МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.І.ВЕРНАДСЬКОГО
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МУНІЦИПАЛЬНОГО УПРАВЛІННЯ ТА МІСЬКОГО ГОСПОДАРСТВА
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

До захисту допущено

Завідувач кафедри
_____ Олександр ГУЙДА

"___" _____ 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до бакалаврської кваліфікаційної роботи освітнього ступеня "бакалавр"

з галузі знань 12 «Інформаційні технології»

спеціальності 122 «Комп'ютерні науки»

на тему: Інформаційна система безпеки інтелектуального будинку

Студента групи КН – 41 Черненка Олександра Сергійовича _____ (шифр групи) (прізвище, ім'я, по батькові) (підпис)

Керівник роботи к.т.н., доцент Ноженко В. С.,_ _____ (вчені ступінь та звання, прізвище, ініціали) (підпис)

Консультанти:
охорона праці та навко
лишнього середовища ___ доцент Гуйда О.Г._____ _____ (вчені ступінь та звання, прізвище, ініціали) (підпис)

Київ – 2023

ЗАТВЕРДЖЕНО
Наказ Міністерства освіти і науки, молоді та спорту України
29 березня 2012 року № 384

Форма № Н-9.01

ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ

В.І.ВЕРНАДСЬКОГО

Навчально-науковий інститут муніципального управління та міського господарства

Перший (бакалаврський) освітній рівень

Галузь знань 12 «Інформаційні технології»
(шифр і назва)

Спеціальність 122 «Комп'ютерні науки»
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Олександр ГУЙДА

"___" _____ 2022 р.

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

студента Черненка Олександра Сергійовича
(прізвище, ім'я,ПЗ батькові)

1 Тема роботи: Інформаційна система безпеки інтелектуального будинку

керівник роботи к.т.н., доцент Ноженко В. С.,
(прізвище, ім'я,ПЗ батькові, науковий ступінь, вчене звання)

затверджені ректором Університету від " 27" січня 2022 року

2 Строк подання студентом роботи "____" травня 2023 р.

3 Вихідні дані до роботи
Програмні технології дизайну та прототипування мобільних додатків

4 Зміст розрахунково-пояснювальної записки:
4.1 Проаналізувати сучасні методи інформаційних систем безпеки інтелектуальних будинків;
4.2 Обрати метод реалізації, провести вибір обладнання та програмного забезпечення;
4.3 Розробити тестовий варіант системи безпеки та протестувати його; 4.4 Розкрити питання охорону праці та навколишнього середовища.
5 Перелік графічного матеріалу:

Графічна робота виконана у вигляді мультимедійної презентації

6 Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада	Підпис, дата

	консультанта	завдання видав	завдання прийняв
Загальна частина	доцент Володимир НОЖЕНКО		
Технологічна частина	доцент Володимир НОЖЕНКО		
Спеціальна частина	доцент Володимир НОЖЕНКО		
Охорона праці та навколишнього середовища	доцент Олександр ГУЙДА		
Графічна частина	ст. викладач Олена ФУРТАТ		

7 Дата видачі завдання «30» січня 2023 року

КАЛЕНДАРНИЙ ПЛАН

Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Загальна частина	*січень*	
Технологічна частина	*березень*	
Спеціальна частина	*квітень*	
Охорона праці та навколишнього середовища	*лютий*	
Графічна частина	*Травень*	

Студент _____ Олександр ЧЕРНЕНКО (підпис) (прізвище та ініціали) **Керівник роботи** _____ Володимир НОЖЕНКО (підпис) (прізвище та ініціали)

РЕФЕРАТ

В останні роки розвиток інформаційних технологій сприяв появі нових концепцій життєдіяльності людини. Одна з таких концепцій - інтелектуальний будинок, що може керувати різними системами, такими як освітлення, опалення, кондиціонування повітря, безпека, медіа і т.д. Але, разом зі зростанням автоматизації, виникає потреба в забезпеченні безпеки цих систем, а також захисту від несанкціонованого доступу.

Для реалізації безпеки в інтелектуальному будинку можна використовувати інформаційну систему безпеки (ІСБ). Це система, що складається з різних компонентів, що забезпечують захист від вторгнень, вірусів, шкідливих програм, а також контролюють дії користувачів і надають доступ до системи з правами, які відповідають їх ролям в системі.

Метою дослідження кваліфікаційної бакалаврської роботи є аналіз проблем та викликів, пов'язаних із забезпеченням безпеки та захисту інтелектуальних будинків, а також у розробці та впровадженні інформаційної системи безпеки, яка забезпечить ефективний контроль і управління різними системами і пристроями в будинку.

Результатом дослідження є розроблена та впроваджена інформаційна система безпеки для інтелектуального будинку, яка дозволяє забезпечити безпеку життя та майна власників будинку, а також знизити ризик виникнення аварійних ситуацій та нещасних випадків. Проведене експериментальне дослідження показало ефективність розробленої інформаційної системи безпеки для інтелектуального будинку, а саме її здатність своєчасно виявляти та усувати можливі загрози безпеці мешканців та їх майна.

ЗМІСТ

ОСНОВНІ УМОВНІ ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

IoT (Internet of Things) – мережа фізичних пристроїв, які з'єднані між собою та з Інтернетом, і можуть збирати та обмінюватись даними.

AI (Artificial Intelligence) - галузь комп'ютерних наук, що займається розробкою алгоритмів і програм, які дозволяють комп'ютерам робити розумні рішення та виконувати завдання, які традиційно вимагають людської інтелектуальної діяльності.

API (Application Programming Interface) - набір інструкцій та стандартів, які дозволяють різним програмним додаткам взаємодіяти один з одним, зазвичай використовується для забезпечення комунікацій між різними програмними додатками.

LAN (Local Area Network) – мережа комп'ютерів та інших пристроїв, які знаходяться в межах невеликого географічного району, такого як будинок, офіс або кампус для локального спільного доступу до ресурсів.

RFID (Radio-Frequency Identification) – технологія для ідентифікації за допомогою радіочастот, використовуючи RFID-тег, які містять в собі мікрочип та

антенну систему.

IP (Internet Protocol) – стандарт, що визначає формат та правила обміну даними між пристроями в мережі інтернет, є одним з основних елементів інтернет протоколоу, який використовується для ідентифікації та адресації кожного пристрою, що підключений до Інтернету.

ПЗ (Програмне Забезпечення) – комп’ютерні програми, що використовуються для виконання різноманітних завдань на комп'ютері або інших електронних пристроях, може включати в собі операційні системи, текстові процесори, бази даних та інші.

ВСТУП

Інтелектуальні будинки стають все популярнішими в сучасному світі, оскільки вони можуть покращувати якість життя людей, забезпечувати безпеку та енергоефективність. З розвитком технологій, зокрема Інтернету речей (IoT), стає все більш актуальною потреба у створенні інформаційних систем безпеки для інтелектуальних будинків.

Актуальність теми полягає в тому, що окрім того, як інтелектуальні будинки стають все більш популярними, збільшення їхньої автоматизації призводить до збільшення кількості електронних пристроїв та сенсорів, що вимагає належної інформаційної системи безпеки. Така система забезпечує захист інформації та фізичну безпеку власників будинку, а також дозволяє уникнути можливих аварійних ситуацій.

З іншого боку, зростає кількість кібератак на системи IoT, що може призвести до порушення безпеки будинку, викрадення конфіденційної інформації, або інших небажаних наслідків. Тому створення ефективної інформаційної системи безпеки для інтелектуального будинку є важливим завданням, яке потребує наукових досліджень та розробки.

Ця бакалаврська робота присвячена розробці та впровадженню

інформаційної системи безпеки для інтелектуального будинку. Дослідження включає в себе аналіз сучасних рішень та технологій в області інформаційної безпеки та IoT, проектування та розробку системи, тестування її функціональності та ефективності, а також розробку методів управління та моніторингу системи.

Метою цієї роботи є розробка та впровадження інформаційної системи безпеки для інтелектуального будинку, яка забезпечує високий рівень безпеки та комфорту для жителів будинку.

1 ЗАГАЛЬНА ЧАСТИНА

АНАЛІЗ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ БЕЗПЕКИ 1.1 Основне визначення поняття “Інформаційна система безпеки інтелектуального будинку”

Концепція “Інтелектуальний будинок” полягає у створенні такого будинку, який забезпечує комфортне, ефективне та безпечне проживання в ньому, завдяки використанню різноманітних технологій та систем автоматизації. Інтелектуальний будинок здатний автоматично контролювати та регулювати роботу різних систем, таких як опалення, кондиціонування, освітлення, системи безпеки, медіа, електроприладів тощо.

Основна мета інтелектуального будинку полягає у тому, щоб забезпечити максимальний рівень комфорту та безпеки для мешканців. За допомогою вбудованих сенсорів, систем контролю та управління, будинок може аналізувати дані та забезпечувати оптимальний рівень функціонування різних систем, що дозволяє зменшити витрати на енергію та забезпечити ефективне використання ресурсів.

Інтелектуальний будинок може бути віддалено керованим за допомогою мобільних додатків або веб-інтерфейсу, що дозволяє мешканцям контролювати роботу будинку з будь-якого місця та в будь-який час.

Усе це підтримується завдяки технології IoT – Internet of Things, або інтернет речей, яка уявляє з себе мережу фізичних пристроїв, що підключені до інтернету та обмінюються даними між собою без необхідності взаємодії з людиною або іншими пристроями. Пристрої IoT можуть бути різного типу, включаючи датчики, контролери, розумні домашні пристрої, автомобілі, медичні прилади та інші.

Існує кілька моделей зв'язку в мережі IoT, які визначають взаємодію між різними пристроями:

1) Клієнт-серверна модель зв'язку: У цій моделі один пристрій виступає в ролі клієнта, який надсилає запити на сервер, що знаходиться в Інтернеті. Сервер оброблює запит та повертає результат клієнту. Ця модель використовується для збору даних та взаємодії з розумними пристроями, такими як датчики вимірювання температури та вологості.

2) Peer-to-peer модель зв'язку: У цій моделі пристрої взаємодіють безпосередньо між собою, без посередництва сервера. Кожен пристрій може виступати як клієнт і сервер одночасно, що дозволяє їм взаємодіяти та обмінюватися даними в реальному часі. Ця модель використовується, наприклад, у взаємодії між датчиками та пристроями управління освітленням в будинку.

3) Hybrid модель зв'язку: У цій моделі пристрої використовують як клієнт-серверну модель, так і peer-to-peer модель зв'язку в залежності від потреб користувача та типу пристрою. Наприклад, датчики можуть використовувати peer-to-peer модель зв'язку для взаємодії з пристроями управління температурою в кімнаті, але одночасно надсилати дані на сервер для аналізу та моніторингу.

Кожна з моделей зв'язку має свої переваги та недоліки, які потрібно враховувати при проектуванні та розробці системи IoT. Клієнт-серверна модель забезпечує простоту та ефективність в обробці даних, але може стати залежною від доступності сервера та мережі Інтернет. Peer-to-peer модель зв'язку дозволяє

пристроям взаємодіяти безпосередньо та надійніше, але вона може бути складною для реалізації та управління. Hybrid модель забезпечує компроміс між простотою та надійністю, але може бути складною для розуміння та підтримки.

Застосування IoT безмежні. Він використовується в багатьох сферах, включаючи:

1) Смарт-будинки: IoT може включати у себе всі електронні прилади та розумні пристрої в домі, такі як освітлення, термостати, аудіосистеми та інші, що дозволяє забезпечити енергоефективність та зручність користувача.

2) Індустрія: IoT може бути використаний для збору та аналізу даних про виробничі процеси, що дозволяє підвищити продуктивність та ефективність виробництва.

3) Медицина: IoT може бути використаний для збору та аналізу даних про здоров'я пацієнтів, що дозволяє лікарям діагностувати хвороби та призначати ефективне лікування.

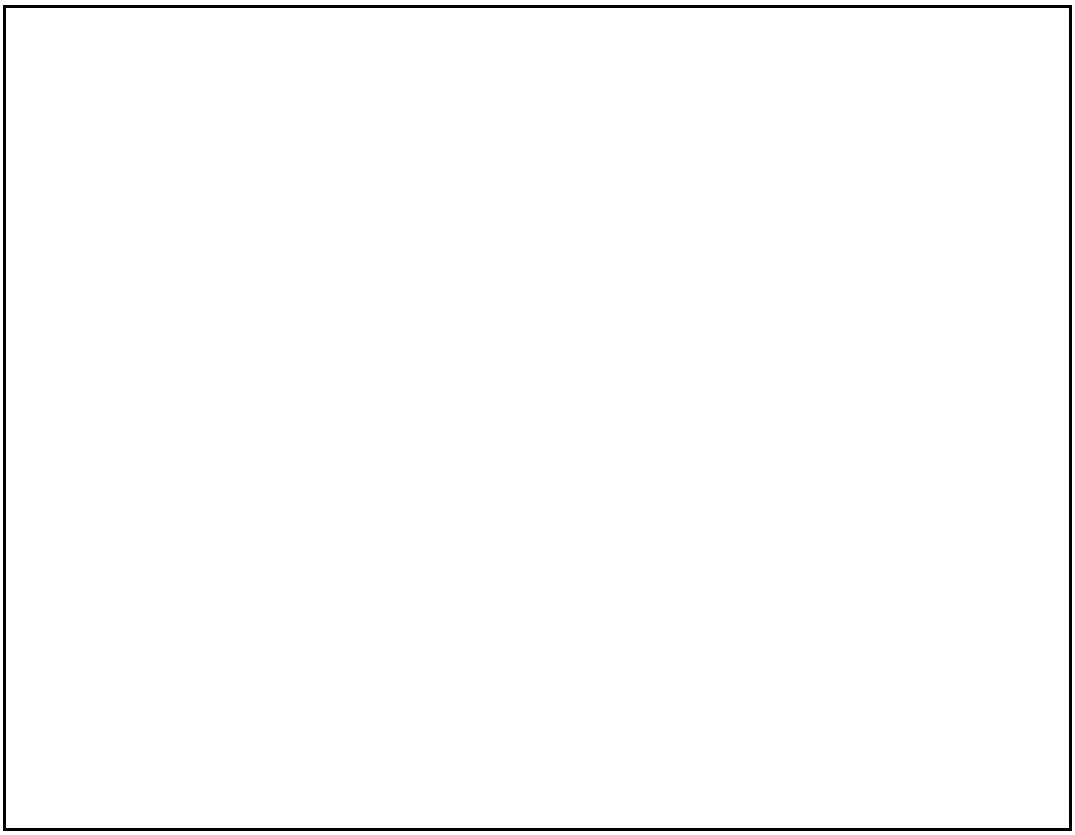

Рисунок. 1.1 Приклад розгорнутої системи інтелектуального будинку

У комерційній галузі інтелектуальні будинки можуть бути використані для забезпечення максимального рівня комфорту та безпеки для співробітників та клієнтів. Вони можуть забезпечувати контроль за роботою систем опалення, кондиціонування, освітлення та інших систем.

У промисловій галузі інтелектуальні будинки можуть бути використані для автоматизації процесів та забезпечення максимальної ефективності виробничих процесів. Вони можуть контролювати температуру, вологість та інші параметри, що впливають на процес виробництва.

Загалом, концепція інтелектуального будинку має великий потенціал для застосування в різних галузях, дозволяючи забезпечити максимальний рівень комфорту та безпеки для мешканців або працівників, зменшити витрати на енергію та забезпечити ефективне використання ресурсів.

Одним з найбільш важливих аспектів є система безпеки. Вона може включати в себе різноманітні системи, такі як системи відеоспостереження, датчики руху, датчики вікон та дверей, системи автоматичного виклику служб безпеки тощо. Завдяки системі безпеки, інтелектуальний будинок забезпечує максимальний рівень безпеки та захисту мешканців та їх майна.

Інформаційна система безпеки інтелектуального будинку - це комплекс програмно-апаратних засобів, призначених для захисту фізичної та інформаційної безпеки власників будинку, а також для забезпечення ефективного та безпечного взаємодії всіх електронних пристроїв та систем, що працюють у ньому.

Така система забезпечує цілодобовий контроль над різними параметрами будинку, такими як освітлення, опалення, кондиціонування повітря, а також безпекою, включаючи контроль доступу, виявлення пожежі, витоку газу та інші небезпечні ситуації.

Одна з основних проблем полягає у забезпеченні безпеки передачі даних між різними компонентами системи. Недостатньо захищена передача даних може призвести до витоку конфіденційної інформації та збільшити ризик кібератак. Крім того, важливо забезпечити захист від хакерських атак та вірусів, які можуть пошкодити електронні пристрої та знизити ефективність роботи системи.

Іншою проблемою є забезпечення надійності та стійкості системи. Інтелектуальний будинок містить багато різних електронних пристроїв, які повинні співпрацювати між собою, і неправильно налаштована система може привести до несправностей та аварій.

Важливо також забезпечити сумісність інформаційної системи безпеки з іншими системами та пристроями, що може бути проблемою через різні стандарти та протоколи. Недостатня сумісність може призвести до неправильної роботи системи та зменшення її ефективності.

Крім того, така система безпеки може стати об'єктом кібератак.

Зловмисники можуть намагатися зламати систему з метою отримання

конфіденційної інформації, зниження рівня безпеки системи чи захоплення контролю над системою в цілому. Для запобігання кібератакам потрібно розробляти системи забезпечення безпеки, які включають в себе захист від відомих видів атак, моніторинг системи на випадки несправностей та швидкий відгук на них.

Рисунок 1.2 Розпис недоліків інформаційної системи безпеки інтернету речей

Для розробки інформаційної системи безпеки необхідно враховувати різні вимоги, що можуть залежати від конкретної ситуації та вимог замовника. Наприклад, до загальних вимог в першу чергу відноситься безпека даних - система повинна забезпечувати захист конфіденційної та особистої інформації, яку вона обробляє. Це означає, що система безпеки повинна мати механізми для захисту даних від несанкціонованого доступу, змін та видалень. Сюди також відноситься захист від вірусів, шкідливих програм та інших загроз, що можуть впливати на її безпеку та працездатність.

Система повинна мати механізми для відновлення роботи після непередбачуваних ситуацій, таких як катастрофи, відключення електропостачання або втрати зв'язку.

Крім того, така система має відповідати визначеним стандартам безпеки, таким як ISO/IEC 27001, який визначає вимоги до управління інформаційною безпекою, та інших відповідних стандартів. Це забезпечить високий рівень безпеки системи та впевненість замовника у її безпеці.

При цьому, важливо забезпечити безпеку та захист системи від можливих кібератак та витоків конфіденційної інформації. Інформаційна система безпеки інтелектуального будинку, яка забезпечує захист від кіберзагроз та зламів, є ключовим елементом системи розумного будинку.

Забезпечення ефективної інформаційної системи безпеки вимагає комплексного підходу, що включає застосування технічних рішень, організаційних процедур та політик безпеки, основні компоненти яких включають:

1) Аутентифікація користувачів та пристроїв: забезпечення перевірки ідентичності користувачів, що намагаються отримати доступ до ресурсів системи, та перевірки автентичності пристроїв, що підключаються до мережі інтелектуального будинку.

2) Контроль доступу: регулювання доступу користувачів та пристроїв до активів розумного будинку з дотриманням принципу найменших привілеїв, що передбачає надання мінімальних необхідних прав доступу для виконання конкретних завдань.

3) Шифрування даних: застосування криптографічних методів для захисту конфіденційності, цілісності та доступності даних, які передаються або зберігаються в рамках розумного будинку.

4) Захист від зовнішніх атак та внутрішніх загроз: впровадження рішень та заходів, які допомагають виявляти, запобігати та реагувати на атаки з боку хакерів,

шкідливе програмне забезпечення або інші зловмисні дії, а також контролювати та мінімізувати ризик з боку внутрішніх користувачів або систем

5) Резервне копіювання та відновлення даних: створення регулярних резервних копій критичних даних та систем, що дозволяє відновити їх у разі втрати, пошкодження або компрометації.

6) Організаційні процедури та політики безпеки: розробка та впровадження внутрішніх політик, стандартів та процедур, що спрямовані на підтримку культури безпеки серед співробітників, контроль за доступом до активів, а також відповідне реагування на інциденти безпеки.

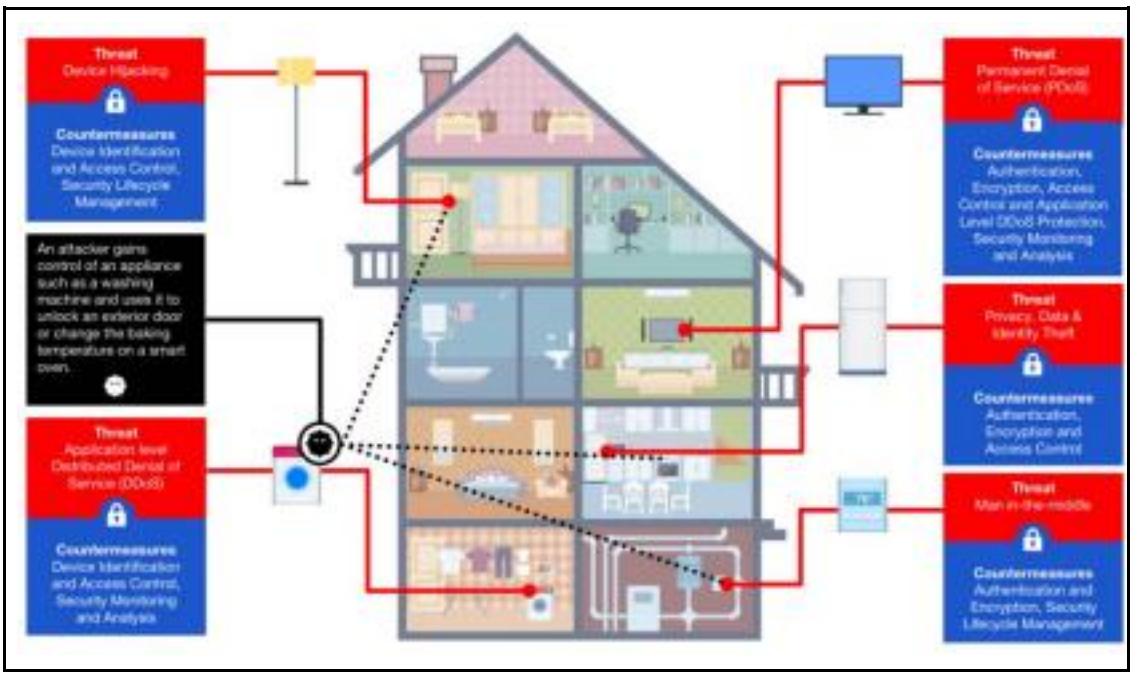

Рисунок. 1.3 Приклад загроз системи безпеки та заходи щодо їх уникнення

1.2 Аналіз ринку та огляд наявних рішень в області інформаційної безпеки будинків

Завдяки розвитку Інтернету речей (IoT) та штучного інтелекту (AI), ринок інформаційних систем безпеки продовжує зростати. Проводячи аналіз ринку з теми бакалаврської роботи “Інформаційної системи безпеки інтелектуального

будинку”, я провів огляд основних аспектів ринку, включаючи драйвери росту, ключових гравців, сегментації ринку, конкурентного середовища та можливих перспектив розвитку:

1) Ринкові драйвери

1) Зростання попиту на енергоефективні рішення: Системи розумних будинків дозволяють знижувати витрати на опалення, водопостачання, електроенергію та інші комунальні послуги.

2) Бажання забезпечити безпеку та захист від злому: Інформаційна система безпеки інтелектуального будинку надає можливість віддаленого контролю за будинком та використання сучасних методів ідентифікації та аутентифікації користувачів.

3) Розвиток інфраструктури Інтернету речей (IoT): Зростання кількості пристроїв IoT забезпечує більші можливості для впровадження інформаційних систем безпеки.

4) Збільшення кількості смартфонів та планшетів: Це дозволяє користувачам легко взаємодіяти з системами безпеки через додатки на своїх пристроях.

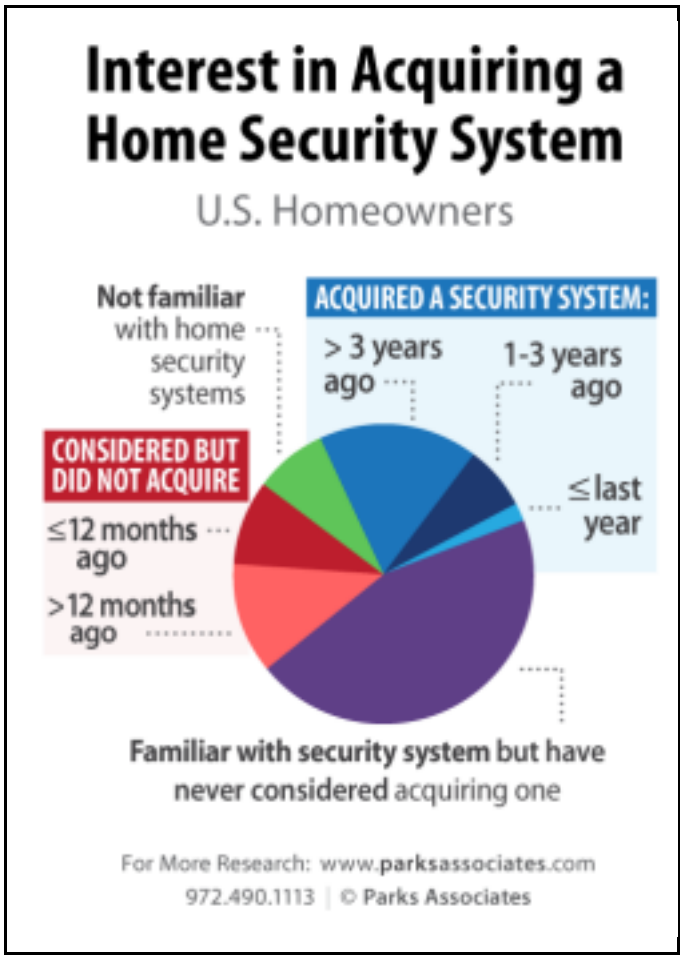

Рисунок 1.4 Аналіз попиту на системи безпеки інтелектуальних будинків у США

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

2) Ключові гравці

На ринку систем безпеки розумного будинку представлені провідні компанії, такі як Google Nest, Amazon Ring, ADT, Honeywell, SimpliSafe, та інші. Ці компанії пропонують різні продукти та послуги, включаючи сенсори, камери відеоспостереження, системи контролю доступу та пожежної безпеки.

До списку головних гравців також можна додати:

1) Honeywell International Inc - Міжнародний виробник систем безпеки та автоматизації.

2) Siemens AG - Німецька компанія, що пропонує рішення з енергетики, інфраструктури та будівельних технологій.

3) Schneider Electric - Французький виробник електрообладнання та систем автоматизації.

4)Johnson Controls - Американська корпорація, що спеціалізується на системах опалення, вентиляції та автоматизації.

5) ABB Ltd. – Швейцарська компанія, яка займається виробництвом енергетичного обладнання та автоматизаційних систем

6) Legrand - Французький виробник електричного та цифрового будівельного інфраструктурного обладнання.

7) Samsung Electronics Co., Ltd. - Південнокорейський гігант, що пропонує широкий спектр електроніки, включаючи системи безпеки та розумних будинків.

8) Apple (HomeKit) - Відома американська компанія, що розробляє платформу HomeKit для керування розумними пристроями та системами безпеки.

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

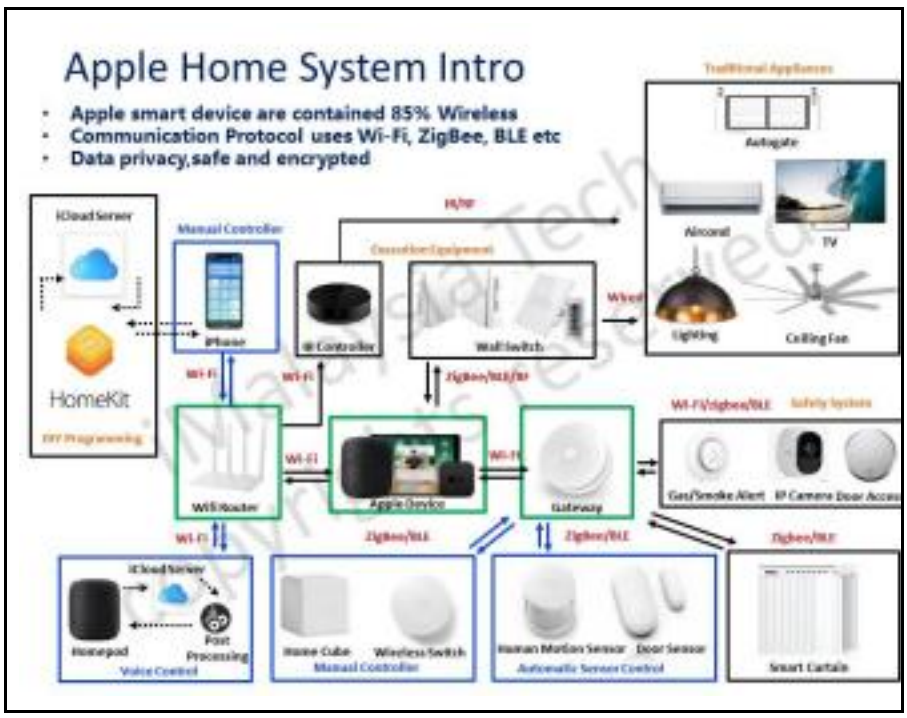

Рисунок 1.5 Система безпеки Apple Home Kit

3) Сегментація ринку: Ринок безпеки розумного будинку можна розділити на сегменти за типом продуктів (сенсори, камери, системи контролю доступу тощо), за рівнем цін (економ, преміум), за каналами дистрибуції (роздріб, онлайн продажі), за типами будівель ринок поділяється на житлові (особняки, квартири, багатоквартирні будинки) та комерційни (офіси, готелі, магазини, ресторани) та за географічними регіонами (Північна Америка, Європа, Азія-Тихоокеанський регіон, Латинська Америка, Близький Схід та Африка)

4) Конкурентне середовище: Ринок систем безпеки розумного будинку є досить конкурентним, з численними гравцями, що пропонують різні рішення. Деякі компанії фокусуються на інноваційних технологіях та передових можливостях, тоді як інші пропонують доступні рішення для широкого спектра користувачів. Основні конкурентні фактори включають інноваційність, якість продуктів, ціну та доступність.

Розвиток ринку інформаційних систем безпеки інтелектуальних будинків є важливою тенденцією в галузі домашньої автоматизації і розумного будинку. Завдяки зростаючій популярності інтелектуальних будинків та зростаючій увазі до безпеки даних, ринок інформаційних систем безпеки в цьому секторі прогнозується рости швидко в найближчі роки.

Однією з головних тенденцій розвитку ринку інформаційних систем безпеки інтелектуальних будинків є зростаюча популярність технологій штучного інтелекту та машинного навчання. Ці технології дозволяють системам безпеки будинку бути більш інтелектуальними та адаптивними, забезпечуючи більш точне та ефективне виявлення порушень безпеки. Наприклад, системи безпеки з машинним навчанням можуть відрізняти поведінку мешканців будинку від поведінки зловмисників, тим самим зменшуючи кількість хибних спрацювань.

Іншою важливою тенденцією розвитку є збільшення кількості підключених

до мережі пристроїв у будинку, що потребують захисту. Це може включати пристрої розумного освітлення, камери спостереження, системи опалення та кондиціонування повітря, аудіо та відео системи, а також будь-які інші електронні пристрої. Однак, збільшення кількості підключених пристроїв також може збільшити загрози для безпеки мережі, тому системи безпеки повинні бути здатні захистити всі пристрої від зловмисників.

Крім того, зростаюча кількість хмарних технологій та збільшення використання IoT також відіграють важливу роль у розвитку ринку інформаційних систем безпеки інтелектуальних будинків. Хмарні технології дозволяють зберігати дані та виконувати аналітику даних в режимі реального часу, що допомагає покращити ефективність систем безпеки будинку. Використання IoT пристроїв також може забезпечити більш точне виявлення порушень безпеки та забезпечити швидку реакцію на них.

Однак, зростаюча кількість підключених пристроїв і застосування хмарних технологій також можуть відкрити додаткові ризики для безпеки даних. Тому розробники інформаційних систем безпеки повинні забезпечити надійний захист даних та зменшити ризики злому систем безпеки.

У майбутньому розвиток ринку інформаційних систем безпеки інтелектуальних будинків буде спрямований на покращення ефективності, точності та надійності систем безпеки. Розробники систем безпеки будинку також будуть працювати над зменшенням ризиків та забезпеченням захисту даних. Будь-який прогрес в цих напрямках допоможе забезпечити більш

безпечну та комфортну роботу інформаційних систем безпеки в інтелектуальних будинках.

На основі аналізу ринку, я зміг визначити ряд можливих рішень інформаційної системи безпеки розумного будинку, які відповідають потребам різних сегментів ринку та актуальним тенденціям.

Бездротові системи безпеки відрізняються легкістю установки та налаштування, а також гнучкістю та можливістю розширення. Проте вони можуть страждати від затримки сигналу або втрати з'єднання, а також мають потенційну вразливість до електронного втручання або злому.

Інтелектуальні камери відеоспостереження використовують передові технології обробки зображення та алгоритми машинного навчання для автоматичного виявлення подій та сповіщення. Ці камери можуть інтегруватися з іншими системами безпеки та інтелектуального будинку, але мають вищу вартість у порівнянні з традиційними камерами та залежать від постійного підключення до Інтернету.

Біометричні системи контролю доступу використовують унікальні фізичні характеристики людей, такі як відбитки пальців, риси обличчя або радужки ока, для ідентифікації осіб та надання доступу до інтелектуального будинку. Ці системи мають високу точність та надійність ідентифікації, але можуть бути дорогими та складними у встановлені та обслуговуванні. Також біометричні системи можуть мати потенційні проблеми з конфіденційністю та захистом особистих даних, а також можуть помилятися при ідентифікації користувачів.

Інтегровані системи безпеки поєднують різні види технологій та пристроїв, таких як відеоспостереження, контроль доступу, датчики руху, системи пожежної безпеки та інше. Ці системи можуть пропонувати комплексний підхід до захисту інтелектуального будинку, проте можуть бути відносно складними та дорогими у реалізації та обслуговуванні.

Інтернет речей (IoT) також відіграє важливу роль у сфері безпеки інтелектуальних будинків. Це дозволяє підключати різні пристрої та системи, такі як освітлення, опалення, камери безпеки та датчики руху, до однієї мережі,

що спрощує керування та моніторинг. Використання IoT дозволяє користувачам контролювати та налаштовувати системи безпеки за допомогою мобільних

пристроїв, а також отримувати сповіщення про події у режимі реального часу. Однак IoT може мати проблеми з безпекою, якщо пристрої не належним чином захищені від хакерів та вірусів.

Один з недавніх трендів у сфері безпеки інтелектуальних будинків - використання блокчейн-технологій для забезпечення надійності та прозорості даних. Блокчейн може застосовуватися для створення децентралізованої мережі датчиків та пристроїв, що забезпечує захист від хакерів та злому. Однак ця технологія все ще знаходиться у стадії розвитку та може бути складною та дорогою у впровадженні.

Існує багато готових рішень, які можуть входити до складу системи розумного будинку та допомагати у забезпеченні контролю та безпеки. Деякі з найпоширеніших прикладів таких рішень:

1) Модульна системи безпеки: Основним напрямком є створення модульної системи безпеки, яка дозволить користувачам налаштовувати та масштабувати рішення відповідно до своїх потреб та бюджету. Це може включати різні види сенсорів, камер та систем контролю доступу, які можуть легко інтегруватися та співпрацювати між собою.

2) Використання штучного інтелекту та машинного навчання: Застосування алгоритмів штучного інтелекту та машинного навчання для аналізу даних, збирання інформації про навколишнє середовище та передбачення потенційних загроз безпеки. Це може підвищити ефективність системи та забезпечити швидке виявлення та відгук на події, пов'язані з безпекою.

3) Енергоефективні рішення: Розробка енергоефективних технологій для систем безпеки розумного будинку, таких як сенсори з низьким споживанням енергії та оптимізація алгоритмів для зменшення енерговитрат.

4) Кібербезпека та захист даних: Враховуючи актуальні питання кібербезпеки та захисту даних, розробляти систему безпеки розумного будинку та забезпечити використання сучасних методів шифрування, аутентифікації та

авторизації для захисту даних користувачів та запобігання несанкціонованому доступу.

5) Системи дистанційного керування - ці пристрої дозволяють власникам будинку керувати освітленням, опаленням, кондиціонером та іншими пристроями в будинку з допомогою смартфона або планшета.

6) Системи "розумних" вікон та дверей - ці пристрої можуть відкриватися та закриватися автоматично з допомогою датчиків руху, датчиків освітлення або інших параметрів.

Рисунок. 1.6 Приклад системи безпеки розумного будинку

Ці приклади є лише частковим переліком можливих рішень, які можуть бути використані в системі розумного будинку. Розвиток технологій швидко збільшує кількість доступних пристроїв, які можуть бути включені до системи Важливо пам'ятати, що система розумного будинку повинна бути гнучкою та можливою до розширення, оскільки вимоги та потреби користувачів можуть змінюватися з часом.

У підсумку, на ринку інформаційних систем безпеки інтелектуальних будинків існує широкий вибір технічних рішень, кожне з яких має свої переваги та недоліки. При виборі найкращого рішення для конкретного будинку, важливо враховувати фактори, такі як розмір та структура будівлі, індивідуальні потреби та бажання власників, доступність ресурсів та бюджет, а також пріоритети з

точки зору безпеки та приватності. Важливо провести ретельний аналіз та порівняти різні рішення, щоб знайти найбільш ефективний та оптимальний варіант.

На даний момент, немає універсального рішення, яке відповідало би всім вимогам та обставинам. Однак постійний розвиток технологій та зростання конкуренції на ринку сприяють створенню все більш інноваційних та доступних рішень. Важливо стежити за новими трендами та розвитком технологій, щоб бути в курсі найсвіжіших можливостей та підходів до захисту інтелектуальних будинків.

У рамках моєї бакалаврської роботи з розробки інформаційної системи безпеки для інтелектуального будинку, з метою знайти найбільш оптимальні варіанти для використання, провівши дослідження рішень провідних виробників та їх пропозицій, я вирішив розглянути також "домашній" або дешевий варіант системи безпеки, що має свої переваги.

Домашній варіант системи безпеки може включати використання відкритих або безкоштовних платформ, таких як Home Assistant або OpenHAB. Ці платформи дозволяють користувачам створювати власні налаштування та інтеграції з різними пристроями, використовуючи різні технології, такі як Wi-Fi, Zigbee, Z-Wave та інші. Вони також надають можливість створювати автоматизації та сценарії для розумного будинку, забезпечуючи безпеку та комфорт для мешканців.

Основними перевагами домашнього варіанту системи безпеки є низька вартість, висока гнучкість та можливість адаптації до індивідуальних потреб користувача. Це також дозволяє мені, як студенту, досліджувати різні технології та методи в рамках моєї бакалаврської роботи, розвиваючи свої навички та розуміння сучасних тенденцій у галузі розумних будинків та інформаційної безпеки.

Враховуючи результати аналізу ринку, я планую розробити інформаційну систему безпеки для інтелектуального будинку, яка буде базуватися на комбінації

провідних рішень з програмного забезпечення та домашнього

варіанту з обладнання. Це дозволить створити ефективну та доступну систему безпеки, яка відповідатиме потребам мешканців розумного будинку та забезпечить високий рівень захисту. Однак, необхідно також врахувати можливі обмеження домашнього варіанту, такі як менша надійність та складність налаштування та підтримки.

2 ТЕХНОЛОГІЧНА ЧАСТИНА. ПРОЕКТУВАННЯ ТА РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ БЕЗПЕКИ

2.1 Визначення вимог до інформаційної системи безпеки

Для розробки інформаційної системи безпеки розумного будинку, необхідно врахувати ряд вимог, які забезпечать захист системи та зручність її використання. Основні вимоги до розробки такої системи можна поділити на кілька категорій: функціональні, технічні, безпеки, ергономічні та регулятивні.

Щодо функціональності, система має забезпечувати моніторинг різних параметрів безпеки. Вона повинна інтегруватися з різними пристроями та системами розумного будинку, надсилати користувачам повідомлення про потенційні загрози або аварійні ситуації, а також дозволяти віддалене керування через мобільний додаток або веб-інтерфейс.

Система повинна забезпечувати можливість контролю доступу до будинку,

використовуючи різні методи аутентифікації, такі як паролі, картки доступу або RFID-зчитувачи. Також необхідно мати можливість моніторингу входів і виходів з будинку, а також відстежувати та реєструвати всі події, що відбуваються зі системою контролю доступу.

Для моніторингу та контролю руху в будинку система повинна забезпечувати можливість встановлення камер відеоспостереження або сенсорів руху. Також важливо мати можливість відстежувати та реєструвати всі події, що відбуваються з системою моніторингу та контролю руху.

Система повинна мати можливість сигналізувати про можливу небезпеку, таку як вторгнення в будинок. Також необхідно мати можливість автоматичного управління, наприклад, управління температурою в будинку або вимикання електроприладів. Важливо відстежувати та реєструвати всі події, що відбуваються зі системою сигналізації та автоматичного управління.

Окремим пунктом є управління енергоспоживанням. Для цього необхідно мати можливість автоматичного управління електричними пристроями та освітленням в будинку, яке буде залежати від потреби та встановленої програми.

Це дозволить не тільки економити електроенергію, але й створювати більш комфортні умови для мешканців будинку.

Враховуючи технічні характеристики, система безпеки має бути надійною та стабільною, швидко реагувати на події, бути сумісною з іншими пристроями. Протокол TLS/SSL використовується для забезпечення безпеки при передачі даних по мережі Інтернет. Він шифрує дані, що передаються між користувачем та сервером, тим самим запобігаючи несанкціонованому доступу. Протокол WPA3 використовується для захисту бездротових мереж Wi-Fi в розумному будинку. Він забезпечує підтримку шифрування з використанням більш сильних алгоритмів, що зменшує ризик порушення безпеки. Стандарт безпеки Open Web Application Security Project (OWASP) зосереджується на захисті веб-додатків від

атак. OWASP надає список найпоширеніших вразливостей та методів їх запобігання.

Стандарт ISO/IEC 27001 визначає вимоги до систем управління інформаційною безпекою та надає рамки для її ефективного управління. Іншим прикладом є стандарт NIST (National Institute of Standards and Technology), який надає рамки та рекомендації для керування кібербезпекою, включаючи рекомендації з розробки програмного забезпечення та захисту від зломів та вірусів.

Система повинна бути здатна працювати на різних масштабах - від невеликих квартир до великих будинків з кількома поверхами. При цьому необхідно забезпечити стабільну роботу системи незалежно від розміру будинку.

Також важливо, щоб система була стійкою до збоїв та атак з боку зловмисників. Для цього необхідно забезпечити ефективний захист системи від вірусів, шкідливих програм та зловмисних атак.

Крім того, система повинна мати простий та зрозумілий інтерфейс для користувачів, що дозволить легко керувати різними системами в будинку. Для цього важливо, щоб система мала можливість дистанційного керування з допомогою мобільних додатків або інтернет-порталів.

Безпека системи є критично важливою: від несанкціонованого доступу до захисту даних на фізичному та кібернетичному рівні. Шифрування даних, передачі та зберігання, регулярні оновлення програмного забезпечення та виявлення потенційних уразливостей, а також резервне копіювання та відновлення даних у разі аварії – це основні питання безпеки, які слід враховувати.

Основні вимоги безпеки, які повинні бути враховані при створенні системи безпеки розумного будинку, включають:

1) Захист від зламу та несанкціонованого доступу. Для цього можна використовувати сильні паролі, аутентифікацію двох факторів та захищені мережі

інтернету, а також уникати можливості виконання несанкціонованих команд.

2) Захист від кібератак. Розумний будинок може бути вразливим для кібератак, які можуть спричинити втрату контролю над будинком, його системами безпеки та особистою інформацією власників. Для уникнення цих ситуацій розробники мають застосовувати заходи безпеки, такі як криптографія, захист мережі та захист від вразливостей.

3) Захист персональної інформації. Розумний будинок містить велику кількість персональної інформації про власників та їхню діяльність. Розробники мають забезпечити безпеку цих даних та їхню конфіденційність шляхом шифрування та захисту від несанкціонованого доступу.

4) Захист від фізичного доступу. Для забезпечення безпеки системи безпеки розумного будинку необхідно встановити міцний фізичний захист та контроль доступу до компонентів системи.

5) Захист від вірусів та шкідливих програм. Для цього можна використовувати антивірусне програмне забезпечення та застосовувати регулярні оновлення системи та програмного забезпечення

Ергономічні вимоги полягають у забезпеченні зручності використання системи безпеки, читабельності інтерфейсу, безпеці та захисті, компактності та зручності розміщення компонентів системи та можливостях мультимедіа.

Зручність використання системи безпеки полягає в легкості управління та мінімальній кількості кроків для виконання необхідних дій. Інтерфейс користувача повинен бути чітким, зрозумілим та легко читабельним. Безпека та захист даних користувачів є однією з найважливіших вимог. Компоненти системи безпеки повинні бути компактними та зручно розміщуватись у будинку. Система безпеки повинна мати можливості мультимедіа для зручності користувачів.

Компактність та зручність розміщення компонентів системи безпеки дозволять забезпечити оптимальну роботу системи та легкий доступ до її

компонентів у разі необхідності. Розробники повинні враховувати необхідність розміщення компонентів системи безпеки в просторі та забезпечення їхньої безпеки. Наприклад, датчики руху повинні бути розміщені в таких місцях, щоб забезпечити максимальну ефективність їхньої роботи, але в той же час не бути зрушеними або пошкодженими у разі переміщення меблів чи інших предметів у приміщенні.

Щоб забезпечити мультимедійні можливості системи безпеки, розробники можуть використовувати функції аудіо- та відеозапису, щоб забезпечити більш детальний контроль над безпекою в будинку. Наприклад, за допомогою відеозапису можна відслідковувати рухи в будинку та контролювати доступ до різних зон, а звукові сигнали можуть повідомляти користувачів про можливі небезпечні ситуації.

Крім того, розробники повинні враховувати різноманітність потенційних користувачів системи безпеки та забезпечувати їхню взаємодію з системою у різних форматах. Наприклад, для людей з поганим зором або слухом можуть бути розроблені спеціальні інтерфейси, які забезпечать їм рівний доступ до всіх функцій системи безпеки.

Щодо регулятивних вимог, то вони зазвичай встановлюються державними органами та міжнародними стандартними організаціями з метою забезпечення безпеки, якості та ефективності системи.

Одна з основних галузей регулятивних вимог стосується безпеки даних користувачів. Вимоги до безпеки можуть встановлювати вимоги до захисту особистих даних користувачів від несанкціонованого доступу, включаючи захист від хакерських атак та інших потенційних загроз. Законодавство про захист даних, таке як загальний регламент про захист даних в Європейському Союзі (GDPR) та Закон про захист особистих даних у США (CCPA), надають розробникам системи безпеки важливу інформацію щодо вимог до захисту даних та обов'язків з

повідомлення про порушення безпеки даних.

Стандарти якості, такі як ISO 9001, можуть бути вимогами до системи управління якістю розробки та впровадження системи безпеки. Ці стандарти забезпечують високу якість процесів та систем керування якістю, а також до захисту інформації та над управлінням ризиками, що можуть виникнути в процесі розробки та експлуатації системи безпеки.

Інша важлива галузь регулятивних вимог стосується екологічної ефективності системи. З метою зменшення споживання енергії та зниження екологічного впливу системи можуть бути встановлені вимоги до споживання електроенергії та до використання екологічно чистих матеріалів та технологій.

Крім того, регулятивні вимоги можуть стосуватись інтероперабельності системи з іншими системами та обміну даними між ними. Вимоги до стандартів та протоколів обміну даними допомагають забезпечити сумісність та інтеграцію системи з іншими пристроями та системами.

Узагальнюючи, як розробник інформаційної системи безпеки інтелектуального будинку у цій бакалаврській роботі, я маю дотримуватись усіх зазначених вимог для забезпечення зручності та комфорту користування системою, а також забезпечити захист приватної сфери та безпеки користувачів.

2.2 Вибір протоколу з’єднання, обладнання та програмного забезпечення

Розробка інформаційної системи безпеки для розумного будинку потребує вибору протоколу з’єднання, завядки якому пристрої зможуть передавати та

обробляти дані між собою, правильного обладнання та програмного забезпечення, які забезпечать безпеку та надійність системи.

При виборі протоколу з'єднання для розробки інформаційної системи безпеки інтелектуального будинку, варто враховувати такі фактори, як доступність на ринку, функціональність та можливості пристроїв, бюджет та інші особисті

потреби та переваги. Найбільш популярними для вибору є Wi-Fi, ZigBee, Z-Wave та Bluetooth. Розглянемо детальніше кожен з варіантів протоколів з'єднання та їхні переваги та недоліки.

Wi-Fi - це один з найбільш поширених та зручних протоколів з'єднання для інтелектуального будинку. Він дозволяє підключати пристрої до будь-якої мережі Wi-Fi, що робить його дуже зручним у використанні. Крім того, він забезпечує швидкий та стабільний зв'язок з пристроями, а також високий рівень безпеки.

Проте, Wi-Fi має деякі недоліки. Він може вимагати більше енергії, ніж деякі інші протоколи, що може призвести до скорочення терміну служби батареї пристроїв. Крім того, він може бути досить дорогим у використанні, якщо вам потрібно підключити багато пристроїв.

Zigbee - це протокол мережі, який використовується для з'єднання різних розумних пристроїв, таких як лампи, датчики руху та термостати. Його основна перевага полягає в тому, що він забезпечує низький рівень споживання енергії, що дозволяє пристроям працювати довший час на одній батареї. Крім того, він має широку підтримку різних типів пристроїв. Із недоліків можна зазначити, що він може бути дещо складним у використанні та налаштуванні, оскільки він вимагає спеціальних шлюзів, щоб працювати з мережами Wi-Fi та іншими типами протоколів. Крім того, не всі пристрої підтримують Zigbee, що може обмежити ваш вибір.

Z-Wave - це ще один протокол мережі, який використовується для з'єднання різних пристроїв у інтелектуальному будинку. Він забезпечує дуже надійне та стабільне з'єднання, а також має широку підтримку пристроїв.

Головний недолік протоколу – вартість обладнання, який на ньому базується, а також ще більш вужчу підтримку пристроїв, що може ускладнити процес подальшого вибору обладнання.

Bluetooth - це протокол з'єднання, який використовується для з'єднання різних

пристроїв. Він забезпечує швидке та зручне з'єднання, а також має досить широку підтримку різних типів пристроїв. Він може бути зручним для підключення невеликих пристроїв, які потребують обмеженого діапазону дії.

Перевагою є простота використання та налаштування.

Однак із недоліків, він має дуже обмежений діапазон дії, до 10 метрів, що є критичним, якщо система безпеки розробляється у великих приміщеннях, багатоквартирних будинках і так далі. Також треба зазначити менш стійкий сигнал з’єднання, порівняно з іншими протоколами, який дуже чутливий до перешкод у вигляді стін, металевих предметів та інших електронних пристроїв, що може впливати на якість зв’язку.

Для розробки системи безпеки був обраний протокол з’єднання Wi-FI, оскільки він є самим найпоширенішим, є зручним у використанні, має невелику вартість пристроїв з його підтримкою та має широку підтримку різних пристроїв, що дозволяє мати більш широкий вибір обладнання для розробки системи безпеки інтелектуального будинку.

Для вибору обладнання, необхідно перевірити продавців та виробників на ринку, виконати дослідження їхньої репутації та огляди користувачів. Це допоможе зробити виважені рішення щодо вибору обладнання.

Після відбору можливих варіантів обладнання, варто провести їх детальну оцінку. Зокрема, важливо порівняти їх технічні характеристики, можливості масштабування, сумісність з існуючими системами компанії та рівень підтримки від виробника. Також варто проаналізувати відгуки користувачів та оцінки експертів для кращого розуміння якості та надійності обраного обладнання.

Камери відеоспостереження є одним із компонентів інформаційної системи безпеки інтелектуального будинку, оскільки вони дозволяють отримувати візуальну інформацію про дії в приміщенні. Приділену увагу слід надати

наступним характеристикам – роздільна здатність, кут огляду, функції як

основні, так і додаткові, та вартість.

До уваги були узяті наступні моделі:

1) 3MP E27 Bulb Camera Wi-Fi

Рисунок 2.1. Графічна репрезентація моделі камери E27 Bulb Camera 2) Lenovo 3MP PTZ WIFI IP Camera

Рисунок 2.2. Графічна репрезентація моделі камери Lenovo 3MP PTZ

3) Xiaomi Mijia IP Camera 2K 1296P

Рисунок 2.3. Графічна репрезентація моделі камери Xiaomi Mijia IP Camera
Нижче наведено порівняльну характеристику камер відеоспостереження, які я обрав, опираючись на торгівельний майданчик AliExpress:

Таблиця 2.1

Порівняльна характеристика камер відеоспостереження

Назва моделі	Роздільна здатність	Швидкість кадрів	Функції, додаткові характеристики	Кут огляду	Вартість
3MP E2 7 Bulb Camera Wi-Fi	2048x1536p	15 FPS	Захист від води IP66, кодек H.265, 360 градусів розвороту камери.	107 градусів	785 гривень

Lenovo 3MP PTZ WIFI IP Camera	2304x1296p	15 FPS	Захист від води IP66, кодек H.264, можливість нахилу на 90 градусів	95 градусів	650 гривень

Xiaomi Mijia IP Camera 2K 1296P	1920x1080p	15 FPS	Кодек H.264, 180 градусів розвороту, магнітне кріплення	125 градусів	800 гривень

За вимогами до системи безпеки мені більше за все підходить модель Lenovo 3MP PTZ WIFI IP Camera, вона має наступні переваги на відміну від інших моделей:

1) PTZ-функціонал: Lenovo 3MP PTZ WiFi має можливість обертання / нахилу (PTZ), що дозволяє контролювати положення камери та охоплювати більшу площу. Це дає більшу гнучкість при налаштуванні кута огляду та можливість відстежувати рух у режимі реального часу.

2) Висока роздільна здатність: Камера Lenovo 3MP PTZ WiFi має роздільну здатність 3 мегапікселі (що забезпечує чітке та деталізоване зображення), а сама роздільна дальність сягає 2304x1296 пікселів. Це може бути особливо корисно для розпізнавання об'єктів або осіб на знятих відеозаписах.

3) Wi-Fi підключення: Камера підтримує підключення до Wi-Fi, що дозволяє вам віддалено контролювати камеру за допомогою смартфона або іншого пристрою з підтримкою Wi-Fi. Ви можете переглядати живий стрім, записувати відео та отримувати сповіщення про події безпеки на відстані.

4) Додаткові функції безпеки: Камера Lenovo 3MP PTZ WiFi підтримує функції, такі як детектор руху, інфрачервона підсвічування для нічного бачення та двосторонній аудіо зв'язок. Це дозволяє ефективно виявляти рух, спостерігати вночі та взаємодіяти з людьми або тваринами в режимі реального часу.

5) Довірена марка: Lenovo відома своєю якістю та надійністю продуктів. Ви можете мати більшу впевненість в якості та підтримці, яку надає відомий виробник.

6) Вартість: дана модель має збалансовану вартість, та навіть пропонує більш розширений функціонал, хоча і має деякі технічні аспекти трішки гірші

ніж інші моделі, як наприклад, не дуже великий кут огляду, але це компенсується можливістю розвертати камеру на 360 градусів.

Наступним компонентом системи безпеки є система автентифікації до будинку, які також можна розмістити до певних зон, якщо на те є потреба. Я розглядаю методи і технології, які дозволяють ідентифікувати користувачів та контролювати доступ до різних пристроїв та функцій в будинку. Це важлива складова частина забезпечення безпеки та захисту оселі, а також може сприяти зручності та автоматизації різних процесів.

Існує безліч різних методів автентифікації, від класичних ключів і пін-кодів до біометричних технологій, таких як сканування відбитків пальців і розпізнавання обличчя. Кожен метод має свої переваги та обмеження, а вибір підходящої системи автентифікації залежить від вимог і бюджету.

Для домашнього варіанту, більш за все підходять системи доступу за допомогою RFID-брелків або з використанням ключових карток. Ці картки або

брелоки можуть бути простими у вигляді пластикових карток або невеликими пристроями. Розумна система будинку зчитує коди з цих карток або брелоків і відкриває доступ до певних зон або функцій в будинку. Також є варіант використовувати цифрові клавішні замки, де користувач буде автентифікуватись за PIN-кодом, але така система доступу потребує постійної ревізії, такі як постійна зміна коду автентифікації для уникнення можливостей зламу, а також може бути не надійною, якщо користувач забуде код доступу.

До уваги були взяті наступні моделі:

1) LUCKING DOOR SF2-MF-W

Рисунок 2.4 Графічна репрезентація моделі системи доступу LUCKING DOOR SF2-MF-W

2) ASIA TECO M203

Рисунок 2.5 Графічна репрезентація моделі системи доступу ASIA TECO M203

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

3) LUCKING DOOR K7612N

Рисунок 2.6 Графічна репрезентація моделі системи доступу LUCKING DOOR K7612N

Нижче наведена порівняльна характеристика цих моделей, які я обрав, опираючись на торгівельний майданчик AliExpress:

Таблиця 2.1

Порівняльна характеристика систем контролю доступу

Назва моделі	Сумісність	Водонепроникність	Способи доступу	Вбудована пам’ять	Ціна
LUCKING DOOR SF2-MFW	Wi-Fi	Так	Пароль, Картки, RFID брелок,	1000 користувачів	880 гривень

			відбитки		

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

			пальців		
ASIA TECO M203	Wi-Fi	Hi	Картки, пароль, RFID брелок	1000 користувачів	250 гривень
LUCKING DOOR K7612N	Wi-Fi	Hi	Картки, пароль, RFID брелок	1000 користувачів	675 гривень

Враховуючи усі дані з порівняння, кращим для мене вибором буде модель ASIA TECO M203, оскільки вона має наступні переваги:

1) Технологія RFID - ASIA TECO M203 використовує технологію RFID, яка є відносно дешевою, надійною і легкою в управлінні. Ця технологія також

забезпечує достатній рівень безпеки для більшості домашніх застосувань.

2) Сумісність – дана модель системи доступу підтримує протокол з'єднання Wi-Fi, що забезпечує інтегрованість у систему безпеки та її сумісність з іншими приладами.
3) Технічні характеристики – дана модель має аналогічні характеристики, як у набагато дорожчих моделей, і єдиним її недоліком є відсутність біометричної автентифікації за відбитком пальца, але все одно має можливість налаштувати одночасно автентифікацію як за паролем, так і за RFID-брелком.
4) Ціна – набагато вигідніша, ніж у конкурентів, і дає не гірший спектр функціоналу та забезпечення вимог до інформаційної системи безпеки інтелектуального будинку.

Маю зауважити, що із суттєвих недоліків можна відмітити лише відсутність стандарту водонепроникності, але якщо використовувати його у закритих приміщеннях або під дахом, цього можна уникнути.

Останнім компонентом моєї системи безпеки для інтелектуального будинку будуть датчики руху, вони грають важливу роль у виявленні незвичайної або підозрілої активності в будинку. Вони забезпечують постійний моніторинг руху в приміщенні і можуть виявляти потенційно небезпечні або небажані події, такі як злам, вторгнення або небажана присутність.

Датчики руху дозволяють розпізнавати зміни в оточуючому середовищі, такі як інфрачервоне, ультразвукове або мікрохвильове випромінювання, що відбувається при русі. Коли датчик руху реєструє ці зміни, він активується і може ініціювати тривогу або відправити сповіщення власнику будинку чи службі безпеки.

Крім виявлення руху, деякі датчики руху можуть розрізняти між рухом людей, тварин або інших об'єктів. Це дозволяє уникнути спрацьовування тривоги в разі

безпечного або несуттєвого руху, що сприяє зменшенню ложних тривог.

Датчики руху також можуть бути інтегровані з іншими системами в розумному будинку, такими як відеоспостереження, системи освітлення або автоматизації дверей. Це дозволяє спрощувати управління безпекою шляхом автоматичного активування відеозапису, освітлення або блокування доступу, залежно від виявленої активності.

Усі ці можливості датчиків руху допомагають забезпечити ефективний рівень безпеки у розумному будинку, зменшуючи ризик ідентифікації небажаних або небезпечних ситуацій, а також забезпечуючи швидку реакцію та вчасне сповіщення власникам або відповідним службам.

На основі вимог до розробки інформаційної системи безпеки, я обрав наступні моделі:

1) WiFi Tuya Smart PIR Motion Detector 808WT

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

Рисунок 2.7 Графічна репрезентація моделі 808WT

2) Tuya WiFi Light + PIR Motion Sensor FH-PIR400A

Рисунок 2.8 Графічна репрезентація моделі FH-PIR400A

3) ZSVIOT Tuya ZigBee/WiFi PIR Motion Sensor WKD-ZMS01

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

Рисунок 2.9 Графічна репрезентація моделі WKD-ZMS01

Нижче наведена порівняльна характеристика моделей, які я обрав, опираючись на торгівельний майданчик AliExpress:

Таблиця 2.3

Порівняльна характеристика датчиків руху

Назва моделі	Живлення	Інтерфейс	охоплення	Дальність виявлення	Вартість
808WT	Батарейки, USB	Wi-Fi	110 градусів	8-10 метрів	130 гривень
FH PIR400A	Батарейки, USB	Wi-Fi	120 градусів	6 метрів	156 гривень
WKD ZMS01	Батарейки	Zigbee, Wi-Fi	110 градусів	5 метрів	220 гривень

Враховуючи вимоги та дані з порівняння, мені більше за все підходить модель WiFi Tuya Smart PIR Motion Detector 808WT, оскільки вона має наступні переваги

над іншими моделями:

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

1) Живлення: працює високоефективно і має низьку споживання енергії. Він живиться від батареї, що забезпечує зручність встановлення без необхідності підключення до джерела живлення, але також може живитися від USB, який можна використовувати як резервний варіант живлення.

2) Дистанційне управління: Завдяки підключенню до мережі Wi-Fi, цей датчик може бути дистанційно керованим через мобільний додаток або інші пристрої, що підтримують зв'язок з мережею. Це дозволяє контролювати та налаштовувати датчик руху з будь-якого місця, де є доступ до Інтернету.

3) Сповіщення і тривоги: Датчик руху може надсилати сповіщення на мобільний телефон або інші пристрої при виявленні руху, дозволяючи оперативно реагувати на потенційну небезпеку або небажану активність в будинку

4) Інтелектуальні функції: Цей датчик руху має вбудовані інтелектуальні функції, такі як розпізнавання людей та ігнорування домашніх тварин, що дозволяє зменшити кількість ложних спрацювань тривоги

Ці переваги роблять модель датчику руху WiFi Tuya Smart PIR Motion Detector 808WT зручним і надійним вибором для розробки системи безпеки інтелектуального будинку.

Останньою вимогою для розробки інформаційної системи безпеки розумного будинку є вибір програмного забезпечення, яке забезпечить надійну і ефективну роботу всіх компонентів системи. Правильний вибір програмного забезпечення є критичним етапом моєї бакалаврської роботи, оскільки воно визначає функціональність, безпеку та зручність використання системи.

При виборі програмного забезпечення для інформаційної системи безпеки інтелектуального будинку слід враховувати декілька ключових факторів. По перше, програмне забезпечення повинно бути сумісним з апаратними компонентами системи, такими як датчики, камери, замки та інші пристрої.

Важливо переконатися, що обране програмне забезпечення може взаємодіяти з усіма потрібними пристроями, що забезпечує їхню взаємодію та функціонування.

					БКР. 122.016. ПЗ
Зм.	Арк.	№ докум.	Підп.	Дата	

По-друге, безпека є критичним аспектом для розумних будинків, тому програмне забезпечення повинно мати високий рівень захисту даних. Воно має включати механізми шифрування, аутентифікації та авторизації, щоб запобігти несанкціонованому доступу до системи. Також важливо, щоб програмне забезпечення мало постійні оновлення та патчі, які виправляють виявлені уразливості та забезпечують безпеку системи.

По-третє, зручність використання є важливим критерієм при виборі програмного забезпечення. Інтерфейс користувача повинен бути інтуїтивно зрозумілим і простим у використанні, щоб власники будинків могли легко керувати системою та налаштовувати її параметри за своїми потребами. Також важливо, щоб програмне забезпечення мало додаткові функції, такі як відстеження подій, сповіщення, збереження журналів та інші, які дозволяють користувачам отримувати повну інформацію про стан свого розумного будинку.

Зважаючи на це, на ринку є багато різних програмних забезпечень, які працюють або з вже готовими рішеннями від відомих брендів, такі як Google, Amazon, Xiaomi та інших, або які є з відкритим кодом, що дозволяють розробити повністю свою інформаційну систему безпеки інтелектуального будинку та налаштувати її під себе. Для цього, дослідивши різні варіанти такого програмного забезпечення, я зміг обрати для порівняння три програмних забезпечення: Home Assistant, OpenHAB та Hubitat.

Одним з найпопулярніших і надійних програмних забезпечень на ринку є Home Assistant. Home Assistant є відкритою платформою з великою спільнотою користувачів і розвитком, яка забезпечує інтеграцію та керування різними пристроями в розумному будинку, включаючи системи безпеки.

Основні переваги Home Assistant:

1) Відкрите програмне забезпечення: Home Assistant базується на відкритих стандартах і має велику спільноту розробників, що забезпечує широкі можливості розширення та підтримку різних пристроїв.

2) Широкий спектр інтеграцій: Home Assistant підтримує багато протоколів та пристроїв, таких як системи безпеки, камери спостереження, датчики руху,

датчики диму, замки, системи виявлення витоків і багато інших. Ви зможете підключити різні бренди та моделі пристроїв в одну систему.

3) Гнучкість та настроювання: Home Assistant дозволяє гнучко налаштовувати автоматизацію, розклади, сповіщення, створювати складні сценарії та правила для реагування на події в будинку. Ви зможете створити власні панелі керування та інтерфейс, що відповідають вашим потребам.

4) Безпека: Home Assistant надає важливі функції безпеки, включаючи шифрування комунікацій, авторизацію користувачів, перевірку доступу та можливість встановлення системи на локальному сервері для більшої контролю над даними.

5) Мобільний додаток: Home Assistant має мобільний додаток для iOS та Android, що дозволяє вам керувати розумним будинком з будь-якого місця.

Рисунок 2.10 Приклад інтерфейсу розгорнутої системи безпеки у програмному забезпеченні Home Assistant

OpenHAB також є відкритою платформою з багатими можливостями і інтеграціями, але його основна особливість полягає в легкості розширення та гнучкості.

Рисунок 2.11 Інтерфейс програмного забезпечення OpenHAB з прикладом налаштованої системи безпеки

Серед переваг програмного забезпечення OpenHAB можна зазначити наступне:

1) Широкий спектр інтеграцій: OpenHAB підтримує багато протоколів та пристроїв, включаючи Zigbee, Z-Wave, KNX, MQTT, Modbus, EnOcean та інші. Це означає, що ви можете підключати різні бренди та моделі пристроїв і управляти ними з одного інтерфейсу.

2) Гнучкість та розширюваність: OpenHAB надає гнучкі можливості

налаштування та розширення. Ви можете створювати правила та автоматизацію за допомогою вбудованої мови правил, або використовувати сценарії на основі JavaScript, Python або інших мов програмування. OpenHAB також підтримує розширення через додаткові модулі та розширення, що розширюють його можливості.

3) Візуалізація та керування: OpenHAB надає можливість створювати власні налаштовані панелі керування та інтерфейси користувача. Ви можете створювати

веб-сторінки, мобільні додатки або навіть інтегрувати OpenHAB зі смарт дисплеями або голосовими помічниками, такими як Amazon Alexa або Google Assistant.

4) Розподілена архітектура: OpenHAB працює на розподіленій архітектурі, що дозволяє розгортати його на різних пристроях та серверах. Ви можете встановити сервер OpenHAB на комп'ютері, Raspberry Pi або використовувати хмарні платформи. Це забезпечує більшу надійність та гнучкість управління вашим розумним будинком.

5) Активна спільнота: OpenHAB має велику та активну спільноту користувачів і розробників. Це означає, що ви можете отримати підтримку, консультації та допомогу вирішення проблем від експертів та інших користувачів.

Hubitat - це програмне забезпечення для розумного будинку, яке надає локальне керування та автоматизацію без необхідності в зовнішньому хмарному доступі. Основна ідея Hubitat полягає у збереженні усіх даних та обробці на локальному контролері, що забезпечує більшу приватність та незалежність від інтернет-з'єднання.

Рисунок 2.12. Інтерфейс програмного забезпечення Hubitat

1) Основними перевагами програмного забезпечення Hubitat є наступне: Локальне керування: Hubitat працює в локальній мережі, що означає, що весь

обмін даними та обробка відбуваються безпосередньо на вашому пристрої. Це забезпечує більшу надійність, швидкість реакції та збереження приватності. 2) Широкий спектр підтримки пристроїв: Hubitat підтримує багато різних протоколів та пристроїв, таких як Zigbee, Z-Wave, Wi-Fi та багато інших. Це означає, що ви можете підключати різні бренди та моделі пристроїв в одну систему.

3) Гнучкість та настроювання: Hubitat надає гнучкість у створенні правил та автоматизації. Ви можете налаштовувати різні сценарії та правила, використовуючи інтуїтивний інтерфейс. Це дозволяє вам створювати складні автоматизовані сценарії для розумного будинку.

4) Локальний веб-інтерфейс: Hubitat має власний локальний веб-інтерфейс, який дозволяє вам налаштовувати та керувати вашим розумним будинком. Ви можете створювати панелі керування, розклади, налаштування правил та багато іншого.

5) Резервне копіювання та відновлення: Hubitat надає можливість резервного копіювання та відновлення конфігурації. Це дозволяє вам зберігати свої налаштування та зручно відновлювати їх у разі необхідності.

6) Розширення та інтеграції: Hubitat підтримує розширення через власну платформу інтеграцій. Ви можете розширювати функціональність за допомогою додаткових драйверів, аплікейшенів та інтеграцій з сторонніми сервісами.

В моїй бакалаврській роботі я вирішив розробляти інформаційну систему безпеки за допомогою програмного забезпечення OpenHAB, на те є декілька причин, які виходять із порівняння цих програмним забезпечень між собою.

У порівнянні з Home Assistant, OpenHAB пропонує більш широкий спектр інтеграцій та дозволяє розробникам легше додавати нові компоненти. Він також відомий своєю гнучкістю та можливістю налаштовування правил і автоматизації. З іншого боку, Home Assistant має зручний інтерфейс та потужні функції безпеки та захисту даних. OpenHAB також має велику та активну спільноту користувачів і пропонує різні способи розширення та налаштування системи.

Порівнюючи OpenHAB з Hubitat, OpenHAB також виграє у більш широкому спектру підтримуваних протоколів та інтеграцій, що дає більшу гнучкість при виборі та підключенні пристроїв. У порівнянні з OpenHAB та Home Assistant, Hubitat може бути варіантом для тих, хто шукає локальне керування та приватність без необхідності в розширенні та гнучкості.

В моєму варіанті інформаційної системи безпеки все акцентується на роботі пристроїв між собою за допомогою бездротової мережі Wi-Fi на основі ПК серверу, тому OpenHAB для цього буде найкращим рішенням. **2.3 Процес реалізації системи**

Процес реалізації інформаційної системи безпеки інтелектуального будинку включає в себе декілька етапів, а саме:

1) Встановлення та налаштування обладнання системи безпеки у будинку. На

цьому етапі вибране обладнання (датчики руху, камери безпеки, смарт-замки тощо) встановлюється в розумному будинку і налаштовується для подальшої роботи. Це включає фізичне розміщення пристроїв, підключення до електромережі та мережі Wi-Fi, налаштування параметрів пристроїв.

2) Встановлення програмного забезпечення OpenHAB. На цьому етапі програмне забезпечення встановлюється на підходящий пристрій (ПК-сервер в будинку) і налаштовується для подальшої роботи.

3) Налаштування программного забезпечення OpenHAB з інтеграцією обладнання системи безпеки. Останнім етапом є інтеграція вже встановленого та налаштованого обладнання системи безпеки з OpenHAB. Це включає додавання пристроїв до OpenHAB, налаштування їх параметрів, створення правил для автоматизації та налаштування сценаріїв безпеки.

До моєї системи безпеки входять два датчика руху WiFi Tuya Smart PIR Motion Detector 808WT, три камери відеоспостереження Lenovo 3MP PTZ WIFI IP Camera та одна система доступу (замок) ASIA TECO M203

Важливою частиною розробки системи безпеки є правильне встановлення обладнання. Кожна із них має свої вимоги до встановлення та рекомендації, де вони можуть встановлені для досягнення їх максимальної ефективності у роботі.

Першими будут камери відеоспостереження – вони повинні бути розміщені на стратегічних місцях, зазвичай на входах до будинку та інших ключових зонах. Камери повинні бути спрямовані таким чином, щоб максимізувати поле зору та врахувати освітлення, щоб забезпечити якісні зображення навіть вночі. Після встановлення, камери повинні бути підключені до електромережі та мережі Wi Fi (якщо вони бездротові) або до мережі даних (якщо вони дротові). Датчики руху зазвичай встановлюються в коридорах, біля входів та в інших місцях, де є велика ймовірність проходження людей. Вони повинні бути встановлені на висоті, яка забезпечує найкращу детекцію руху. Після встановлення, датчики

руху повинні бути підключені до живлення (якщо вони не працюють від батарейок) і налаштовані для спілкування з центральною системою безпеки

RFID-замок встановлюється на вхідних дверях замість або разом з традиційним замком. Встановлення RFID-замка може вимагати деяких знань про столярні роботи та електрику, тому може знадобитися допомога професійного монтажника. Після встановлення, RFID-замок повинен бути налаштований для роботи з RFID-картами або брелоками, а також підключений до центральної системи безпеки для віддаленого керування та моніторингу.

Для встановлення програмного забезпечення OpenHAB на ПК-сервер на базі Windows, нам потрібно мати встановленим пакет мови програмування Java 11, який можна отримати на офіційному сайті виробника Oracle.

Інтерфейс встановленого програмного забезпечення OpenHAB виглядає наступним чином:

Рисунок 2.13. Інтерфейс налаштованого OpenHAB

Для підключення та налаштування обладнання в OpenHAB знадобиться працювати з біндінгами, які служать для сполучення зовнішніх пристроїв та сервісів з openHAB. Біндінги розробляються спільнотою OpenHAB та

покривають величезний спектр пристроїв та технологій. Ви можете встановити біндінги через веб-інтерфейс OpenHAB. Наприклад, для камери відеоспостереження вам може знадобитися IP Camera Binding, для датчиків руху – Motion Wi-Fi Binding тощо в залежності від технології пристрою.

Після встановлення біндінга можна додавати пристрої через розділ "Inbox" в Paper UI. Тут можна виявити та додати нові пристрої. Для кожного пристрою мені потрібно налаштувати різні параметри, такі як IP-адреса, порт, логін та пароль тощо, в залежності від пристрою.

Наступним потрібно створити “Items”. "Items" в OpenHAB це абстрактне представлення функцій об'єктів дому. Наприклад, у випадку камери відеоспостереження, "Item" може бути зображенням з камери або статусом камери. Ви можете створювати Items через файл конфігурації (в директорії conf/items/) або через Paper UI.

Інтерфейс для користувача для керування пристроями створюється через Sitemap, він створюється в директорії conf/sitemaps/

Для прикладу, я налаштую камери відеоспостереження, для цього потрібно спочатку створити файл Thing, в якому я визначу пристрій:

Рисунок 2.14 Код для визначення камери відеоспостереження у системі

Тепер я створюю файл Item, який буде використовувати зображення з камери:

Рисунок 2.15 Код для використання зображення з камери

Тепер я налаштую датчик руху, додаю його у веб-інтерфейсі як Thing, і після цього визначаю його як Item:

Рисунок 2.16 Код для визначення датчику руху

“wifi:device:bridge:node2:sensor_binary” - це ID мого Thing, який я додав через веб-інтерфейс.

Останнім я налаштовую систему доступу, також спочатку додаю його як Thing у веб-інтерфейсі OpenHAB, після цього визначаю Item для системи доступу:

Рисунок 2.17 Код для визначення системи доступу

“network:device:192_168_1_3:online” – це ID мого Thing для датчику руху, який я додав через веб-інтерфейс.

3 СПЕЦІАЛЬНА ЧАСТИНА.
ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ
БЕЗПЕКИ 3.1 Тестування та оцінка ефективності системи

Перед проведенням тестування інформаційної системи безпеки інтелектуального будинку, потрібно визначити вимоги, яких потрібно дотримуватись під час проведення тестування:

1) Наявність усього обладнання: Всі компоненти системи безпеки (включаючи камери відеоспостереження, датчики руху, RFID-замки тощо) повинні бути на місці та правильно встановлені.

2)Доступ до системи управління: Необхідно мати доступ до програмного забезпечення, через яке керуються всі пристрої, щоб перевірити їх роботу.
3)Доступ до інтернету: Деякі пристрої можуть вимагати підключення до інтернету для повноцінного тестування їх функціональності.

4) Наявність відповідних даних для перевірки: Наприклад, для перевірки RFID-замка вам потрібна RFID-карта або брелок.

5) Наявність часу та ресурсів: Тестування може зайняти певний час, особливо якщо система велика або складна. Ви також можливо знадобите додаткове обладнання для перевірки (наприклад, для вимірювання сили сигналу Wi-Fi).

6) Безпека тестування: Переконайтеся, що всі тести виконуються безпечно, без ризику пошкодження обладнання або без ризику для людей, що знаходяться в будинку.

Усе обладнання встановлене на своїх місцях та правильно встановлено, ніяких перешкод у їх роботі не виявлено.

План тестування усіх компонентів системи безпеки виглядає наступним чином: 1) Тестування камер відеоспостереження**:** мені потрібно перевірити зображення камери, якість зображення з кожної камери через систему управління, зробити тест реакції на рух, проходження перед камерою і перевірка, чи вона вірно реагує, а також провести тест нічного режиму: перевірити камери в темній кімнаті для тестування нічного режиму.

2) Тестування датчиків руху: мені потрібно провести тест детекції: прохід через зони детекції кожного датчика руху і перевірити, чи вони вірно спрацьовують. Також потрібно провести тест відповіді системи: перевірити, чи система вірно реагує на сигнали з датчиків руху.

3) Тестування RFID-замка: мені потрібно провести тест відкриття та закриття дверей: перевірити, чи замок вірно реагує на RFID-карту або брелок. Також мені потрібно провести тест віддаленого керування, чи можна віддалено керувати замком через систему управління.

4) Загальне тестування системи: перевірити, чи відображаються усі компоненти системи у програмному забезпеченні, перевірити налаштування відповідно до вимогам при розробці інформаційної системи безпеки інтелектуального будинку

Цей план тестування дає мені змогу систематично перевірити кожен компонент інформаційної системи безпеки і переконатися, що вони всі працюють вірно.

Спочатку я провів тести камер відеоспостереження, для цього через систему управління камерами в програмному забезпеченні я перевірив зображення на кожній камері, реакцію на рух, роботу нічного режиму.

За результатами тесту, всі камери відеоспостереження правильно показують зображення в реальному часі. Реакція на рух спрацьовує вірно. Нічний режим автоматично активується при низькому рівні освітлення, і зображення залишається чітким.

Наступним я провів тестування датчиків руху, для цього я проходив по зонам їх детекції та спостерігав за відповідною реакцією в системі управління програмного забезпечення OpenHAB.

За результатами тесту, всі датчики руху спрацьовували на рух в зоні детекції, та відправляли сповіщення до центральної системи безпеки.

Також я провів тестування роботи системи доступу до будинку, для цього я спробував відкрити двері за допомогою RFID-брелка, а потім за допомогою

пароля, а також перевірив, чи вдається віддалено керувати замком через систему управління у програмному забезпеченні.

За результатами тесту, система доступу вірно реагувала на роботу з RFID брелком та паролем, відкриваючи і закриваючи двері. Замок також відкривається та закривається віддалено через центральну систему безпеки.

Останнім я зробив загальне тестування системи безпеки, де потрібно було перевірити відображення усіх пристроїв у веб-інтерфейсі та чи налаштування відповідають вимогам безпеки.

За результатами тесту, Всі пристрої вірно відображаються в системі управління. Всі налаштування відповідають вимогам безпеки. На основі проведеного тестування, можна зробити висновок, що система безпеки розумного будинку працює відповідно до очікувань і вимог, зазначених у початковому проекті. Всі компоненти, включаючи камери відеоспостереження, датчики руху і системи доступу, успішно пройшли тестування та продемонстрували відмінну роботу в реальних умовах.

Таким чином, система безпеки розумного будинку відповідає поставленим вимогам, але існує потенціал для подальшого вдосконалення та адаптації системи до специфічних потреб користувача. З урахуванням цих результатів, можна рекомендувати впровадження цієї системи в реальному житловому будинку.

3.2 Аналіз результатів тестування

Аналіз результатів тестування роботи компонентів інформаційної системи безпеки інтелектуального будинку вказує на ефективність цих компонентів та їх взаємодії для забезпечення безпеки будинку. Нижче я привів основні результати тестування:

1) Охоплення тестування: Система камер відеоспостереження працює належним чином та забезпечують покриття всіх важливих зон в будинку. Вони здатні

реєструвати відео високої якості та зберігати його в безпечному місці. Датчики руху виявляють рухи відповідно до заданого режиму. Вони активують відповідні заходи безпеки, такі як сповіщення власнику будинку або активація аварійних сигналів. Також я перевірив, що система доступу RFID забезпечує контроль доступу до будинку. Вона використовує безпечні RFID-брелки для

ідентифікації користувачів, також має додаткову можливість входу за допомогою пароля.

2) Методи тестування: Динамічним методом я виконав тестування в реальних умовах, щоб перевірити реакцію системи на різні сценарії, включаючи спроби несанкціонованого доступу, спрацювання датчиків руху та запис відео з камер. Також я провів тестування на проникнення, де був здійснений сценарій спроби вторгнення в систему, щоб виявити можливі вразливості та перевірити їхню відповідність стандартам безпеки.

3) Результати тестування: Всі компоненти системи безпеки успішно виконали свої функції. Камери відеоспостереження забезпечували чітку інформацію про дії в будинку, датчики руху ефективно виявляли неправомірні рухи, а система доступу RFID контролювала доступ до будинку. Під час динамічного тестування система ефективно реагувала на виявлені події, такі як спрацювання датчиків руху або спроби несанкціонованого доступу. Під час тестування на проникнення не було виявлено серйозних вразливостей, які би здатні зламати систему безпеки.

4) Реагування на виявлені вразливості: Хоча серйозних вразливостей не виявлено, були рекомендовані деякі заходи для поліпшення системи безпеки, такі як оновлення програмного забезпечення камер відеоспостереження та системи доступу RFID для виправлення можливих слабких місць.

5) Загальна оцінка безпеки: За результатами тестування, система безпеки інтелектуального будинку з камерою відеоспостереження, датчиками руху та системою доступу RFID може бути визнана ефективною та забезпечувати достатній рівень безпеки для будинку.

6) Рекомендації: За результатами аналізу, важливо вказати на потребу регулярного оновлення програмного забезпечення всіх компонентів системи безпеки для забезпечення виправлення потенційних вразливостей, також потрібно проводити періодичні тестування безпеки для виявлення нових загроз та забезпечення постійного покращення системи безпеки, також треба забезпечувати фізичну безпеку компонентів системи, зокрема, захист від фізичного доступу до камер відеоспостереження та системи доступу RFID.

4 ОХОРОНА ПРАЦІ ТА НАВКОЛИШНЬОГО СЕРЕДОВИЩА 4.1 Охорона праці під час робіт з монтажу обладнання

Розумний будинок - це житло, обладнане спеціальними системами автоматизації та управління, що дозволяє забезпечити комфортне та безпечне життя. При налаштуванні обладнання для розумного будинку необхідно враховувати високу небезпечність цих робіт, проводити аналіз потенційних небезпек та ризиків та дотримуватись спеціальних правил та вимог з охорони праці: У цій бакалаврській роботі було розглянуто ряд методів та практик з охорони праці, які використовуються в процесі монтажу та налаштування, а саме:

1) Ризик ураження електричним струмом: робота з електрикою вимагає певних знань та вмінь, а неправильне виконання монтажу може призвести до ураження електричним струмом, що загрожує життю та здоров'ю людини.

2) Ризик пожежі внаслідок несправності електроприладів: неправильно виконаний монтаж може призвести до появи короткого замикання та пожежі, яка також може стати загрозою для життя та здоров'я людини.

3) Ризик нещасних випадків з використанням інших пристроїв: під час монтажу можуть використовуватись різні інструменти, тому важливо дотримуватись правил їх використання, щоб уникнути нещасних випадків

4) Забезпечення захисту особистих даних: при монтажі обладнання для

розумного будинку необхідно дотримуватись правил збереження та захисту особистих даних, щоб уникнути можливості їх витоку.

5) Знання принципів роботи обладнання: необхідно мати достатні знання про принципи роботи обладнання, щоб правильно виконати його монтаж та налаштування.

6) Проведення тестування: після монтажу та налаштування обладнання необхідно провести тестування для перевірки його правильної роботи та відповідності заданим параметрам.

Зважаючи на те, що монтаж та налаштування обладнання для розумного будинку може включати в себе ризики травм та пошкодження обладнання, необхідно вживати заходів для забезпечення безпеки праці під час виконання цих робіт.

Щоб забезпечити належну охорону праці, слід дотримуватись ряду правил техніки безпеки. Перед початком роботи необхідно ознайомитись з інструкціями по експлуатації та технічними характеристиками обладнання. Це допоможе уникнути пошкоджень обладнання, що може стати причиною аварій та нещасних випадків.

Задача охорони праці при монтажі обладнання для розумного будинку полягає у запобіганні потенційних небезпек і ризиків, що можуть виникнути під час виконання робіт. Для цього рекомендується враховувати наступні фактори та вимоги:

1) Перевірка безпеки пристроїв: Перед розпочаттям монтажу необхідно перевірити відповідність пристроїв вимогам безпеки, зазначеним в технічній документації виробника, а також дотримуватися вимог щодо установки, зазначених в інструкції з монтажу.

2) Захист від електричного струму: Необхідно захистити працівників від можливих уражень електричним струмом, наприклад, шляхом використання

ізоляційних матеріалів і заземлення. Також необхідно перевірити стан електромережі в будинку та дотримуватися відповідних вимог при з'єднанні нового обладнання з електромережею.

3) Запобігання падінням: Розміщення обладнання на висоті може створювати небезпеку падіння. Уникайте цього, розміщуючи обладнання на безпечній висоті, або використовуючи захисні пристрої, такі як ліси або стропи.

4) Захист від шуму та вібрацій: Працівники повинні мати можливість захистити свої вуха від шуму, який може виникнути під час монтажу обладнання, а також від вібрацій, що можуть стати причиною небажаних наслідків для здоров'я.

Під час монтажу та налаштування обладнання, слід дотримуватися правил електробезпеки. Особливу увагу необхідно приділити підключенню до джерела електропостачання та розміщенню електроджерел у безпечному відстані від води та інших рідин.

Необхідно забезпечити захист від пожежі шляхом встановлення димових, термічних та газових датчиків та відповідних систем аварійного відключення електропостачання.

Крім того, необхідно надавати співробітникам достатньо часу для відпочинку та відновлення сил. Завжди слід дотримуватись правил техніки безпеки, щоб уникнути травм та нещасних випадків на робочому місці.

Важливо мати необхідні знання та навички для роботи зі спеціалізованим обладнанням. Перед початком роботи необхідно переконатись, що весь інструмент належним чином підготовлений та перевірений на відповідність нормам безпеки

В разі виникнення будь-яких проблем з обладнанням, необхідно припинити роботу та звернутись до відповідальних осіб. Необхідно також забезпечити належне зберігання та транспортування обладнання, щоб уникнути пошкоджень

та аварій.

Під час роботи з монтажу обладнання, робочий простір має бути розміщений на безпечній відстані від джерел електричного струму та інших потенційно небезпечних матеріалів, таких як пальне та хімічні речовини. Для запобігання можливим нещасним випадкам, важливо забезпечити належну організацію робочого простору, позначення меж робочої зони та безпечних зон доступу.

У разі виявлення будь-яких неполадок у роботі обладнання під час монтажу, працівники повинні негайно повідомляти відповідних осіб та припинити роботу до усунення проблеми. Також необхідно проводити регулярний технічний огляд та планову профілактику обладнання, щоб запобігти можливим аваріям та нещасним випадкам на робочому місці.

У підсумку, охорона праці під час монтажу та налаштування обладнання для розумного будинку є критично важливою, оскільки ці процеси пов'язані з ризиком травм та нещасних випадків для працівників. Ретельне планування, оцінка ризиків, виконання необхідних заходів з охорони праці та надання належної підготовки працівникам з цієї теми є важливими кроками, які допоможуть уникнути таких ризиків. Дотримання правил безпеки та належна підготовка співробітників дозволять запобігти травмам та нещасним випадкам, збільшити продуктивність роботи та забезпечити безпеку обладнання.

4.2 Правила техніки безпеки з експлуатації електроприладів В контексті кваліфікаційної бакалаврської роботи актуальним є вивчення основних принципів та рекомендацій щодо охорони праці та техніки безпеки при експлуатації електрообладнання, що входить до складу систем безпеки інтелектуальних будинків. Це допоможе забезпечити безпечні умови для працівників, які займаються установкою та обслуговуванням розумних будинків, а також підвищити надійність роботи електроустановок.

Важливо дотримуватися вимог законодавства, нормативних документів,

інструкцій виробника та встановлених правил при експлуатації такого обладнання, а саме:

1) Спеціалізована підготовка персоналу. Регулярні курси та тренінги для працівників, які включають теоретичні та практичні заняття з основ охорони праці та техніки безпеки, а також періодичні перевірки знань з охорони праці та техніки безпеки, що можуть проводитися у формі тестування або індивідуальних співбесід з експертами.

2) Відповідність електрообладнання вимогам електробезпеки. Наявність захисних пристроїв, таких як автоматичні вимикачі, дифавтомати, що захищають від перевантажень, короткого замикання та змін в напругах, регулярний технічний огляд та профілактичне обслуговування, що допомагає виявити та усунути можливі порушення норм безпеки та продовжити термін служби обладнання.

3) Організація безпечного робочого місця. Надання комфортних та безпечних умов для працівників, забезпечення ергономічного оформлення робочого простору, відповідне освітлення на робочих місцях, використання природного або штучного освітлення для створення оптимальних умов праці, а також встановлення електрообладнання на безпечній відстані від робочих місць, що забезпечує зручний доступ до обладнання та відсутність електромагнітних впливів на здоров'я працівників.

4) Забезпечення доступу до засобів безпеки. Вогнегасники, аптечки першої допомоги та інші засоби безпеки розміщуються на видимих та легкодоступних місцях, а їх наявність та працездатність регулярно перевіряються, також розробляється план евакуації та проводяться навчання з евакуації персоналу у випадку надзвичайних ситуацій.

Персонал, який працює з електрообладнанням розумних будинків, має проходити спеціалізовану підготовку та періодично перевіряти свої знання з охорони праці та техніки безпеки. Електрообладнання, використовуване в

системах безпеки розумних будинків, повинно відповідати вимогам електробезпеки та містити захисні пристрої, такі як автоматичні вимикачі, дифавтомати та інші.

Організація робочого місця має забезпечувати комфортні та безпечні умови для працівників. Освітлення на робочих місцях має бути достатнім, а електрообладнання встановлене на безпечній відстані від робочих місць. Необхідно забезпечити доступ до вогнегасників, аптечок першої допомоги та інших засобів безпеки.

Працівники, які працюють з електрообладнанням, повинні користуватися особистими засобами захисту, такими як діелектричні рукавиці, взуття, захисні окуляри та інші. Потрібно регулярно проводити навчання та інструктажі з охорони праці та техніки безпеки для працівників, які працюють електрообладнанням, і забезпечте доступ до актуальної інформації про правила безпеки та методи роботи з електрообладнанням для усіх працівників. Також

потрібна організація системи контролю за дотриманням правил охорони праці та техніки безпеки на робочих місцях.

Також важливо регулярно проводити технічний огляд та профілактичне обслуговування електрообладнання з метою виявлення та усунення можливих порушень норм безпеки. Це допоможе забезпечити безпечні умови для працівників, які займаються установкою та обслуговуванням розумних будинків, а також підвищити надійність роботи електроустановок.

Відповідне навчання, дотримання правил безпеки, використання захисного обладнання та регулярний технічний огляд електрообладнання сприятимуть створенню безпечного робочого середовища при експлуатації електрообладнання в інформаційній системі безпеки розумного будинку.

Дотримання охорони праці та техніки безпеки при експлуатації електрообладнання під час розробки інформаційної системи безпеки

інтелектуальних будинків є важливим аспектом забезпечення безпечних умов праці, зниження ризику нещасних випадків та підвищення надійності роботи електроустановок. Звернення уваги на наведені вище деталі, включаючи підготовку персоналу, відповідність обладнання вимогам безпеки, організацію безпечного робочого місця, доступ до засобів безпеки, використання особистих засобів захисту та проведення регулярних навчань та інструктажів, допоможе забезпечити високий рівень безпеки для працівників, які працюють з електрообладнанням.

Також важливо постійно відстежувати зміни в законодавстві, нормативних документах та нові технологічні рішення, що можуть вплинути на підвищення рівня безпеки при експлуатації електрообладнання. Реалізація систематичного підходу до охорони праці та техніки безпеки допоможе не тільки запобігти нещасним випадкам та забезпечити безпечні умови праці, але і покращити продуктивність та ефективність роботи працівників.

Врахування принципів охорони праці та техніки безпеки при проектуванні та реалізації інформаційної системи безпеки розумного будинку є одним з

ключових факторів успішної реалізації проекту та забезпечення безпеки його користувачів.

4.3 Екологічні аспекти утилізації комп’ютерної техніки

Утилізація комп'ютерної техніки є одним з важливих аспектів охорони навколишнього середовища, оскільки комп'ютери та інша електроніка містять велику кількість шкідливих речовин, які можуть негативно вплинути на здоров'я людей та навколишнє середовище.

Одним з найбільш ефективних способів утилізації комп'ютерної техніки є переробка. В процесі переробки, компоненти комп'ютерів та іншої електроніки, такі як метали та пластик, можуть бути вилучені та повторно використані в інших пристроях, що зменшує потребу в нових ресурсах та зменшує кількість відходів.

Для того, щоб забезпечити ефективну утилізацію комп'ютерної техніки, можна використовувати спеціалізовані служби з переробки електронних відходів. Ці служби зазвичай приймають старі комп'ютери та іншу електроніку та переробляють їх, забезпечуючи безпечне та екологічне вилучення шкідливих речовин.

Крім того, можна відновлювати та переробляти окремі компоненти комп'ютерної техніки, такі як батареї та диски. Це зменшує кількість відходів, що потрапляють на смітники та зменшує негативний вплив на довкілля.

Нарешті, ще один важливий аспект утилізації комп'ютерної техніки полягає в повторному використанні. Наприклад, старі комп'ютери можна використовувати як резервні пристрої або передавати в організації та школи, які можуть використовувати їх для освітніх та інших цілей. Це зменшує кількість відходів та збільшує термін служби комп'ютерної техніки.

Під час утилізації комп'ютерної техніки важливо дотримуватися екологічних стандартів та правил. Наприклад, перед відправкою комп'ютера на переробку потрібно видалити всі конфіденційні дані, щоб уникнути їхнього неправомірного використання. Також важливо не викидати електронні відходи в звичайний смітник, оскільки це може призвести до забруднення довкілля.

Поміж інших важливих аспектів утилізації комп'ютерної техніки варто згадати про регулювання та законодавство в цій сфері. Багато країн встановлюють стандарти для екологічної утилізації електронних відходів, а також вимагають від виробників комп'ютерної техніки дотримуватися певних норм та стандартів у виробництві пристроїв.

Нарешті, важливо звернути увагу на освіту та підвищення обізнаності про утилізацію комп'ютерної техніки. Люди повинні розуміти, як правильно викидати та переробляти електронні відходи, а також як використовувати комп'ютерну техніку з мінімальним впливом на навколишнє середовище.

Отже, утилізація комп'ютерної техніки є складним та важливим процесом при розробці інформаційної системи безпеки, який включає в себе переробку, відновлення та повторне використання компонентів техніки, а також врахування екодизайну та встановлення норм та стандартів у цій сфері.

ЗАГАЛЬНИЙ ВИСНОВОК

Бакалаврська робота на тему "Інформаційна система безпеки інтелектуального будинку" є високоактуальним дослідженням, що досліджує важливий аспект сучасного життя - безпеку в інтелектуальних будинках. Ця робота детально описує інформаційну систему безпеки, яка дозволяє мешканцям ефективно контролювати та забезпечувати безпеку свого будинку за допомогою сучасних технологій.

У ході дослідження мною було проведено аналіз існуючих систем безпеки інтелектуальних будинків, вивчено їхні переваги та недоліки, а також визначено основні вимоги до інформаційної системи безпеки. На основі цього аналізу я розробив власну інформаційну систему безпеки, яка враховує специфіку інтелектуальних будинків та забезпечує надійний захист.

Завдяки цій роботі я зміг продемонструвати свої знання в галузі інформаційних систем та безпеки, а також здатність до систематичного аналізу, проектування та реалізації комплексних систем. Дослідження додало нові знання та інсайти в галузі безпеки інтелектуальних будинків і може послужити основою для подальших розвідок та практичних застосувань.

Загальний висновок полягає в тому, що інформаційна система безпеки інтелектуального будинку є необхідною компонентою сучасного життя, сприяючи підвищенню безпеки та комфорту мешканців. Це поле досліджень ще не повністю досліджене, тому результати цієї роботи вносять вагомий внесок у розвиток цієї галузі та можуть бути використані для подальшого розширення та вдосконалення систем безпеки інтелектуальних будинків.

ПЕРЕЛІК ПОСИЛАНЬ

1. Liu H. Handbook of Smart Homes, Health Care and Well-Being / H. Liu. – Springer, 2018. – 528 с.
2. Jalal A. A Home Automation Security System: An Android-Based Home Automation System / A. Jalal, S. Kamal, D. Kim // IEEE Transactions on Consumer Electronics. – 2015. – Т. 61, № 4. – С. 462-470.
3. Nof S.Y. Handbook of Automation / S.Y. Nof. – Springer, 2016. – 1816 с. 4. Jeyanthi N. A Comprehensive Study on Internet of Things / N. Jeyanthi, S. Natarajan // International Journal of Computer Science and Information Security. – 2019. – Т. 17, № 5. – С. 60-68.
5. Weber R.H. Internet of Things – Legal Perspectives / R.H. Weber. – Springer, 2010. – 141 с.
6. Solove D. J. Understanding Privacy / D. J. Solove. – Harvard University Press, 2013. – 314 с.
7. Kostyk T. Designing the Architecture of a Smart Home Security System / T. Kostyk, V. Yevsieiev // Electronics and Control Systems. – 2021. – № 1(65). – С. 94-101.
8. Roman R. Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges / R. Roman, J. Lopez, M. Mambo // Future Generation Computer Systems. – 2018. – Т. 78. – С. 680-698.
9. Alur D. Digital World: Connectivity, Identity, and Security in a Networked Society / D. Alur. – Apress, 2019. – 336 с.
10. Pacheco J. Internet of Things Security: Challenges and Research Opportunities / J. Pacheco, S. Hariri // Digital Threats: Research and Practice. – 2016. – Т. 1, № 1. – С. 1-9.
11. Vermesan O., Friess P. Internet of Things: Converging Technologies for Smart

Environments and Integrated Ecosystems / O. Vermesan, P. Friess. – River Publishers, 2013. – 364 c.