програмну інфраструктуру.

Отже, підсистема захисту "розумного" дому є важливим продуктом, оскільки вона забезпечує ефективний захист від кіберзагроз, забезпечує зручність користування та інтеграцію з існуючими системами, що робить її привабливим вибором для споживачів, які цінують безпеку свого "розумного" дому.

4.1.1. Фінансові відомості проєкту

За даними, які можуть бути використані для приблизних оцінок, основні відомості можуть бути наступними:

1. Прогнозні обсяги продажу на найближчі роки: Орієнтований прогноз обсягу продажу може бути визначений на основі розрахунку потенційного ринкового попиту на "розумний" дім, а також конкурентної аналітики та маркетингових досліджень. Наприклад, прогнозні обсяги продажу можуть збільшуватися з року в рік на основі збільшення попиту на "розумні" рішення для дому та розширення ринку.

2. Прибуток від продажів: Прибуток від продажів може бути розрахований на основі прогнозних обсягів продажу, вирахування витрат на виробництво, маржі прибутку та інших факторів. Наприклад, прибуток від продажу може залежати від ціни продукту, вартості його виробництва, маржі прибутку та орієнтованого обсягу продажу.

3. Витрати на виробництво: Витрати на виробництво включають в себе витрати на сировину, матеріали, працю, обладнання, технічну підтримку та інші витрати, пов'язані з виробництвом "розумного" дому. Витрати на виробництво можуть бути оцінені на основі реальних даних про витрати, аналізу ринкових цін та орієнтованих обсягів виробництва.

4. Валовий прибуток і рівень прибутковості вкладень в майбутню справу: Валовий прибуток може бути розрахований шляхом вирахування витрат на виробництво від валового доходу. Рівень прибутковості вкладень в майбутню справу може бути визначений шляхом відношення валового прибутку до вкладених в підприємство коштів. Це може допомогти оцінити ефективність вкладень у майбутню справу та прийняти рішення щодо її рентабельності.

5. Термін повернення банківського кредиту: Термін повернення банківського кредиту може бути визначений на основі умов кредитування, таких як процентна ставка, розмір позики та розрахунковий період. Зазвичай, термін повернення банківського кредиту повинен бути врахований при розрахунку прибутковості проекту та здатності підприємства відшкодувати кредитні зобов'язання у встановлені терміни.

Всі ці відомості можуть бути оцінені на основі реальних даних, розрахунків та маркетингових аналізів, що дає можливість зробити приблизні оцінки та розрахунки для розвитку "розумного" дому чи іншої бізнес-справи. Проте, важливо враховувати, що ці оцінки можуть бути змінені на основі реальних даних та умов ринку в майбутньому, тому ретельний аналіз та моніторинг є ключовими етапами у веденні бізнесу.

4.2.Проектований продукт або вид послуг

4.2.1. Опис продукту проєкту

1. Потреби, які повинен задовольнити продукт проекту "Розробка підсистеми захисту 'розумного' дому", можуть включати наступні:

- Забезпечення високого рівня безпеки для розумного дому, включаючи захист від несанкціонованого доступу, крадіжок, пожеж та інших небажаних подій.
- Забезпечення контролю та моніторингу різних аспектів розумного дому, таких як відеоспостереження, системи контролю доступу, датчики витоків води та газу тощо.
- Забезпечення зручного та ефективного взаємодії користувача з системою захисту розумного дому, зокрема з використанням мобільних додатків, дистанційного керування та інтеграції з іншими "розумними" пристроями.

2. Особливості та відмінні риси продукту проекту можуть включати:

Висока надійність та ефективність системи захисту, забезпечена застосуванням передових технологій шифрування, автентифікації та інших заходів безпеки. Інтеграція з різними пристроями "розумного" дому, такими як датчики, камери, системи керування, що дозволяє користувачеві отримати комплексний підхід до захисту свого дому. Зручний та легкий в використанні інтерфейс користувача, що дозволяє налаштовувати та керувати системою захисту розумного дому без особливих технічних навичок.

3. Наявність патентів або авторських свідоцтв на продукт проекту може залежати від конкретної розробки та використаних технологій. Для визначення наявності патентів або авторських свідоцтв слід провести відповівідний патентний пошук відповідно до юридичних вимог та регуляцій у вашій країні. Це може включати пошук у патентних базах

даних, консультації з патентним адвокатом або іншими юридичними фахівцями.

4. Щодо наявності наочних зображень продукту проекту, таких як фотографії чи малюнки, це може залежати від стадії розробки проекту та його конфіденційності. Якщо такі зображення є, вони можуть бути використані для візуалізації продукту та його можливостей.

5. Попередня оцінка реалізації ціни виробництва продукту проекту та витрат може бути проведена на основі розрахунків вартості компонентів, робочої сили, виробничих процесів, логістики та інших факторів. Оцінка ціни виробництва може варіюватися в залежності від багатьох факторів, таких як масштаб виробництва, використання новітніх технологій, постачальники та інші.

6. Очікувана величина прибутку, який приноситиме продукт проекту, також може бути розрахована на основі різних факторів, таких як ціна продажу, очікуваний обсяг продажів, вартість виробництва та інші витрати. Це може бути важливий елемент бізнес-плану проекту, що визначає його комерційну вигідність та перспективи рентабельності.

7. Характеристика якісних показників продукту проекту та його переваги можуть включати високий рівень захисту та безпеки, зручний інтерфейс користувача, можливість інтеграції з іншими "розумними" пристроями, наявність резервних систем, ефективність роботи в різних умовах, можливість віддаленого керування та моніторингу, сумісність з різними платформами та протоколами зв'язку, можливість розширення функціональності та адаптації до потреб користувача.

8. Організація сервісу продукту проекту може бути важливим аспектом, особливо якщо це технічний виріб. Це може включати гарантійне та післягарантійне обслуговування, технічну підтримку, оновлення програмного забезпечення, надання допомоги користувачам та вирішення можливих проблем. Ефективна організація сервісу може забезпечити задоволення користувачів, збереження доброї репутації продукту та підтримку його життєвого циклу.

Узагалі, розробка підсистеми захисту "розумного" дому повинна враховувати потреби ринку, бути конкурентоспроможною в порівнянні з іншими продуктами, мати патентну охорону, враховувати вартість виробництва та можливість отримання прибутку, мати вагомі переваги та відмінні риси в порівнянні з конкурентами, а також забезпечувати ефективну організацію сервісу для задоволення потреб користувачів.

4.3.Оцінка ринку збуту

4.3.1. Дослідження відношення продукту до ринку

а) Умови постачання, виробництва і збуту продукту проекту вимагають врахування наступних даних:

1. Постачальники: визначення потенційних постачальників необхідних компонентів, матеріалів або послуг, які використовуються в розробці підсистеми захисту "розумного" дому.
2. Виробничі можливості: визначення виробничих можливостей, таких як виробничі потужності, технічні засоби, технології виробництва, які дозволять забезпечити виробництво продукту проекту.
3. Збутові канали: визначення каналів збуту, таких як дистриб'ютори, роздрібні магазини, онлайн-магазини, які будуть використовуватися для реалізації продукту на ринку.
4. Логістика: врахування логістичних аспектів, таких як транспортування, складське господарство, управління ланцюгом постачання, для забезпечення ефективного постачання та збуту продукту проекту.

б) Для визначення потенціалу своїх можливих конкурентів можна враховувати наступні дані:

1. Конкурентна аналітика: дослідження ринку та аналіз конкурентів, включаючи їх продукти, послуги, ринкову позицію, стратегії збуту,

маркетингові активності та інші фактори, які можуть впливати на успішність продукту проекту.

2. Технічні особливості конкурентів: оцінка технічних характеристик продуктів або послуг конкурентів, включаючи їхні функції, можливості, технології, дизайн та інші аспекти, які можуть бути важливими для вибору споживачами.
3. Репутація конкурентів: оцінка репутації конкурентів на ринку, включаючи їхню історію, відгуки клієнтів, відомості про бренд та інші фактори, які можуть вплинути на сприйняття продукту проекту споживачами.
4. Маркетингові стратегії конкурентів: аналіз маркетингових стратегій, які використовують конкуренти для просування своїх продуктів на ринку, включаючи ціноутворення, промоакції, рекламу, маркетингові кампанії та інші маркетингові заходи.
5. Інновації конкурентів: оцінка рівня інноваційності продуктів або послуг конкурентів, включаючи нові технології, функції, дизайн та інші інноваційні рішення, які можуть конкурентно вплинути на продукт проекту.
6. Клієнтська база конкурентів: оцінка розміру та складу клієнтської бази конкурентів, включаючи їхню лояльність, зв'язки з клієнтами та інші аспекти, які можуть вплинути на залучення та утримання клієнтів продукту проекту.

Ці дані дозволять зрозуміти конкурентну ситуацію на ринку та визначити потенційні переваги свого продукту проекту, що може сприяти розробці ефективної стратегії маркетингу та продажів.

4.3.2. Інформаційні джерела

Власні дослідження можуть бути одним з джерел отримання інформації про умови постачання, виробництва і збуту продукту проекту, а також про потенціал своїх можливих конкурентів. Власні дослідження

можуть включати маркетингові дослідження, аналіз ринку, опитування споживачів, аналітику відносно сегмента ринку, аналіз конкурентної ситуації та інші дослідницькі методи, які дозволяють отримати потрібну інформацію для розробки підсистеми захисту "розумного" дому.

Також, місцеві (регіональні, територіальні) торгові палати, асоціації підприємців, галузеві і торговельні асоціації можуть бути важливим джерелом інформації. Вони можуть надавати статистичні дані про ринок, тренди в галузі, регуляторні вимоги, аналіз конкурентної ситуації та іншу корисну інформацію, яка може бути використана при розробці підсистеми захисту "розумного" дому. Звернення до таких джерел може допомогти отримати офіційні дані та встановити контакти з іншими підприємствами або організаціями, що діють у схожому галузевому середовищі.

4.3.3. Аналіз даних

Аналіз даних є важливим етапом розробки підсистеми захисту "розумного" дому. Ось деталі аналізу даних, що стосуються хто, чому, скільки та коли буде готовий купити продукт проекту в найближчій та подальшій перспективі, а також визначення зразкової реалізаційної ціни продукту проекту в умовах конкуренції:

а) Хто, чому, скільки, коли буде готовий купити продукт проекту в найближчій та подальшій перспективі: Цей аспект аналізу даних передбачає вивчення потенційних споживачів продукту проекту, їхніх потреб і мотивацій для придбання продукту. Це може включати вивчення ринкових сегментів, аналіз демографічних та соціально-економічних характеристик цих сегментів, вивчення споживацьких тенденцій, оцінку потенційного попиту на продукт в найближчій та подальшій перспективі, а також визначення факторів, які впливають на рішення споживачів про купівлю продукту.

б) Визначення зразкової реалізаційної ціни продукту проекту в умовах конкуренції: Цей аспект аналізу даних передбачає вивчення

конкурентного середовища, оцінку діючих конкурентів, їхніх продуктів, цін, маржі та інших факторів, які впливають на ціну продукту. Виконання аналізу даних може включати порівняння цін на аналогічні продукти на ринку, аналіз стратегії ціноутворення конкурентів, визначення оптимальної цінової позиції продукту проекту в умовах конкуренції, а також оцінку впливу різних цінових стратегій на прибутковість та ринкову привабливість продукту проекту.

Джерела даних для проведення аналізу можуть включати різноманітні джерела, такі як ринкові дослідження, звіти торгових асоціацій, даних від потенційних споживачів, аналіз конкурентів, даних з інших джерел, таких як публікації, звіти, аналітичні документи, статистичні дані та інші.

Після збору та аналізу даних можна визначити потенційний попит на продукт проекту в найближчій та подальшій перспективі, розуміти хто та чому може бути зацікавлений у придбанні продукту, а також визначити оптимальну цінову стратегію, враховуючи конкурентний контекст.

Цей аналіз даних є важливим етапом розробки підсистеми захисту "розумного" дому, оскільки дозволяє зробити обґрунтовані рішення щодо розвитку продукту, встановлення цін та визначення його конкурентної позиції на ринку.

4.4.Конкуренція

Найбільші конкуренти на ринку підсистем захисту "розумного" дому є різними компаніями, які також пропонують аналогічні продукти або послуги в цьому сегменті ринку. Декілька з них:

1. Amazon (Ring): Ring є одним з провідних виробників підсистем захисту "розумного" дому, таких як відеодзвінки, відеокамери, датчики руху тощо. Вони також мають екосистему інтегрованих продуктів та послуг, таких як системи моніторингу та підключення до хмарних служб.

2. Google (Nest): Nest, який належить Google, є ще одним відомим виробником продуктів "розумного" дому, таких як термостати, відеодзвінки, камери та інші датчики. Вони також пропонують інтегровані рішення для керування різними аспектами "розумного" дому через одну платформу.
3. Samsung (SmartThings): SmartThings, вироблений Samsung, є іншим відомим брендом в галузі "розумного" дому. Вони пропонують різні продукти та платформи, такі як головні контролери, датчики, засоби керування та інтеграцію з іншими пристроями Samsung.
4. SimpliSafe: SimpliSafe є компанією, яка спеціалізується на домашніх системах безпеки, таких як виявлення вторгнень, відео-нагляд, датчики відкриття вікон та дверей тощо. Вони відомі своєю простотою встановлення та використання, а також конкурентними цінами.
5. Honeywell: Honeywell є відомим виробником продуктів для домашньої автоматизації, включаючи системи безпеки, такі як датчики руху, датчики диму та вуглекислого газу, системи контролю доступу та інші рішення.
6. ADT: ADT є одним з провідних постачальників послуг моніторингу безпеки для домів, включаючи відеонагляд, датчики вторгнень, пожежний захист та інші рішення.
7. Arlo: Arlo є виробником відеокамер "розумного" дому, включаючи багатофункціональні відеокамери для відеонагляду в приміщенні та на вулиці, дверні дзвінки, системи освітлення та інші пристрої.
8. Xiaomi: Xiaomi є китайською компанією, яка також пропонує продукти "розумного" дому, включаючи системи безпеки, системи контролю доступу, розумні датчики та інші рішення.
9. August Home: August Home є виробником "розумних" замків та систем керування доступом, які дозволяють власникам дому керувати доступом до свого житла через мобільний додаток.

Це лише кілька прикладів великих конкурентів на ринку підсистем захисту "розумного" дому. Ринок постійно розвивається, тому можуть бути інші компанії, які також конкурують на цьому ринку з різними продуктами, Важливо враховувати, що ринок швидко розвивається, тому можуть бути інші компанії, які входять в конкуренцію з різними продуктами та рішеннями.

1. Якщо враховувати ж ці дані виробників продуктів "розумного" дому з точки зору їх роботи, то їхні справи можуть відрізнятися в залежності від кожної компанії. Оскільки дані компанії є комерційними суб'єктами, то точна інформація про їхні справи може бути обмежена і підлягати змінам з часом. Проте, в загальному, ось деякі загальні відомості:
2. З об'єктами продажу: Компанії можуть мати різний успіх з об'єктами продажу в залежності від рівня конкуренції, рівня популярності їхніх продуктів, економічної ситуації на ринку та інших факторів. Деякі компанії можуть мати стабільний попит на свої продукти, тоді як інші можуть стикатися зі зниженням продажів.
3. З доходами: Доходи компаній також можуть варіюватися в залежності від багатьох факторів, таких як рівень продажів, ціни продуктів, витрати на виробництво, маржинальність, податкові обов'язки та інші. Успіх компаній може бути визначений їхнім фінансовим здоров'ям, зростанням доходів та зисків.
4. З впровадженням нових моделей: Впровадження нових моделей продуктів може вплинути на успішність компаній. Це може включати розширення лінійки продуктів, вдосконалення функцій, вдосконалення дизайну та інших інновацій. Успіх впровадження нових моделей може впливати на здатність компаній відповідати на змінюючіться вимоги ринку та забезпечувати зростання продажів.
5. З технічним сервісом: Опанування технічного сервісу може бути важливим аспектом бізнесу виробників продуктів "розумного" дому,

особливо коли йдеться про машини або обладнання. Гарний технічний сервіс може вплинути на задоволеність клієнтів, репутацію компанії, а також може вплинути на повторні продажі та відновлення клієнтської бази. Компанії можуть приділяти різну увагу і засоби на розвиток технічного сервісу, такі як надання гарантій, навчання клієнтів, технічну підтримку та вирішення проблем.

6. Рекламна компанія: Реклама є важливим аспектом бізнесу, оскільки вона допомагає привернути увагу клієнтів, зробити продукти відомими та розповісти про переваги в порівнянні з конкурентами. Компанії можуть виділяти різні ресурси на рекламні кампанії, такі як реклама в ЗМІ, соціальні мережі, цифровий маркетинг, спонсорство подій та інші промоційні заходи.

Окрім вищенаведених аспектів, справи виробників продуктів "розумного" дому можуть бути вплинуті багатьма іншими факторами, такими як конкуренція на ринку, зміни в технологіях, споживчих тенденціях, економічному кліматі та багатьох інших. Компанії постійно моніторять ринок та виробляють стратегії, щоб відповідати на змінюючіться умови та залишатися конкурентоспроможними.

4.5.Умови та план виробництва

Умовні питання щодо плану виробництва, можна описати наведеними нижче твердженнями:

- Місце виробництва товарів на діючому або знову створеному підприємстві може бути визначено з урахуванням різних факторів, таких як доступність ресурсів, логістика, ринкові умови та стратегічні цілі підприємства. Вибір місця виробництва може вимагати детального аналізу різних варіантів та врахування можливих вигод, включаючи податкові пільги, інфраструктуру, робочу силу та інші фактори.

•Необхідні виробничі потужності можуть бути визначені на основі прогнозованого обсягу виробництва, технічних вимог та стандартів, а також стратегічних планів розвитку підприємства. Нарощування виробничих потужностей з року в рік може залежати від збільшення попиту на продукцію, введення нових технологій, розширення асортименту товарів та інших факторів.

•Вибір постачальників сировини та комплектуючих може бути важливим аспектом виробництва. Репутація постачальників, досвід роботи з ними, ціни, якість продукції та інші фактори можуть вплинути на якість виробництва, терміни поставок та загальну ефективність підприємства.

•Виробнича кооперація може бути використана для співпраці з іншими підприємствами, включаючи спільне використання ресурсів, обмін технологіями, спільні науково-дослідні роботи та інші форми співпраці. Вибір потенційних партнерів для виробничої кооперації може залежати від стратегічних цілей підприємства, вза

•Лімітація об'ємів виробництва або поставок ресурсів може бути обумовлена рядом факторів, таких як внутрішні обмеження підприємства, регулятивні обмеження, ринкові умови або незавершені угоди з постачальниками. Важливо враховувати можливість таких лімітацій при плануванні виробництва та поставок ресурсів.

•Устаткування, необхідне для виробництва товарів, може бути різноманітним, включаючи машини, обладнання, інструменти, транспортні засоби та інше. Вибір необхідного устаткування може залежати від технічних вимог виробництва, бюджету підприємства, термінів виробництва та інших факторів. Місце придбання устаткування також може бути важливим аспектом, включаючи вибір постачальників, досвід роботи з ними, гарантії, технічну підтримку та інші фактори.

•При виробництві товарів можуть виникати різноманітні проблеми, такі як технічні неполадки, затримки в поставках ресурсів, недостатні кваліфікації працівників, регуляторні обмеження та інші. Важливо передбачати можливі проблеми та розробляти плани дій для їх вирішення,

забезпечувати достатні резерви ресурсів та координацію між різними відділами підприємства для ефективного вирішення виникаючих проблем.

4.6.Організаційний план

4.6.1. Працівники та їх кваліфікація

1. Відповідно до розробки підсистеми захисту "розумного" дому, для успішного ведення справ необхідно мати в команді фахівців з наступними профілями, освітою та досвідом:
2. Фахівці з інформаційної безпеки: особи з відповідною освітою в галузі інформаційної безпеки, знаннями в області криптографії, мережевої безпеки, захисту даних тощо. Заробітна плата може бути відповідною до рівня кваліфікації та досвіду фахівців.
3. Фахівці з програмування та розробки: особи з відповідною освітою в галузі програмування, знаннями мов програмування, алгоритмів, платформ розробки "розумного" дому тощо. Умови прийому на роботу можуть бути різними, включаючи постійну роботу або співпрацю на умовах сумісництва (зовнішні експерти) в залежності від потреб та ресурсів підприємства.
4. Залежно від можливостей та стратегії підприємства, може бути можливість скористатися послугами спеціалізованих організацій з найму фахівців з розробки "розумного" дому, які мають відповідний досвід та компетенції в цій галузі.
5. У випадку, якщо частина персоналу вже найнята, можуть бути надані короткі біографічні дані про співробітників, такі як їхня кваліфікація, досвід роботи та його корисність для підприємства. Наприклад, може бути зазначено, які проекти вони успішно

виконували, які технічні навички та експертизу вони внесли в розробку підсистеми захисту "розумного" дому.

Ось приклад коротких біографічних даних про співробітників:

- Іван Петров - має вищу освіту в галузі інформаційної безпеки, зі спеціалізацією в криптографії. Має 5 років досвіду роботи в інформаційній безпеці, включаючи розробку захисту мереж та систем "розумного" дому. Вніс вагомий внесок в розробку шифрувальних алгоритмів для захисту даних клієнтів. Заробітна плата - відповідно до рівня експертизи та досвіду.
- Олександра Коваленко - має вищу освіту в галузі програмування, зі спеціалізацією в розробці "розумного" дому. Має 3 роки досвіду роботи в розробці програмного забезпечення для "розумного" дому, включаючи розробку додатків для керування системою та інтеграцію з різноманітними пристроями. Має вміння працювати з різними мовами програмування, такими як Python, Java та JavaScript. Заробітна плата - відповідно до рівня компетенції та ринкової вартості.

Це лише приклади коротких біографічних даних про співробітників, які можуть бути вказані в курсовій роботі про розробку підсистеми захисту "розумного" дому. Фактичні біографічні дані можуть варіюватися в залежності від реальних співробітників та їхнього внеску в проект.

4.7.Юридичний план. Приватна власність розроблюємого продукту

Приватна власність може мати важливий вплив на розробку підсистеми захисту "розумного" дому. У такому випадку, студент може зазначити, що власником підприємства, що займається розробкою підсистеми захисту, є приватна особа або приватна компанія. Це може вплинути на організаційну структуру підприємства, процес прийняття рішень, фінансові можливості та стратегії розвитку проекту.

Наприклад, власник приватного підприємства може мати більший контроль над процесом прийняття рішень та може взяти на себе

відповідальність за ключові аспекти розробки підсистеми. Заробітна плата фахівців може бути визначена власником відповідно до його стратегії та фінансових можливостей. Крім того, власник приватного підприємства може взяти на себе роль координації та контролю за діяльністю всіх служб, враховуючи свої власні вимоги та бажання.

Однак, варто враховувати, що приватна власність також може мати свої виклики, такі як обмежені фінансові ресурси, високий рівень відповідальності власника та більш складний процес прийняття рішень. Студент може розглянути ці аспекти в розділі про організаційну структуру підприємства в контексті розробки підсистеми захисту "розумного" дому.

4.8.Оцінка ризику і страхування

4.8.1. Ризики і конфлікти

Оцінка можливих ризиків є важливим етапом в розробці підсистеми захисту "розумного" дому. Розумний дім використовує розумні пристрої та мережі зв'язку для автоматизації керування різними функціями будинку, такими як освітлення, опалення, безпека, розумні пристрої та інші. Однак, відкритість таких систем може вести до певних ризиків, таких як:

1. Кібербезпека: Розумний дім може бути піддається кібератакам, таким як хакерські атаки, віруси, фішинг та інші. Це може призвести до несанкціонованого доступу до системи, зламу безпеки та витоку особистої інформації власника.
2. Приватність: Використання розумних пристроїв може викликати занепокоєння щодо приватності, так як вони можуть збирати та передавати особисту інформацію про власника та його розпорядження в домашньому середовищі.
3. Фізична безпека: Розумні пристрої можуть контролювати фізичний доступ до будинку, такий як двері, вікна, системи відеоспостереження тощо. В разі несправності або зламу таких

систем, це може призвести до порушення фізичної безпеки власника та його майна.

4. Технічні проблеми: Розумні системи можуть мати технічні проблеми, такі як відмови в роботі, неправильна настройка, сумісність між пристроями, падіння мережі зв'язку тощо. Це може вплинути на надійність та ефективність роботи системи.
5. Людський фактор: Використання розумних систем також може відповідати на людський фактор, такий як помилкив налаштуванні системи, неправильне використання розумних пристроїв, несвоєчасне оновлення програмного забезпечення та інші дії власника, які можуть призвести до виникнення ризиків.
6. Електромагнітна сумісність: Розумні системи можуть бути вразливі до електромагнітних перешкод, таких як радіочастотні перешкоди від інших електронних пристроїв. Це може вплинути на надійність та стабільність роботи системи.
7. Залежність від інтернету: Розумні системи можуть бути залежні від наявності стабільного інтернет-з'єднання для своєї роботи. Відсутність інтернету або його відключення може призвести до недоступності або обмеження функціональності системи.

Оцінка можливих ризиків є важливим кроком у розробці підсистеми захисту "розумного" дому, оскільки дозволяє ідентифікувати потенційні загрози та прийняти відповідні заходи безпеки для забезпечення надійності та захищеності системи. Додаткові заходи безпеки можуть включати використання сильних паролів, захист мережі зв'язку, використання шифрування, регулярні оновлення програмного забезпечення, контроль доступу до системи та інші заходи, що допоможуть знизити ризики та забезпечити безпеку розумного дому.

4.8.2. Зменшення витрат

Для запобігання та профілактики ризиків, пов'язаних з розробкою підсистеми захисту "розумного" дому, можна вживати наступні шляхи:

Забезпечення безпечного налаштування системи: Важливо правильно налаштувати всі розумні пристрої та системи, встановити сильні паролі, вимкнути непотрібні функції та встановити права доступу відповідно до потреб та політик безпеки.

1. Оновлення програмного забезпечення: Регулярне оновлення програмного забезпечення розумних пристроїв та системи може допомогти виправити виявлені вразливості та захистити систему від відомих загроз.
2. Використання захисту мережі: Забезпечення захисту мережі зв'язку, такої як використання захищених Wi-Fi мереж, використання брандмауера та відокремлення мережі розумних пристроїв від основної мережі, може допомогти запобігти несанкціонованому доступу до системи.
3. Контроль доступу: Встановлення контролю доступу до системи, такого як обмеження доступу до адміністративних функцій та віддаленого доступу, може допомогти запобігти несанкціонованому доступу до системи.
4. Користування надійними пристроями: Важливо використовувати надійні та сертифіковані розумні пристрої від відомих виробників, які мають довідку про безпеку та оновлюють своє програмне забезпечення.
5. Свідоме використання системи: Власник розумної системи має бути свідомим користувачем, уникаючи неправильного використання системи, викладення паролів, кодів доступу та інформації про систему в загальнодоступному місці.
6. Інформування користувачів: Проведення нававчання та інформування користувачів про правила безпеки використання розумних систем, розповсюдження рекомендацій та пам'яток з

питань безпеки може допомогти підвищити рівень обізнаності користувачів та знизити ризик виникнення загроз.

7. Фізична безпека: Забезпечення фізичної безпеки системи, такої як захист пристроїв від фізичного доступу сторонніх осіб, використання фізичних засобів захисту, таких як камери відеоспостереження, датчики руху та інші засоби, може допомогти забезпечити захист системи від несанкціонованого доступу.
8. Резервне копіювання: Регулярне резервне копіювання даних та налаштувань системи може допомогти відновити роботу системи в разі виникнення проблем або атаки.
9. Аудит безпеки: Проведення аудиту безпеки системи, виявлення потенційних вразливостей та прийняття заходів для їх виправлення може допомогти забезпечити сталу безпеку системи.

Ці шляхи можуть варіюватися в залежності від конкретної форми організації та вимог безпеки, але загалом вони можуть допомогти знизити ризики, пов'язані з розробкою підсистеми захисту "розумного" дому та забезпечити високий рівень безпеки системи.

4.9.Стратегія фінансування

4.9.1. Засоби реалізації продукту

Для визначення кількості необхідних засобів для реалізації конкретного проекту, потрібно зазначити більше деталей про сам проект. Вимоги до засобів можуть різнитися в залежності від характеру проекту, його масштабів, галузі, в якій він реалізується, та багатьох інших факторів.

Декілька загальних категорій засобів, які можуть бути необхідні для реалізації проекту, включають:

1. Фінансові засоби: це можуть бути грошові кошти, кредити, інвестиції або інші джерела фінансування, які необхідні для

покриття витрат на проект, таких як виробничі витрати, зарплати, закупівля обладнання тощо.

2. Матеріальні засоби: це можуть бути фізичні ресурси, такі як сировина, матеріали, обладнання, машини, транспортні засоби та інші матеріальні ресурси, необхідні для виробництва продукції або виконання робіт проекту.
3. Людські ресурси: це включає кваліфіковані кадри, необхідні для виконання різних функцій в рамках проекту, таких як менеджмент, розробка продукту, виробництво, маркетинг, фінанси тощо.
4. Технічні засоби: це можуть бути програмне забезпечення, інформаційні системи, технічні пристрої, інструменти та інші технічні засоби, необхідні для виконання різних завдань в рамках проекту.
5. Інтелектуальні засоби: це можуть бути патенти, ліцензії, ноу-хау, бренди та інші інтелектуальні права, які можуть бути важливі для реалізації проекту, зокрема в галузі досліджень, розробки нових продуктів або впровадження інноваційних рішень.
6. Інфраструктура: це можуть бути будівлі, споруди, комунікації, електромережі, водопостачання, каналізація та інші інфраструктурні засоби, які необхідні для забезпечення функціонування проекту.
7. Маркетингові засоби: це можуть бути рекламні матеріали, розробка бренду, маркетингові дослідження, рекламні кампанії, PR-заходи та інші засоби для просування продукту або послуги, яку проект пропонує.

Кількість засобів, необхідних для реалізації проекту, буде залежати від його обсягу, складності, тривалості та багатьох інших факторів. Для визначення точної кількості засобів, необхідних для вашого конкретного проекту, рекомендується провести детальний аналіз вимог проекту, розробити бізнес-план або проектний план, враховуючи всі витрати, необхідні для його успішної реалізації.

4.9.2. Джерела фінансування ресурсів

Джерела фінансових ресурсів для реалізації проекту можуть бути різноманітні і залежать від конкретної ситуації та можливостей проекту. Деякі з можливих джерел фінансування можуть включати:

1. Власні засоби: це можуть бути власні кошти, які вкладаються в проект власником або інвестором. Це можуть бути особисті заощадження, капітал, накопичення або інші ресурси, які вкладаються в проект без залучення зовнішнього фінансування.
2. Кредити банків: це можуть бути кредити або позики, надані банками або фінансовими установами підприємству або проекту. Це можуть бути кредити на розвиток бізнесу, інвестиційні кредити, кредитні лінії та інші форми кредитування.
3. Залучення засобів партнерів: це може включати співфінансування проекту з боку партнерів, які можуть бути іншими підприємствами, організаціями або інвесторами. Це можуть бути спільні вкладення, спільні проекти, альянси, договори про співпрацю та інші форми партнерства.
4. Залучення засобів акціонерів: це можуть бути кошти, які залучаються шляхом випуску акцій або інших цінних паперів компанії, в результаті чого акціонери стають власниками певної частки компанії. Це можуть бути внутрішні або зовнішні інвестори, які вкладають кошти в обмін на акції компанії.

Інші джерела фінансування: це можуть бути різноманітні джерела фінансування, такі які джерела фінансування можуть включати державні субсидії, гранти, спонсорську підтримку, продаж активів, залучення інвестицій від ангелів-інвесторів або венчурних фондів, краудфандинг, краудлендінг, факторинг, лізинг, а також інші альтернативні джерела фінансування.

Форма отримання фінансових ресурсів також може варіюватись від проекту до проекту. Це можуть бути:

- Готівкові кошти, отримані від власних джерел фінансування, кредитів банків, залучення засобів партнерів або акціонерів.
- Цінні папери, випущені компанією, такі як акції або облігації, які можуть бути розміщені на ринку і залучити капітал від інвесторів.
- Субсидії або гранти, отримані від держави або інших організацій, які надають фінансову підтримку на певні цілі або проекти.
- Інші форми фінансування, такі як кредитні лінії, лізингові договори, факторинг, краудфандинг або краудлендінг, де кошти можуть бути залучені через спеціальні платформи або угоди з певними учасниками.

Вибір джерел фінансування та форми їх отримання залежить від фінансових потреб проекту, його розмірів, ризиків, стратегії розвитку та доступних опцій фінансування. Планування та управління фінансами проекту має бути відповідальним та ретельно врахувати всі аспекти, щоб забезпечити достатні фінансові ресурси для успішного реалізації проекту та досягнення його цілей. Кожне джерело фінансування має свої переваги та недоліки, і може бути відповідним для різних типів проектів або етапів їх розвитку.

Наприклад, власні засоби можуть бути використані як початковий капітал для розпочатку проекту або як додаткові внутрішні резерви для фінансування його розвитку. Кредити банків можуть бути використані для залучення зовнішнього капіталу на вигідних умовах, але вони можуть мати високі відсоткові ставки та вимоги щодо забезпечення. Залучення засобів партнерів може дозволити поділити ризики та вигоди між різними сторонами, але вимагатиме встановлення партнерських відносин та узгодження умов співпраці. Залучення засобів акціонерів може забезпечити довгострокове фінансування, але також включає передачу власності та відповідальності.

Важливо також враховувати фінансову стабільність та ризики джерел фінансування, а також відповідність з місією та стратегією

проекту. Залежно від потреб та можливостей проекту, може бути використана комбінація різних джерел фінансування та форм їх отримання для забезпечення необхідних ресурсів та фінансової стабільності проекту.

ВИСНОВОК

У ході виконання даного дипломного проекту "Розробка підсистем захисту систем розумного будинку" проведені аналіз та дослідження, проектування задачі, програмування програмного продукту та розробка бізнес-плану. Кожен з розділів мав свою особливість та спрямованість, що дозволило досягти поставлених цілей проекту.

У першому розділі "Аналіз та дослідження" проведено комплексне дослідження систем розумного будинку та їх захисту. Виконано огляд існуючих рішень та стандартів у галузі захисту систем розумного будинку, виявлено потенційні загрози та вразливості. Визначені основні вимоги до системи захисту та проведений аналіз наявних технологій і методів захисту, що дало змогу розробити ефективну підсистему захисту.

Другий розділ "Проектування задачі" мав на меті розробити архітектуру та функціонал системи захисту. Було проведено аналіз вимог до системи, розроблено концептуальну модель, спроектовано структуру та функціонал підсистеми захисту. Крім того, були визначені критерії оцінки ефективності системи та розроблено методи тестування.

Третій розділ "Програмування програмного продукту" присвячений реалізації розробленої архітектури та функціоналу. Було використано сучасні інструменти та мови програмування для розробки програмного продукту. Реалізовано основні модулі та компоненти системи захисту, проведено їх інтеграцію та тестування. Забезпечено стабільну роботу підсистеми захисту та її взаємодію з іншими компонентами системи розумного будинку.

У розділі "Бізнес план" проведена оцінка комерційної придатності розробленої системи захисту. Були визначені цільові ринки та конкурентні переваги продукту. Проведений аналіз ринку показав потенційну популярність та попит на розумні будинки, а також потребу в надійній системі захисту. Були розраховані фінансові показники, включаючи витрати на розробку та виробництво, ціну продажу та очікувані доходи.

Результати аналізу показали перспективність розробленого продукту та його можливість впровадження на ринку.

В цілому, розробка підсистеми захисту систем розумного будинку включила аналіз та дослідження існуючих рішень та загроз, проектування ефективної архітектури та функціоналу, програмування програмного продукту з використанням сучасних інструментів, а також розробку бізнес-плану для оцінки комерційної придатності. Результатом роботи є функціональна та надійна підсистема захисту, яка може бути успішно впроваджена в системи розумного будинку для забезпечення безпеки та конфіденційності. Такий продукт має потенціал для успішного комерціалізації та отримання прибутку на ринку розумних будинків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

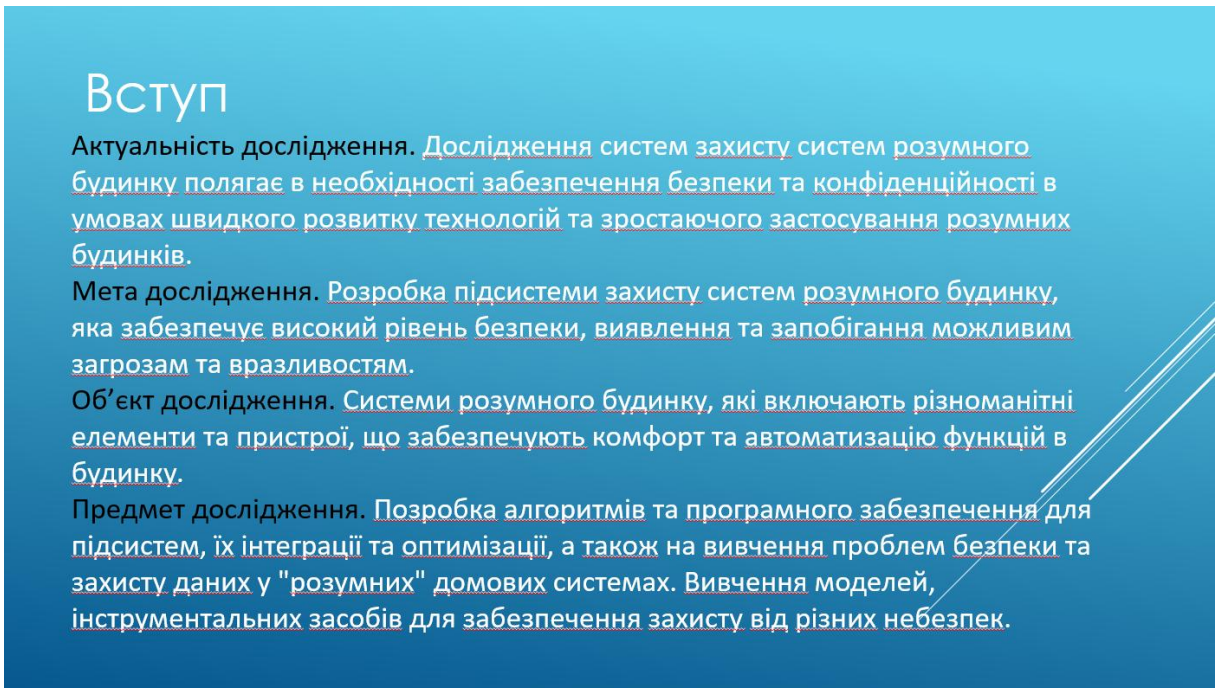
1. Чернишов В.О., Дерега М.В. Захист інформації в системах розумного будинку: підходи та технології. Київ: Видавництво НТУУ "КПІ", 2018.
2. Jones A., Smith B. Security and Privacy Issues in Smart Home Systems: A Survey. IEEE Communications Surveys & Tutorials, 2018, Vol. 20, No. 3, pp. 2234-2253.
3. Pongle P., Shaikh A. Security issues in smart homes: A review. International Journal of Advanced Computer Science and Applications, 2015, Vol. 6, No. 1, pp. 180-184.
4. Андрущак І.О., Стрельникова І.В., Марченко І.А. Безпека в системах розумного будинку. Наукові праці Донецького національного технічного університету, 2016, Вип. 36, С. 68-74.
5. Ghose A., Chakraborty S., Das A.K., Das S., Bhattacharyya D.K. IoT-based security framework for smart homes using fuzzy cognitive maps. Computers & Electrical Engineering, 2019, Vol. 79, pp. 61-76.
6. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 2015, Vol. 17, No. 4, pp. 2347-2376.
7. Кулинич В.М., Шаповалова О.В. Безпека в Інтернеті речей. Вісник Київського національного університету імені Тараса Шевченка. Серія: Радіофізика та електроніка, 2017, Вип. 1, С. 69-73.
8. Zeadally S., Siddiqui F., Baig Z., Adnan A. Security issues in wireless sensor networks: a survey. International Journal of Network Security & Its Applications, 2013, Vol. 5, No. 1, pp. 51-70.
9. Whitmore A., Agarwal A., Xu L. The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 2015, Vol. 17, No. 2, pp. 261-274.

10. Kheir N., Ahmed R., Elleithy K.M. Securing the Internet of Things (IoT) in Smart Homes: Opportunities and Challenges. In: Advances in Ubiquitous Networking 2. Singapore: Springer, 2017, pp. 139-162.
11. Ріболовлев О.А., Шинкаренко О.В. Захист систем розумного будинку від кіберзагроз. Проблеми інформаційної безпеки, 2019, № 3, С. 59-66.
12. Dey A., Karandikar A., Deshmukh S. Security Mechanisms for IoT-based Smart Homes: A Comprehensive Survey. International Journal of Computer Applications, 2018, Vol. 182, No. 38, pp. 32-39.
13. Tanwar S., Kumar N., Parekh K., et al. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Communications Surveys & Tutorials, 2018, Vol. 20, No. 3, pp. 2234-2271.
14. Ojo O., Mesbah A., Bozzon A. Security and Privacy Vulnerabilities of In-home Displays in Smart Metering Systems: A Comprehensive Survey. ACM Computing Surveys, 2019, Vol. 52, No. 5, Article No. 98.
15. Блинова А.В., Киселева А.М., Паршина О.М. Безпека Інтернету речей: загрози та заходи забезпечення. Міжнародний науковий журнал "Інтернаука", 2018, № 3, С. 36-39.
16. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 2013, Vol. 29, No. 7, pp. 1645-1660.
17. Andreu-Perez J., Wichert A., Melenhorst M., et al. Security and Privacy Framework for the Internet of Things. In: Building the Future Internet through FIRE. Amsterdam: IOS Press, 2011, pp. 41-56.

Додаток А

Презентація Атестаційної випускної роботи

Слайд 1 – Розробка підсистем захисту розумного будинку

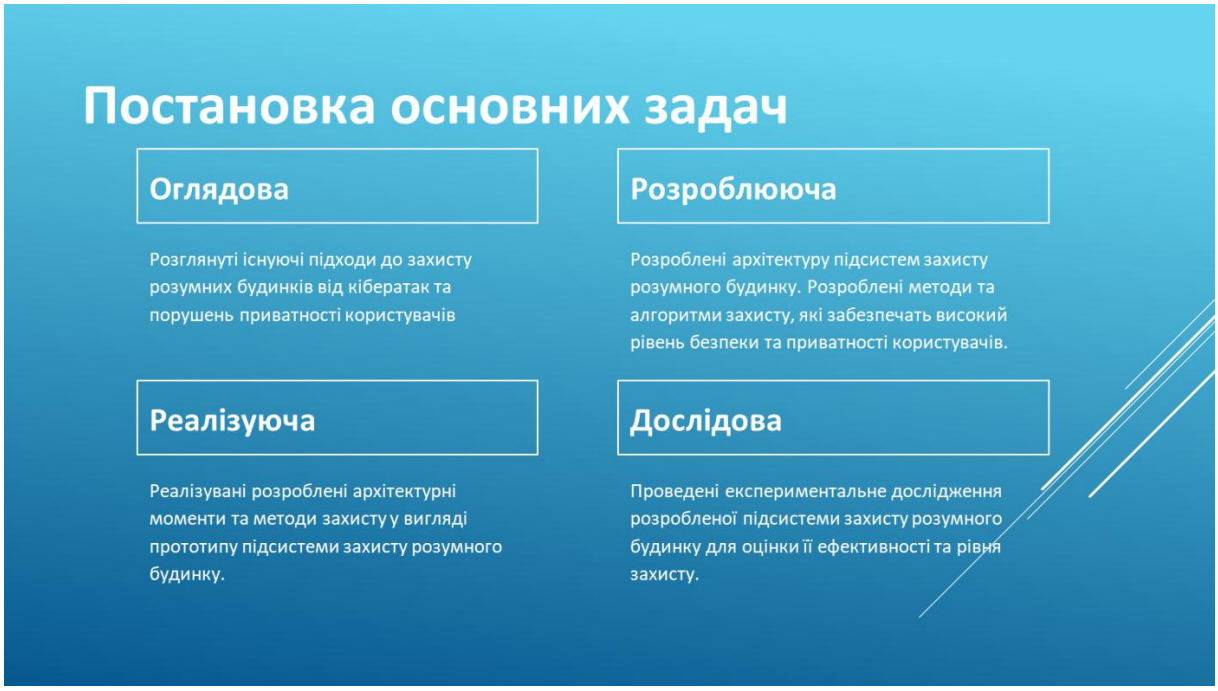


Слайд 2 – Вступ

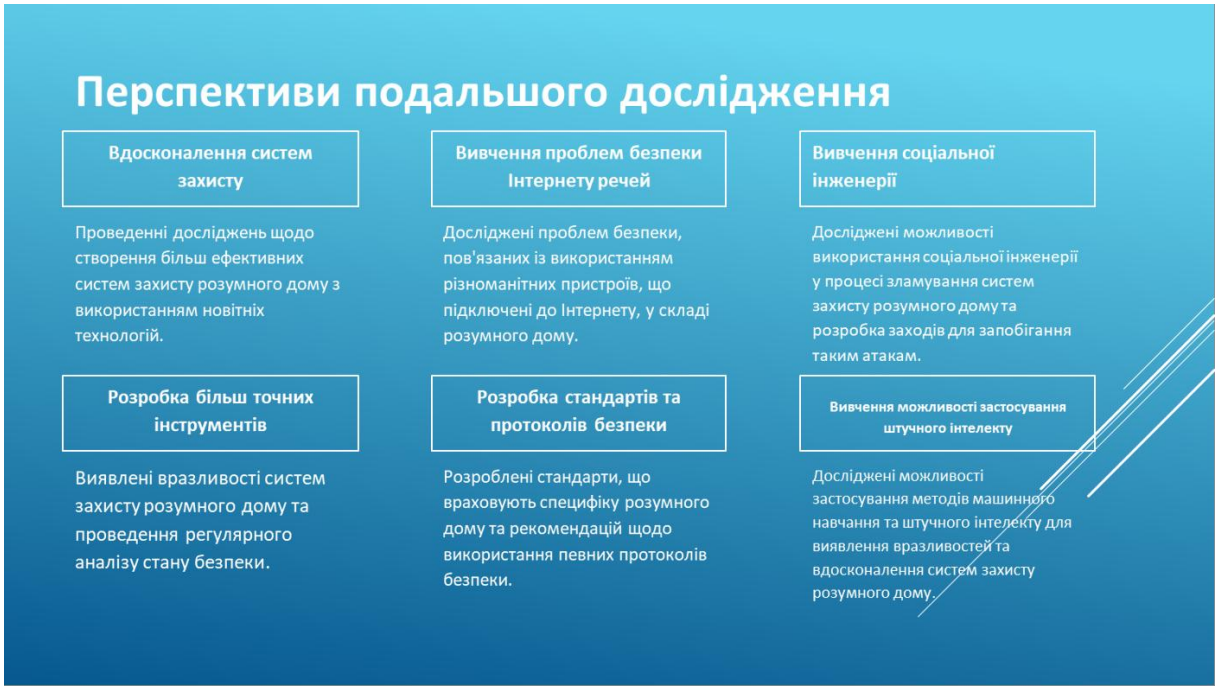
Слайд 3 – Дерево цілей

Слайд 4 – Загрози та контрзаходи

Слайд 5 – Три основні методики шифрування

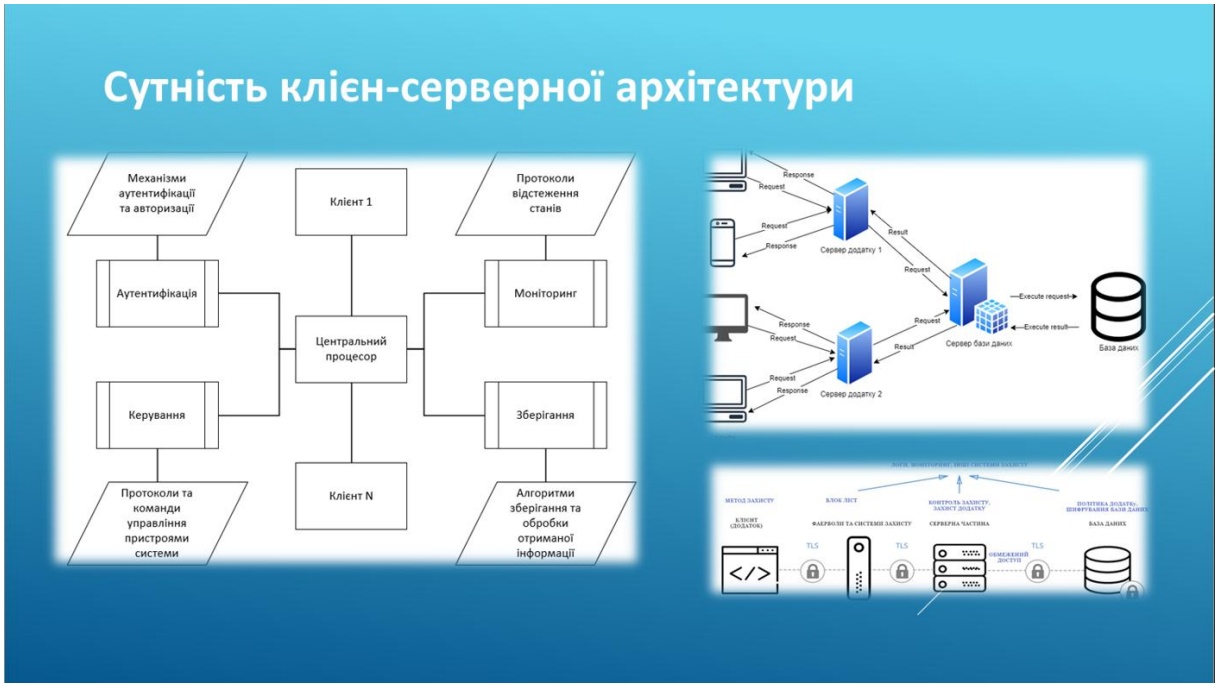


Слайд 6 – Постановка основних задач



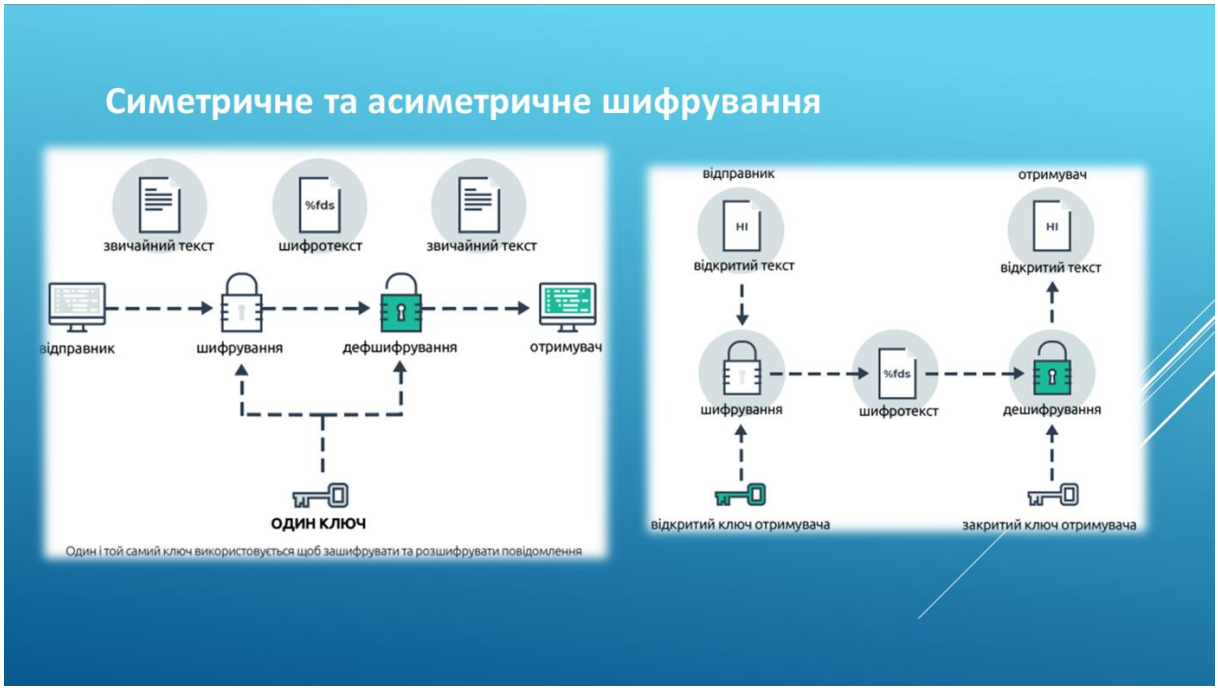
Слайд 7 – Перспективи подальшого дослідження

Слайд 8 – Нефункціональні та функціональні вимоги

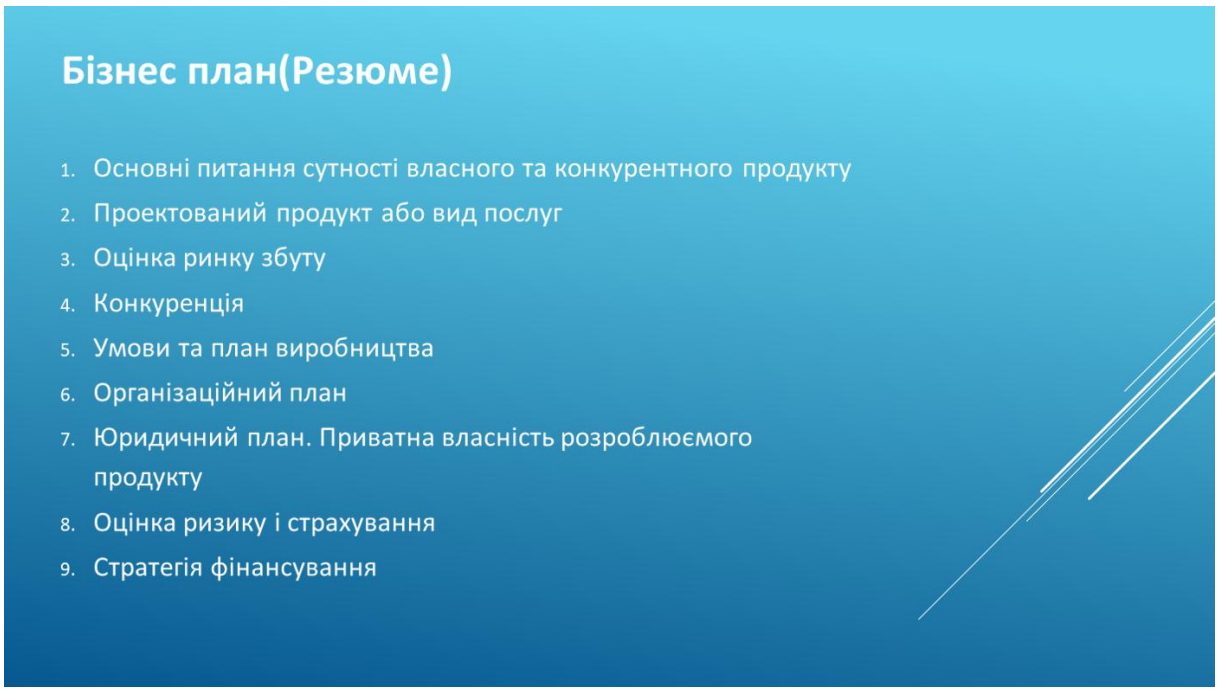


Слайд 9 – Сутність клієнт-серверної архітектури

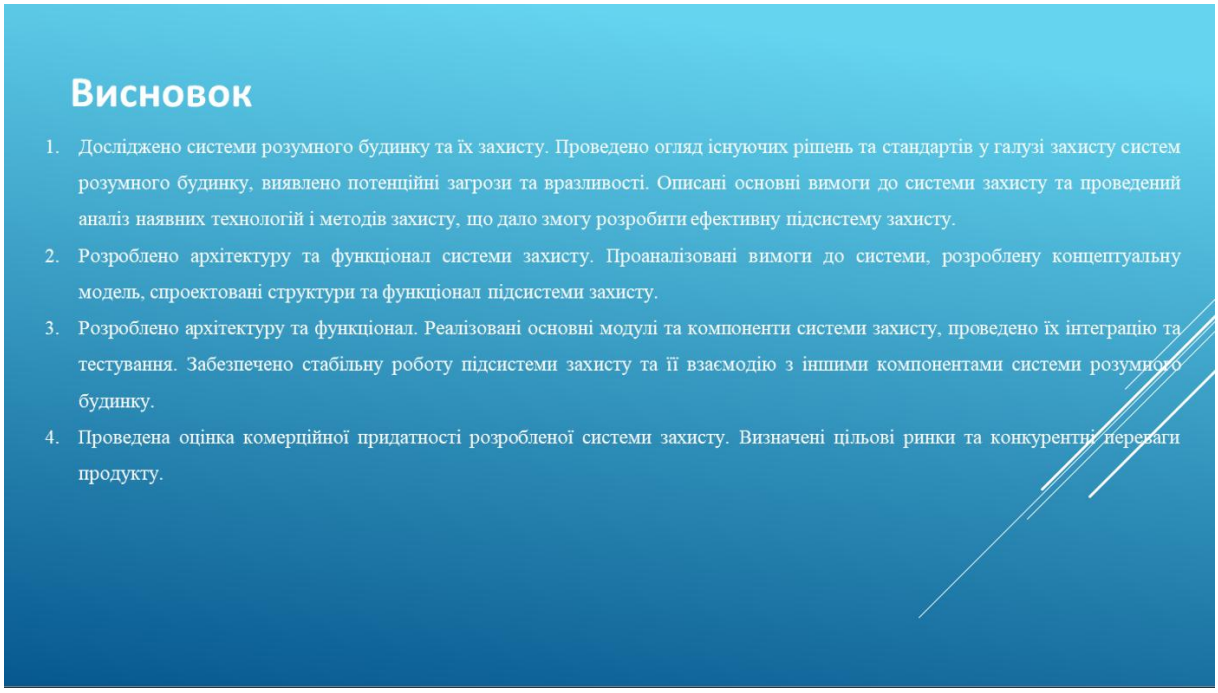
Слайд 10 – Розподіл функцій та компонентів між модулями ПЗ



Слайд 11 – Симетричне та асиметричне шифрування



Слайд 12 – Бізнес план(Резюме)



Слайд 13 – Висновок