КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

До захисту допущено

В.о. завідувача кафедри ІСТ

_____ Олексій КОЛЕСНІКОВ

(підпис) (ім'я, ПРІЗВИЩЕ)

"___"_____2021р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

спеціальності 126 «Інформаційні системи та технології»

освітньої програми «Програмні технології інтернет речей» _____

на тему:_____

Виконав (-ла): студент (-ка) __4__ курсу, групи ІР-41

(шифр групи)

Владислав КЛІШ_____ _____

(Ім'я, ПРІЗВИЩЕ) (підпис)

Керівник к.т.н доцент Ростислав ЛІСНЕВСЬКИЙ _____

(посада, науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ) (підпис)

Консультант нормо контроль к.т.н доц. Ростислав ЛІСНЕВСЬКИЙ _____

(назва розділу) (посада, вчене звання, науковий ступінь, Ім'я, ПРІЗВИЩЕ) (підпис)

Рецензент _____ _____

(посада, науковий ступінь, вчене звання, науковий ступінь, Ім'я, ПРІЗВИЩЕ) (підпис)

Засвідчую, що у поянювальна записка немає запозичень з праць інших авторів без відповідних посилань.

Здобувач освіти _____

(підпис)

Київ – 2021 року

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет інформаційних технологій

Кафедра: Інформаційних систем та технологій

Освітньо-кваліфікаційний рівень: Бакалавр

Спеціальність: 126 – Інформаційних систем та технологій

Програма: Програмних технологій інтернет речей

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

Д.т.н., Колесніков О.Є.

_____

“____” _____2021 року

ЗАВДАННЯ

НА ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Студент: *Владислав КЛІШ*

Група: ІР-41

1. Тема кваліфікаційної роботи:

Система безпеки для приватної прибудинкової території підприємства ТОВ”Примавера компані”

Затверджена протоколом засідання кафедри ІСТ №16/20 від «09» листопада 2020 р.

Керівник проекту: *к.т.н доцент Ростислав ЛІСНЕВСЬКИЙ*

2. Строк подання студентом готової роботи – «24» червня 2021 р.

3. Цільова установка та вихідні дані до роботи:

Обрати рішення для забезпечення безпеки території підприємства. Розробити IoT систему для приватної прибудинкової території, що відповідає наступним вимогам:

- *врахувати виявлені недоліків у аналогічних систем і успішно їх нівелювати;*
- *IoT система має бути легко масштабована;*

До функціоналу проектованої системи можна віднести:

- *фіксація посторонніх осіб на території за рахунок розумних пристроїв;*
- *мобільний додаток та база даних, для управлінням та контрою системи;*
- *реалізація алгоритму захисту території.*

4. Зміст роботи:

- *постановка задачі та аналіз рішення;*
- *аналіз існуючих продуктів для забезпечення безппеки території;*
- *опис обраних технологій та розумних пристроїв;*
- *опис методу обробки та стиснення інформації;*
- *розробка проекту IoT системи в Packet Tracer;*
- *опис процесу розробки програмного інтерфейсу для перегляду бази даних;*
- *опис мобільного додатку для кервування системою;*

5. Перелік графічних матеріалів (слайдів):

- *актуальність розумних систем безпек;*
- *опис існуючих систем безпеки;*
- *підбір обладнання для системи;*
- *створення 3D-моделі підприємства та розміщення пристроїв;*
- *алгоритм роботи та структурна схема системи оптимізації;*
- *мобільний додаток для керування.*

6. Календарний план виконання роботи:

№ з/п	**Етапи виконання кваліфікаційної роботи бакалавра**	**Термін виконання**	**Термін виконання**

1	Вибір тематики кваліфікаційної роботи бакалавра	до 01.12.2020	**Виконано**
2	Наказ про затвердження тем кваліфікаційної роботи бакалавра та призначення керівників	01.12.2020	**Виконано**
3	Розробка плану кваліфікаційної роботи бакалавра і його погодження з керівником	25.12.2020	**Виконано**
4	Написання І розділу кваліфікаційної роботи	20.01.2021	**Виконано**
5	Написання ІІ розділу кваліфікаційної роботи	19.02.2021	**Виконано**
6	Написання ІІІ розділу кваліфікаційної роботи	05.03.2021	**Виконано**
7	Підготовка висновків і пропозицій	05.04.2021	**Виконано**
8	Попередній захист кваліфікаційної роботи	20.04.2021	**Виконано**
9	Перевірка на плагіат	до 15.06.2021	**Виконано**
10	Нормоконтроль	до 17.06.21	**Виконано**
11	Рецензування кваліфікаційної роботи бакалавра і представлення роботи на кафедру в друкованому вигляді	до 21.06.2021	**Виконано**
12	Захист кваліфікаційної роботи бакалавра	24.06.2021	

Дата видачі завдання «10» листопада 2021 р.

Керівник роботи*: к.т.н. доцент кафедри інформаційних систем та технологій Ростислав ЛІСНЕВСЬКИЙ*

_____

(підпис)

Завдання прийняв до виконання:

студент групи Владислав КЛІШ

_____

(підпис)

АТОНАЦІЯ

Кваліфікаційна робота бакалавра на тему: «Система безпеки для приватної прибудинкової території підприємства ТОВ "Примавера компані"» складається зі вступу, де описано тему, актуальність, методи дослідження, об’єкти дослідження та завдання, робота містить в собі 3 розділи : аналіз систем та технологій, опис та проектування, створення та опис.

У першому розділі теоретичної частини було проаналізовано велику кількість інформаційних джерел для вирішення поставленого завдання, також було описано комунікаційні технології та системи. Далі було поставлено основне завдання та проаналізовано системи безпеки.

У другому розділі відбувається проектування контекстної логічної та фізичної моделі бази даних, використовуючи різне програмне забезпечення, також було створено 3D-модель підприємства та інтегровано в програму Packet Tracer. Також відбулось розміщення пристроїв на території та опис обраних розумних пристроїв та технологій.

У третьому розділі йде опис програмної реалізації, опису алгоритмів роботи та створення сценаріїв роботи системи, створено мобільний додаток для керування системою та перегляд підприємство.

Робота складається з 75 сторінок, містить в собі 41 рисунок. При написанні роботи було використано 50 інформаційних джерел.

Ключові слова: База даних, безпека, розумна безпека, Логічна модель, Фізична модель, Packet Tracer, розумна безпека території, IoT, Zigbee, мобільний додаток, розумний пристрій, камера відеоспостереження, датчик руху датчик периметра

SUMMARY

Thesis on the topic: "Security system for the private area of the company LLC" Primavera Company "" consists of an introduction, which describes the topic, relevance, research methods, research objects and tasks, the work contains 3 sections: analysis of systems and technologies, description and design, creation and description.

The first section of the theoretical part analyzed a large number of information sources to solve the problem, as well as described communication technologies and systems. Next, the main task was set and security systems were analyzed.

The second section designs the contextual logical and physical model of the database using various software, also created a 3D model of the enterprise and integrated into the program Packet Tracer. There was also a placement of devices on the territory and a description of selected booster devices and technologies.

The third section describes the software implementation, describes the algorithms and scenarios of the system, created a mobile application for system management and enterprise viewing.

The work consists of 75 pages, contains 41 drawings. 50 information sources were used in writing the work.

Keywords: Database, Security, Smart Security, Logical Model, Physical Model, Packet Tracer, Smart Territory Security, IoT, Zigbee, Mobile App, Smart Device, CCTV Camera, Motion Sensor Perimeter Sensor

ЗМІСТ

ВСТУП

Мета і завдання дослідження. Основною метою цієї кваліфікаційної роботи бакалавра є дослідження IoT систем безпеки та порівняння різних компаній та характеристик датчиків відеоспостереження, руху, датчиків периметру, аналіз об’єкту розробки та пошук оптимального рішення для забезпечення IoT безпеки на основі різних досліджень, розробка та проектування системи.

Основні завдання, що потрібно виконати для досягнення мети:

1. Аналіз базових принципів роботи IoT систем.
2. Аналіз технологічних стадій розробки систем.
3. Аналіз готових рішень.
4. Дослідження комунікаційних систем та технологій.
5. Розробка фізичної та логічної моделі бази даних.
6. Розробка 3D-моделі підприємства.
7. Вибір розумних пристроїв.
8. Розміщення пристроїв на підприємстві.
9. Програмування сценаріїв роботи системи.
10. Створення алгоритму роботи.
11. Розробка інтерфейсу для перегляду бази даних.
12. Розробка мобільного додатку для керування системою.

Необхідність в безпеці є ключовим питанням для людини, оскільки кожна людина хоче почуватись спокійно та в безпеці, але не всі системи виконують цю роботу на 100% тому, що в таких системах потрібен постійний контроль та приймання рішень самостійно. Людина яка поїхала на відпочинок час від часу замислюється, що відбувається на її приватній власності, квартирі, дачі і тд. Розумні системи безпеки пропонують різні джерела для збору даних, такі як датчики присутності, камери відеоспостереження які можуть проводити аналітику отриманих даних, виявлення руху та ідентифікацію осіб. Предметом

дослідження будуть пристрої які фіксують рух зловмисників та пристрої які будуть спрацьовувати після фіксування .

Актуальність розумних систем безпеки росте швидкими темпами, адже десять років тому люди навіть уявити не могли, що існуватимуть системи які вмикаються самостійно або через мобільний пристрій. Стрімкий розвиток технологій IoT спричинив появу великої кількості різних технологій, програмних рішень, а реалізація можлива на всі сфери послуг, від розумного освітлення до розумних замків. Система також повинна автоматично виконувати та створювати сценарії.

Навіщо нам потрібні системи IoT? Такі системи мають великий потенціал який здатний знизити вартість різних послуг. Якщо проаналізувати прості пристрої та IoT, то можна виділити вагому перевагу в підвищені комфортності та економії часу. Під час подорожі користувач розумної системи безпеки зможе відчути на собі переваги даної технології, оскільки користувач зможе контролювати захист своєї території та заощаджувати на електроенергії і поліпшити своє здоров’я. Основним завданням таких системи є здатність підключати пристрої, які зможуть обмінюватись даними, щоб бути дієвими. IoT об‘єднує автоматизовані інтелектуальні пристрої, що дозволяє датчикам приймати своєчасні рішення.

Отже, потрібно дослідити основні розумні систем безпеки для приватної території прибудинкової території, проектування різних аналогічних системи в ПО, також проаналізувати алгоритми для захисту території які отримані шляхом статичної розробки . Основна мета даної дипломної роботи полягає в розробці прототипу системи безпеки та бази даних для неї. Завданням також є підбір пристроїв для цієї системи та розрахунок ціни, що дасть можливість побудувати систему в реальному житті. Також важливим завданням є розробка алгоритмів роботи системи та їх опис.

РОЗДІЛ 1. ПОСТАНОВКА ЗАДАЧІ ТА АНАЛІЗ РІШЕННЯ

1.1 Постановка задачі дипломної роботи

Система безпеки для території зовнішнього двору – це встановлення функціональних приладів, апаратів та методів на периметрі мережі для захисту ресурсів та даних. Безпека периметра є частиною більшої безпеки і вона має свою роль в активному захисті системи. Розумна система безпеки призначена для зручності у користуванні та енергоефективності. У наш час більшість людей зосереджені на захисті свого приватного будинку, оскільки кількість грабежів росте з кожним роком і тому потрібно переконатись, що зовнішня частина вашої території захищена.

Безпека території забезпечується вбудованою багатофункціональною системою, яка виявляє можливі загрози, також система здійснює спостереження та аналізує схеми атак. Вона служить першою лінією захисту мережі від багатьох небезпек, які можуть завдати шкоди системам. Аеропорт, який служить певним шлюзом до країни та назад, завжди використовує систему безпеки території , яка складається із системи виявлення вторгнень, камер відеоспостереження, сигналізації, щоб забезпечити вилов злочинця в разі потреби.

Вся система оборони «Розумний Будинок» взаємодіє з іншими підсистемами такими як: система відеоспостереження, система контролю присутності, вони виконують одну функцію – збереження безпеки та захист. Завдяки різним програмам та додаткам можливо спостерігати за нашим об’єктом за допомогою відеокамер і тому у власника системи є вся інформація про всіх суб’єктів, що потрапили на територію і далі вже відбувається сповіщення на додаток або дзвінок.[1]

Оскільки вся система «розумна» тобто повністю автоматизована вона є енергоефективною, тому що всі датчики та прилади самі контролюють своє включення і виключення. Наприклад, на дворі вже темно і система розуміє, що у цей час на зовнішньому дворі нікого немає, оскільки кожний прилад та датчик

містить інформацію яка година на даний момент, але система не може самостійно ввімкнути режим захисту приватної території і тому вона завжди інформує про будь-які зміни у системі. Але якщо людина йде з дому і забуває зачинити двері або хвіртку, тоді датчики які містяться у замках та хвірtках спрацюють і автоматично зачинять та повідомлять про це людину.

Розумна система охорони – попереджає власника цієї системи про наближення не відомих людей до воріт або паркану. Для цього встановлюється декілька камер відеоспостережень та детекторів руху для охорони периметра житла . І при будь-якому наближенні непрошених відвідувачів система буде реагувати так: наприклад, буде різко лунати звуковий сигнал або включатися світло. Також, можливо відразу відобразити картинку на камерах за бажанням на будь-який монітор в будинку на якому буде зображення з відеокамери. Дуже цікава та зручна функція перегляду активних зон. На панелі відображається детальна карта всіх приміщень будинку, і на ній різними кольорами підсвічуються так звані активні зони. Тобто, ті місця, в яких в останні декілька годин (5, 10, 40 хвилин) були якісь рухи і колір буде змінюватися залежно з часом.

Отже, основним завданням дипломної роботи є розробка системи безпеки для території зовнішнього двору з стадії діагностики та обчислень до кінцевого результату, отримання нових знань у різних галузях, зокрема IoT безпека. Побудова бази даних для системи, розробка логічної та фізичної моделі. Приписання алгоритмів роботи після яких система буде автоматизована. Далі застосування своїх вмінь на практиці , створення та написання різних програмних рішень і додатків до нього.

1.2 Аналіз існуючих у світі способів її вирішення

У роботі [2] надається опис продукту який самостійно може виконати функцію безпеки невеликої території. Пристрій який не потребує жодних хабів та допоміжних приладів, окрім додатку на смартфон за допомогою якого буде здійснено контроль та перегляд відеокамер. Також даний пристрій

працює з Google Assistant та Alexa ,що допоможе нам за допомогою голосових команд здійснювати певні дії в програмі. Розумна камера відеоспостереження отримує сповіщення в середньому між 5 та 10 секундами після початку події руху. Незважаючи на невелику затримку між початком руху та отриманням сповіщення, камера виконує свою роботу досить добре, зафіксувавши достатньо рухової активності в базі даних збережених кліпів.Доступ до даних відбувається за допомогою хмари яка легка у користуванні. Також разом із цим пристроєм можна створити певну зону виявлення руху навколо дверей , щоб власник отримував сповіщення, які трапилися в певній області. Якщо хтось йшов поруч із дверима то власних не отримував жодних сповіщень та попереджень, але як тільки хтось зупинився перед дверима, щоб відчинити їх, власник відразу отримав попередження, що виявлено рух. Дане рішення буде хорошим для власників квартир, де потрібна лише одна камера відеоспостереження.

В статті [3] відбувається опис та аналіз компанії яка надає послуги для захисту та контролю домашньої безпеки та безпеки прибудинкової території. Також описано з яких компонентів складається система охорони та як відбувається контроль системи. Розглянута загальна інформація про компанію та якій країні вона належить

Робота [4] присвячена опису проблеми захисту зовнішньої території яка віддалена від будинку. Також у даній роботі описано як підвищити безпеку за допомогою автономного рішення з використанням живлення від сонячної енергії. Також вона містить інформацію про переваги та недоліки для віддалених об’єктів.

В статті[5] представлено провідний у світі відео орієнтований смарт-проект який має підтримку штучного інтелекту. Також розповідається, що даний продукт може точно індефікувати людину та транспортні засоби, а також може фільтрувати помилкові тривоги, які були викликані різними невідповідними об’єктами. Представлені функції та перелік приладів які сумісні з даним продуктом.

Робота [8] присвячена опису новітньої технології для перевірки вторгнення по периметру. Йде опис теплової камери відеоспостереження, порівняння з схожими системами безпеки периметру. Далі в роботі пропонується де слід використовувати даний прилад та дослідження переваг над аналогами.

Метою роботи [9] є опис системи безпеки та компанії яка базується у північній частині Вірджинії йде опис діяльності та основні напрямки розвитку. Дана робота містить повний перелік можливостей продукту та її характеристику. Даний продукт вирішує повністю проблему безпеки для приватної території прибудинкової території.

Стаття [10] містить інформацію про програмне забезпечення яке використовується для підтримки безпеки приватної мережі. Далі описано як можна реалізувати його та його функції, також представлено методи для підтримки безпеки приватної мережі.

В статті [11] представлений постачальник для IP-відеоспостереження який використовує технологію Trend Micro IoT Security. Також там описані основні та додаткові функції для цієї камери, актуальність її на ринку.

У Роботі [12] описано високотехнологічний пристрій який буде компонентом розумної системи безпеки для приватної території прибудинкової території підприємства, Запропонований пристрій має дивовижну кількість функцій за свою ціну і тому це хороший варіант для тих, хто хоче недорогу зовнішню безпеку. Проаналізовано переваги та недоліки пристрою та рекомендації для нових користувачів.

Робота [13] містить загальну інформацію про компанію та продукти, обґрунтовано актуальність даної системи на ринку також приведені основні характеристики системи, і конструктивні рішення певних проблем, які використовуються при її проектуванні. Технологія заснована на інтеграції кращих якостей ЕС. Її використання забезпечує скорочення трудомісткості розробки та аналізу програм.

В статті [14] описується підхід до створення системи безпеки для приватної території прибудинкової території підприємства. Освітлена структура побудови системи також містить інформацію про склад цієї системи, як відбувається управління системою.

Стаття [15] описує бездротовий протокол, який фокусується тільки на підключенні до розумного будинку також розглянуто тенденцію розвитку бездротових протоколів. Далі ресурс містить інформацію про користувачів та актуальність протоколу. Також зображено як працює бездротовий протокол(рис.1.1)

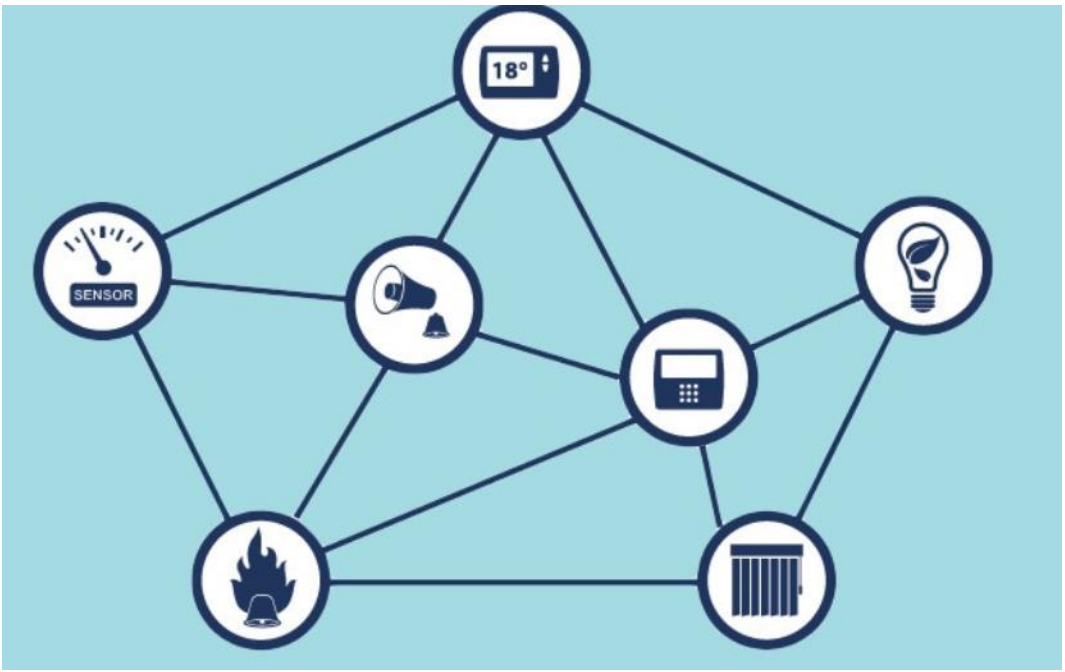


Рисунок 1.1. Принцип роботи Z-Wave

Робота [16] описує програмну реалізацію для професійного моніторингу та безпеки зовнішнього подвір’я її переваги над аналогами. Розглянуті компоненти продукту їх плюси та мінуси також, робота містить різні характеристики та опис тестування власного додатку. Також йде опис хмарного збереження інформації та аналіз з будь-якого пристрою у якого є доступ.

Робота[29] розповідає про програмний продукт від відомої компанії, який використовується для аналізу та моделювання віртуальних мереж та систем.

Також використання даного продукту застосовується в IoT будинках, Описано та представлено доступ до всіх пристроїв як iot так і простих маршрутизаторів та комутаторів.

Стаття [17] містить важливу інформацію про автоматизацію для різних розумних систем. Описано бездротову технологію, яка дозволяє багатьом домашнім пристроям та розумним домашнім пристроям підключатися до єдиної системи. Також розглядаються сфери у яких використовується дана технологія її переваги над аналогами. Описані основні кроки для підключення даної технології на пристрої.

1.3 Аналіз комунікаційних технологій та систем.

Аналіз системи безпеки – це важливий етап який включає поєднання в собі програмного забезпечення, алгоритмів та різних аналітичних процесів, що використовуються для виявлення потенційних загроз в системах. Потреба в технологіях аналітики безпеки з кожним роком зростає завдяки швидкому прогресу зловмисному програмному забезпеченні. Для створення механізму безпеки потрібно знайти безпечний протокол передачі даних, який буде відповідати різним критеріям забезпечення цілісності, доступності та конфіденційності даних, важливим елементом в розробці буде пошук ефективного способу спілкування з іншими структурними елементами системи. Розвиток розумної безпеки і бездротових модулів для автоматизації призвело до часткового створенню стандартів і є можливість використання загальної інфраструктури мережі.

Дивлячись на розвиток і офіційну стандартизацію технологій в напрямку розумної безпеки території і будь-якої домашньої автоматизації, постає великій вибір протоколів передачі даних та інформації між керованими розумними пристроями, датчиками та іншими приладами. Особливою є проблема, коли необхідно забезпечити конфіденційність і цілісність динамічних та статичних даних.

Метою даного аналізу є пошук універсального та захищеного мережевого протоколу, який дозволить при використані в розумних пристроях забезпечити безпечний, чіткий зв’язок який буде перевіряти цілісність інформації та даних без використання спеціальних програмних рішень. Однак, також важливою метою є забезпечення доступність даних пристроїв шляхом автономної роботи системи.

Отже, основні захищені протоколи які використовуються в розумних системах безпеки можна поділити на два типи:

Застосування бездротових систем таких як: Z-Wave, WLAN, WeMo, ZigBee, та систем які використовуються при дротових рішеннях: TLS, Ipsec, SSl. У житлових приміщеннях можуть бути застосовані різні технології та пристрої для створення розумної системи безпеки тому провідні рішення потрібно розглядати в умовах впровадження домашньої автоматизаціях на перших етапах будівництва приміщень та квартир. При використанні бездротових новітніх протоколів і пристроїв постає також питання у забезпечені належного рівня цілісності даних і конфіденційності, оскільки є великий вплив на існуючі бездротові мережі в зоні застосування, поширеність протоколів зв’язку та можливість перехоплення сигналу з його подальшою атакою або аналізом. Також є певні правила щодо забезпечення доступності даних в розумних системах безпеки і здатності проводити роботу в автономному режимі.

Було розглянуто чотири відомі бездротові технології, які допоможуть реалізувати системи безпеки в захищеному виконанні. В якості порівняння було обрано декілька характеристик:

1. Топологія нашої мережі: які можливі різні варіанти підключення розумних пристроїв в домашню мережу.
2. Шифрування та цілісність даних: наявність надійних технологій для створення безпечного каналу передачі інформації.
3. Пропускна здатність: велика швидкість передачі даних для забезпечення швидкого відгуку між різними запитами на дію та виконання задачі.

4. Автономність та доступність: наявність додаткових способів самоорганізації домашньої мережі і самовідновлення.

Доступність є одним з найголовніших критеріїв для організації та створені системи безпеки. Якщо в якийсь можливий момент дані не будуть переслані з датчиків контролю присутності, бар'єрних датчиків, можуть відбутися надзвичайні ситуації. Якщо аналізувати Z-Wave, він зберігає повністю свою працездатність при відсутності електроспоживання у системі, тоді як протокол WeMo повністю залежить від свого маршрутизатора і тому він не зможе підтримати роботи системи у разі відключення енергоспоживання, що є великим мінусом при створені системи безпеки. У протоколі Thread більш сучасні технології передачі даних, але відсутність інформації про застосовуваних приладах не дозволяє говорити про можливу заміну в майбутньому технології Zig-Bee. Thread та Zig-Bee харчуються від акумуляторів і вони мають чудовий алгоритм самоорганізації і відновлення мережі, що дозволить підтримувати повну доступність системи у разі відсутності електроспоживання [24].

Бездротові протоколи передачі даних в основному використовують мережу типу зірка, у якій є центральний пристрій, який буде виступати в ролі єднальної ланки. Дану систему легко розгорнути, але також вона має свій недолік, при виході центрального хабу, можливо буде відбуватись порушення доступності.

Швидкість передачі інформації, протоколи які працюють на малопотужних частотах мають досить не велику швидкість передачі даних, але для передачі простих команд вони легко впораються. Потрібно виділити протокол WeMo, пропускна здатність якого повністю залежить від можливостей маршрутизатора. Zig-Bee має дуже хорошу швидкість передачі даних і має низку переваг над своїми конкурентами.

Також однією із важливих критеріїв оцінки бездротових технологій є шифрування. Всі сучасні протоколи використовують певне шифрування, проте воно дуже багато має відмінностей. Порівнявши два протоколи Zig-Bee I Z-Wave, вони обидва використовують досить відоме шифрування AES-128, але Zig-Bee

використовує дану технологію на всіх вузлах системи, а Z-wave тільки на відведених вузлах. WeMo даний протокол повністю залежить від свого маршрутизатора і всі можливе шифрування неможливе без нього. Thread використовує сучасні системи шифрування на основі еліптичних кривих.

Отже, проаналізувавши всі системи з точки створених характеристик, найбільш актуальною та слушною є технологія Zig-Bee, дана технологія повністю закриває проблеми у разі відсутності електроенергії, також даний протокол є енергоефективним. Zig-Bee повністю закриває проблему цілісності і доступності даних в автоматизованих системах безпеки. Хорошим аналогом цієї системи є WeMo, але він не підходить для створення захищених систем безпеки.

1.4 Опис систем для забезпечення захисту території

1.4.1 Frontpoint Home Security System

Якщо користувач потребує компанію яка пропонує високо настроюванні та повністю бездротові системи з трьома рівнями охоплення моніторингу, Frontpoint – найкращий варіант, адже системою можна керувати дистанційно, вона допомагає захистити як від зловмисників, так і від збитків навколишнього середовища і система має велику кількість функцій. Система використовує панелі управління General Electric з потужними та надійними стільниковими з’єднаннями для моніторингу. Датчики Frontpoint, відеокамери та інше обладнання є бездротовими. Встановлення не залишає постійних слідів, також обладнання легко перенести на нове місце проживання. Незвичайна функція Frontpoint може попередити користувача системи, коли він йде з дому, не включаючи систему охорони. Ви можете отримати сповіщення у додатку про вимкнену систему безпеки[6].

1.4.2 ADT Security Services

Якщо користувачу потрібна компанія яка є провідною в галузі систем охорони то компанія ADT буде хорошим варіантом безпеки. Компанія велику кількість переваг, можливий вибір системи: дротовий або бездротовий. Також у систему можливо побудувати які для будинку так і для зовнішнього двору. Системою можливо керувати віддалено також є можливість масштабування, доповнення новими пристроями. Що стосується монтажу, самостійно систему встановити буде складно тому, ADT вимагає професійного монтажу з майстром. Ця послуга буде за великі гроші, а оновлення пакетів вимагають також додаткової плати. Тому дану систему можна рекомендувати користувачам які готові заплатити велику кількість грошей для обслуговування та монтажу даної системи безпеки для приватної території прибудинкової території[18].

1.4.3 Wyze Cam v3

Даний пристрій легко рекомендувати, доступна ціна, працює добре, також є хмарне сховище яке безкоштовне протягом певного часу. Також є можливість використовувати карту пам'яті для локального зберігання. Цей пристрій можливо приєднувати до інших пристроїв за допомогою додатка на смартфонах і за допомогою цього можливо створити систему безпеки для приватної території прибудинкової території підприємства самостійно. Ця камера також працює з різними асистентами. Якщо користувач шукаю бюджетний варіант системи безпеки то Wyze Cam v3 буде хорошим варіантом[2].

1.4.4 Brinks Home Security

Brinks поєднує недорогі пакети домашньої безпеки з одним із найнадійніших планів моніторингу. Професійний моніторинг та безпека є дуже надійною і він забезпечує швидкий час реагування, але ціна для простих користувачі буде занадто великою. Система містить свій власний додаток який

включає в себе камери спостереження території. Також є хмара у яку користувач може записувати кліпи та переглядати потік через додаток. Далі у користувача системи має пульт який має контроль над зняття з охорони системи та встановлення охорони. Brinks Home Security - це надійний вибір для тих користувачів, які шукають домашню безпеку "зроби сам" з великою кількістю чудових функцій[22].

1.4.5 Ajax

Компанія яка повністю займається безпекою будинку та зовнішньої території. Система розроблена даною компанією є повністю автоматизована та містить датчики власного виробництва. Систему можливо підключити до відеокамер, щоб у будь-який момент оцінити ситуацію. Ajax має власний додаток на смартфон у якому збережено повністю всю інформацію, оскільки він містить журнал подій де зображений час активності і де відбулась активність. Також компанія надає пульт тривоги в разі проникнення на об’єкт зловмисників. Компанія надає повну консультацію новим клієнтам, розробляючи систему та механізм спеціально під ваш об’єкт, де будуть враховані всі нюанси. Важливою перевагою даної системи є використання певних сценаріїв для автоматизації безпечного будинку. Ajax – є надзвичайною системою за доступною ціною, дана система яскраво піддійте користувачам які прагнуть повністю автоматизувати свою безпеку[25].

Проаналізувавши кожну з систем можна зрозуміти, що на ринку дана тематика з розумної безпеки актуальна, оскільки кожна система є повністю індивідуальна і кожна з них забезпечує безпечну роботу інженерних систем на території і здійснює охоронну функцію. Але найкращим варіантом серед проаналізованих систем є система Brinks Home Security оскільки компанія пропонує сучасне обладнання, яке орієнтоване на розумну автоматизацію будинку. У системі також є можливість додавання нових датчиків, приладів в систему будь це: внутрішні камери ,камери для дзвінка або датчики руху та

контролю присутності. Компанія також продає продукти для розумного будинку і з кожним планом домашньої безпеки можна отримати домашній центр, який буде контролювати систему та обладнання. Система працює в бездротовій мережі і усі системи зовнішньої безпеки дозволяють встановлювати їх самостійно, що є великою перевагою. На ринку дана компанія має велику кількість відгуків і вони є досить великі для такої системи за такою ціною. Отже захист близьких та майна – це найголовніша проблема. Для того, щоб захистити те, що вам найбільше подобається і ви повинні переконатися, що отримуєте найвищій рівень безпеки – навіть коли ви не в дома. Але це є більшим, ніж просто доступ до системи безпеки, важливо також розуміти, які функції та переваги найкраще підходять для вашого власного майна і тому розробка системи безпеки зовнішнього подвір’я є актуальною і буде актуальною протягом багатьох років.

1.5 Висновок по розділу

Отже, в даному розділі було проведено дослідницьку роботу в якій було проаналізовано велику кількість наукових робіт які пов'язані з розробкою розумної системи для безпеки території. Також відбулась робота в якій було порівняно 5 великих компаній якій займаються даною тематикою, тобто розробкою розумних систем безпеки. Було поставлено задачу яка полягає в створені розумної системи безпеки для приватної території прибудинкової території підприємства, обрати найкращі пристрої та технології зв’язку між ними, створити базу даних для системи. Та зробити систему повністю автоматизованою. Оцінка вартості розробленої розумної системи.

РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ТА СТВОРЕННЯ БАЗИ ДАНИХ ДЛЯ СИСТЕМИ

Кожний проект залежить від ступеня складності, адже це документація, яка містить різні принципові конструктивні рішення і дає загальне уявлення про будову та принцип дії вибору. Слід зауважити, що підготовка до створення проекту про систему безпеки передбачає виконання певних операцій, що потребують спеціальних знань і великого досвіду, — розробка проектної документації, формування проектних команд, вибір підрядників, організація будівництва об'єкта. Виконання будь-якого завдання, особливо творчого, відбувається за індивідуальним планом. Виконується необхідна документація, розглядаються аналоги та подається вся необхідна інформація про процес створення продукту. Ця діяльність має назву – проект. Система передбачає створення нової ідеї, виготовлення та оформлення всієї інформації. Також відбувається побудова основних етапів для створення системи. На першому етапі підготовчому, виконується підготовча робота для виконання завдання. Визначається доцільність створення системи, також відбувається формулювання вимог та створення певного банку пропозицій та ідей. На конструкторському етапі відбувається основна творча діяльність: розробка візуального продукту, малювання ескізів, та створення таблиць. Технологічний етап представляє собою написання програми для автоматизації системи згідно плану, внесення певних корективів.

Також розробка проекту означає проходження загальних етапів:

- Визначення завдання.
- Вибір стратегії для реалізації проекту.
- Оцінка вартості .
- План побудови.
- Реалізація проекту .
- Тестування.
- Написання звіту.

Для розробки проекту або системи для зручності потрібно використовувати різне програмне забезпечення для управління проектом. Платформа, яка допоможе розробникам контролювати, планувати та звітувати про проекти: це допомагає розробнику керувати своєю роботою там роботою свої помічників. Хороше ПО розширює можливості проектних команд, завдяки чому вони можуть керувати всіма деталями, що входять до складу успішного проекту або системи. Оскільки кожна система має свій життєвий цикл створення і кожний з таких циклів потрібно контролювати , усі системи та проекти проходять низку етапів і тому для зрозумілості на якому етапі розробки система потрібно використовувати програмне забезпечення для контролю.

Отже для контролю розробки системи безпеки для приватної території прибудинкової території підприємства було використано програмне забезпечення Trello. Багато платформна система управління проектами в якій кожний проект зображується дошками, а кожна дошка має свій список. Після виконання певної частини роботи вона переходить далі по списку. За допомогою інструментів які надає даний продукт, проект можна охопити до найдрібніших деталей. Кожна карточка може бути простим завданням, також для кожної окремої задачі може бути призначений окремий виконавець. Для цього потрібно вибрати людину і назначити в програмі завдання. Кожне завдання має свій пріоритет при створені системи і залежно від нього можливо переносити список вгору або вниз, що допоможе розрахувати час і інші ресурси. Даний продукт є практично бездоганним помічником у веденні колективного або персонального проекту, також важливою перевагою Trello є його вартість, оскільки продукт є повністю безплатним в користуванні у ньому можна повноцінно працювати абсолютно безкоштовно .По суті, Trello втілює в собі мрію кожної людини, так як є універсальним та простим у використані інструментом, як для особистого користування так і для роботи в команді. Розроблено систему для контролю розробки системи безпеки для приватної території прибудинкової території(рис.2.1)

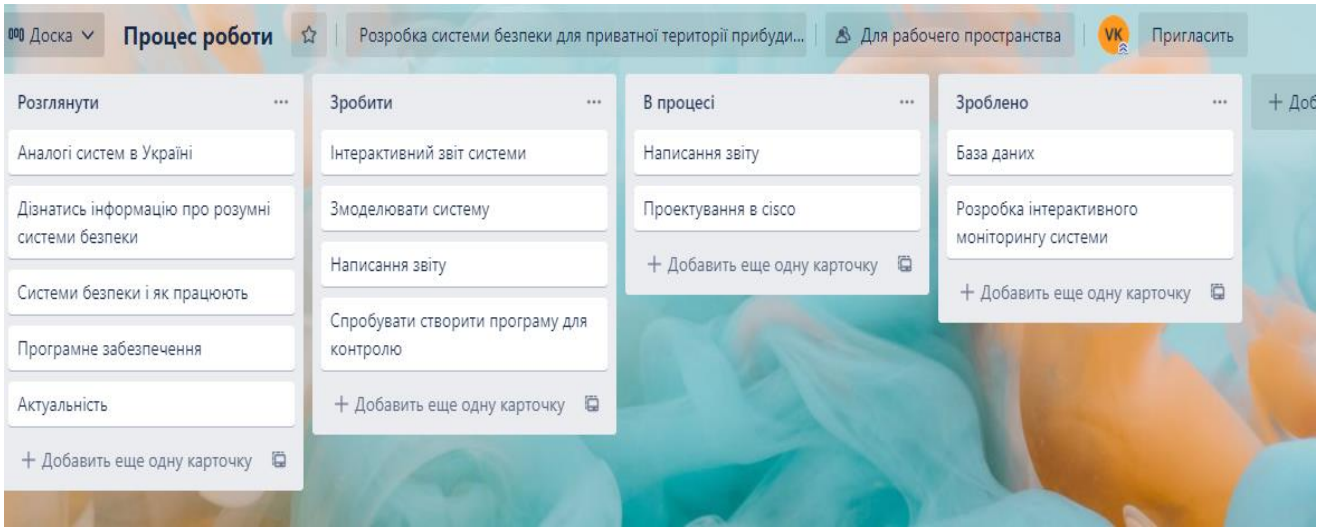


Рисунок 2.1. Дошка для контролю розробки системи безпеки

Було створено дошку для перегляду стадій створення системи безпеки. Дана система допоможе визначити зроблену роботу і яка в процесі. Також тепер можливо спостерігати за розробкою програмних продуктів, скласти певний план та допоможе розробникам системи безпеки зробити день та роботу більш продуктивною та корисною. За допомогою створеної дошки можливо спостерігати за продуктивністю роботи.

2.1 Розробка проекту 3D-проект та розміщення пристроїв в Cisco Packet tracer

Сучасні розумні системи безпеки дозволяють здійснювати управління автоматизованими системами клімат-контролю, безпекою, розумним освітленням та різними побутовими пристроями і лічильниками. По суті розумна система безпеки – це комплексна система, яка працює автоматизовано та як один механізм для досягнення повної безпеки та комфортного проживання в будинку. На сьогоднішній момент є велика кількість представників які можуть надати свої пропозиції для розвитку цього напрямку, але реалізація та розробка проекту досить не легка і має бути врахована ряд нюансів які будуть впливати певним чином на систему, тому перед реалізацією доцільно провести не тільки проектування, а і моделювання за допомогою різних програмних забезпечень.

Проаналізувавши декілька систем для розроблення проекту та моделювання її було обрано Cisco Packet Tracer

Cisco Packet Tracer – це програмне забезпечення, потужний інструмент для моделювання, роботи з пристроями Iot та розробки проектів мережі створений компанією Cisco. Програма є повністю безкоштовна для всіх користувачів яка допомагає змоделювати або відточити практичні навички у підключені розумних пристроїв та налаштувати мережу для своїх пристроїв.

Було створено методику для моделювання Iot проекту «Система безпеки для приватної території прибудинкової території підприємства»

1. Підготовка та аналіз території. На даному етапі отримуються, або розробляються креслення і йде уточнення про вимоги.
2. Загрузка схожого об’єкту або загрузка існуючого для точного проектування системи.
3. Підбір із набору різних візуальних моделей Iot-приладів, які відповідають поставленому завданю
4. Важливим етапом розробки є моделювання системи. На даному етапі потрібно врахувати всі можливі пристрої відносно території, їх розміщення на ній.
5. Весь проект потрібно розділити на підсистеми: системи бар’єрів, датчики руху та камери, розумні замки
6. Наступним кроком моделювання є підключень до мережі інтернет.
7. Створення певних автоматизованих систем. Тобто розробка різних сценаріїв роботи системи.

Аналіз території при розробки проекту для системи безпеки для приватної території прибудинкової території підприємства є дуже важливим завданням, адже тільки після аналізу можна зрозуміти як будувати систему які технології буде використано та яка кількість пристроїв буде використано, отже відбувся повний аналіз системи і побудовано її у системі Visio. Microsoft Visio – це програма для створення моделей, різних структур та схем. Програма схожа зі

своїми аналогами, вона також надає доступ до шаблонів та фігур, які допоможуть створити план будинку або схему. При правильному користуванням можливо створити професійну схему та візуальний проект. Але для більшості користувачів цього продукту вона є лише допоміжною програмою, яка використовується разом з Microsoft SQL Server, Exel та іншими продуктами даної компанії. Іншими словами, замість того щоб вводити власноруч дані, в більшості випадках це дуже довго та витрачає дуже багато дорогоцінного часу. Простіше пов’язати діаграму Visio даними , які обробляються та вводяться спеціально для окремої діаграми. Використання зовнішніх джерел має свої переваги. Важливою перевагою при використанні зовнішніх джерел оновлення інформації відбувається повністю автоматично — при певних змінах файлу або іншого джерела дані на діаграмі Visio теж будуть змінюватись[26]. Створено 3D-модель підприємства для якого буде розроблено автоматизовану систему безпеки зображено на рис(2.1.1)

Рисунок 2.1.1 3D-проект підприємства ТОВ” Примавера компані ”

На розробленій 3D-моделі чітко зображено всю зовнішню територію, це допоможе розробникам системи проаналізувати ділянки які потрібно захистити та де очікує можлива небезпека. Даний рисунок можливо інтегрувати відразу до

програми Cisco Packet Tracer для розробки проекту системної безпеки, оскільки розміщення датчиків відіграє ключову роль в роботі системи. Кожний тип датчиків має певний стандарт розміщення, оскільки немає сенсу встановлювати датчик бар'єру біля вхідних дверей або воріт, а краще його розмістити на огорожі об'єкта який буде захищатись, де бар'єр ніколи не перетинає, окрім можливих злодіїв. Отже проаналізувавши територію для якої буде розроблено розумну систему безпеки, було спроектовано та розташовано датчики таким чином(рис.2.1.2)

Рисунок. 2.1.2 Розміщення датчиків на об'єкті

Було повністю проаналізовано зовнішню територію, щоб забезпечити повну безпеку підприємства та його території. Датчики було розміщено енергоефективно, жодних зайвих давачів не було додано в розумну систему, за допомогою розташування пристрої які зображено на рисунку (рис.2.1.2), розроблена система повністю буде автоматизована, також буде налаштована глобальна мережа інтернет для контроль системи та внесення змін.

2.2 Вибір датчиків та хабу

ADT Security Services – є найстарішою і найбільш авторитетною компанією постачальником безпеки в США. Створена компанія була заснована в 1860 – ті роки. Вони пропонують надійний сервіс та безпеку, професійний монтаж та найкращу гарантію в бізнесі. Також компанія має досить велику кількість нагород на ринку[18]. Але у даній системі є кілька недоліків, які потрібно врахувати перед покупкою.

Однією із найуспішніших систем компанії є ADT Pulse® Home Automation + Video. Це бездротова, інтелектуальна система управління безпекою, що пропонує розумне рішення для безпеки для приватної території прибудинкової території підприємства. Стартовий комплект також є сумісний з Google Home та Alexa .

ADT Pulse® Home Automation + Video використовує одну з новітніх видів бездротових технологій – Z-Wave. Дана технологія Z-wave створює бездротову сітчасту мережу, яка являє собою сукупність різних розумних пристроїв, які з'єднуються та взаємодіють між собою. За допомогою технології Z-хвиль пристрої поєднуються, передаючи сигнали через низько енергетичні радіохвилі на виділеній частоті. (технологія Z-Wave використовуються для домашньої автоматизації та має велику швидкість передачі інформації.) Всі пристрої Z-Wave мають крихітний вбудований ретранслятор сигналу, який надсилає та отримує мережеву інформацію. Безпека та гнучкість - це дві основні сильні сторони системи які пропонують безліч можливостей повністю адаптувати безпеку до різних потреб[15].

Samsung SmartThings та ADT об'єднали разом зусилля і пропонують продукти для безпеки для приватної території прибудинкової території також вагомою перевагою цієї системи є відсутність довгострокового контракту.

Для даної розумної системи було використано наступне обладнання:

1. Бездротова сенсорна клавіатура DSC ADT(рис.1.2). Оскільки вона бездротова, то її можна встановити в будь-якому місці будинку. Використовувати цю клавіатуру з системою ADT так само просто, як записати її в програмування панелі, як і будь-який інший пристрій. Ви перейдете до програмування до розділу реєстрації бездротових мереж, а потім натисніть кнопку реєстрації на клавіатурі, і вона сама навчиться програмуванню панелі. Основні характеристики бездротової сенсорної клавіатури DSC[21].

Рисунок 2.2.1 Бездротова сенсорна клавіатура DSC

2. Датчик руху eMACROS 1/2 Mile Solar Driveway Alarm Motion(рис.1.3) - це сонячний датчик руху з бездротовим сигналом руху - це зручна та доступна система безпеки. Інфрачервоний бездротовий детектор сигналізації на відкритому повітрі, який надійно попереджатиме вас про активність навколо вашого майна. Помилкові тривоги зводяться до мінімуму шляхом регулювання чутливості. Погодо стійкий зовнішній сонячний датчик з регульованим регулюванням чутливості. Також вагомою перевагою цих пристроїв є живлення,

тому що датчик живиться від вбудованої літій-іонної акумуляторної батареї, тому замінювати батарею не потрібно. Оповіщення зі світлом і звуком, коли транспортні засоби або пішоходи наближаються в радіусі 10 метрів. Розширюваний до необмеженої кількості сонячних датчиків та необмеженого приймача, він ідеально підходить для дому, бізнесу, майна та робочого місця. Надзвичайно прості у налаштуванні. Налаштування займає лише кілька хвилин. Легко зробити самостійно установку. Набір включає чотири сонячні датчики та один приймач. Виявляє рух до 4 різних зон, включаючи індикатор низького заряду акумулятора. Приймач можна підключити за допомогою адаптера змінного струму, що входить до комплекту, або працювати від (4) батареї типу AA. Сонячний датчик може бути розміщений на відстані до 1 милі від базового блоку в ідеальному стані[20].

Рисунок 2.2.2 Датчик руху eMACROS

3. 1/2 Mile Supplemental Driveway Alarm Solar Receiver(1.4) – це невеличкий сонячний приймач додаткової тривоги який від’єднується до датчиків руху eMACROS. Він взаємодіє з іншими пристроями за допомого бездротового протоколу Zigbee.

Рисунок 2.2.3 Приймач додаткової тривоги

4. Arlo VMS4230P-100NAS Pro 2 - Wireless Home Security Camera System(рис.1.5) – це розумні камери відеоспостереження які передають зображення у дуже хорошій якості (1080p). Arlo Smart додає потужний інтелект до системи камер Arlo. Можливе налаштування сповіщень, щоб виявляти людей, конкретні зони та зв’язуватися з особами прямо з екрана блокування вашого смартфона. Бездротова конструкція дозволяє розміщувати камери в будь-якому місці зовнішнього двору, де ви хочете спостерігати за своїм будинком під будь-яким можливим кутом. Відео 1080P HD якості з чіткішими та яскравішими деталями. Також ці камери містять міцний акумулятор 2440mAh. Час роботи акумулятора залежить від налаштувань, використання та температури. Діапазон фокусування (ST): фіксований фокус (від 0.5м до 1км); Нічне бачення: автоматично вмикається при слабкому освітленні, щоб ви могли чітко бачити навіть у темряві. Включає довговічні акумуляторні батареї, що позбавляє потреби купувати одноразові акумулятори. Гнучкі варіанти живлення використовують

акумулятори, джерело змінного струму або сонячну панель Arlo яка під’єднується до системи. Сертифіковані IP65, стійкі до атмосферних впливів камери дозволяють розміщувати їх де завгодно в приміщенні та поза ним[13].

Рисунок 2.2.4 Бездротова камера Arlo Pro 2.

5.Arlo – SmartHub(рис.1.6) – це концентратор якій надійно з’єднує камери Arlo Pro 2 які є бездротові з інтернетом. Хаб забезпечить зв’язок з камерами на великій відстані. Пристрій підтримує такі бездротові технології зв’язку: Wi-Fi 2,4 ГГц, Wave, Zigbee, також даний пристрій здатний до локального резервного копіювання, розумна сирена та розширене покриття використовуючи додаткові базові станції.

Рисунок 2.2.5 Arlo – SmartHub

6. Aqara HomeKit Smart LED Light Bulb ZigBee(рис.1.7) – смарт-лампочка, яка відрізняється високою енергоефективністю та тривалим експлуаційним терміном. Також дана лампочка використовує стандартний цоколь, так що складнощів з її встановленням і підключенням не виникне. Лампочка також взаємодіє за допомогою бездротового протоколу Zigbee. Після того як було прив'язано лампочку до HomeGateway шлюзу, далі він може керуватись за допомогою пристроїв, телефонів, налаштування часу світла та коли потрібно, щоб ввімкнулось світло. Дана лампочка буде хорошим варіантом імітації присутності людини на підприємстві в якому потрібно забезпечити безпеку[32].

Рисунок 2.2.6 Aqara HomeKit Smart LED Light Bulb ZigBee

Основні переваги проекту:

- Не потрібні кабелі – система повністю працює на бездротових носіях і завдяки цьому немає потрібності в додаткових кабелях. Це є великою, перевагою під час певних ремонтів.
- Також просте введення в експлуатацію, здійснюється це за допомогою мобільних додатків. Немає необхідності в різних допоміжних пультах керування.
- Простота встановлення продукту – система дуже проста встановленні, для роботи системи потрібна мережа та додаток на смартфоні. Також можливо самостійно встановлювати та додавати пристрої у свою систему.
- Віддалений доступ – систему можливо вмикати та контролювати віддалено, але при цьому потрібно мати доступ до опублікованого запису.
- Сповіщення – у разі можливого порушення безпеки, або інших різних ситуацій, система негайно надсилає текстові сповіщення про небезпеку, щоб повідомити про порушення безпеки.
- Масштабування – у систему у будь який момент часу можливо додати нові камери, датчики руху, розумні замки, оскільки зв’язок у системі між пристроями відбувається за допомогою бездротових технологій
- Функціональність – система безпеки містить велику кількість сценаріїв для задоволення всіх необхідних потреб для різних середовищ. Для нових власників території, або зміни паркування транспортного засобу, можна використати зміну налаштувань.
- Енергоефективність – пристрої не вимагають періодичних замін акумуляторів і тому одному заряді зможуть виконувати свої функції багато років.
- Простота виведення з експлуатації – користувач системи самостійно спроможний до внесення незначних змін.

2.3 Проектування контекстної, логічної та фізичної моделі бази даних

Всі сучасні системи мають великий обсяг даних і ще вони також вимагають управління і тому вся доступна інформація підприємств, або системи заноситься в бази, для управління яких використовуються система управління базою і різні мови структурованих запитів. Проектування та створення сучасних інформаційних систем являє собою складну задачу, рішення якої вимагає застосування спеціальних інструментів.

SQL – це декларативна мова програмування для бази даних, яка орієнтована на інформацію яка буде оброблятись в великому обсязі. Така мова є непроцедурного характеру, тобто в ній перш за все приділятиметься увага даним які потрібно викликати, вставляти, або проводити інші операції. Ще за допомогою SQL можна обробляти значні обсяги інформації в різних групах. Також дана програма може виконувати велику кількість завдань:

- Оновлення вмісту вже створеної бази даних.
- Отримання нової важливої інформації.
- Налаштувань повноважень для користувачів бази.
- Можливість змінювати різні параметри безпеки.
- Також можливість модифікації бази даних.

SQl можливо використовувати тільки для управління створеної бази даних. Таких мов для створення існує велика кількість наприклад: Sybase, або Informix Microsoft Access, Oracle.

Для розробки бази даних системи безпеки було обрано середовище Oracle SQL Developer DataModeler. Оскільки даний продукт є повністю безплатний та професійний, легкий в створені різних таблиці та проектуванні моделей, також він підтримує роботу з усіма операційними системами.

Логічне створення задачі це основне завдання, оскільки при створенні потрібно урахувати основні процеси та функції без яких система не зможе працювати. Логічна модель є джерелом всієї інформації перед створенням фізичної бази, оскільки вона повністю відображує функціонування системи та проаналізувати

вплив на прикладні програми і дані, які вже наявні у базі даних. Вона також відіграє роль на етапі експлуатації та супроводження готової системи. Створену логічну модель для системи безпеки зображено на рисунку(рис 2.3.1)

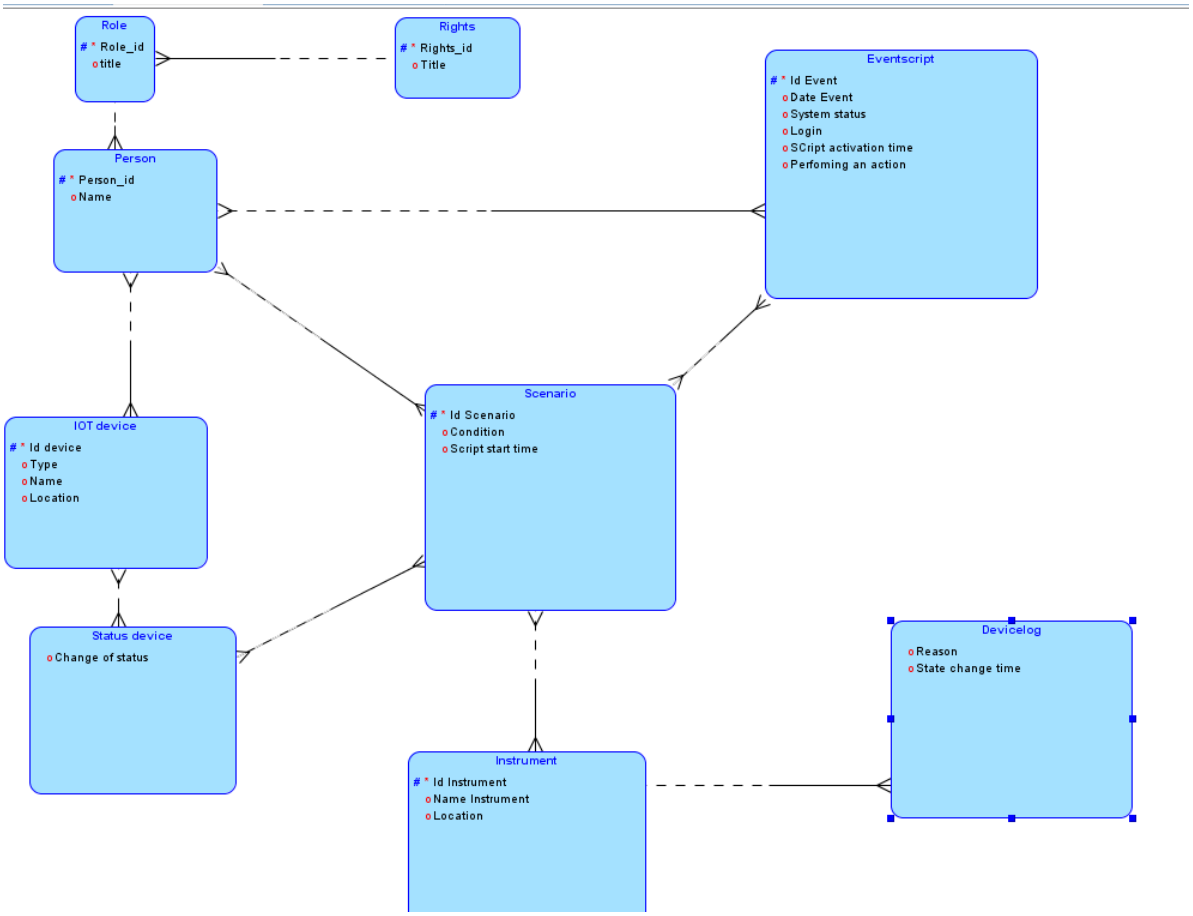


Рисунок 2.3.1. Логічна модель системи безпеки для приватної території прибудинкової території підприємства

Логічна модель бази даних містить у собі 9 таблиць(рис.2.3.1):

1. Person(Користувач).
2. IOT_Device(Іот прилад).
3. Role(Роль).
4. Rights(Права).
5. Status device(Статус пристрою).
6. Scenario(сценарій).
7. Instrument(Інструмент).
8. Devicelog(Журнал пристрою).

9. Eventscript(Скрипт події).

1.Таблиця Person містить в собі 2 поля –Person_id,Name,де Person_id- первинний ключ . Тип даних для Person_id- Integer,Name-Varchar.

Також тиблиця містить поле іншої таблиці ,яке буде призначати роль користувачу.

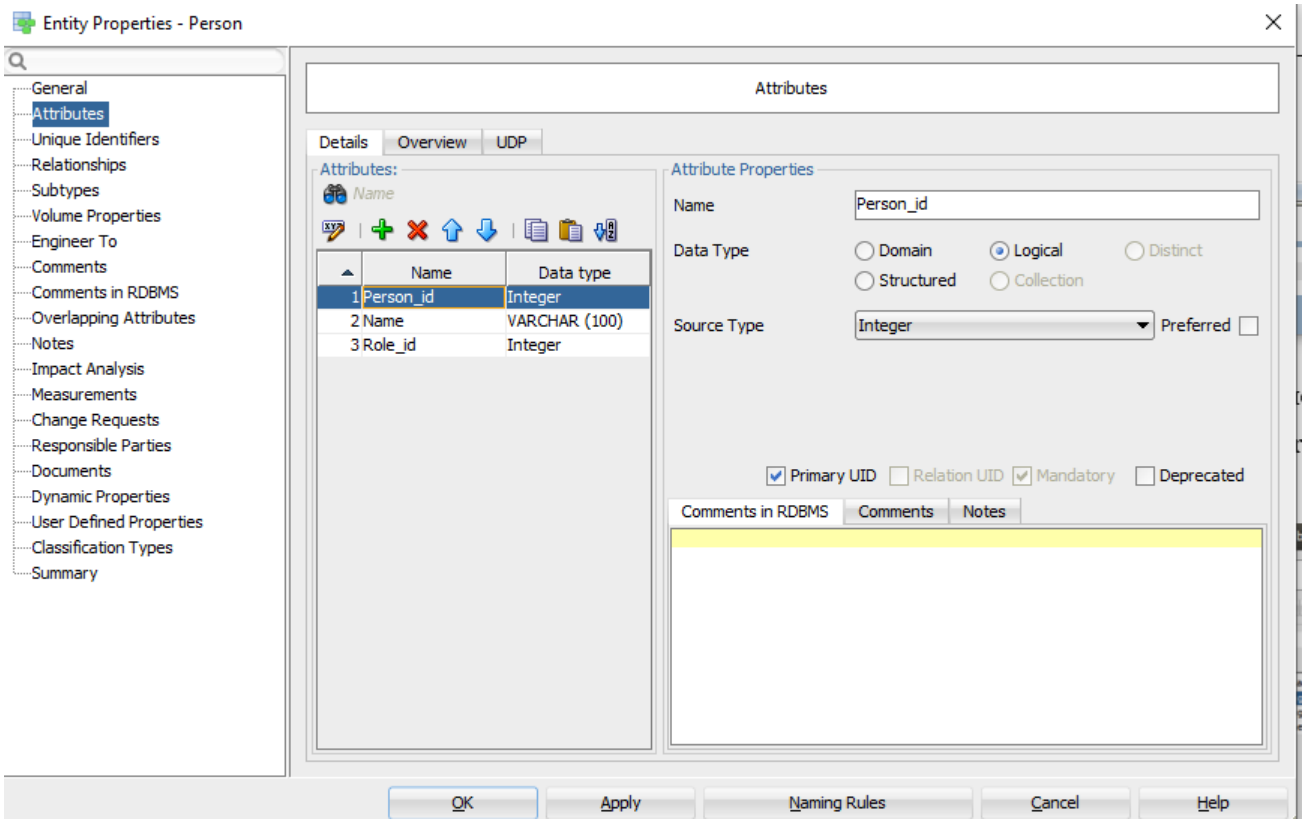


Рисунок 2.3.2. Налаштування таблиці Person

2. В таблиці IOT_Device чотири поля – id-device,Type,Name,Location,де Id - device –первинний ключ. Тип данних Id-device-Integer, Type-Varchar, Name Varchar,Location-Varchar

3. Role 2 поля –Role-id,title,де Role_id-первинний ключ,Rights_id-зовнішній ключ.

Тип даних Role_id-Integer,title-Varchar.

4. Rights 2 поля – Rights -id,title,де Rights _id-первинний ключ.

Тип даних Rights -id -Integer,title-Varchar.

5. Таблиця Status device 1 поле- Change of status-Varchar.

6. В таблиці Scenario міститься 3 поля – Id Scenario,Condition,Script start time, Id Scenario –первинний ключ.

Типи даних в таблиці Id Scenario-Integer,Condirion-Varchar,Script start time –Date.

7. В таблиці Instrument три поля – id- Instrument,,Name Instrument ,Location,де Id-Instrument –первинний ключ.

Тип данних Id- Instrument -Integer, ,Name Instrument -Varchar,Location-Varchar

8.Devicelog міститься 3 поля –Reason,State change time,Id Instrument-зовнішній ключ. Типи даних в таблиці Reason-Varchar,State change time-Date,Id Instrument-Integer.

9.Eventscript 6 полів –Id Event, Date Event,System status,Login,Script activation,Perfoming an action. Id Event- первинний ключ.

Типи даних в таблиці- Id Event- Integer, Date Event – Date, System status-Integer, Login-Varchar, Script activation-Date, Perfoming an action-Varchar.

Зв'язки між таблицями:

Person-IOT Device –багато до багатьох.

Eventscript-Person- багато до багатьох.

IOT Device - Status device- багато до одного.

Scenario - IOT Device- багато до багатьох.

Eventscript- Scenario- багато до багатьох.

Person- Scenario- багато до багатьох.

Instrument- Scenario- багато до багатьох.

Instrument- Devicelog-один до одного.

Побудова фізичної моделі бази даних створюється на принципах, які вже реалізовані в логічній моделі. Створюючи базу даних для різних система розробники створюють відразу 2 моделі, але якщо дана система є великою в розробці то створення відразу паралельно фізичну та логічну буде проблематично.

Фізична модель була створена з логічної за допомогою інструмента “Engineer” .

Рисунок 2.3.3. Кнопка Engineer

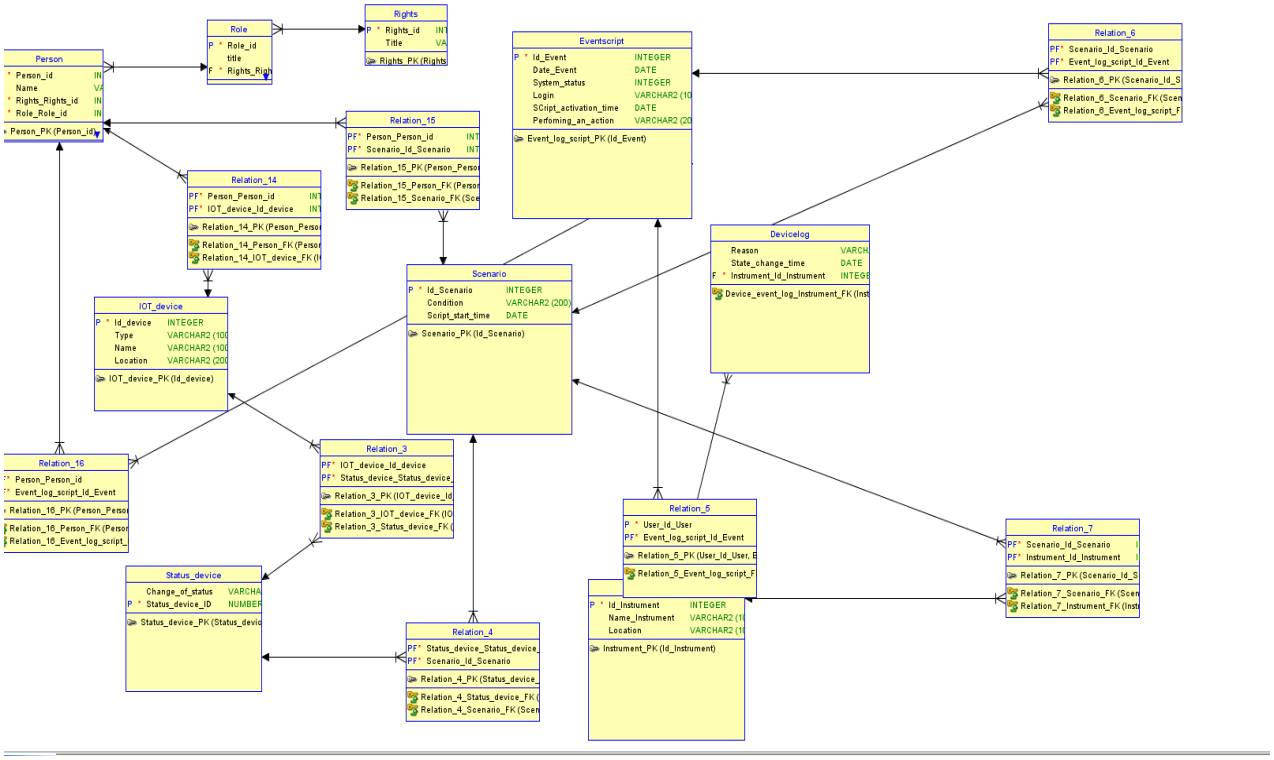


Рисунок 2.3.4. Фізична модель бази даних підприємства ”Примавера компані”

Фізична модель бази даних містить в собі 13 таблиць(рис.2.3.4):

1. Person(Користувач).
2. IOT_Device(Іот прилад).
3. Role(Роль).
4. Rights(Права).

5. Status device(Статус пристрою).
6. Scenario(сценарій).
7. Instrument(Інструмент).
8. Devicelog(Журнал пристрою).
9. Eventscript(Скрипт події).
10. Relation_3.
11. Relation_4.
12. Relation_16.
13. Relation_5.
14. Relation_14.
15. Relation_6.
16. Relation_7.
17. Relation_15.

При створені фізичної моделі було створено декілька суміжних таблиць Relation.

Таблиця Relation_15,містить в собі 2 поля.
Person_Person_id,Scenario_id_Scenario.

Типи даних обидва будуть Integer.

Створена фізична модель дає змогу зрозуміти які зв’язки відбуваються між пристроями, та як взаємодіють ці пристрої. Створення фізичної моделі відіграє важливу роль у проектуванні різних систем.

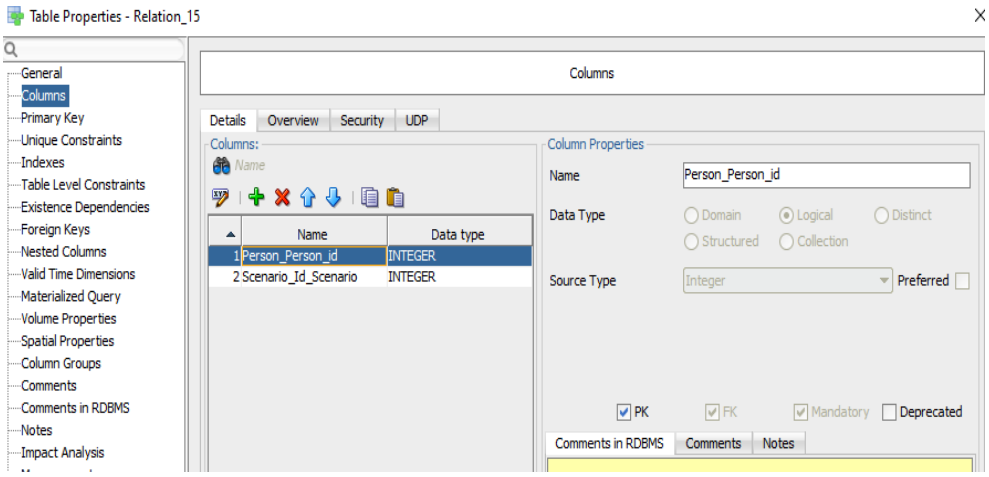


Рисунок 2.3.5. Налаштування таблиці Relation_15

Relation_3 містить в собі 2 поля.
IOT_device_id_device,Status_device_Status_device,

Типи даних IOT_device_id_device-Integer,Status_device_Status_device-Integer,

Relation_4 містить в собі 2 поля-
Status_device_Status_device,Scenario_Id_Scenario.

Типи даних Scenario_Id_Scenario -Integer,Status_device_Status_device-Integer,

Relation_16 містить в собі 2 поля Person_Person_id,Event_log_script.

Типи даних обидва будуть Integer.

Relation_5 містить в собі 2 поля- User_id_User,Event_log_script_id_event.

Типи даних обидва будуть Integer.

Relation_14 містить в собі 2 поля Person_Person_id, IOT_device_id_device.

Типи даних IOT_device_id_device-Integer , Person_Person_id-Integer.

Отже в даному підрозділі було ознайомлено з різними sql мовами для створення унікальних баз даних, також вивчено принципи побудови бази даних. Також було повністю створено базу даних для системи безпеки, ознайомлено з логічною та фізичною базою даних та створення їх для проекту.

2.4 Методи та засоби обробки і стиснення інформації для системи безпеки

В час коли технології розвиваються з величезною швидкістю також розвивається обробка інформації для цих технологій, захист інформації та обмін є ключовим питанням у напрямку розвитку інформаційного суспільства. Розумні системи є продовженням систем наглядного контролю та збору даних і отримала назву SCADA. Програма яка збирає дані з усіх пристроїв і зберігає всю отриману інформацію, вона також є досить популярною в країнах де розвинуті системи IoT, також промислове програмне забезпечення реалізує повний обмін даними з контролером.

Висока ефективність функціонування системи ґрунтується на вирішені комплексних проблем які постають в ході розробки які пов’язані з відбором інформації в мережу, кодуванням, обробкою та передачею даних. Незалежно від мережі передачі даних будь це провідна система або безпровідна, якщо правильно задати частоти канал зв’язку F та ймовірність прийому помилкового сигналу або кодової послідовності P_n і тоді ефективність роботи мережі в системі безпеки буде характеризуватись швидкістю передачі інформації R яка повністю залежить від рівня шумів у різних каналах зв’язку і буде однією функцією багатьох параметрів[29]. Іншими словами

$$R = f\,(F, P_{n,} E_{b,} | N_0, B, K_c), \tag{2.4.1}$$

В якій E_b та N_0 – це відношення одиниці енергії сигналу на один біт до густини потужності на один герц. E_b є потужністю сигналу який виходить і розраховується за формулою $E_b = S \cdot T_b$, Т – тривалість бітового сигналу, S-потужність сигналу. Також важливим в системах безпеки є швидкість передачі інформації R яка досягаються за рахунок стиску даних та збільшення елементів M канального сигналу, який передається несучою і за рахунок формування передачі L ортогональних каналів який перебуває у спільному спектрі частот F. Виходячи

з отриманих інформації можливо визначити максимальну швидкість передачі інформації яка визначається за формулою.

$$R_{max} = K_c \cdot 1/T_b \cdot L/B = k_1 \cdot k_2 \cdot k_i \cdot log_2 M_m \cdot 1/T_b \cdot L/B \qquad (2.4.2)$$

В якій M_m – кількість рівнів маніпуляцій, який визначає розмір наборів за рахунок багаторівневих маніпуляцій. Також k_i – це коефіцієнт підвищення швидкості передачі інформації за рахунок різних кодувань та формування імпульсних сигналів на інформаційному рівні[27]. Також із ефективних способів формування М полягає в використанні нерівномірного кодування різних двійкових даних в темпі введення, обробки та передачі даних або з накопиченням відповідних під масивів даних, при цьому короткі інтервали використовуються для передачі відповідних послідовностей бітів, що апріорно або з визначеною ймовірністю частіше зустрічаються, а більш тривалі які використовуються для передачі послідовностей, які менш частіше зустрічаються [27]. Одним з найяскравіших прикладів формування М є застосування всім відомого методу множин несучих в локальних та регіональних мережах стандартів IEEE 802 в якому робочий діапазон може розбиватись на півканали з різними частотами OFDM по якому передається потік даних по паралельних каналах. Пакети які передаються між розумними пристроями мають бути компактними, безпечними та крипостійкими. Більшість процесів які підлягають дослідженню та контролю є частиною часової функції. Кожний сигнал буде характеризуватись максимальним або мінімальним значенням амплітудних і частотних параметрів. Найбільш суттєвими відділками відеосигналів є екстремум та різні точки зміни опуклості обвідної, які характеризуються різними значеннями і мають додаткові параметри, такими як поточне вхідне співвідношення сигналу та шуму. Під час процесу стиску аналогових сигналів які є контрольованими виявляються суттєві відлік на чистих ділянках де немає шумів, вони кодуються більш точно в порівнянні із зачумленими відділками. Формат даних які виходять з сучасних відео сенсорів суттєво залежить від технологій розміщення світлофільтрів перед чутливим елементом який буде реагувати на яскравість світла. Також потік даних з відео

сенсора повністю залежить від формату відеокадру $M \cdot N$, де N – це кількість пікселів у стовпчику, а M – це кількість пікселів у рядку. Також суттєво залежить схеми кольорового відео кодування, топології побудови світлофільтрів та яка кількість біт потрібна для кодування градацій яскравості світла. І тому виходячи з цього сумарний потік даних з різних відео сенсорів можна визначити даною формулою. Дана формула є дуже ефективною для систем які містять відео сенсори

$$V_{bc} = K_v \cdot M \cdot N \cdot q, \qquad (2.4.3)$$

де $M \cdot N$ – роздільна здатність відео сенсора; Kv − кількість кадрів/с; q C − кількість бітів які були виділені для кодування кольорових сигналів у залежності від схеми кодування відеоданих. Також виживим є компактне кодування суттєвих і несуттєвих відділків сигналів та відеосигналів яке відіграє велику роль в розумних системах і за допомогою нього здійснюється введення даних або з накопиченням необхідної вибірки даних з наступною їх обробкою та кодуванням. Додатковий стиск масивів даних може здійснюватися за рахунок безутратних методів стиску інформації. Ефективним способом захисту інформації є гравіювання даних з довготривалими псевдо хаотичними послідовностями, які від пакета до пакета є змінними. При цьому закони генерації абонентських псевдо послідовностей можуть бути різноманітними та локально визначеними на короткому інтервалі часу. Кодові ключі генерації абонентських псевдо послідовностей задаються бітами секретного ключа асиметричної криптосистеми. Для завадостійкого кодування інформаційних кадрів у залежності від якості каналу зв’язку доцільно використовувати різноманітні за ефективністю, швидкодією та складністю алгоритми Ріда − Соломона, каскадного кодування, турбокодування, багато порогового кодування[28]. Також в системах IoT важливим є перетворення дискретних даних та стиснення них в мережі інтернет речей. Існує багато різних методів для стиснення даних але було розглянуто основні з них.

IoT завжди має великий обсяг даних які передаються досить повільно, а пам‘ять та інші енергетичні ресурси досить дорогі і тому потрібно шукати вихід, а він полягає у тому, що дані, які будуть зберігати інформацію мають буди стиснені, що дозволить зменшити кількість даних, що передаються. Основним прикладом перетворень таких даних є дискретне перетворення Чебишева та дискретне конусне перетворення. Однак для різних типів перетворень оптимальними є різні типи сигналів, тому актуальним є пошук інших унітарних перетворень. Нижче ми розглянемо коротко методи, засновані на ДКП та ДПЧ[29].

Основну парну функцію Фур‘є для визначення апроксимації зображено на рисунку(формула 2.4.1)

$$s_f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos\left(\frac{\pi n t}{L}\right), \tag{2.4.4}$$

Даний вираз є інверсним та прямим ДКП сигналу. Пряме перетворення використовується для стиснення зі втратами вхідних даних.

Для того, щоб визначити поліноми першого виду та апроксимацію Чебишевського потрібно використати формулу яка зображена на формулі(2.4.5, 2.4.6)

$$T_n(t) = \frac{(-2)^n n!}{(2n)!}\sqrt{1-t^2}\,\frac{d^n}{dt^n}\left(\sqrt{1-t^2}\right)^{2n-1}, \tag{2.4.5}$$

$$s_c(t) = c_0 + \sum_{n=1}^{\infty} c_n T_n(t) \quad -1 < t < 1, \tag{2.4.6}$$

Дані два вирази вони ж повністю інверсними та прямими ДЧП сигналу. Також важливою особливістю Чебишевських поліноміальних апроксимацій є їх похибка яка становить -1<t<1. Також можливо написати програмний код, який дасть інформацію про складність даного алгоритму. Розглянуті методи для стиснення даних доцільно використовувати у бездротових IoT мережах для побудови розумної системи безпеки, на нижньому рівні архітектури, коли

формуються великі обсяги даних, пряме надсилання яких за протоколом MQTT є неефективним, оскільки йде велика затрата на електроенергію на роботу передавача та у разі спотворення пакету він буде змушений повторно відправити пакети. Завдяки стисненню даних зменшується обсяг даних, що надсилається, також загальні витрати на електроенергію теж зменшуються через низьке споживання сучасних пристроїв під час стиснення та завдяки модифікації алгоритму перетворення.

Для досягнення стиску даних на підставі ОДПЧ та ДКП, потрібно для розуміння розробити архітектуру в якій кожне перетворення матиме свої переваги і застосування на певних вхідних даних, а їх комплексне використання дозволить підвищити КС. Розроблена архітектура зображена(рис.2.4.4)

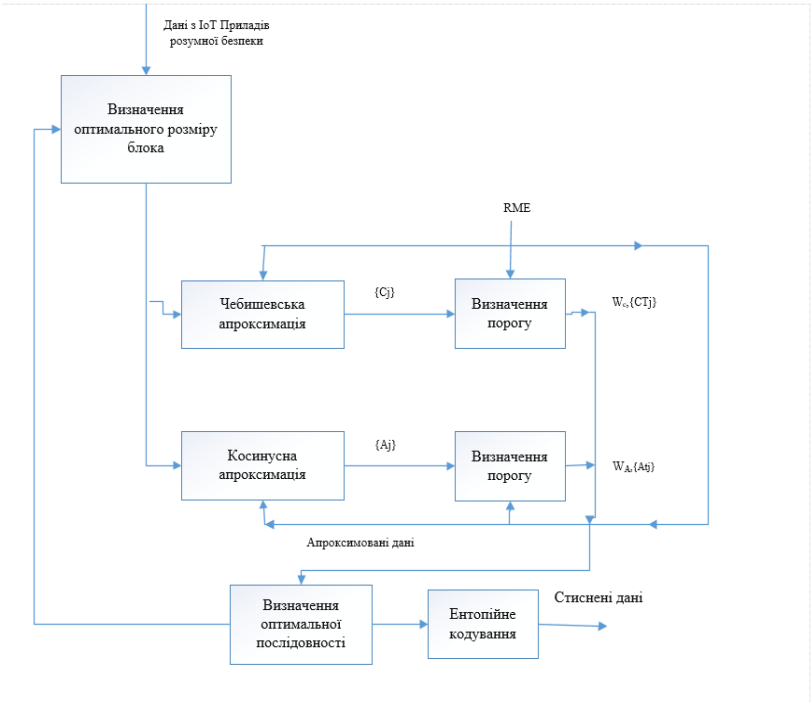


Рисунок 2.4.4. Функціональна архітектура адаптивних стиснень сигналів

Отже на першому кроці, для того щоб досягти максимального канального сигналу процесор підрахує ДКП та ОДПЧ для мінімального блогу даних, а максимальний розмір даних визначається найвищим степенем узагальненого поліному Чебишева, максимум може складати 64. Після проведених операцій буде отримано множини коефіцієнтів апроксимації A_i, C_i.

Для проведення апроксимації Чебишева та конусної апроксимації, потрібно використати алгоритм. Було використано для дослідження алгоритм чебишевської апроксимації[29].

Вхідні дані:[a;b] – інтервали апроксимації, - помилка апроксимації, яку потрібно задати користувачеві, наприклад p = 10^{-2}, n- кількість відділків сигналу $s(t_i)$.

Вихідні дані: $\{C_j\}$ – вектор коефіцієнтів чебишевської апроксимації.

Початок алгоритму для стиснення даних.

1. Потрібно зафіксувати порядок m=n.
2. Далі відбувається перетворення вхідних часових рядів в інтервалі [a;b]. Для цього потрібно використати формулу яка описана вище і знайти C_i використовуючи інтерполяцію вхідних даних.
3. Будуємо функцію, що апроксимує s. Для цього потрібно використати відповідну формулу.
4. Далі потрібно провести розрахунок RME.
5. І якщо значення RME< p, тоді потрібно призначити m=m-1 та повернутись до кроку 2.

   Кінець алгоритму чебишевської апроксимації.

Після проходження першого кроку, процесор відповідно до точності апроксимації вхідних даних створює дві підмножини коефіцієнтів $\{C_{Ti}\},\{A_{Ti}\}$ та контрольні слова W_C ,W_A . Елементи отриманих множин менша кількості елементів у апроксимуючих множинах коефіцієнтів. Також ненульовий біт у контрольних словах визначає стан ненульового елементу у вхідних множинах системи. Перший біт у контрольних множинах має бути рівний одиниці для ДКП та нулю для ОДПЧ. Після того як все підходить встановлюється подвоєний розмір блоку даних. Якщо ж новий розмір блоку менше за максимальний розмір, тоді потрібно повторити і пройти перший крок знову. Після кількох повторів досягається оптимальний КС, який відповідає оптимальному розміру блока даних.

На третьому кроці, за допомогою кодування, досягається додаткове стиснення і ми можемо надіслати дані до інших приладів, або зберегти їх у пам’яті. Операції кроків 1-3 повторюються для повно.

Отже в даному підрозділі було проаналізовано засоби для обробки інформації та розглянуто алгоритми для стиснення даних в системах IoT. Розглянуті методи стиснення даних доречно використовувати у бездротових системах безпеки, оскільки витрати на електроенергії зменшуються. Також алгоритми стиснення інформації збільшує продуктивність майже у три рази.

2.5 Комунікаційні технології та системи

Інтернет на даний момент складається з великої кількості наукових, корпоративних, комп’ютерних мереж. Об’єднання мереж різних архітектури і топології здійснюється за допомогою протоколів IP. Всім учасникам розумних системи присвоюється IP-адреса, ці адреса можуть бути тимчасовими або постійними. IoT системи також складаються з великої кількості мереж які взаємодіють між собою, також для інтернет речей проблема нестачі адрес може стати обмежуючим фактором. Проаналізувавши технології для зв’язку між розумними пристроями, було обрано технологію яка чудово піддійте для систем безпеки для приватної території прибудинкової території підприємства дана технологія має назву Zigbee. Дана технологія чудова для системи, оскільки система яка розробляється має короткий діапазон, також вона схожа на Bluetooth. Обрана технологія має несучу частоту 2,4 та споживає мало енергії, що робить систему енергоефективною. Мережа Zigbee може включати дуже велику кількість пристроїв і вона використовується в основному для домашніх систем автоматизації, розумна безпека, термостати або освітлення[30]. Zigbee - єдине повне рішення loT - від мережевої мережі до мови, яка дозволяє інтелектуальним об’єктам працювати разом. Вибрана технологія збільшить вибір та гнучкість та розробників та забезпечує впевненість у тому, що продукти та послуги будуть

працювати разом шляхом стандартизації та тестування всіх шарів стеку. Продукти, сертифіковані Zigbee, можуть зв’язуватися та спілкуватися на одній і тій же мові IoT між собою, а мільйони продуктів Zigbee вже розміщені в розумних будинках та будівлях. Zigbee створений з урахуванням сумісності назад і вперед. Мережевий протокол який був використаний в системі Zigbee. Для розробки було вибрано стандарт IEEE 802.15.4. Протокол сумісний взаємозв'язок для пристроїв передачі даних, що використовують низьку швидкість передачі даних, низьку потужність та низьку складність передач радіочастот короткого діапазону (РЧ) в дротовій менш персональній мережі (WPAN), були визначені в IEEE Std 802.15.4 . IEEE Std 802.15.4-2006. Стандарт забезпечує наднизьку складність, надвисоку вартість, надвисоке споживання енергії та низьку швидкість передачі даних бездротового зв’язку серед недорогих пристроїв. Швидкість вихідних даних достатньо висока (250 кб / с), щоб задовольнити набір програм, але також масштабована для потреб датчиків та потреб автоматизації (20 кб / с або нижче) для бездротового зв'язку. Крім того, один із альтернативних PHY забезпечує точну дальність вимірювання з точністю до одного метра. Кілька PHY визначені для підтримки різних діапазонів частот, включаючи - 868-868,6 МГц - 902-928 МГц - 2400-2483,5 МГц - 314-316 МГц, 430-434 МГц і 779-787 МГц для LR -WPAN системи в Ch. Також для шифрування інформації було використано симетричний алгоритм блочного шифрування, який також прийнятий як американський стандарт і він має назву AES-128. Безпечна форма шифрування, яка буде передавати інформацію в зашифрованому вигляді.

2.6 Висновок по розділу

Було побудовано 3D – модель підприємства, щоб забезпечити повну безпеку підприємства та його території. Датчики було розміщено енергоефективно, також було проаналізовано засоби для обробки інформації та розглянуто алгоритми для стиснення даних в системах IoT. В даному розділі було створено базу даних для системи

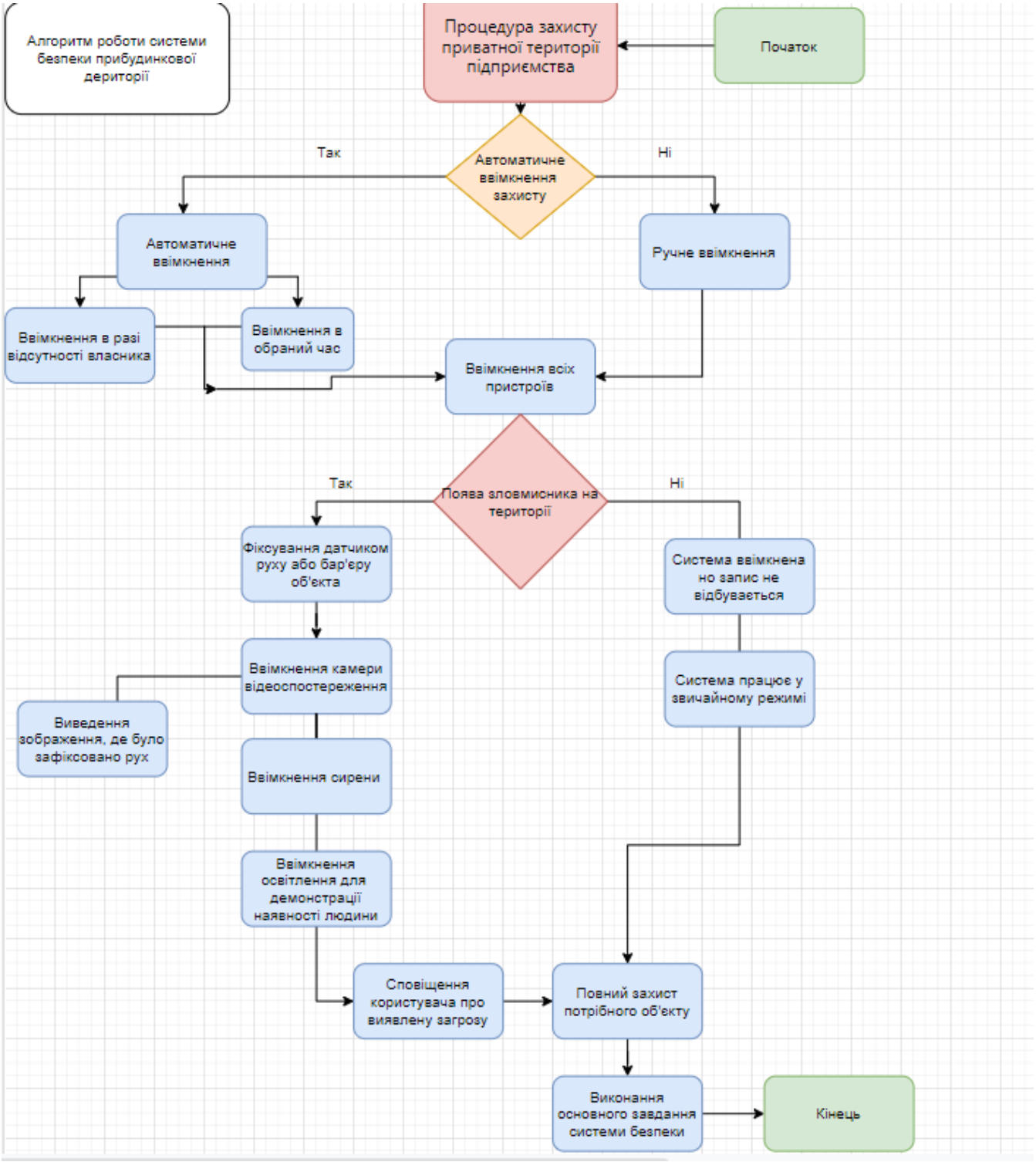
РОЗДІЛ 3. РЕАЛІЗАЦІЯ РІШЕННЯ ДЛЯ СИСТЕМИ БЕЗПЕКИ ПРИВАТНОЇ ТЕРИТОРІЇ ТА ЇЇ ОПИС

3.1 Алгоритм роботи системи

Алгоритми різних систем в IoT відіграють дуже важливу роль, оскільки алгоритм є записом послідовності вказівок, виконання яких призводить до розв'язання певних задач та функцій системи. Алгоритм – штучна конструкція, яку потрібно створити для досягнення основної мети системи безпеки прибудинкової території. Всі алгоритми будуються за певними правилами. Перше правило – під час будування алгоритму потрібно повністю проаналізувати систему, та що має бути на виході, оскільки система починає працювати тільки з деяким набором інформації теж саме відбувається з алгоритмом, ця інформація має назву вхідні дані[31]. Далі для того, щоб система працювала створеним алгоритмам потрібна пам'ять, оскільки там будуть зберігатись вхідні дані і вже відомо, що алгоритм починає свою роботу з цих даних, проміжні та вихідні дані, будуть результатом роботи системи та алгоритму. Пам'ять буде складатись з певних частин. Також створений алгоритм з блок-схем будується з окремих кроків та дій і після кожного кроку необхідно наголошувати, який крок виконується наступний та надати команду для зупинки алгоритму. Однією важливих функцій алгоритму є результативність. Він повинен завершувати основну функцію безпеки після кінцевого числа дій. При цьому встановити, який має бути результат алгоритму, тобто що вважається завершенням алгоритму[31].

Весь алгоритм системи подають в графічній формі – це подання алгоритму блок-схемою, оскільки їх зручно використовувати для пояснення роботи вже готового алгоритму. Блок-схема служить для зрозумілого зображення алгоритму роботи розумної системи, а не для ускладнення. Тоді кожну окрему вказівку потрібно записати у зображені геометричної фігури яка має певний вигляд, далі вони з'єднуються між собою стрілками і вони зображують напрям переходу для наступної вказівки. Отже було створено блок-схему алгоритму для системи

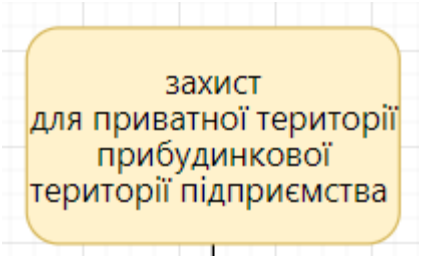
безпеки для приватної території прибудинкової території підприємства який повністю описує послідовність роботи системи та як вона працює, побудовану блок-схему зображено на рисунку(рис.2.6.1)



- Рисунок 2.6.1. Алгоритм роботи системи безпеки підприємства ”Примавера компані”.

Опис алгоритму розробленої системи:

Основним завданням цієї системи є забезпечення захисту для приватної території прибудинкової території підприємства і цей блок зображено на рисунку(див.рис.2.6.2)



Рисуно 2.6.2. Основне завдання

Система є повністю автоматизована однак, для цього її потрібно ввімкнути, але ввімкнення відбувається двома шляхами, перший – це автоматично, тобто в програмі задається час, коли людина відсутня або відпочиває і потрібно ввімкнути систему, а другій спосіб – це ввімкнення системи самостійно, тобто за допомогою мобільного пристрою або планшету. Дану блок-схему зображено на рисунку дивитись(рис.2.6.3).

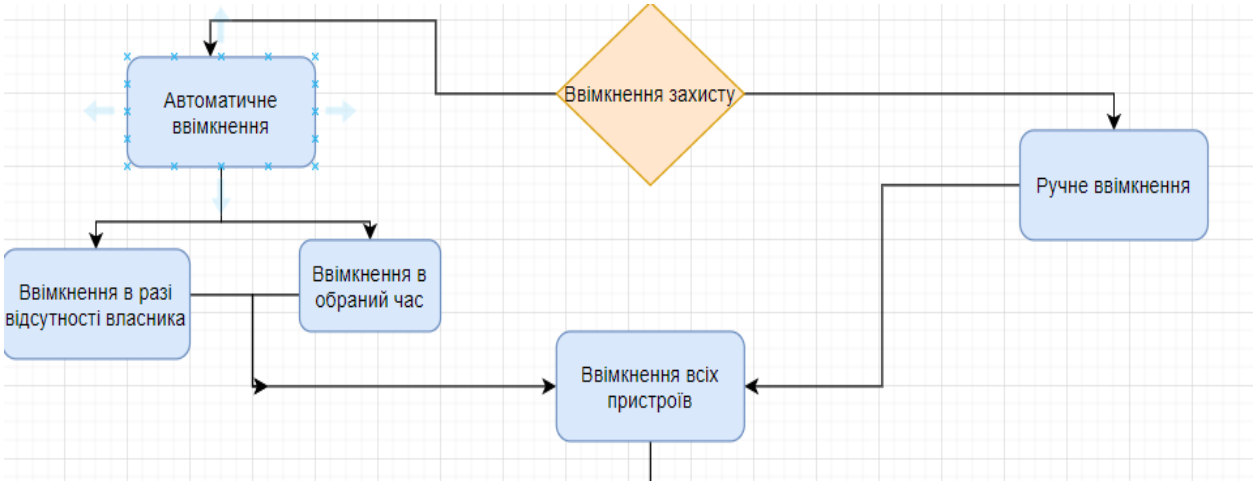


Рисунок 2.6.3. Варіанти включення системи

Після вибору варіанту для включення системи, йде ввімкнення всіх пристрої в. І тоді після цієї операції територія буде вважатись повністю захищеною і підприємство буде повністю в безпеці, а це основна ціль яку потрібно досягти.

Наступним кроком після ввімкнення системи є два варіанти подій, перший – це поява зловмисника на приватній території, а другій – це на території ніхто з по сторонніх осіб не з’являвся, зображено на рисунку (див.рис.2.6.4), в цьому випадку система буде працювати в звичайному режимі, користувач не буде отримувати сповіщення, оскільки територія в повній безпеці,

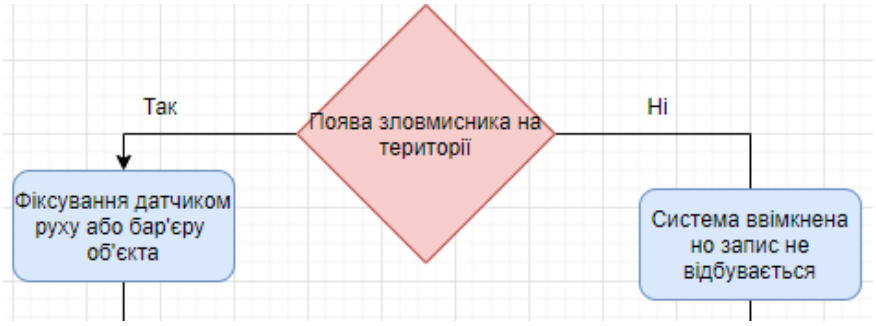


Рисунок .2.6.4. Алгоритм системи в основних варіантах подій на підприємстві”Примавера компані”

Як система зрозуміє, що зловмисник на території? Насправді система автоматично зрозуміє коли на території зловмисник, оскільки по периметру всієї території розташовані датчики периметру та датчики руху, після фіксування особи на розумних пристроях спрацьовує алгоритм захисту території. Даний алгоритм зображений на рисунку(див .рис .2.6.5)

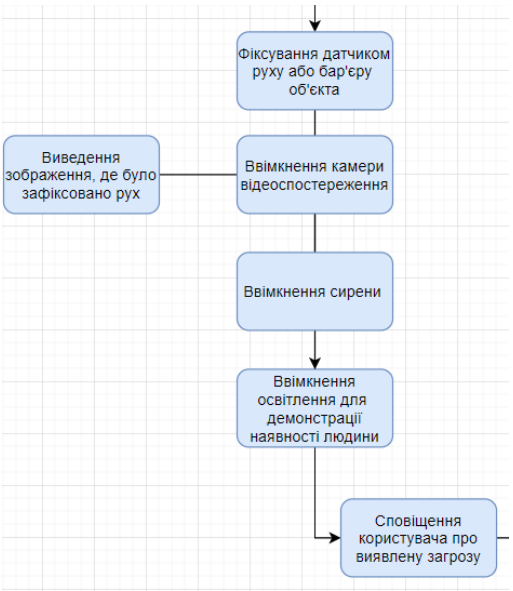


Рисунок. 2.6.5. Алгоритм захисту території підприємства “Примавера”

Після фіксування об’єкта датчиком руху або бар’єру, йде автоматичний захист території, оскільки в системі прописані сценарії роботи, в ході яких спрацьовують розумні пристрою, далі після фіксування вмикаються камери відеоспостереження, які розташовані на ділянки де спрацювали датчики руху або бар’єру, після ввімкнення камер вони автоматично виводять картинку з камер відеоспостереження на монітор, після цього йде автоматичне спрацьовування сирени.

Якщо зловмисники дізнались, що власник підприємства відсутній, тоді сирена не запобіжить вчиненню шкоди. Проаналізувавши всі можливі варіанти для забезпечення безпеки було розроблено хорошу альтернативу, яка з великим відсотком захистить територію і запобіжить вторгненню. І суть цього алгоритму ввімкнення світла в будинку або на підприємстві, а саме у кімнаті яка розташована біля розумних пристроїв, де було зафіксовано зловмисника. Чи буде в такому випадку система захищена? Так, оскільки зловмисники зрозуміють, що на підприємстві присутні особи. Даний алгоритм захисту зображено на рисунку(див.рис.2.6.6).

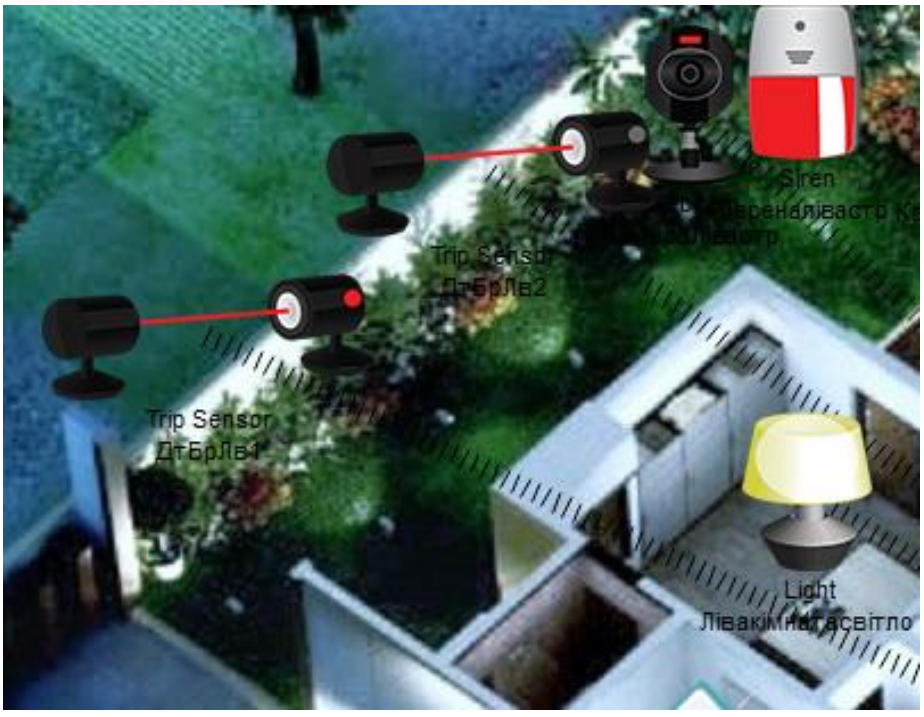


Рисунок 2.6.6. Спрацювання режиму захисту системи на підприємстві

Після спрацювання алгоритму користувач розумної системи отримає сповіщення на пристрій, після отримання даного сповіщення буде викликана поліція, що забезпечить повну безпеку приватної території прибудинкової території підприємства.

І після цього буде виконане основне завдання створеної системи, тобто забезпечити повну безпеку для підприємства та її території.

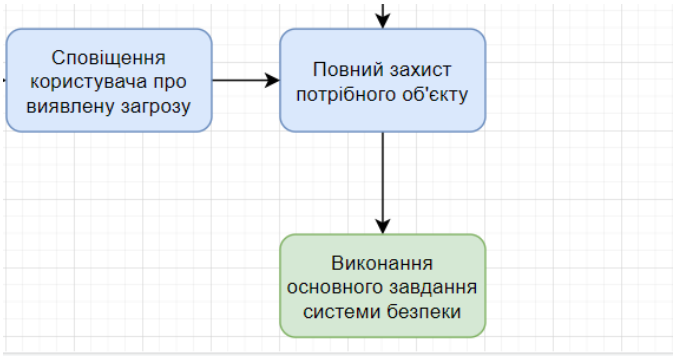


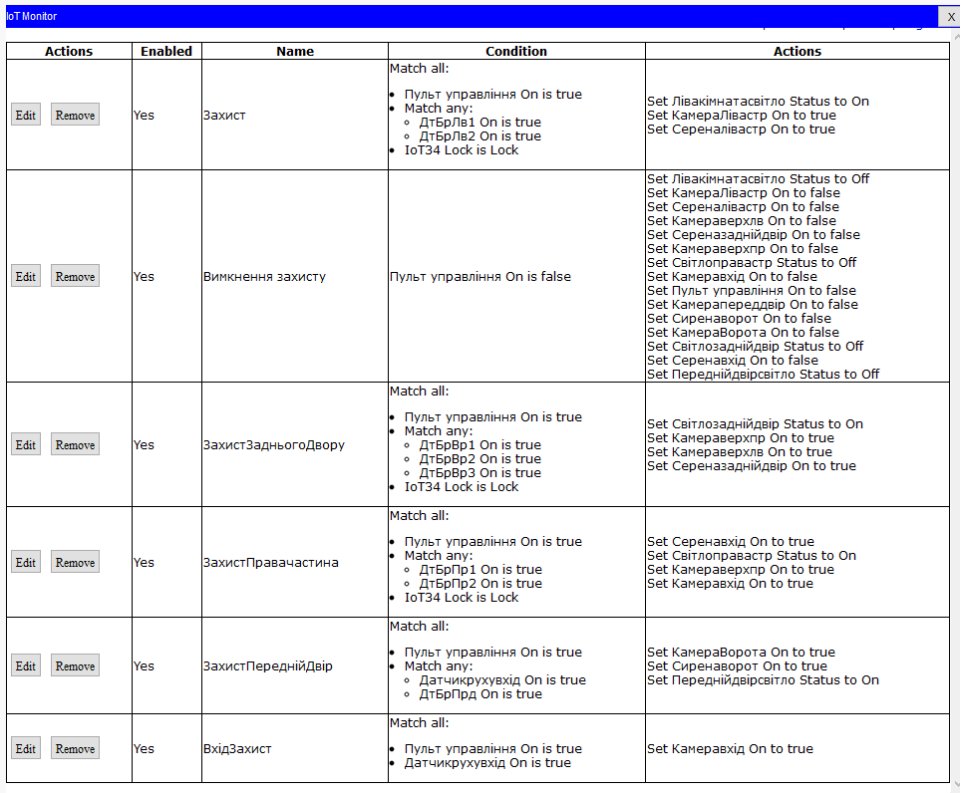
Рисунок 2.6.7. Виконання основного завдання системи

Також для створеної системи було написано сценарії роботи, оскільки в системі можливі різні варіанти безпеки.

3.2 Створення сценаріїв автоматизації для побудованої системи захисту

Розроблена система для безпеки для приватної території прибудинкової території підприємства, містить в собі автоматизацію, що дозволяє підняти рівень абстракції з рівня моделей і елементарних складових пристрої до рівня бізнес-процесів. В основі концепції лежить ідея створення блоку-схеми для будь-якого процесу, що містить певні значення і переходи між ними, за принципом кінцевих автоматів. Кожний сценарій автоматизації складається з точки запуску, змінних із відповідними значеннями прив'язки та вихідного коду. Також в системі є можливість створення бібліотечних сценаріїв які є багаторазовими фрагментами мови програмування, які сценарії автоматизації можуть викликати з тіла свій код.

При створені сценаріїв для системи безпеки потрібно задати точку запуску, це може бути або пульт або зачинені двері, а вже після цього потрібно налаштовувати та вказувати змінні, які визначають, як інформація передається або отримується зі сценарію в програмах майстра. Змінні не є обов'язковими, але коли ви використовуєте змінні, це спрощує кількість коду, який слід записати, і полегшує повторне використання коду. Для системи було створено сценарії автоматизації які повністю забезпечують безпеку підприємства і система є повністю автоматизована. Створені сценарії зображено на рисунку(рис.3.2.1)


IoT Monitor

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Захист	Match all: • Пульт управління On is true • Match any: ◦ ДтБрЛв1 On is true ◦ ДтБрЛв2 On is true • IoT34 Lock is Lock	Set Лівакімнатасвітло Status to On Set КамераЛівастр On to true Set СереналівастрOn to true
Edit Remove	Yes	Вимкнення захисту	Пульт управління On is false	Set Лівакімнатасвітло Status to Off Set КамераЛівастр On to false Set СереналівастрOn to false Set Камераверхлв On to false Set Сереназаднійдвір On to false Set Камераверхпр On to false Set Світлоправастр Status to Off Set Камеравхід On to false Set Пульт управління On to false Set Камерапереддвір On to false Set Сиренаворот On to false Set КамераВорота On to false Set Світлозаднійдвір Status to Off Set Серенавхід On to false Set Передній двірсвітло Status to Off
Edit Remove	Yes	ЗахистЗадньогоДвору	Match all: • Пульт управління On is true • Match any: ◦ ДтБрВр1 On is true ◦ ДтБрВр2 On is true ◦ ДтБрВр3 On is true • IoT34 Lock is Lock	Set Світлозаднійдвір Status to On Set Камераверхпр On to true Set Камераверхлв On to true Set Сереназаднійдвір On to true
Edit Remove	Yes	ЗахистПравачастина	Match all: • Пульт управління On is true • Match any: ◦ ДтБрПр1 On is true ◦ ДтБрПр2 On is true • IoT34 Lock is Lock	Set Серенавхід On to true Set Світлоправастр Status to On Set Камераверхпр On to true Set Камеравхід On to true
Edit Remove	Yes	ЗахистПередній Двір	Match all: • Пульт управління On is true • Match any: ◦ Датчикрухувхід On is true ◦ ДтБрПрд On is true	Set КамераВорота On to true Set Сиренаворот On to true Set Передній двірсвітло Status to On
Edit Remove	Yes	ВхідЗахист	Match all: • Пульт управління On is true • Датчикрухувхід On is true	Set Камеравхід On to true

Рисунок 3.2.1. Сценарії захисту підприємства

Було створено декілька сценаріїв, оскільки датчики знаходяться по всій території і для того щоб система працювала коректно, систему було розділено на частини.

Розглянемо один з сценаріїв захисту приватної території, наприклад захист правої частини підприємства.

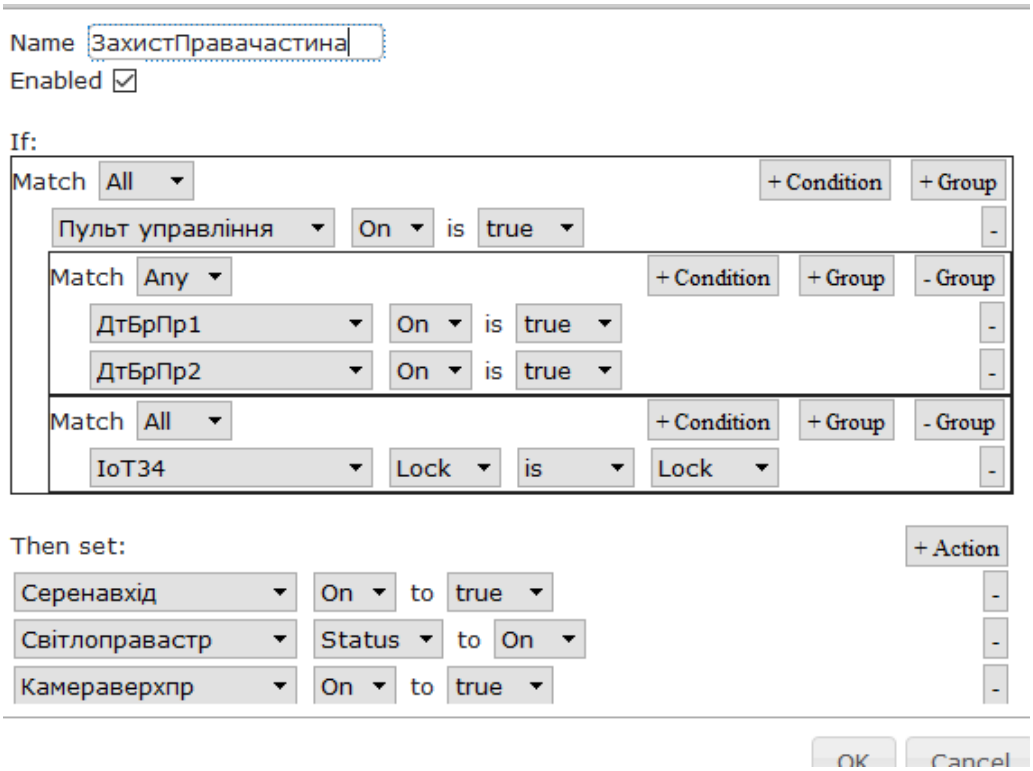


Рисунок 3.2.2. Сценарій захисту частини території підприємства

Система захисту буде працювати тільки тоді коли власник системи ввімкне в додатку бепеку та зачинить двері, це також буде зображено в додатку, даний приклад зображено на рисунку(3.3.3)

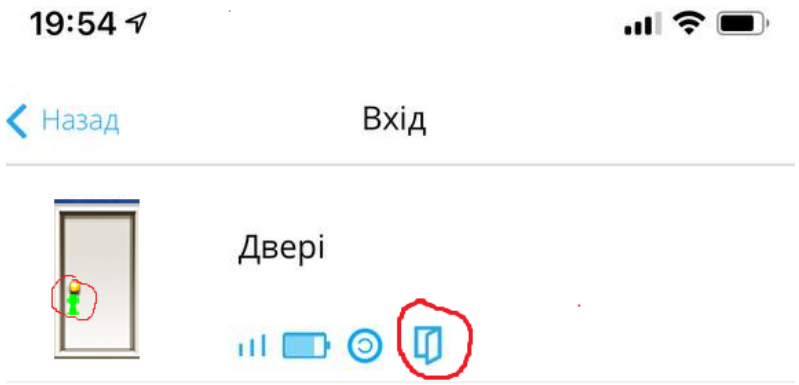


Рисунок 3.2.3. Сповіщення про відчинені двері.

Після ввімкнення системи, безпека території забезпечена, оскільки були розроблені сценарії взаємодії пристроїв, також для більш зрозумілого зображення роботи сценарцію було створено блок-схему. Створену схему зображено на рисунку (рис.3.3.4)

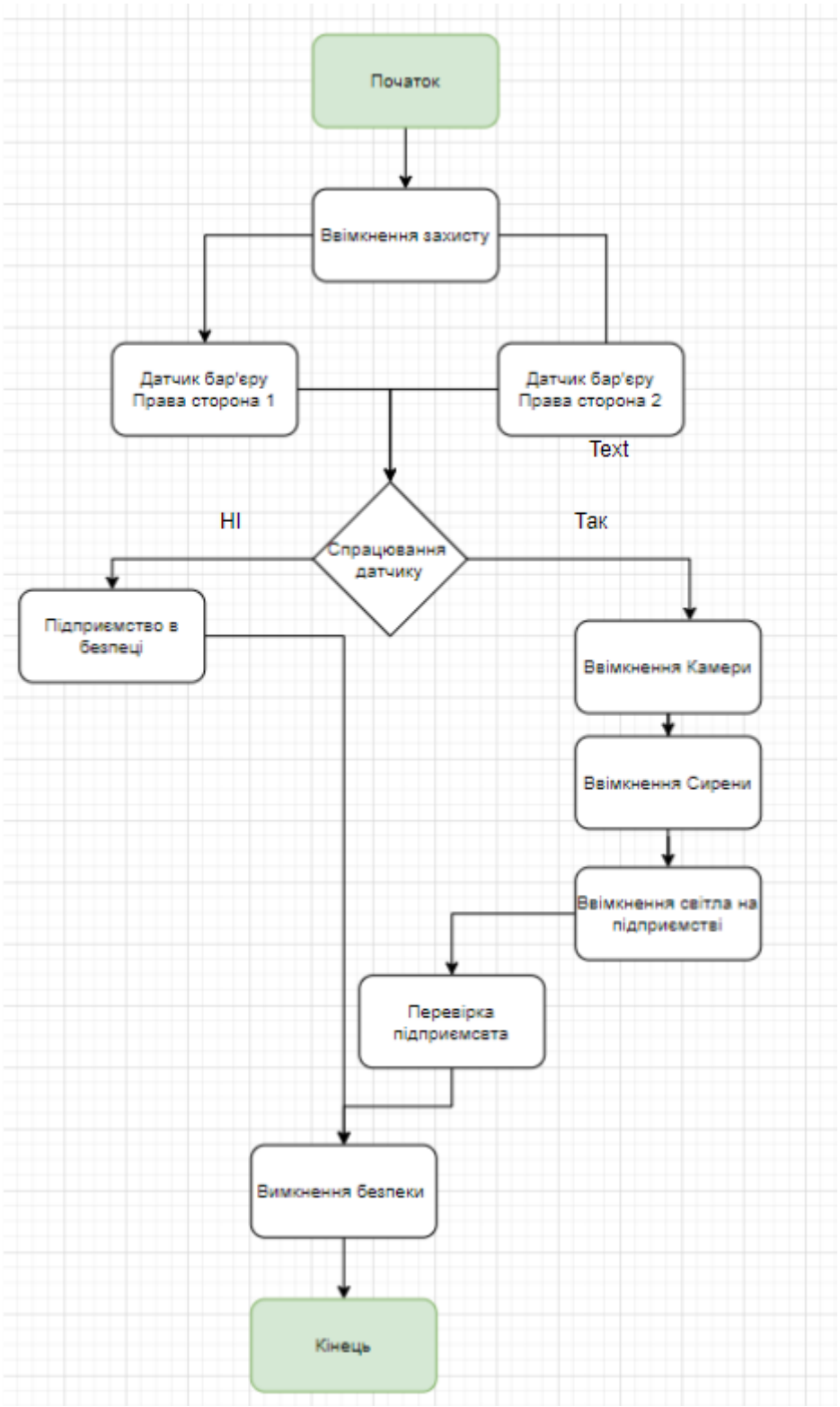


Рисунок 3.2.4. Алгоритм захисту частини території підприємства

Отже в даному підрозділі було описано та створено сценарії автоматизації системи для приватної території прибудинкової території підприємства. Було

прописано всі можливі варіанти подій, також дані сценарії забезпечать безпеку обраного підприємства.

3.3 Опис процесу розробки програмного інтерфейсу для перегляду бази даних

Для того ,щоб увійти на головну сторінку потрібно пройти автентифікацію(Рис.3.2.1)

Для цього потрібно ввести логін і пароль який задав собі користувач і написнути кнопку”Sing in”

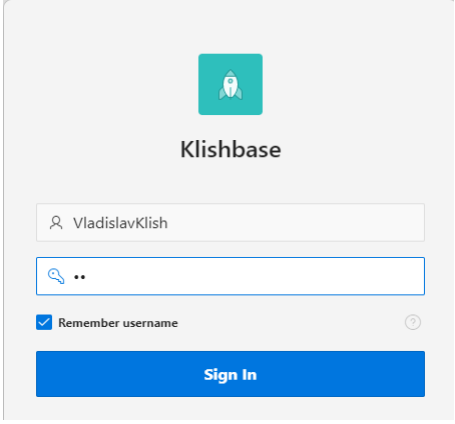


Рисунок 3.3.1. Вікно автентифікації

Після того як користувач авторизувався з'явиться головне меню,в якому знаходяться всі створені таблиці бази даних (Рис.3.3)

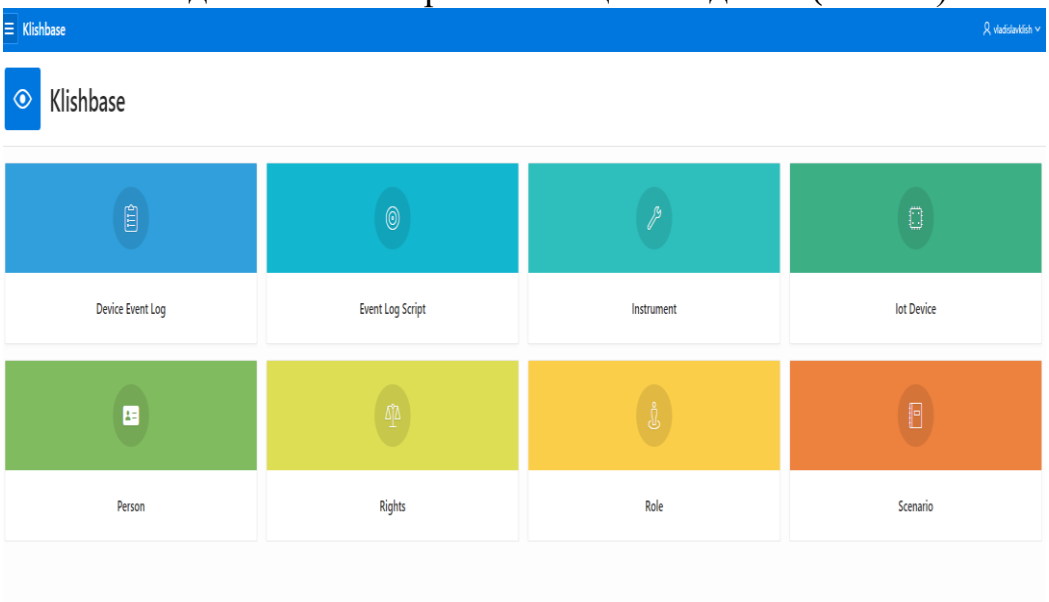


Рисунок 3.3.2. Головна сторінка

Головне меню містить такі таблиці:

1. Person(Користувач).
2. IOT_Device(Іот прилад).
3. Role(Роль).
4. Rights(Права).
5. Status device(Статус пристрою).
6. Scenario(сценарій).
7. Instrument(Інструмент).
8. Devicelog(Журнал пристрою).
9. Eventscript(Скрипт події).

Також у лівій верхній частині меню можна знайти меню навігації за допомогою якого буде зручніше знайти потрібну таблицю (Рис.3.4). Дані мманіпуліції дають змогу користувачеві системи переглянути всі можливі пристрої та стан системи. Меню яке було створено легке в користувані новим користувачам

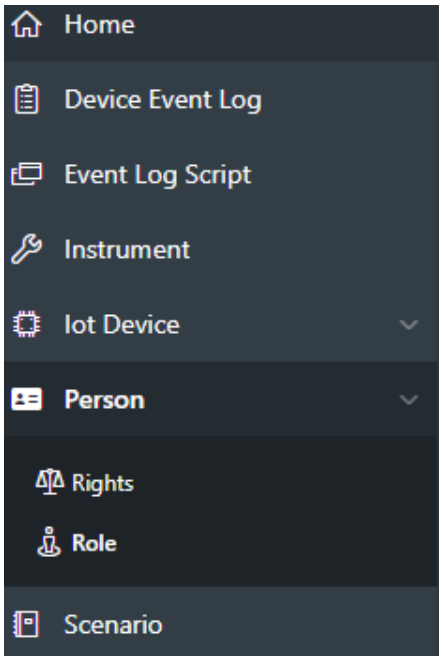


Рисунок 3.3.3. Меню навігації

Для перегляду таблиць потрібно натиснути на потрібну таблицю лівою кнопкою миші(рис.3.5)

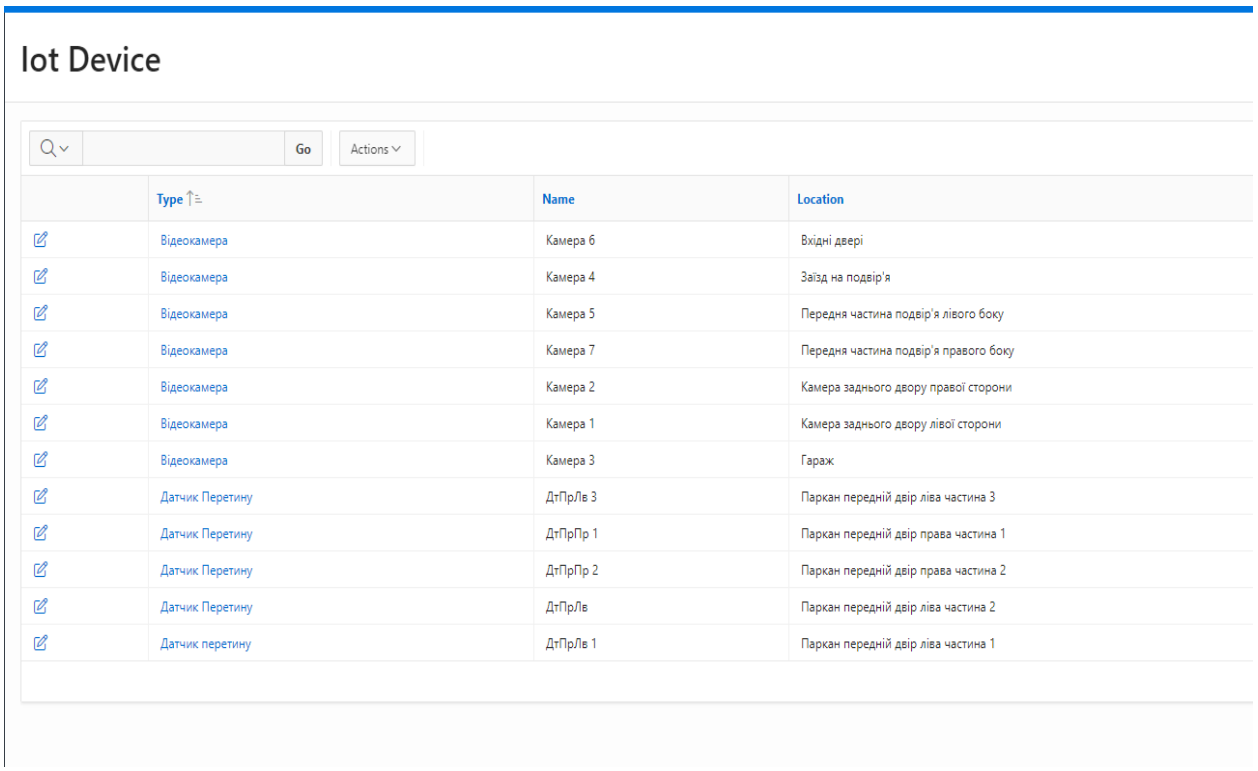


Рисунок 3.3.4. Перегляд даних таблиці “Iot Device”

Для того ,щоб додати нові дані в таблицю потрібно написнути кнопку “Create” яка знаходиться у правому верхньому куті(рис.3.6.)

Далі потрібно вписати потрібні дані у спеціальні поля і натиснути кнопку “Create”(рис.3.6.).

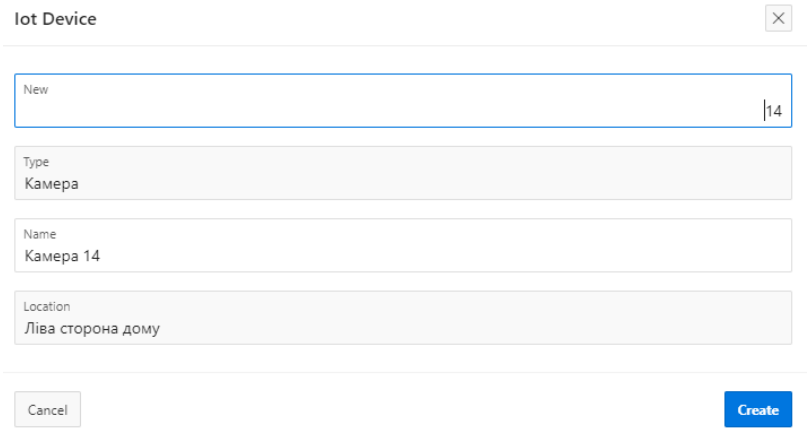


Рисунок 3.3.5. Створення новго запису

Для перевірки потрібно оновити сторінку і дані будуть оновлені

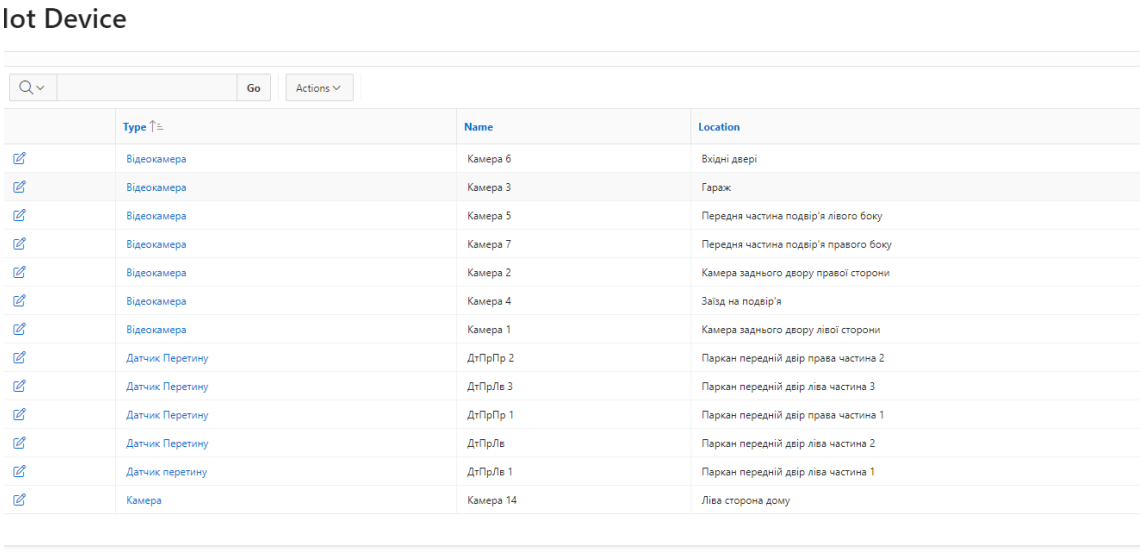


Рисунок 3.3.6. Перегляд нових даних

Для видалення даних треба обрати рядок який буде видалено і зліва натиснути на піктограму редагування(Див. Рис. 3.8)

Рисунок 3.3.7. Кнопка для видалення елементу

3.4 Опис мобільного додатку для керування системою

Мобільний додаток є чудовим рішенням та способом для контролю системи. Через додаткі можливо зробити велику кількість дій, від перегляду компонентів системи так і для постановки і зняття підприємства з охорони, перевіряти кількість заряду, рівень сигналу. Також програма може надсилати повідомлення про тривогу у вигляді повідомлень в мобільний додаток, або телефонує на номер власника системи. Вибрати спосіб також можливо у додатку. Додаток в розумних системах відіграє дуже важливу роль, він робить систему автоматизованою та зручною в моніторингу. Отже для системи безпеки для приватної території прибудинкової території підприємства було написано мобільний додаток для перегляду системи її компонентів і для постановки і зняття підприємства з охорони. Для створення додадку було використано програму Mit

App Inventor – це онлайн- платформа, яка призначена для розробки мобільних додатків[40]. Дана програма розрахована на користувачів Android, але команда розробників зробила даний продукт і для користувачів IOS і тепер вона доступна в Apple App Store[42]. Середовище розробки являє собой простий додаток для створення інтерфейсу. За допомогою цього середовища можливо зробити додаток для керування автомобілем. Отже було розроблено додаток для керування системою безпеки. Для того щоб підгрузити наш додаток на телефон або планшет потрібно ввести код або просканувати QR-код і лише після того дані почнуть підгружатись це зображено на рисунку(рис.3.4.1)

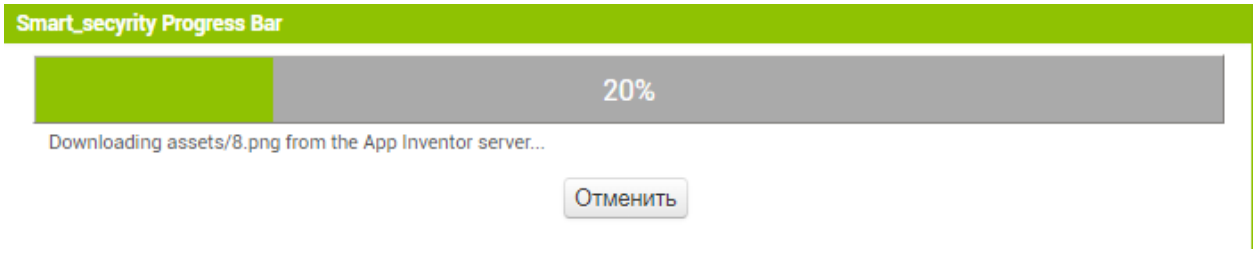


Рисунок 3.4.1. Встановлення додатку

Після загрузки додаток успішно буде встановлений на пристрій і після того вже можливо керувати системою. Головна сторінка додатку містить в собі кнопки для встановлення режиму безпеки та її вимкнення, також вона містить ще кнопки для перегляду всіх пристроїв, роботу системи її огляд та можливість ввімкнути режим тривоги. Також для користувачів було розроблені сповіщення, тобто коли користувач захоче переглянути робочу систему йому повідомлять що система не працює, також в додатку зрозуміло коли система працює, оскільки після встановлення режиму захисту або зняття з охорони користувачу системи вискочить повідомлення про її стан, це зображено на рисунку(рис.3.4.2).

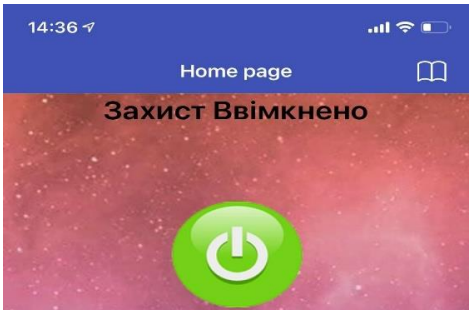


Рисунок 3.4.2. Повідомлення про стан системи

Тільки після того користувач ввімкнув систему, у нього буде можливість переглянути робочу систему. Додаток створений для нових користувачів, оскільки він простий в користуванні та має зрозумілий інтерфейс, головну сторінку додатку зображено на рисунку(рис 3.4.3)

Рисунок 3.4.3. Головна сторінка додатку

Після переходу на вкладку пристрої, користувачу системи буде показано всі його розумні пристрої та їх місце знаходження на підприємстві, це зображено на рисунку(рис.3.4.4).

Рисунок 3.4.4. Пристрої системи

Також вкладка пристрої містить в собі кнопки для взаємодії, вона містить кнопку головна, що поверне користувача на головну сторінку, приклад робочих пристрої, дана вкладка розрахована на нових користувачів, оскільки там містяться зображення ввімкнених пристроїв, ламп, сирен, відеокамер.

Рисунок 3.4.5. Приклад робочих пристроїв.

Далі програма також містить в собі сторінку, в якій можливо переглянути своє підприємство та розташування пристроїв на ньому(рис.3.4.6)

Рисунок 3.4.6. Огляд підприємства

На рисунку(рис.3.4.6) зображено сторінку додатку на якій можливо переглянути своє підприємство, також вона містить в собі кнопки кожна з яких відповідає за певну функцію, система з пристроями зображує підприємство на якому вже розташовані всі наші пристрої, режим тривоги зображує як буде поводити себе система в разі режиму тривоги, пристрої системи відкриє вище описану сторінку яка зображена на рисунку(див.рис.3.4.4), а кнопка головна поверне користувача на головну сторінку системи. Було створено на описано додаток для системи безпеки підприємства, що надає користувачу низку переваг, від поставки до зняття з охорони об’єкта, було описано повністю програму та під’єднання її на смартфон планшет або пк. Створений додаток наддасть власнику системи всю інформацію про пристрої системи та їх розташування.

Рисунок 3.4.7. Огляд підприємства з пристроями

Сторінка яка зображена на рисунку(див.рис.3.4.7) дає користувачу системи зрозуміти, де знаходяться розумні пристрої та датчики на підприємстві.

Отже, в даному підрозділі було описано програмний продукт для створення мобільних додатків, пультів керування, калькуляторів. Також в даному підрозділі

3.5 Висновок по розділу

В третьому розділі було описано алгоритм роботи системи безпеки. Було побудовано блок-схеми системи, також було налаштовано програму в Packet Tracer. Було створено логіку роботи системи, створено сценарії роботи системи в Packet Tracer та описано їх роботу, було розроблено в середовищі Apex інтерфейс для моніторингу системи, також за допомогою блок-схем описано сценарій захисту підприємства та його території, в якій зображено послідовність дій системи. Також було створено додаток для мобільних пристроїв, який допоможе здійснювати контроль постановку та зняття охорони для підприємства, описано середовище розробки даного додатку.

ВИСНОВОК

У кваліфікаційні роботі бакалавру було створено систему для приватної території прибудинкової території підприємства для забезпечення безпеки. Також було виконано всі поставлені завдання:

- Розроблено фізичну та логічну модель бази даних для підприємства ”Примавера компані”.
- Розроблено 3D-модель підприємства.
- Вибрано для системи розумні пристрої.
- Розміщено пристрої на підприємстві.
- Створено сценарії роботи системи.
- Розроблено інтерфейс для перегляду бази даних підприємства ”Примавера компані”.
- Розроблено мобільний додаток для керування системою безпеки підприємства.

Перед тим як було розпочато розробку системи було проаналізовано способи забезпечення безпеки, також було проаналізовано актуальність систем безпеки та основну задачу безпеки. В першому розділі було проаналізовано книги, статті та різні роботи для вирішення проблеми безпеки, також було проаналізовано готові рішення безпеки та представлені найкращі представники які існують на даний час у сфері безпеки території підприємства. Відбувся аналіз комунікаційних технологій та систем, отже в першому розділі відбувся аналіз систем та їх компонентів. У другому розділі було описано створення проекту та опис програми для контролю розробки системи безпеки для приватної території прибудинкової території підприємства. Відбувся опис та вибір розумних пристроїв для системи безпеки далі було обрано ПО в якому було побудовано підприємство в 3D та його зовнішню територію, далі було описано середовище в якому розроблялась система безпеки та розміщення всіх пристроїв на території підприємства, після всіх операцій відбулось проектування контекстної, логічної та фізичної моделі бази даних та описано обрані методи та засоби обробки і стиснення інформації

для системи безпеки. Також в даній роботі було описано алгоритм роботи захисту підприємства та зображення у вигляді блок-схем, також для системи було написано сценарії роботи, що робить систему автоматизованою, також було створено веб-інтерфейс для неї в Oracle APEX, було детально описано процес створення веб-інтерфейсу, також для системи безпеки для приватної території прибудинкової території підприємства було створено мобільний додаток для керуванням системою та перегляд стану пристрої і їх опис. Під час виконання роботи всі поставлені завдання були виконані, системи безпеки для приватної території прибудинкової території підприємства була створена, що забезпечить повну безпеку підприємству. Всі пристрої були підключені створені додатки для моніторингу та налаштовано сценарії роботи системи.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Система безпеки та захисту(Security and protection system)[Електроннний ресурс] / Режим доступу: https://www.britannica.com/technology/security-and-protection-system (дата звертання 05.03.2021)

2. Wyze Cam v3 review: This security camera now goes inside or outside [Електроннний ресурс] / Режим доступу : https://www.cnet.com/home/security/wyze-cam-v3-review/ (дата звертання 05.03.2021)

3. Vivint Home Security System Review and Prices[Стаття] / Режим доступу: https://www.usnews.com/360-reviews/home-security/vivint(дата звертання 05.03.2021)

4.Bezpeka.club [Електроннний ресурс] / Режим доступу: https://bezpeka.club/ru/pidvyshhennya-bezpeky-viddalenyh-obyektiv-hikvision-na-sonyachnyh-batareyah/ (дата звертання 05.03.2021)

5. Dahua Technology Launches Cooper-I Series XVR to Enrich AI Product Range [Електронний ресурс] / Режим доступу: https://www.dahuasecurity.com/newsEvents/pressRelease/4917 (дата звертання 05.03.2021)

6. Frontpoint Home Security System [Електронний ресурс] / Режим доступу :

https://www.safehome.org/security-systems/frontpoint/ (дата звертання 06.03.2021)

7. What is Perimeter Security? [Електронний ресурс] / Режим доступу : https://www.techslang.com/definition/what-is-perimeter-security/ (дата звертання 06.03.2021)

8. Dahua Eureka Series Thermal Camera Defines Perimeter Intrusion Detection [Електронний ресурс] / Режим доступу : https://www.dahuasecurity.com/newsEvents/pressRelease/4907 (дата звертання 06.03.2021)

9. Frontpoint Home Security System [Електронний ресурс] / Режим доступу : https://www.safehome.org/security-systems/frontpoint/ (дата звертання 08.03.2021)

10. Firewall [Електронний ресурс] / Режим доступу : https://www.techopedia.com/definition/5355/firewall (дата звертання 08.03.2021)

11. Vivotek представляє нову камеру відеоспостереження з технологією Trend Micro IoT Security[Електронний ресурс] / Режим доступу : https://worldvision.com.ua/ua/vivotek-predstavlyaet-novuu-kameru-videonabludeniya-s-tekhnologiey-trend-micro-iot-security/ (дата звертання 08.03.2021)

12. Ring – Most Affordable [Електронний ресурс] / Режим доступу :

https://www.safehome.org/doorbell-cameras/ring/ (дата звертання 08.03.2021)

13. Arlo Security Camera System [Електронний ресурс] / Режим доступу : https://www.arlo.com/en_eu/home (дата звертання 06.03.2021)

14. HagroyHR-10000 [Електроннний ресурс] / Режим доступу: http://perimetr.ua/index.php/oborudovanie-ohranyi-perimetra/Электрошоковые-системы/Электрошоковая-система-охраны-периметра-hagroy-hr-10000/29-44& (дата звертання 06.03.2021)

15. Z-Wave explained: What is Z-Wave and why is it important for your smart home? [Електроннний ресурс] / Режим доступу: https://www.the-ambient.com/guides/zwave-z-wave-smart-home-guide-281 (дата звертання 08.03.2021)

16. Wyze Home Monitoring Review [Електроннний ресурс] / Режим доступу: https://www.pcmag.com/reviews/wyze-home-monitoring (дата звертання 08.03.2021)

17. Outfitting Your Smart Home: Zigbee Devices [Електроннний ресурс] / Режим доступу: https://www.safewise.com/zigbee-devices/ (дата звертання 08.03.2021)

18. ADT Home Security [Електроннний ресурс] / Режим доступу: https://www.adt.com/(дата звертання 10.04.2021)

19. Dsc adt wireless touchscreen keypad [Електроннний ресурс] / Режим доступу: https://zionssecurity.com/product/dsc-adt-wireless-touchscreen-keypad/ ()

20. eMACROS 1/2 Mile Solar Driveway Alarm Motion sensor [Електроннний ресурс] / Режим доступу: https://www.emacros.com/collections/driveway-alarm/products/emacros-no-diy-security-alert-system-monitor-wireless-solar-driveway-alarm-no-need-to-replace-battery

21. Home Security Systems [Електроннний ресурс] / Режим доступу: http://cteksecurity.com/?page_id=52

22. Brink's Home Security System [Електроннний ресурс] / Режим доступу: https://www.safehome.org/security-systems/brinks/

23. Проектний аналіз (2000) [Електроннний ресурс] / Режим доступу: https://library.if.ua/book/134/9098.html

24. Стариковский А.В. Исследование уязвимостей систем умного дома [Книга] // Спецтехника и связь. 2012. №2. С. 55-57

25 AJAX StarterKit [Електроннний ресурс] / Режим доступу: https://alarm.bezpeka.systems/ua/?gclid=Cj0KCQjws-oebhckarisaphokiyjq4ftt6czhkorazzuxx9renijgywibhwek10qb7liucw1t5pe-tgaaoadealw_wcb

26. Microsoft Visio [Електроннний ресурс] / Режим доступу: https://uk.wikipedia.org/wiki/Microsoft_Visio

27. Шевчук Б.М. Теоретичні основи побудови високоінформативних інтелектуальних радіомереж обробки і передачі інформації // Праці міжнар. конф. "Питання оптимізації обчислень (ПОО-XX111)". – К.: Ін-т кібернетики ім. В.М. Глушкова НАН України. – 2007. – С. 310–311 OFDM (Orthogonal Frequency Division Multiplexing) (дата звертання 12.04.2021)

28.Комп’ютерні засоби, мережі та системи [Електроннний ресурс] / Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/6525/11-Chevchuk.pdf?sequence=1(дата звертання 12.04.2021)

29.Метод стиснення даних у мережі інтернет [Електроннний ресурс] / Режим доступу: http://nti.khai.edu:57772/csp/nauchportal/Arhiv/REKS/2020/REKS420/Manzhos.pdf(дата звертання 12.04.2021)

30. Comparison of Wireless Technologies [Електронний ресурс]. Режим доступу: https://predictabledesigns.com/wireless_technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/(дата звертання 12.04.2021)

31. Основи алгоритмізації та програмування [Електроннний ресурс] / Режим доступу: http://lib.mdpu.org.ua/e-book/osnovy_informatyky/Lesson6.htm(дата звертання 20.04.2021)

32. Смарт-лампочка Aqara HomeKit Smart LED Light Bulb ZigBee / Режим доступу:https://rozetka.com.ua/258740861/p258740861/?gclid=cj0kcqjwwlkfbhdparisapzpiidbl2rpog44qbukjgcrkewar7v97qx0tevqk_yhcqties6cuxeetkaapenealw_wcb (дата звертання 12.04.2021)

33. Методи забезпечення безпеки розумного будинку [Електроннний ресурс] / Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/119

34.Cisco Packet Tracer [Електроннний ресурс] / Режим доступу: https://www.netacad.com/ru/courses/packet-tracer (дата звертання 14.04.2021)

35.Cisco Packet Tracer [Електроннний ресурс] / Режим доступу: https://ru.wikipedia.org/wiki/Cisco_Packet_Tracer36. (дата звертання 14.04.2021)

37.Apex oracle [Електроннний ресурс] / Режим доступу: https://apex.oracle.com/en/(дата звертання 14.04.2021)

38. Руководство Oracle APEX для начинающих[Електроннний ресурс] / Режим доступу: (APEX 5.0)https://betacode.net/10345/oracle-apex-tutorial-for-beginners

39. Фізична модель бази даних[Електроннний ресурс] / Режим доступу: https://lib.chmnu.edu.ua/pdf/metodser/172/10.pdf (дата звертання 12.04.2021)

40. MIT App Inventor[Електроннний ресурс] / Режим доступу: https://appinventor.mit.edu (дата звертання 12.04.2021)

41. Getting Started with MIT App Inventor [Електроннний ресурс] / Режим доступу: https://appinventor.mit.edu/explore/get-started(дата звертання 12.04.2021)

42.AppStore Preview [Електроннний ресурс] / Режим доступу:https://apps.apple.com/us/app/mit-app-inventor/id1422709355(дата звертання 12.04.2021)

43. Draw.io - Diagrams.net [Електроннний ресурс] / Режим доступу: https://app.diagrams.net(дата звертання 20.04.2021)

44. App Inventor[Електроннний ресурс] / Режим доступу: https://uk.wikipedia.org/wiki/App_Inventor (дата звертання 20.04.2021)

45. Нерівність Чебишова [Електроннний ресурс] / Режим доступу: https://uk.wikipedia.org/wiki/Нерівність_Чебишова(дата звертання 24.04.2021)

46. Ряди Фур'є. Перетворення Фур'є [Електроннний ресурс] / Режим доступу: http://www.dstu.dp.ua/Portal/Data/3/21/3-21-kl35.pdf (дата звертання 24.04.2021)

47. Розробка та імплементація мобільних додатків та IoT пристроїв з метою інформатизації суспільства [Електроннний ресурс] / Режим доступу: https://buki.com.ua/blogs/rozrobka-ta-implementatsiya-mobilnykh-dodatkiv-ta-iot-prystroyiv-z-metoyu-informatyzatsiyi-suspilstva/(дата звертання 24.04.2021)

48. Дослідження процесів захисту інформації в іothttps://conf.ztu.edu.ua/wp-content/uploads/2019/06/38-1.pdf(дата звертання 24.04.2021)

49. internet of things [Електроннний ресурс] / Режим доступу: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT(дата звертання 24.04.2021)

50. ioT technology stack [Електроннний ресурс] / Режим доступу https://www.i-scoop.eu/internet-of-things-guide/iot-technology-stack-devices-gateways-platforms/(дата звертання 24.04.2021)

ДОДАТОК А

Рисунок А 1 – Слайд 1 Тема доповіді

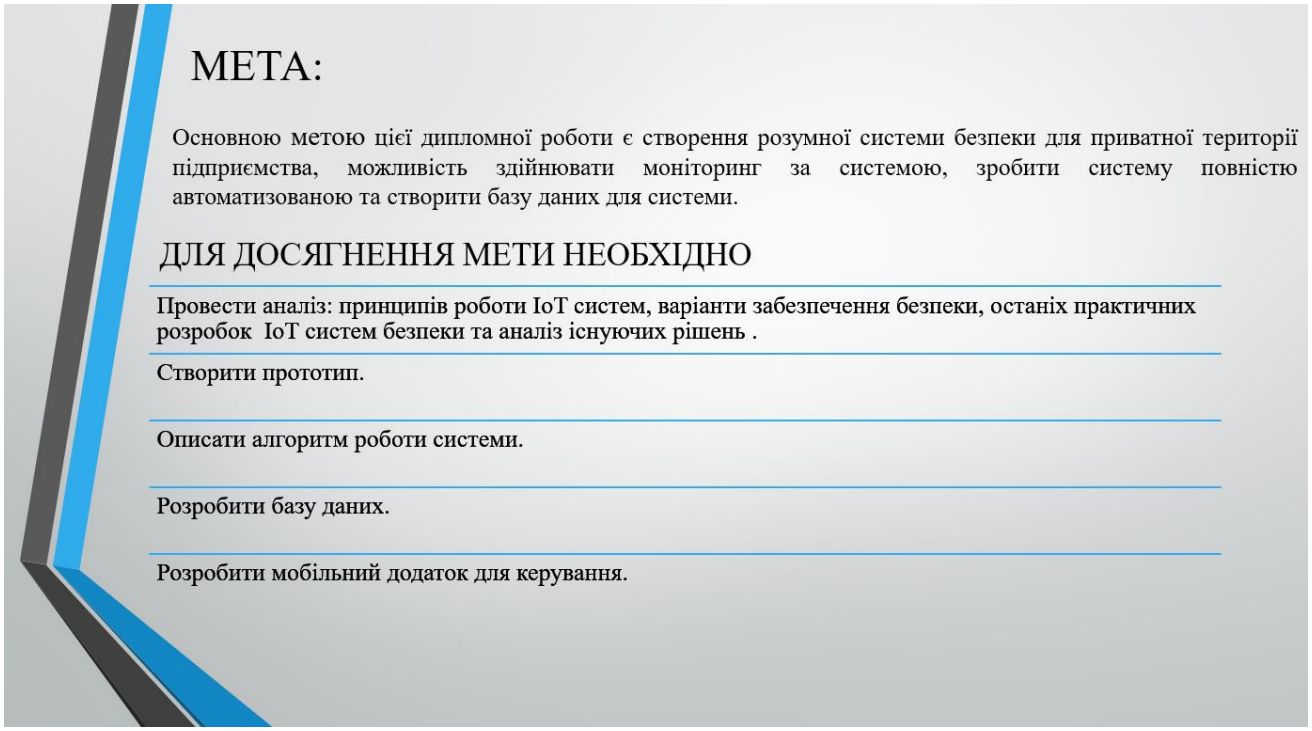


Рисунок А 2 – Слайд 2 Мета роботи

Рисунок А 3 – Слайд 3 Актуальність

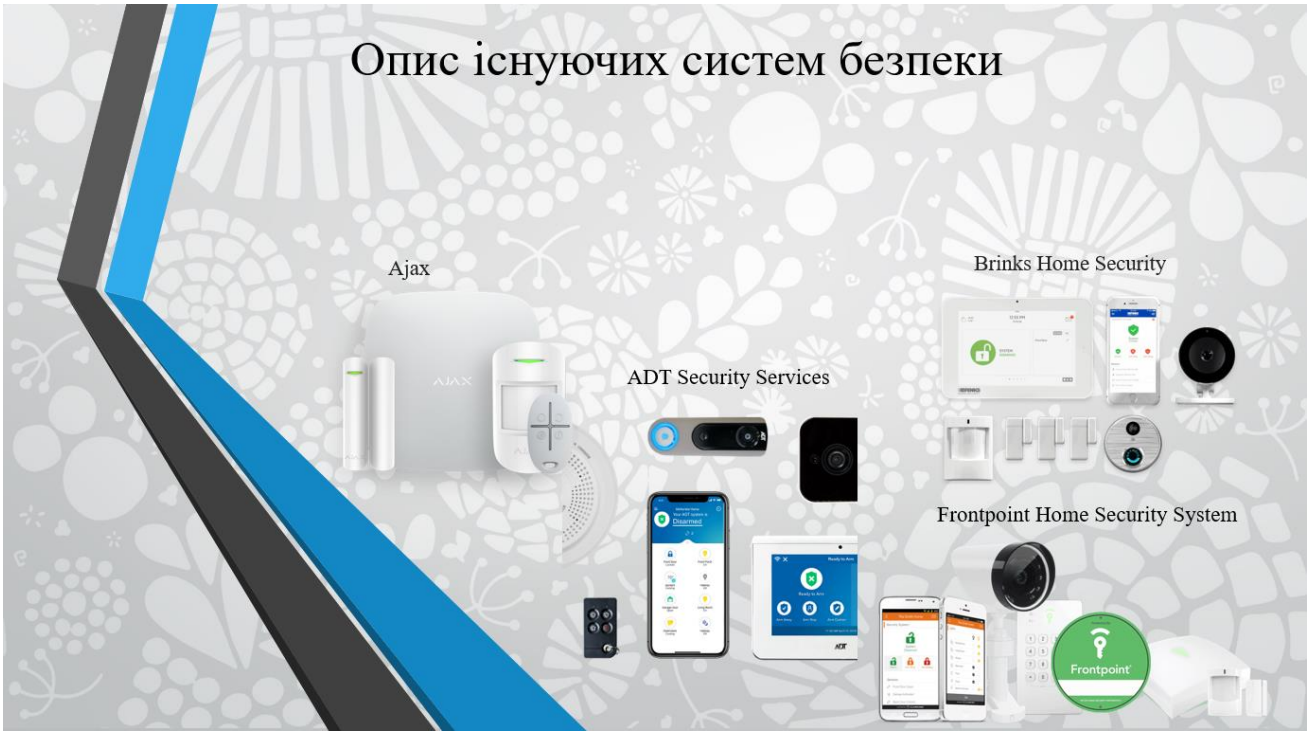


Рисунок А 4 – Слайд 4 Опис існуючих систем

Рисунок А 5 – Слайд 5 Підбір обладнання для системи безпеки

Рисунок А 6 – Слайд 6 Розміщення пристроїв

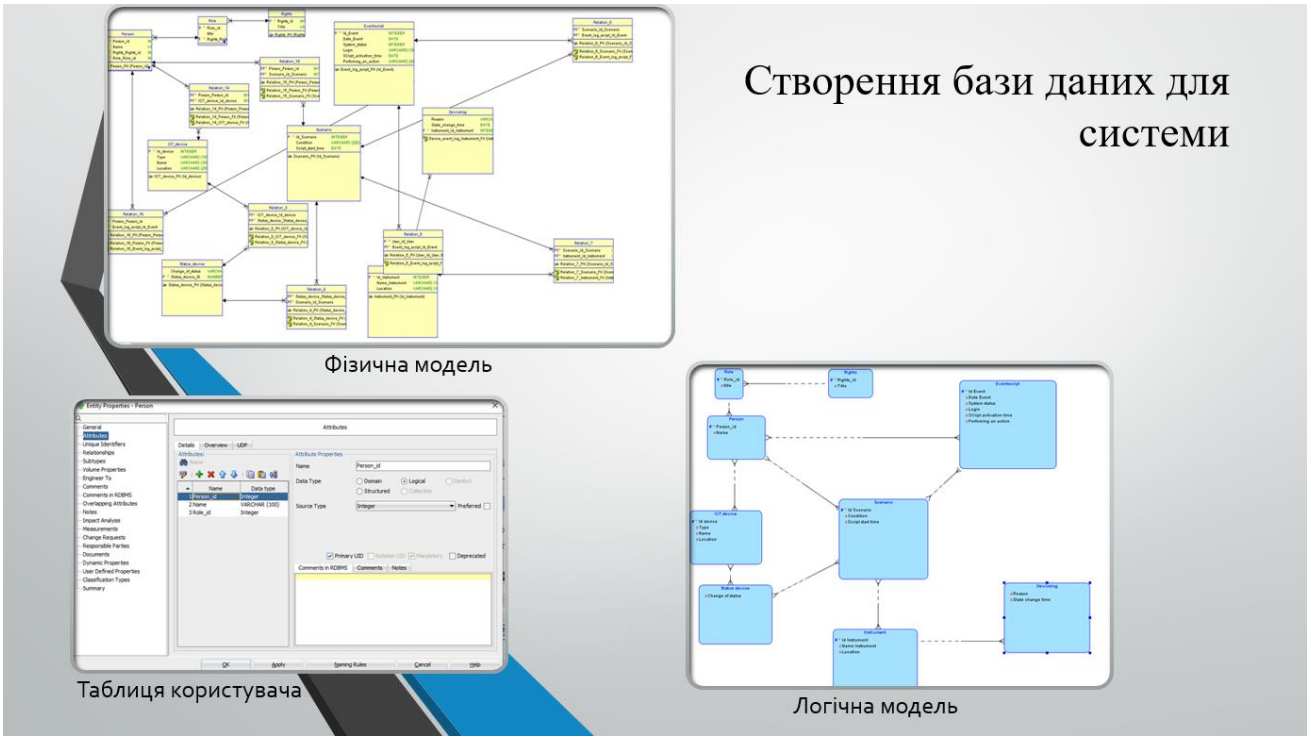


Рисунок А 7 – Слайд 7 Створення бази даних для системи

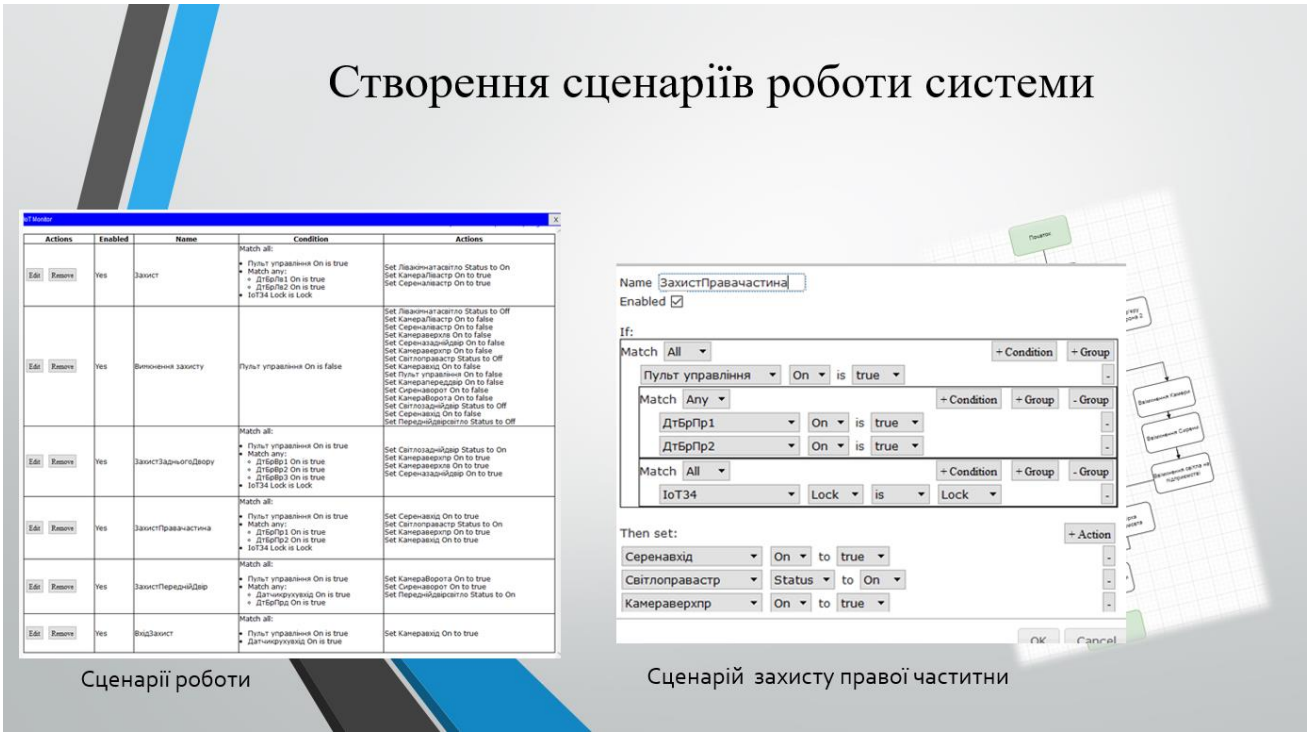


Рисунок А 8 – Слайд 8 Створення сценаріїв роботи системи

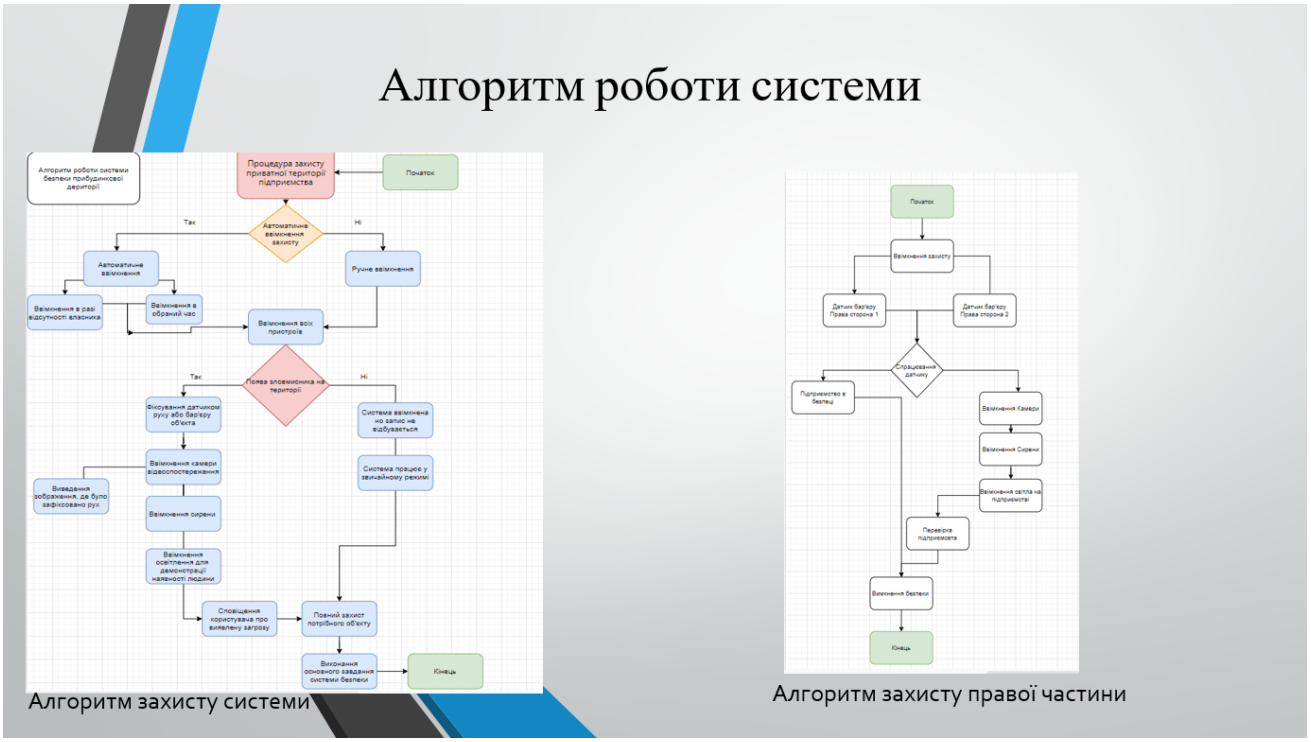


Рисунок А 9 – Слайд 9 Алгоритм роботи

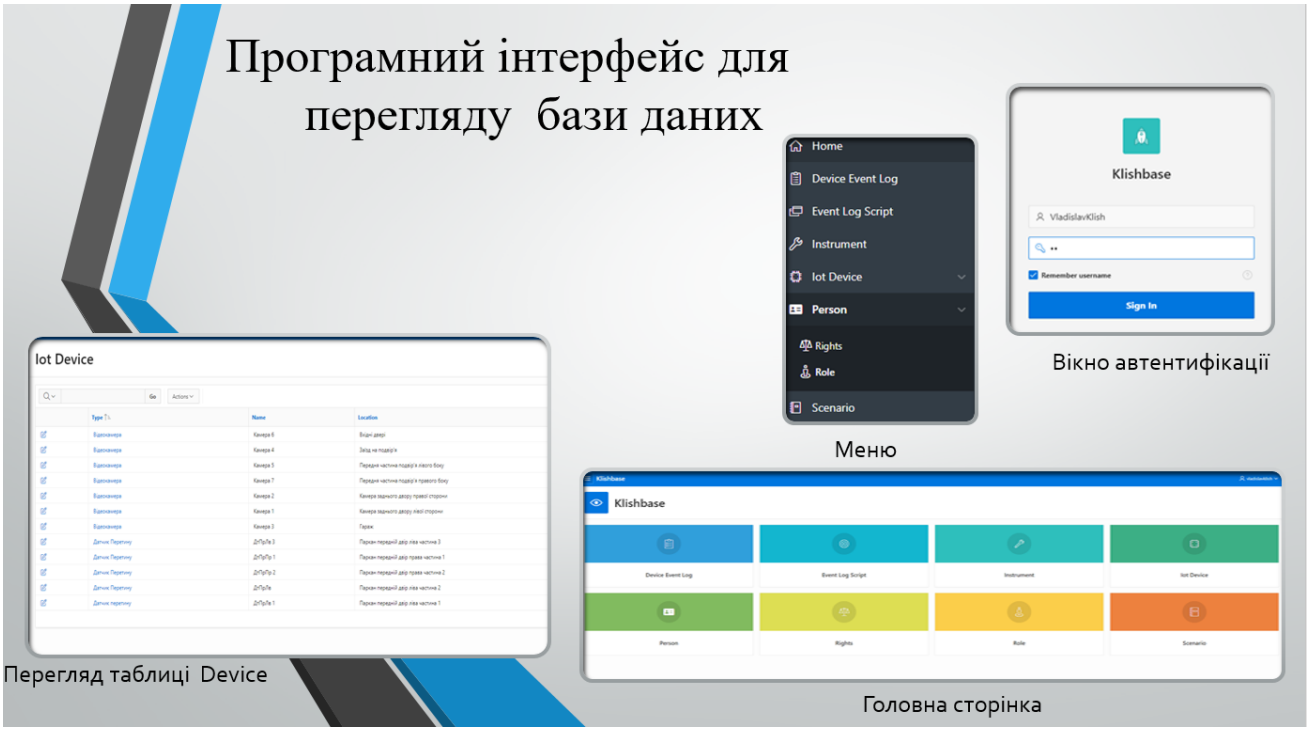


Рисунок А 10 – Слайд 10 Програмний інтерфейс для бази даних

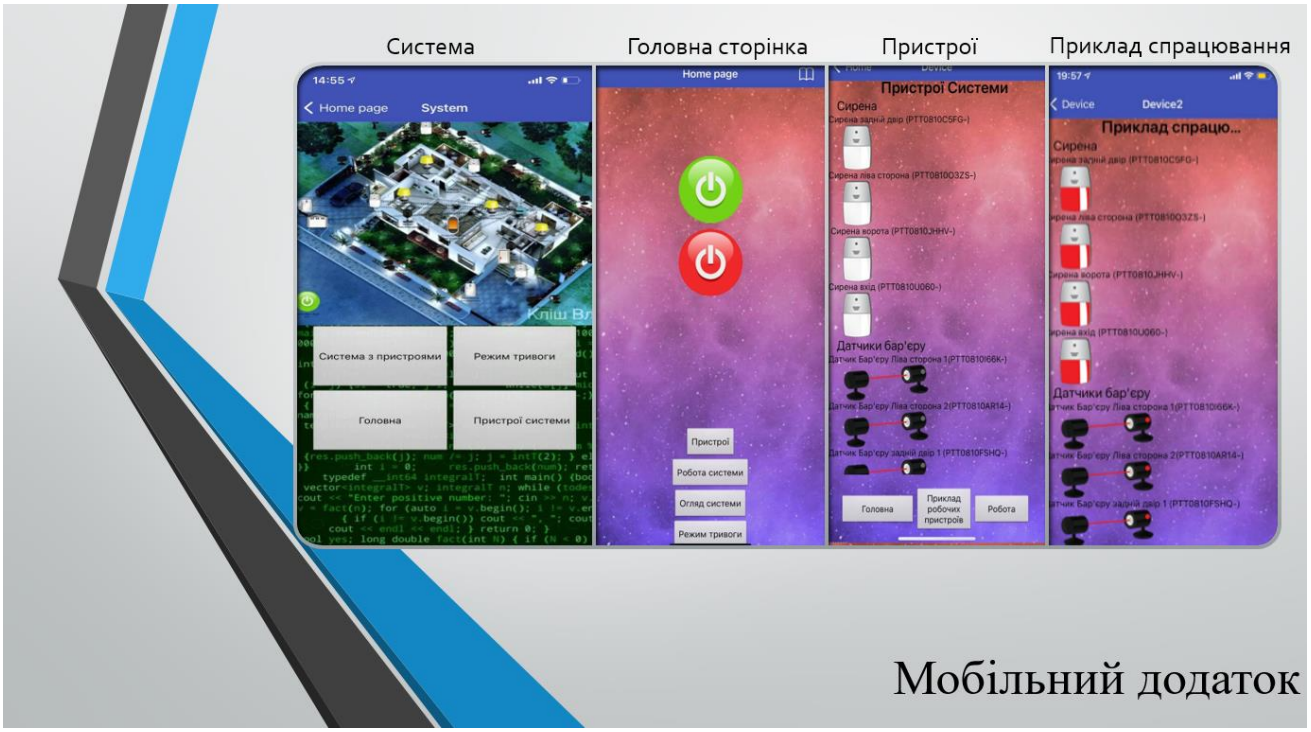


Рисунок А 11 – Слайд 11 Мобільний додаток

Рисунок А 12 – Слайд 12 Основні переваги системи

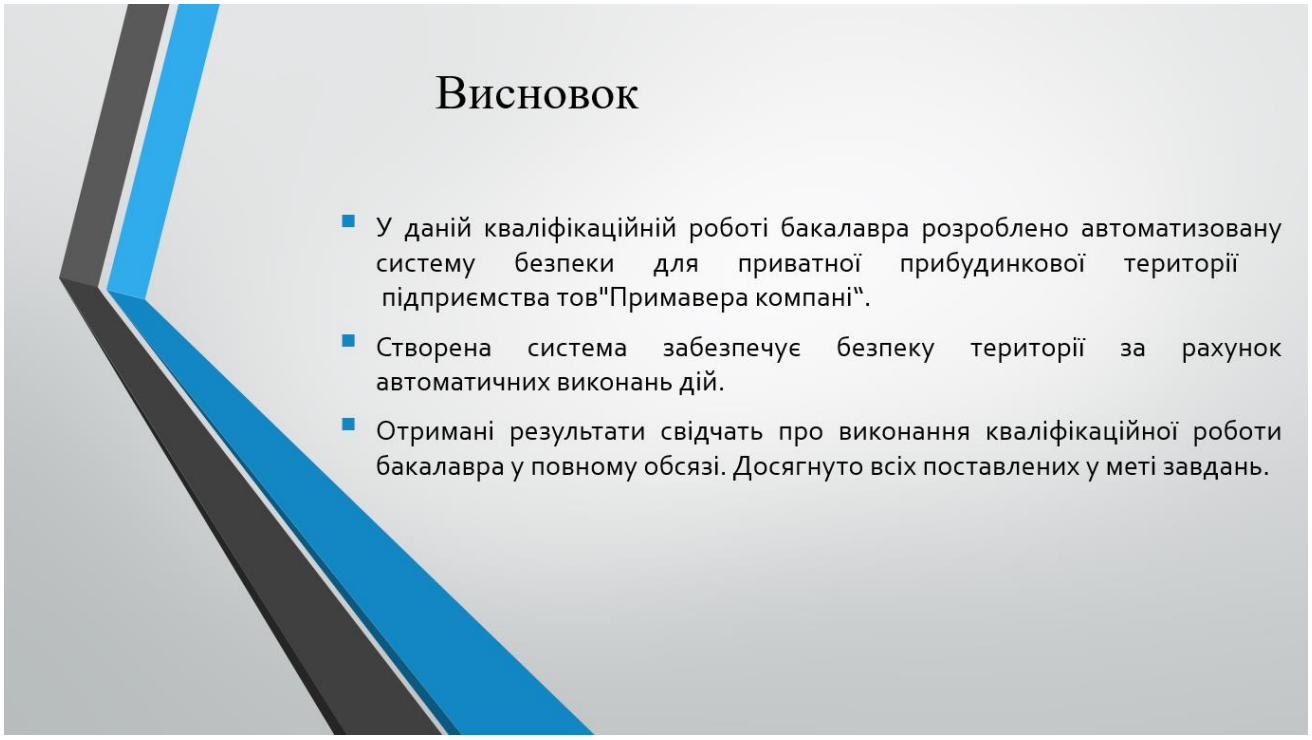


Рисунок А 13 – Слайд 13 Висновок

ДОДАТОК Б

Фрагмент коду програми

```
prompt --application/set_environment
set define off verify off feedback off
whenever sqlerror exit sql.sqlcode rollback
------------------------------------------------
--
-- ORACLE Application Express (APEX) export file
--
-- You should run the script connected to SQL*Plus as the Oracle user
-- APEX_200200 or as the owner (parsing schema) of the application.
--
-- NOTE: Calls to apex_application_install override the defaults below.
--
------------------------------------------------
begin
wwv_flow_api.import_begin (
 p_version_yyyy_mm_dd=>'2020.10.01'
,p_release=>'20.2.0.00.20'
,p_default_workspace_id=>16842236517098884741
,p_default_application_id=>107433
,p_default_id_offset=>0
,p_default_owner=>'WKSP_KLISHBASE'
);
end;
/
```

```
--  Application:     107433
--  Name:            Klishbase
--  Date and Time:   16:53 Monday December 14, 2020
--  Exported By:     KLISHMEAT@GMAIL.COM
--  Flashback:       0
--  Export Type:     Application Export
--    Pages:                   35
--      Items:                 48
--      Processes:             52
--      Regions:               68
--      Buttons:               97
--      Dynamic Actions:       32
--    Shared Components:
--      Logic:
--        Items:               1
--      Navigation:
--        Lists:               3
--        Breadcrumbs:         1
--          Entries:           17
--      Security:
--        Authentication:      1
--        Authorization:       1
--      User Interface:
--        Themes:              1
--        Templates:
--          Page:              9
--          Region:            17
--          Label:             7
--          List:              13
--          Popup LOV:         1
```

```
--          Calendar:           1
--          Breadcrumb:         1
--          Button:             3
--          Report:            11
--         LOVs:                9
--          Shortcuts:          1
--        Globalization:
--        Reports:
--        E-Mail:
--      Supporting Objects:  Included
--   Version:         20.2.0.00.20
--   Instance ID:     63113759365424
--

prompt --application/delete_application
begin
wwv_flow_api.remove_flow(wwv_flow.g_flow_id);
end;
/
prompt --application/create_application
begin
wwv_flow_api.create_flow(
 p_id=>wwv_flow.g_flow_id
,p_owner=>nvl(wwv_flow_application_install.get_schema,'WKSP_KLISHBASE')
,p_name=>nvl(wwv_flow_application_install.get_application_name,'Klishbase')
,p_alias=>nvl(wwv_flow_application_install.get_application_alias,'KLISHBASE')
,p_page_view_logging=>'YES'
,p_page_protection_enabled_y_n=>'Y'
,p_checksum_salt=>'F3086847927804AA01BF57618EF15DCA8AAB2A2AACB
```

```
,p_bookmark_checksum_function=>'SH512'
,p_compatibility_mode=>'19.2'
,p_flow_language=>'en'
,p_flow_language_derived_from=>'FLOW_PRIMARY_LANGUAGE'
,p_allow_feedback_yn=>'Y'
,p_date_format=>'DS'
,p_timestamp_format=>'DS'
,p_timestamp_tz_format=>'DS'
,p_direction_right_to_left=>'N'
,p_flow_image_prefix => nvl(wwv_flow_application_install.get_image_prefix,'')
,p_documentation_banner=>'Application created from create application wizard
2020.12.08.'
,p_authentication=>'PLUGIN'
,p_authentication_id=>wwv_flow_api.id(16844675625577316614)
,p_application_tab_set=>1
,p_logo_type=>'T'
,p_logo_text=>'Klishbase'
,p_app_builder_icon_name=>'app-icon.svg'
,p_proxy_server=>nvl(wwv_flow_application_install.get_proxy,'')
,p_no_proxy_domains=>nvl(wwv_flow_application_install.get_no_proxy_domain
s,'')
,p_flow_version=>'Release 1.0'
,p_flow_status=>'AVAILABLE_W_EDIT_LINK'
,p_exact_substitutions_only=>'Y'
,p_browser_cache=>'N'
,p_browser_frame=>'D'
,p_rejoin_existing_sessions=>'N'
,p_csv_encoding=>'Y'
,p_auto_time_zone=>'N'
```

```
,p_substitution_value_01=>'Klishbase'
,p_last_updated_by=>'KLISHMEAT@GMAIL.COM'
,p_last_upd_yyyymmddhh24miss=>'20201212151600'
,p_file_prefix => nvl(wwv_flow_application_install.get_static_app_file_prefix,'')
,p_files_version=>3
,p_ui_type_name => null
,p_print_server_type=>'INSTANCE'
);
end;
/
prompt --
application/shared_components/navigation/lists/desktop_navigation_menu
begin
wwv_flow_api.create_list(
 p_id=>wwv_flow_api.id(16844676447541316615)
,p_name=>'Desktop Navigation Menu'
,p_list_status=>'PUBLIC'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16846832851964316800)
,p_list_item_display_sequence=>10
,p_list_item_link_text=>'Home'
,p_list_item_link_target=>'f?p=&APP_ID.:1:&APP_SESSION.::&DEBUG.:'
,p_list_item_icon=>'fa-home'
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16846834359303316804)
,p_list_item_display_sequence=>20
```

```
,p_list_item_link_target=>'f?p=&APP_ID.:2:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-clipboard-list'
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16846848670561317344)
,p_list_item_display_sequence=>30
,p_list_item_link_text=>'Event Log Script'
,p_list_item_link_target=>'f?p=&APP_ID.:4:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-window-restore'
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16846864277029318056)
,p_list_item_display_sequence=>40
,p_list_item_link_text=>'Instrument'
,p_list_item_link_target=>'f?p=&APP_ID.:6:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-wrench'
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16846876918896318539)
,p_list_item_display_sequence=>50
,p_list_item_link_text=>'Iot Device'
,p_list_item_link_target=>'f?p=&APP_ID.:8:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-microchip'
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
```

```
,p_list_item_display_sequence=>170
,p_list_item_link_text=>'Status Device'
,p_list_item_link_target=>'f?p=&APP_ID.:32:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-bullseye'
,p_parent_list_item_id=>wwv_flow_api.id(16846876918896318539)
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16846890748716319087)
,p_list_item_display_sequence=>60
,p_list_item_link_text=>'Person'
,p_list_item_link_target=>'f?p=&APP_ID.:10:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-address-card'
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16847192387701322089)
,p_list_item_display_sequence=>140
,p_list_item_link_text=>'Rights'
,p_list_item_link_target=>'f?p=&APP_ID.:26:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-balance-scale'
,p_parent_list_item_id=>wwv_flow_api.id(16846890748716319087)
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16847503817777322441)
,p_list_item_display_sequence=>150
,p_list_item_link_text=>'Role'
,p_list_item_link_target=>'f?p=&APP_ID.:28:&SESSION.::&DEBUG.::::'
```

```
,p_parent_list_item_id=>wwv_flow_api.id(16846890748716319087)
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16847517451764322891)
,p_list_item_display_sequence=>160
,p_list_item_link_text=>'Scenario'
,p_list_item_link_target=>'f?p=&APP_ID.:30:&SESSION.::&DEBUG.::::'
,p_list_item_icon=>'fa-notebook'
,p_list_item_current_type=>'TARGET_PAGE'
);
end;
/
prompt --application/shared_components/navigation/lists/desktop_navigation_bar
begin
wwv_flow_api.create_list(
 p_id=>wwv_flow_api.id(16846815847400316744)
,p_name=>'Desktop Navigation Bar'
,p_list_status=>'PUBLIC'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16847656607085323819)
,p_list_item_display_sequence=>10
,p_list_item_link_text=>'&APP_USER.'
,p_list_item_link_target=>'#'
,p_list_item_icon=>'fa-user'
,p_list_text_02=>'has-username'
,p_list_item_current_type=>'TARGET_PAGE'
)
```

```
 p_id=>wwv_flow_api.id(16847657149987323820)
,p_list_item_display_sequence=>20
,p_list_item_link_text=>'---'
,p_list_item_link_target=>'separator'
,p_parent_list_item_id=>wwv_flow_api.id(16847656607085323819)
,p_list_item_current_type=>'TARGET_PAGE'
);
wwv_flow_api.create_list_item(
p_id=>wwv_flow_api.id(16847657548866323820)
,p_list_item_display_sequence=>30
,p_list_item_link_text=>'Sign Out'
,p_list_item_link_target=>'&LOGOUT_URL.'
,p_list_item_icon=>'fa-sign-out'
,p_parent_list_item_id=>wwv_flow_api.id(16847656607085323819)
,p_list_item_current_type=>'TARGET_PAGE'
);
end;
/
prompt --application/shared_components/navigation/lists/page_navigation
begin
wwv_flow_api.create_list(
 p_id=>wwv_flow_api.id(16847649590668323812)
,p_name=>'Page Navigation'
,p_list_status=>'PUBLIC'
);
wwv_flow_api.create_list_item(
 p_id=>wwv_flow_api.id(16847649909874323812)
,p_list_item_display_sequence=>20
,p_list_item_link_text=>'Device Event Log'
,p_list_item_link_target=>'f?p=&APP_ID.:2:&SESSION.::&DEBUG.::::'
```

ДОДАТОК В

Фрагмент коду DDL

```
-- Generated by Oracle SQL Developer Data Modeler 20.2.0.167.1538
--   at:        2020-12-14 20:17:16 EET
--   site:      Oracle Database 11g
--   type:      Oracle Database 11g
-- predefined type, no DDL - MDSYS.SDO_GEOMETR
-- predefined type, no DDL - XMLTYPE
CREATE TABLE devicelog (
   reason                 VARCHAR2(100),
   state_change_time      DATE,
   instrument_id_instrument  INTEGER NOT NULL
);
CREATE TABLE eventscript (
   id_event               INTEGER NOT NULL,
   date_event             DATE,
   system_status          INTEGER,
   login                  VARCHAR2(100),
   script_activation_time DATE,
   perfoming_an_action    VARCHAR2(200)
);
ALTER TABLE eventscript ADD CONSTRAINT event_log_script_pk
PRIMARY KEY ( id_event );
CREATE TABLE instrument (
   id_instrument    INTEGER NOT NULL,
   name_instrument VARCHAR2(100),
   location        VARCHAR2(100)
);
```

```
ALTER TABLE instrument ADD CONSTRAINT instrument_pk PRIMARY KEY
( id_instrument );
CREATE TABLE iot_device (
    id_device INTEGER NOT NULL,
    type      VARCHAR2(100),
    name      VARCHAR2(100),
    location  VARCHAR2(200)
);
ALTER TABLE iot_device ADD CONSTRAINT iot_device_pk PRIMARY KEY
( id_device );
CREATE TABLE person (
    person_id        INTEGER NOT NULL,
    name             VARCHAR2(100),
    rights_rights_id INTEGER NOT NULL,
    role_role_id     INTEGER NOT NULL
);
ALTER TABLE person ADD CONSTRAINT person_pk PRIMARY KEY (
person_id );
CREATE TABLE relation_14 (
    person_person_id      INTEGER NOT NULL,
    iot_device_id_device  INTEGER NOT NULL
);
ALTER TABLE relation_14 ADD CONSTRAINT relation_14_pk PRIMARY
KEY ( person_person_id,
                                          iot_device_id_device );
CREATE TABLE relation_15 (
    person_person_id      INTEGER NOT NULL,
    scenario_id_scenario  INTEGER NOT NULL
);
```

```
ALTER TABLE relation_15 ADD CONSTRAINT relation_15_pk PRIMARY
KEY ( person_person_id,
                                        scenario_id_scenario );
CREATE TABLE relation_16 (
   person_person_id          INTEGER NOT NULL,
   event_log_script_id_event  INTEGER NOT NULL
);
ALTER TABLE relation_16 ADD CONSTRAINT relation_16_pk PRIMARY
KEY ( person_person_id,
                                        event_log_script_id_event );
CREATE TABLE relation_3 (
   iot_device_id_device           INTEGER NOT NULL,
   status_device_status_device_id  NUMBER NOT NULL
);
ALTER TABLE relation_3 ADD CONSTRAINT relation_3_pk PRIMARY KEY
( iot_device_id_device,
                                        status_device_status_device_id );
CREATE TABLE relation_4 (
   status_device_status_device_id NUMBER NOT NULL,
   scenario_id_scenario           INTEGER NOT NULL
);
ALTER TABLE relation_4 ADD CONSTRAINT relation_4_pk PRIMARY KEY
( status_device_status_device_id,
                                        scenario_id_scenario );
CREATE TABLE relation_5 (
   user_id_user              INTEGER NOT NULL,
   event_log_script_id_event  INTEGER NOT NULL
);
ALTER TABLE relation_5 ADD CONSTRAINT relation_5_pk PRIMARY KEY
```

```
                                        event_log_script_id_event );
CREATE TABLE relation_6 (
   scenario_id_scenario       INTEGER NOT NULL,
   event_log_script_id_event  INTEGER NOT NULL
);
ALTER TABLE relation_6 ADD CONSTRAINT relation_6_pk PRIMARY KEY
( scenario_id_scenario,
                                        event_log_script_id_event );

CREATE TABLE relation_7 (
   scenario_id_scenario      INTEGER NOT NULL,
   instrument_id_instrument  INTEGER NOT NULL
);
ALTER TABLE relation_7 ADD CONSTRAINT relation_7_pk PRIMARY KEY
( scenario_id_scenario,
                                        instrument_id_instrument );
CREATE TABLE rights (
   rights_id INTEGER NOT NULL,
   title     VARCHAR2(100)
);
ALTER TABLE rights ADD CONSTRAINT rights_pk PRIMARY KEY (
rights_id );
CREATE TABLE role (
   role_id          INTEGER NOT NULL,
   title            VARCHAR2(100),
   rights_rights_id  INTEGER NOT NULL
);
ALTER TABLE role ADD CONSTRAINT role_pk PRIMARY KEY ( role_id );
CREATE TABLE scenario (
```

```
    condition          VARCHAR2(200),
    script_start_time  DATE
);
ALTER TABLE scenario ADD CONSTRAINT scenario_pk PRIMARY KEY (
id_scenario );
CREATE TABLE status_device (
    change_of_status VARCHAR2(100),
    status_device_id  NUMBER NOT NULL
);
ALTER TABLE status_device ADD CONSTRAINT status_device_pk PRIMARY
KEY ( status_device_id );
ALTER TABLE devicelog
    ADD CONSTRAINT device_event_log_instrument_fk FOREIGN KEY (
instrument_id_instrument )
        REFERENCES instrument ( id_instrument );
ALTER TABLE person
    ADD CONSTRAINT person_role_fk FOREIGN KEY ( role_role_id )
        REFERENCES role ( role_id );
ALTER TABLE relation_14
    ADD CONSTRAINT relation_14_iot_device_fk FOREIGN KEY (
iot_device_id_device )
        REFERENCES iot_device ( id_device );
ALTER TABLE relation_14
    ADD CONSTRAINT relation_14_person_fk FOREIGN KEY (
person_person_id )
        REFERENCES person ( person_id );
ALTER TABLE relation_15
    ADD CONSTRAINT relation_15_person_fk FOREIGN KEY (
person_person_ );
```

```
ALTER TABLE relation_15
    ADD CONSTRAINT relation_15_scenario_fk FOREIGN KEY (
scenario_id_scenario )
        REFERENCES scenario ( id_scenario );
-- ERROR: FK name length exceeds maximum allowed length(30)
ALTER TABLE relation_16
    ADD CONSTRAINT relation_16_event_log_script_fk FOREIGN KEY (
event_log_script_id_event )
        REFERENCES eventscript ( id_event );
ALTER TABLE relation_16
    ADD CONSTRAINT relation_16_person_fk FOREIGN KEY (
person_person_id )
        REFERENCES person ( person_id );
ALTER TABLE relation_3
    ADD CONSTRAINT relation_3_iot_device_fk FOREIGN KEY (
iot_device_id_device )
        REFERENCES iot_device ( id_device );
ALTER TABLE relation_3
    ADD CONSTRAINT relation_3_status_device_fk FOREIGN KEY (
status_device_status_device_id )
        REFERENCES status_device ( status_device_id );
ALTER TABLE relation_4
    ADD CONSTRAINT relation_4_scenario_fk FOREIGN KEY (
scenario_id_scenario )
        REFERENCES scenario ( id_scenario );
ALTER TABLE relation_4
    ADD CONSTRAINT relation_4_status_device_fk FOREIGN KEY (
status_device_status_device_id )
        REFERENCES status_device ( status_device_id );
```

```
   ADD CONSTRAINT relation_5_event_log_script_fk FOREIGN KEY (
event_log_script_id_event )
      REFERENCES eventscript ( id_event );
ALTER TABLE relation_6
   ADD CONSTRAINT relation_6_event_log_script_fk FOREIGN KEY (
event_log_script_id_event )
      REFERENCES eventscript ( id_event );
ALTER TABLE relation_6
   ADD CONSTRAINT relation_6_scenario_fk FOREIGN KEY (
scenario_id_scenario )
      REFERENCES scenario ( id_scenario );
ALTER TABLE relation_7
   ADD CONSTRAINT relation_7_instrument_fk FOREIGN KEY (
instrument_id_instrument )
      REFERENCES instrument ( id_instrument );

ALTER TABLE relation_7
   ADD CONSTRAINT relation_7_scenario_fk FOREIGN KEY (
scenario_id_scenario )
      REFERENCES scenario ( id_scenario );

ALTER TABLE role
   ADD CONSTRAINT role_rights_fk FOREIGN KEY ( rights_rights_id )
      REFERENCES rights ( rights_id );

CREATE SEQUENCE status_device_status_device_id START WITH 1
NOCACHE ORDER;

CREATE OR REPLACE TRIGGER status_device_status_device_id BEFORE
   INSERT ON status_device
```

```
    FOR EACH ROW
    WHEN ( new.status_device_id IS NULL )
BEGIN
    :new.status_device_id := status_device_status_device_id.nextval;
END;
/

-- Oracle SQL Developer Data Modeler Summary Report:
--
-- CREATE TABLE                            17
-- CREATE INDEX                             0
-- ALTER TABLE                             34
-- CREATE VIEW                              0
-- ALTER VIEW                               0
-- CREATE PACKAGE                           0
-- CREATE PACKAGE BODY                      0
-- CREATE PROCEDURE                         0
-- CREATE FUNCTION                          0
-- CREATE TRIGGER                           1
-- ALTER TRIGGER                            0
-- CREATE COLLECTION TYPE                   0
-- CREATE STRUCTURED TYPE                   0
-- CREATE STRUCTURED TYPE BODY              0
-- CREATE CLUSTER                           0
-- CREATE CONTEXT                           0
-- CREATE DATABASE                          0
-- CREATE DIMENSION                         0
-- CREATE DIRECTORY                         0
```

-- CREATE DISK GROUP 0

-- CREATE ROLE 0

-- CREATE ROLLBACK SEGMENT 0

-- CREATE SEQUENCE 1

-- CREATE MATERIALIZED VIEW 0

-- CREATE MATERIALIZED VIEW LOG 0

-- CREATE SYNONYM 0

-- CREATE TABLESPACE 0

-- CREATE USER 0

--

-- DROP TABLESPACE 0

-- DROP DATABASE 0

--

-- REDACTION POLICY 0

--

-- ORDS DROP SCHEMA 0

-- ORDS ENABLE SCHEMA 0

-- ORDS ENABLE OBJECT 0

--

-- ERRORS 1

-- WARNINGS 0