КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від 2024 року, протокол №
Завідувач кафедри доктор фіз.-мат. наук, професор
_____ Ігор АНІСІМОВ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА
на тему:
«АЛГОРИТМІЗАЦІЯ КОНСТРУЮВАННЯ СИСТЕМ ЗАХИСТУ НА БАЗІ РОЗУМНОГО ПРОСТОРУ»

Виконав:
студент 3-го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОПП «Інформаційна безпека телекомунікаційних систем і мереж»
Завадський Олександр Олегович_____

Науковий керівник:
доктор технічних наук, доцент
Ольшевський Сергій Валентинович _____

Рецензент:

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент_____Олександр ЗАВАДСЬКИЙ

Київ – 2024

РЕФЕРАТ

Дипломна робота: 46 с., 1 табл., 2 дод., 9 рис., 12 джерел.

Мета роботи – Розробка алгоритму встановлення та модернізації охоронних систем в житлових та нежитлових установах.

Розроблено алгоритм для оцінки придатності об’єкту нерухомості запропонованим стандартам безпеки, підібрано методи інтеграцій захисних механізмів до системи «Розумний Простір», створено візуальну симуляцію роботи охоронної системи.

Як результат порівняльного аналізу різних напрямків методології та програмних продуктів керування обладнанням та захисними механізмами нерухомості, був розробений алгоритм, за допомогою якого можливо швидко порівняти між собою доступні варіанти систем і обрати найбільш ефективну залежно від типу приміщень/територій.

Завдяки створеній візуалізації на 3Д моделі будівлі вдалось уникнути зайвих витрат на тестові стенди і встановлення тестового обладнання, удешевити розробку та пришвидшити процес підбору необхідних позицій з урахуванням алгоритму і потреб кінцевого споживача.

Запропонований алгоритм добре себе показав на технологічній практиці, був допрацьований з урахуванням виниклих проблем і запитів.

Розроблений алгоритм дозволяє максимально швидко і точно розробляти плани з облаштування захисними системами різноманітні типи будівель.

У подальшому, має місце застосування новітніх технологій ШІ для пришвидшення моделювання планів будівель (в форматі 3д-сканування за допомогою лідарів), розробка спеціального ПЗ для емуляції різних навантажень на пристрої за заданими характеристиками.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

СРП – система «Розумний Простір»;

ШІ – штучний інтелект;

IoT – Internet of Things (інтернет речей)

NVR - Network Video Recorder (мережевий відеореєстратор)

PIR – Passive Infrared (пасивний інфрачервоний датчик)

HD CCTV – High Definition Closed Circuit Television (система відеоспостереження високої чіткості)

IP CCTV – Internet Protocol Closed Circuit Television (система відеоспостереження з використанням інтернет-протоколу)

ВСТУП

IoT, як повсякденна технологія прижилася в сучасному суспільстві ще починаючи з другої декади XXI століття. Основною передумовою її створення була масштабованість серед різноманітних систем. Це означає, що інструменти котрі застосовуються для додатків безпеки та інфраструктури міст суттєво не відрізняються від звичайної розумної системи відеоспостереження, яку ми можемо мати у себе вдома.

Пристрої IoT що ми використовуємо і купуємо для власного використання вдома чи на роботі є всього лиш дещо складнішими по устаткуванню і конструкції аніж ті що складають інфраструктуру розумного міста, яким Київ як на мене можна вважати. Найбільша різниця від міської інфраструктури в домашніх IoT системах - це обсяги даних, що обробляються.

Функціонально, вимоги повсякденного життя та необхідні ускладнення захисту конфіденційності та забезпечення підзвітності означають, що системи безпеки мають бути спеціалізованими та гнучкими, чого поки неможливо добитися в масштабі сучасних великих міст (окрім деяких провінцій Китаю), але можна розгортати на невеликих площах. Саме це основна перевага можливості розгортки сучасних захисних систем в оболонці IoT для власного користування.

Якщо уже й говорити про міську інфраструктуру порівнюючи з невеликими домашніми системами, то перша забезпечує жорсткий захист та ефективне реагування в надзвичайних ситуаціях, а також може плавно змінювати правила безпеки або інфраструктуру. Натомість системи про які я буду розповідати мають переваги над великими. Одними з головних є можливість самостійного контролю ситуації, повна свобода в облаштуванні, контроль та конфіденційність даних, і саме головне це збереження власного майна, а не міської інфраструктури.

1. ОГЛЯД СИСТЕМ ЗАХИСТУ ДЛЯ РОЗУМНОГО ПРОСТОРУ

Представлений розділ є оглядом основних типів систем захисту, їх класифікації, технологічної бази та сучасних підходів до інтеграції та управління цими системами. Він також зосереджується на аналізі викликів, з якими зустрічаються організації при впровадженні та налагодженні ефективних систем безпеки, а також обговорює стратегії, які можуть застосовуватися для максимізації захисту активів та особистостей. Розділ містить інформацію про критичні аспекти проектування систем захисту, включаючи вибір обладнання, планування розташування елементів системи, визначення потреб у підтримці та обслуговуванні, а також розгляд правових та етичних норм при використанні систем відеоспостереження та інших технологій нагляду.

1.1 Види систем захисту для будинків

Сучасні системи захисту поділяються на 3 види:

- Відеоспостереження / Камери безпеки
- Управління доступом
- Охоронна сигналізація.

В свою чергу кожна з них має свої набори інструментарію для здійснення самого захисту.

Для відеоспостереження та камер безпеки це:

- HD системи відеоспостереження (HD CCTV)

Вони слугують для передачі високоякісного зображення там, де це необхідно, та дозволяють в подробицях та деталях бачити все що відбувається в полі зору камер. Прикладом може слугувати камера AHD-BL25 180, що зображена на рисунку 1.1

Рисунок 1.1 – HD CCTV камера AHD-BL25 180

Основною перевагою є чіткість зображення, що може бути критичною для екстраординарних випадків при порушенні безпеки територій. Ця перевага надає змогу з високою точністю отримати детальну інформацію про все що відбувалось в полі зору і виявити порушення та порушника для передачі даних правоохоронцям.

Основним недоліком є те, що такі камери відеоспостереження вимагають локального сховища даних, що ускладнює процес контролю безпеки, якщо знаходитись не безпосередньо на об’єкті охорони чи на сервері. Прикладом такого сховища даних є локальний сервер VT-DVR-4 4ch Viewtron 4K DVR (рис 1.2) що доволяє записувати до 12 ТБ відеоматеріалу

Рисунок 1.2 – Локальний сервер VT-DVR-4 4ch Viewtron 4K DVR

- IP відеоспостереження (IP CCTV)

Камери Інтернет-протоколу (IP) – це сучасний тип камер безпеки , які знімають відео, стискають його та передають через Інтернет. Бездротові IP-камери зазвичай використовують для цього мережу Wi-Fi. Найчастіше відзнятий матеріал зберігається в хмарі або на NVR. На рисунку 1.3 продемонстрована IP відеокамера такого типу - Illustra IES02MFBNWIY.

Рисунок 1.3 – IP відеокамера Illustra IES02MFBNWIY

Деякі IP-камери також дозволяють локально зберігати відзнятий матеріал на карті пам’яті microSD або на вбудованій пам’яті сполученого телефону.

Основними перевагами таких систем є доступність інформації, простота інтеграції в існуючу IoT інфраструктуру та дешевизна, в порівнянні з HD системами. В порівнянні ж із аналоговими камерами відеоспостереження, що в минулому були популярними в комерційних установах, такі види камер можуть покривати більшу територію, давати кращу якість, мають широкі можливості розширення, не обмежені

кабельною інфраструктурою території та мають набагато потужніші функції пошуку [1].

1.2 Сучасні технології в системах захисту

Сучасні технології в системах захисту постійно розвиваються, включаючи в себе широкий спектр рішень, які забезпечують безпеку приміщень та осіб. Перелік ключових технологій:

1. Інтернет речей (IoT). Це смарт-домашні системи. Інтеграція домашніх пристроїв з централізованими системами управління через IoT. Це включає автоматичне регулювання освітлення, температури, моніторинг відкритих дверей чи вікон, а також взаємодію з аудіо та відеосистемами для створення ілюзії присутності власника вдома. Також включає в себе інтелектуальне відеоспостереження - використання алгоритмів машинного навчання для аналізу відео з камер безпеки. Такі системи можуть визначати незвичайну поведінку, автоматично повідомляти про інциденти, а також розпізнавати обличчя.

2. Біометричні технології. Це сканери відбитків пальців та розпізнавання облич. Ці системи забезпечують високий рівень безпеки, дозволяючи доступ тільки авторизованим особам. Розпізнавання райдужки ока використовується в особливо чутливих застосунках, де потрібен вищий рівень безпеки [2].

3. Бездротові та мобільні технології. Бездротові сигналізації це інтеграція з мобільними додатками для віддаленого моніторингу і управління системами безпеки, включаючи сповіщення у разі тривоги. Віддалене управління через додатки дає можливість керування безпекою будинку з будь-якої точки світу.

4. Розумні замки та домофони це смарт-замки. Вони забезпечують можливість відкривати двері через смартфони, PIN-коди або біометричні дані, також інтегровані з іншими системами безпеки в будинку. Їх підвидом, або скоріше різновидом є відеодомофони. Вони дозволяють бачити та спілкуватися з відвідувачами через відео, перш ніж впустити їх у будинок.

5. Штучний інтелект (AI) та машинне навчання це аналіз поведінки за допомогою якого штучний інтелект може аналізувати звичні шаблони поведінки мешканців та виявляти відхилення, які можуть свідчити про

зловмисні дії або надзвичайні ситуації. Системи з ШІ можуть прогнозувати потенційні загрози на основі аналізу великої кількості даних і історичних інформацій.

6. Криптографічні технології, або шифрування даних це процес забезпечення безпеки даних, які передаються або зберігаються в системах безпеки, використовуючи сучасні методи шифрування [3].

Ці технології не тільки підвищують рівень безпеки, але і значно покращують зручність користування системами захисту, роблячи їх гнучкішими та доступнішими для користувачів. Вони відіграють ключову роль в інтеграції систем безпеки з іншими аспектами смарт-просторів, такими як енергоефективність та автоматизація будинків [1].

Змоделюємо сценарій: Смарт-система безпеки в звичайному житловому будинку, яка використовує Інтернет речей (IoT), біометричні технології, і штучний інтелект для забезпечення безпеки, комфорту і енергоефективності.

Необхідний технологічний склад:

Смарт-домофони з відео: Відеодомофони дозволяють власникам будинку бачити і спілкуватися з відвідувачами в режимі реального часу через смартфон або інші пов'язані пристрої. Це забезпечує можливість перевірити особу перед впусканням її у будинок, що є особливо корисним для безпеки.

Система відеоспостереження з ШІ: Камери безпеки встановлені навколо периметру будинку та у важливих точках всередині, об'єднані з алгоритмами штучного інтелекту для виявлення підозрілих дій або незнайомих осіб. ШІ може аналізувати поведінку та навіть відправляти сповіщення, якщо відбувається щось неординарне, наприклад, коли система фіксує незвичайну активність у нічний час.

Смарт-замки з біометричним розпізнаванням: Двері оснащені смарт-замками, які можуть відкриватися за допомогою відбитків пальців, обличчя або додаткових біометричних даних, що забезпечує високий рівень безпеки та зручність. Власники можуть віддалено управляти доступом, наприклад, відкрити двері для сім'ї чи друзів, коли їх немає вдома [7].

Інтеграція з розумними датчиками: Датчики руху, відкриття дверей/вікон, диму та витоку води інтегровані з центральною системою управління, що дозволяє автоматично реагувати на різні надзвичайні ситуації, як-от включення сигналізації або сповіщення власників та екстрених служб.

Користі:

- Підвищена безпека: Комплексне відеоспостереження та контроль доступу знижують ризик несанкціонованого доступу та допомагають швидко реагувати на будь-які порушення.
- Комфорт та зручність: Власники можуть легко контролювати всі системи через смартфон або голосові команди, забезпечуючи легкий доступ до свого дому без ключів.
- Енергоефективність: Інтелектуальне управління освітленням і температурою, в залежності від використання простору та присутності людей, сприяє зниженню витрат на енергію.

Цей приклад показує, як сучасні технології можуть бути використані для створення безпечного, комфортного та ефективного житлового простору, використовуючи синергію між різними системами та технологіями.

1.3. Вимоги до систем захисту

Впровадження розумних просторів дає численні переваги, зокрема:

- Покращена безпека

Моніторинг і аналітика в реальному часі дозволяють проактивно виявляти ризики безпеці, забезпечуючи безпечне середовище для пасажирів.

- Підвищення продуктивності в офісі

Розумні простори спрощують робочі процеси, оптимізують використання простору та автоматизують рутинні завдання, дозволяючи співробітникам зосередитися на стратегічній діяльності.

- Покращений користувальницький досвід

Персоналізація та налаштування внутрішніх приміщень на основі даних у реальному часі забезпечує комфортний та індивідуальний досвід.

- Енергоефективність

Розумні простори оптимізують споживання енергії шляхом автоматичного регулювання освітлення, опалення та охолодження залежно від кількості людей і умов навколишнього середовища.

- Економія коштів

Оптимальне використання ресурсів і енергоефективність призводять до значної економії коштів для організацій.

2. АНАЛІЗ РІЗНИХ ВИДІВ СИСТЕМ ЗАХИСТУ

У цьому розділі я провів глибокий аналіз різних видів систем захисту, від цифрових ключів до комплексних інтегрованих систем безпеки. Обговорюються як традиційні, так і передові технології, що використовуються для захисту житлових та комерційних просторів. Розглядаються їхні технічні характеристики, переваги, недоліки та сценарії застосування. Особлива увага приділяється новітнім розробкам у галузі штучного інтелекту та IoT, які трансформують сферу систем безпеки, забезпечуючи більш ефективний захист та адаптивність до змінних умов використання.

Хочу зауважити що розглядаю сучасні захисні СРП в вигляді саме комплексних рішень [8], що поєднують декілька елементів, як приклад показано на рисунку 2.1

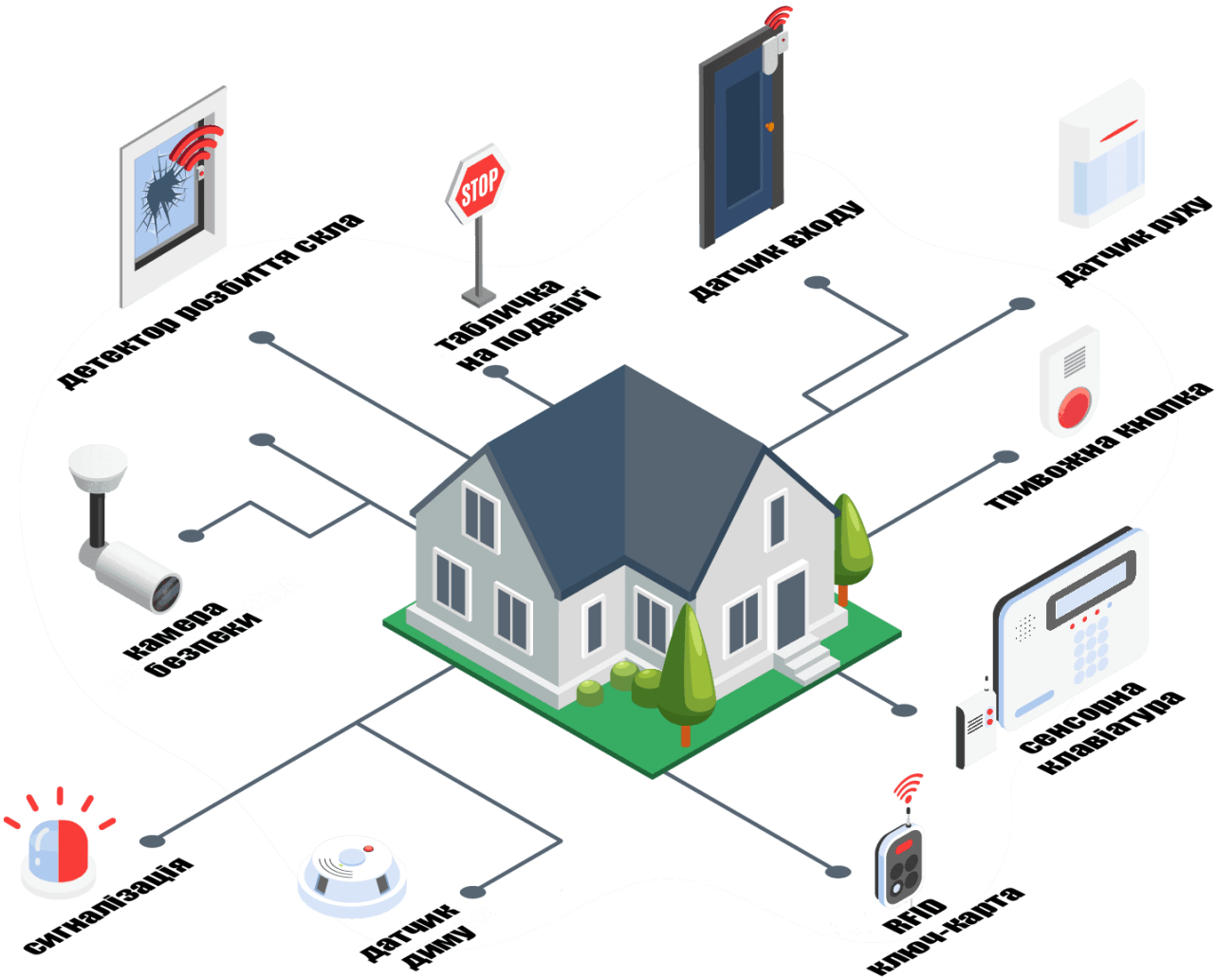

Рисунок 2.1 – Приклад з декількох девайсів що утворюють систему захисту

Сучасні системи захисту включають в себе різноманітні технології та підходи, які допомагають забезпечити безпеку житлових, комерційних та промислових об'єктів. Основні види систем включають:

1. Цифрові ключі

Такі ключі використовують електронні засоби для управління доступом. Це можуть бути RFID-картки, NFC-пристрої або спеціалізовані додатки на смартфонах, які дозволяють відкривати двері без використання традиційних механічних ключів [3].

- Переваги: Забезпечення високого рівня безпеки, можливість віддаленого контролю, інтеграція з іншими системами управління доступом.
- Недоліки: Залежність від електроніки та енергії, потенційні ризики злому або втрати даних.

2. Сканери відбитків пальців

Біометричні системи, що використовують унікальні відбитки пальців для ідентифікації осіб і надання доступу.

- Переваги: Висока точність ідентифікації, складність підробки, швидкий доступ без необхідності пам'ятати паролі або носити ключі.
- Недоліки: Можливі проблеми з читанням при брудних або пошкоджених пальцях, проблеми з приватністю даних.

3. Камери відеоспостереження

Відеокамери, що записують або транслюють відео з місця установки, можуть інтегруватися з системами зберігання даних або аналізу відео.

- Переваги: Можливість моніторингу в реальному часі, запис подій для подальшого розгляду, детерент незаконних дій.
- Недоліки: Великі об'єми даних для зберігання, потенційне порушення приватності, залежність від якості зображення.

4. Інтегровані системи безпеки

Системи, що комбінують відеонагляд, контроль доступу, датчики руху, сигналізації та інші технології в єдину інтегровану платформу.

- Переваги: Комплексний підхід до безпеки, взаємодія різних компонентів для покращення реакції на інциденти, централізоване управління.

- Недоліки: Висока вартість, складність установки та обслуговування, потреба в спеціалізованих знаннях для ефективного управління.

При виборі системи захисту важливо враховувати специфічні потреби об'єкта, бюджет, технічні можливості та потенційні ризики. Оцінка ефективності системи включає аналіз її надійності, здатності адаптуватися до змінних умов, інтеграцію з іншими системами та забезпечення приватності і конфіденційності інформації [5].

2.1 Цифрові ключі

Цифрові ключі стають все більш популярними в сучасних системах захисту завдяки своїм унікальним перевагам та гнучкості використання. Вони включають в себе кілька різних технологій, кожна з яких має свої особливості та застосування.

1. RFID-картки

Використовують радіочастотну ідентифікацію для передачі даних від картки до читача через радіохвилі [3].

Широко використовуються в офісних приміщеннях, готелях та освітніх установах для контролю доступу.

Переваги: Легкість використання та відносно низька вартість.

Недоліки: Вразливість до скімінгу (несанкціоноване зчитування).

2. NFC-технології

Використовує ближнє поле зв'язку для двосторонньої комунікації між пристроями, які знаходяться на короткій відстані.

Застосовується для мобільних платежів, електронних квитків, смартфонів як ключів від дверей.

- Переваги: Висока безпека завдяки шифруванню даних, зручність інтеграції з мобільними пристроями.
- Недоліки: Обмежена дальність дії, залежність від батареї мобільного пристрою.

3. Біометричні системи

Використовують унікальні фізіологічні характеристики людини, як-от відбитки пальців або розпізнавання обличчя, для ідентифікації.

Застосовуються в захищених приміщеннях, високотехнологічних підприємствах, смартфонах [4].

- Переваги: Висока точність ідентифікації, складність підробки.
- Недоліки: Висока вартість, потенційні проблеми з приватністю.

4. Цифрові ключі на основі додатків

Додатки на смартфоні, які генерують тимчасові або постійні ключі для доступу.

Застосовуються в сучасних житловиї комплексах, офісах, каршерінгу [10].

- Переваги: Гнучкість управління доступом, можливість дистанційного контролю та моніторингу.
- Недоліки: Залежність від наявності інтернету, ризики хакерських атак.

Смарт-замки інтегровані з мобільними додатками, що дозволяють власникам будинку віддалено керувати доступом, створювати тимчасові ключі для гостей або сервісних служб і відслідковувати вхід та вихід. Такий підхід не тільки підвищує безпеку, але і надає значний рівень зручності та контролю над особистим простором [3].

Цифрові ключі забезпечують важливу інтеграцію безпеки з цифровими технологіями, що робить системи більш адаптивними та інтелектуальними. Вони відіграють ключову роль у створенні гнучких та ефективних систем доступу, здатних задовольняти різноманітні потреби користувачів у безпеці та зручності.

2.2 Сканери відбитків пальців

Сканери відбитків пальців є однією з найпопулярніших форм біометричних технологій у системах безпеки. Вони використовують унікальні відбитки пальців особи для ідентифікації та контролю доступу.

Сканери відбитків пальців працюють, захоплюючи високоякісне зображення відбитка пальця. Сучасні сканери використовують різні методи

для цього, включаючи оптичні, ємнісні, ультразвукові та термічні технології:

- Оптичні сканери використовують традиційну камеру для створення відображення відбитку пальця.
- Ємнісні сканери створюють зображення за допомогою змін в електричному полі, яке виникає коли палець торкається поверхні датчика.
- Ультразвукові сканери використовують звукові хвилі для виявлення деталей відбитку пальця.
- Термічні сканери фіксують тепловий відбиток пальця.

Після захоплення зображення, система аналізує відбиток пальця, порівнюючи його з відбитками в базі даних для визначення відповідності.

Застосування сканерів

- Контроль доступу: Широко використовуються в комерційних та промислових установах, а також в житлових комплексах для контролю доступу.
- Мобільні пристрої: Більшість сучасних смартфонів та планшетів мають вбудовані сканери відбитків пальців для розблокування пристрою та аутентифікації транзакцій.
- Банківські послуги: Деякі банкомати використовують сканери відбитків пальців для підвищення безпеки при доступі до банківських рахунків [4].

Переваги:

- Висока точність: Відбитки пальців є дуже унікальними, що забезпечує високу точність ідентифікації.
- Швидкість і зручність: Аутентифікація відбувається швидко та не вимагає від користувачів запам'ятовувати паролі або мати спеціальні ключі.
- Високий рівень безпеки: Важко підробити або викрасти відбиток пальця без знання особи.

Недоліки:

- Вразливість до зносу та забруднення: Поверхня сканера може бути забруднена або подряпана, що ускладнює сканування.
- Проблеми з приватністю: Зберігання біометричних даних може викликати занепокоєння щодо приватності та їх потенційного використання без дозволу.
- Технічні обмеження: Деякі системи можуть бути вразливими до певних технічних проблем, наприклад, неспроможність розпізнати відбиток пальця з огрубілою або пошкодженою шкірою.

З розвитком технологій, сканери відбитків пальців стають ще більш інтегрованими в різні системи безпеки, включаючи інтелектуальні домашні системи та IoT пристрої. Очікується подальше покращення точності та швидкості роботи сканерів, а також розробка нових методів захисту біометричних даних від несанкціонованого доступу.

2.3 Камери відеоспостереження

Камери відеоспостереження є ключовим компонентом сучасних систем безпеки, які використовуються для моніторингу, запису та аналізу відеоданих на об'єктах різного призначення. Вони забезпечують реальний візуальний моніторинг та можуть бути інтегровані з іншими системами безпеки для більш ефективного управління та контролю.

Основні характеристики:

- Роздільна здатність: Висока роздільна здатність камер відеоспостереження критично важлива для забезпечення чіткості зображення, що є необхідним для ідентифікації осіб або об'єктів.
- Кут огляду: Широкий кут огляду дозволяє охоплювати більшу територію, зменшуючи кількість необхідних камер для покриття об'єкта.
- Нічне бачення: Камери з інфрачервоним освітленням або технологією збільшення світлочутливості забезпечують якісний запис у нічний час.
- Запис та зберігання даних: Можливість записувати відео на локальні носії або віддалені сервери, з подальшою можливістю швидкого пошуку та відтворення.

Типи камер

1. Домові камери:

Зазвичай мають просту установку та зручні для використання в домашніх умовах. Підключення через Wi-Fi та доступ до відео через смартфонні додатки.

2. Купольні камери:

Встановлюються на стелі або стіні, забезпечуючи 360-градусний огляд. Купольний корпус захищає оптику від пошкоджень та забруднення.

3. PTZ камери (pan-tilt-zoom):

Мають віддалене керування орієнтацією, нахилом і масштабуванням. Використовуються для активного моніторингу великих територій.

4. Камери з високою роздільною здатністю (HD, 4K):

Забезпечують високу деталізацію зображення, що необхідно для розпізнавання номерних знаків та осіб. Часто використовуються на важливих об'єктах з високими вимогами до безпеки.

Камери відеоспостереження використовуються для:

- Моніторингу та запису: Забезпечення постійного візуального контролю над об'єктом.
- Розпізнавання та аналітики: Використання алгоритмів для виявлення небезпечних ситуацій або незаконних дій.
- Інтеграції з іншими системами: Взаємодія з системами контролю доступу та сигналізації для автоматичного реагування на інциденти[2].

Камери відеоспостереження є важливим інструментом для забезпечення безпеки, дозволяючи не тільки пасивно спостерігати, але й активно реагувати на загрози, оптимізуючи загальну систему захисту об'єкта.

2.4 Сигналізація, детектори руху та сенсори

Сигналізація, детектори руху, та різноманітні сенсори є критичними компонентами сучасних систем безпеки, які забезпечують раннє виявлення небезпечних ситуацій та автоматичне сповіщення відповідних служб або власників. Ці системи можуть діяти окремо або інтегруватися з іншими системами для створення комплексної захисної мережі.

Сигналізаційні системи можуть бути поділені на дві основні категорії:

1. Місцеві сигналізації: Не пов'язані з віддаленим моніторинговим центром. Вони видають гучний звуковий або світловий сигнал у випадку виявлення проникнення, що служить для відлякування зловмисників та сповіщення місцевих осіб про інцидент.

2. Системи моніторингу: Пов'язані з центром спостереження, який може відреагувати на тривогу, відправивши охорону або повідомивши поліцію. Часто включають в себе оплату абонентської плати.

Детектори руху виявляють фізичний рух у певній області та активують сигналізацію або включають систему відеоспостереження. Основні типи детекторів руху:

- Інфрачервоні детектори (PIR): Найпоширеніші, реагують на зміни в тепловій картині, спричинені рухом теплих об'єктів, таких як люди або тварини.
- Мікрохвильові детектори: Використовують радіохвилі для виявлення руху; можуть виявляти рух через перешкоди, але є більш чутливими до помилкових спрацьовувань.

Сенсори в системах безпеки можуть включати:

- Датчики відкриття: Встановлюються на дверях та вікнах, реагують на їх відкриття.
- Сенсори розбиття скла: Реагують на звук розбиття скла, що може бути ознакою спроби проникнення.
- Сенсори диму та тепла: Важливі для раннього виявлення пожеж.
- Сенсори витоку води: Використовуються для захисту від затоплень, сповіщаючи про непередбачені витоки води в домі чи на підприємстві.

Інтеграція різних детекторів і сенсорів з централізованими системами управління і моніторингу забезпечує більш ефективний та автоматизований відгук на потенційні загрози. Наприклад, коли датчик руху активується, система може автоматично направляти відео з найближчої камери відеоспостереження до оператора охоронної служби, забезпечуючи швидке і точне реагування.

Під час розробки і впровадження систем з детекторами руху та

різноманітними сенсорами важливо враховувати декілька аспектів:

Помилкові спрацьовування: Особливо важливо для систем великих масштабів з великою кількістю датчиків. Необхідно ретельно налаштовувати чутливість сенсорів та оптимізувати їх розташування для мінімізації помилкових тривог.

Інтеграція з іншими системами: Планування інтеграції з іншими системами безпеки має бути виконане з урахуванням можливостей розширення та оновлення системи, щоб адаптуватися до змінних технологічних вимог і загроз.

Обслуговування та підтримка: Регулярне технічне обслуговування і перевірка всіх компонентів системи є критично важливими для забезпечення їх безперебійної роботи.

Сучасні системи сигналізації, детектори руху та сенсори значно покращують здатність об'єктів виявляти і реагувати на загрози в реальному часі, забезпечуючи важливий шар захисту в комплексних системах безпеки. Їх ефективне впровадження та інтеграція можуть значно знизити ризики для безпеки об'єктів та забезпечити спокій їх власникам і користувачам.

2.5. Інтегровані системи безпеки

Інтегровані системи безпеки представляють собою комплексне рішення, яке об'єднує різні види захисних технологій та обладнання в єдину керовану і централізовану систему. Це дозволяє досягти більшої ефективності у захисті об'єктів завдяки взаємодії між окремими компонентами системи.

Основні складові інтегрованих систем безпеки:

1. Відеоспостереження. Камери відеоспостереження є очима системи, забезпечуючи візуальний моніторинг об'єктів і периметру.

2. Контроль доступу. Системи контролю доступу обмежують доступ до об'єкта або окремих його частин за допомогою карток доступу, біометричних даних або кодових панелей.

3. Сигналізація. Системи сигналізації реагують на неавторизоване проникнення чи інші аномалії, відправляючи сповіщення власникам або службі охорони.

4. Детектори руху та сенсори. Ці пристрої виявляють рух або інші аномальні умови, такі як дим, вогонь, або витік води, що активує відповідні системи відповіді [9].

5. Системи управління та моніторингу. Центральні системи управління збирають дані з усіх підсистем, аналізують їх та забезпечують операторам інтерфейс для моніторингу та керування системою.

Переваги інтегрованих систем безпеки:

- Покращена координація: Інтеграція різних систем дозволяє швидше реагувати на загрози, оскільки всі компоненти спілкуються між собою.
- Ефективність витрат: Зниження витрат на установку та обслуговування, оскільки одна інтегрована система може виконувати функції декількох окремих систем.
- Масштабованість: Інтегровані системи легко масштабуються, дозволяючи додавати нові компоненти або технології без необхідності повного перепроєктування системи.

Виклики при реалізації:

Комплексність установки. Інтегровані системи вимагають ретельного планування і професійної установки, а також регулярного технічного обслуговування.

Сумісність компонентів. Не всі системи безпеки спроєктовані для взаємодії одна з одною, що може вимагати додаткових витрат на інтеграційні компоненти або програмне забезпечення.

Залежність від технологій. Інтенсивне використання цифрових технологій збільшує вразливість до кібератак та технічних збоїв [6].

Інтегровані системи безпеки представляють собою потужне рішення для забезпечення всебічного захисту об'єктів. Однак їх ефективність залежить від якості компонентів, рівня їх інтеграції та кваліфікації персоналу, який з ними працює.

3. РОЗРОБКА ТА МОДЕЛЮВАННЯ АЛГОРИТМУ ОЦІНКИ СИСТЕМ ЗАХИСТУ

У цьому розділі я описав процес розробки та моделювання алгоритму для оцінки ефективності систем захисту. Алгоритм базується на поєднанні процесів: порівняння ринку, вибір системи, написання топ-скрипту, моделювання та візуалізації. Моделювання включає в себе використання програмного забезпечення для візуалізації та симуляції роботи системи, що дозволяє оптимізувати параметри перед реальним впровадженням.

Такий підхід дозволяє значно удешевити традиційні методи встановлення охоронних систем, коли для збору даних необхідна була ціла команда спеціалістів, то за допомогою мого способу це можна робити невеликою командою з 2-3 людей, а виміри брати спеціалізованим ПЗ котре слугує для створення 3D скану приміщення за допомогою лідару чи камери.

Чому важливо приділяти увагу саме комплексним системам захисту? Згідно статистиці, кількість IoT пристроїв у використанні стрімко зростає, що показано на рисунку 3.1, тому що такі системи гарно себе зарекомендували. Саме через це моєю ідеєю було впровадження СРП у різноманітні захисні комплекси навідміну від старих, аналогових методів [12].

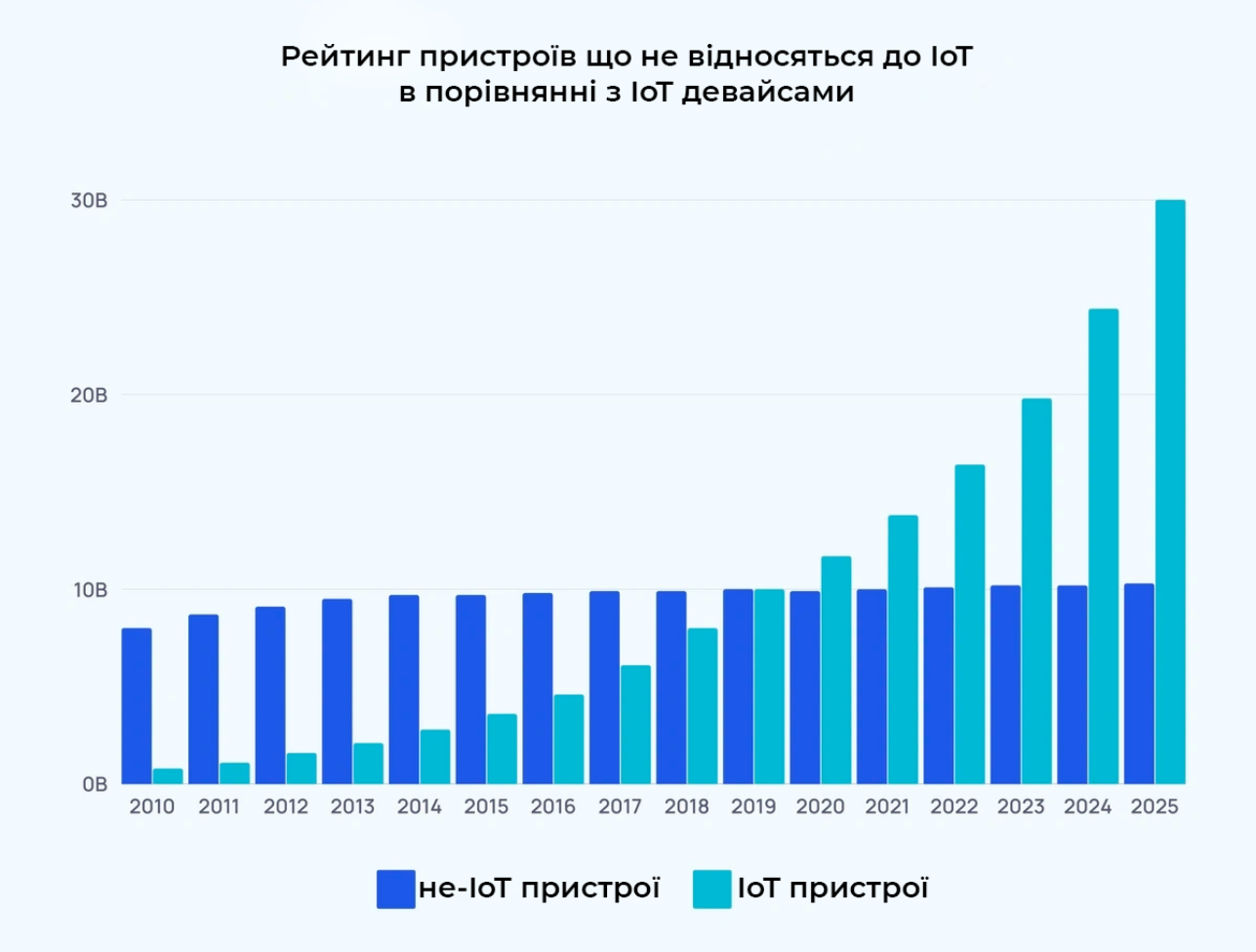

Рисунок 3.1 – Графік відносності кількості пристроїв за останні 14 років

Розробка алгоритму оцінки систем захисту включає кілька ключових етапів: визначення критеріїв оцінки, створення методики побудови алгоритму та його практичне втілення у вигляді моделі, яка може бути симульована для візуалізації роботи системи. Розглянемо кожен з цих етапів детальніше.

1. Основні критерії оцінки

Перший крок у розробці алгоритму оцінки - це визначення критеріїв, за якими буде вимірюватися ефективність систем захисту. [11] Для систем відеоспостереження та датчиків руху ці критерії можуть включати:

- Дальність дії: Максимальна відстань, на якій система ефективно здійснює моніторинг.
- Кут огляду: Важливо для камер; більший кут огляду може зменшити кількість камер, необхідних для покриття тієї ж площі.
- Роздільна здатність: Висока роздільна здатність важлива для ідентифікації облич або інших важливих деталей на відеозаписах.

- Чутливість до руху: Для датчиків руху, здатність виявляти рух на різних дистанціях і при різних умовах освітлення.
- Надійність: Частота помилкових тривог або пропущених подій.

2. Методика побудови алгоритму

Алгоритм оцінки систем захисту розроблений мною представлений у вигляді таблиці в Microsoft Excel, де кожен рядок відповідає окремому пристрою (наприклад, камері або датчику руху), а стовпці містять параметри для порівняння. Кожен параметр вимірюється і порівнюється з базовими вимогами, що дозволяє оцінити придатність кожного пристрою для конкретної зони захисту, це зображено на таблиці 3.

Назва системи або компонента	Надійність	Стійкість до зовнішніх впливів	Масштабованість	Взаємодія з іншими системами	Вартість встановлення та експлуатації	Зручність користування	Загальна оцінка
Vivint SmartHome	5	5	5	5	2	5	4,40
Arlo Pro 2	5	5	4	4	3	5	4,35
SimpliSafe	4	4	5	4	4	5	4,30
U-Prox MP WiFi S	5	3	4	5	5	3	4,20
Ring Alarm Pro	5	4	4	5	3	4	4,15
Cove Essential	4	4	4	4	4	4	4,00
Frontpoint	4	3	5	4	3	5	3,95
ADT Command	4	3	3	4	4	4	3,75
Abode	3	3	4	3	5	4	3,70
Nest Secure	4	4	4	3	3	4	3,65
Canary All-in-One	3	4	3	3	5	3	3,55

Таблиця 3 – Порівняння оцінок ринкових систем захисту

Для кожного пристрою розраховується оцінка з урахуванням важливості кожного параметра, що дозволяє зрозуміти його ефективність в контексті

конкретних потреб безпеки. Можна застосувати вагові коефіцієнти для критеріїв в залежності від їхньої значущості.

Мною була представлена таблиця рейтингу, в якому я оцінив різноманітні системи захисту доступні на ринку, включає такі критерії оцінки:

- Надійність
- Стійкість до зовнішніх впливів
- Масштабованість
- Взаємодія з іншими системами
- Вартість встановлення та експлуатації
- Зручність користування

Результатом є виведений і відсортований рейтинг з загальними оцінками по якому можна швидко обрати найкращу систему захисту для приміщення.

3. Моделювання та симуляція за допомогою Sweet Home 3D

Для візуалізації як система захисту працює на практиці, можна використати програму Sweet Home 3D, яка дозволяє створити 3D модель будинку або будь-якого іншого об'єкта. У цій моделі розміщуються віртуальні пристрої відеоспостереження та датчики руху, що дозволяє симулювати їхню роботу і оцінити покриття об'єкта.

4. 3D моделювання будинку

Вже створена 3D модель може бути використана для демонстрації взаємодії між різними компонентами системи захисту та для наочного представлення того, як різні зони об'єкта захищені. Ви створили відеоролик, який показує візуалізацію роботи всієї системи, що є чудовим способом продемонструвати потенційним користувачам або оцінювачам ефективність розробленої системи.

Ці кроки дозволяють не тільки розробити ефективний алгоритм оцінки, але й наочно продемонструвати його практичну придатність і взаємодію з реальними об'єктами.

3.1 Основні критерії оцінки

При розробці алгоритму оцінки систем захисту, ключовими критеріями,

які потрібно розглядати, є:

1. Ефективність детекції

Цей критерій вимірює здатність системи точно виявляти реальні загрози без частих помилкових спрацьовувань. Для камер відеоспостереження це може оцінюватися за чіткістю зображення та здатністю розпізнавати об'єкти за певних умов освітленості. Для детекторів руху — через чутливість та здатність відрізняти рух від фонових змін у середовищі.

2. Стійкість до зовнішніх впливів

Включає здатність системи захисту працювати в різноманітних екологічних умовах, в тому числі при екстремальних температурах, вологості, а також умовах високої запиленості чи механічних впливів. Це особливо важливо для обладнання, що використовується на відкритому повітрі.

3. Масштабованість

Масштабованість оцінюється як можливість системи адаптуватися до збільшення або зменшення кількості об'єктів моніторингу або зміни обсягу захищеної території без потреби в повній заміні компонентів.

4. Взаємодія з іншими системами

Критерій визначає, наскільки легко система інтегрується з іншими системами безпеки або автоматизації. Це може включати інтеграцію з системами контролю доступу, пожежною сигналізацією, а також можливість управління через централізовані платформи управління.

5. Вартість встановлення та експлуатації

Цей критерій включає первинну вартість придбання та встановлення обладнання, а також витрати на його обслуговування та ремонт. Також розглядається економічна ефективність системи з погляду співвідношення вартості та функціональності.

6. Юзабіліті (зручність користування)

Оцінюється легкість налаштування та щоденного використання системи кінцевими користувачами, включаючи інтуїтивність інтерфейсів, доступність функцій моніторингу та управління через мобільні додатки чи веб-інтерфейси.

Ці критерії слугують базою для створення оціночної матриці в Microsoft

Excel, де можливо систематично порівнювати різні системи захисту згідно з введеними параметрами і визначати їх придатність для конкретних застосувань.

3.2 Методика побудови алгоритму

Розробка алгоритму оцінки систем захисту включає створення структурованого підходу до збору, аналізу та порівняння даних про різні компоненти безпекових систем. Основною метою є створення об'єктивного і відтворюваного процесу оцінки, що дозволяє зрозуміло класифікувати та вибрати оптимальні системи для конкретних умов використання.

Кроки побудови алгоритму

1. Визначення параметрів для оцінки:

На основі визначених у попередньому розділі критеріїв (надійність, стійкість до зовнішніх впливів, масштабованість, взаємодія з іншими системами, вартість експлуатації, юзабіліті), визначити ключові параметри, які будуть вимірюватися для кожного типу обладнання.

2. Створення матриці оцінки:

Використання таблиці Microsoft Excel для створення матриці, де кожен рядок відповідає конкретній системі або компоненту, а стовпці містять параметри для оцінки.

3. Розробка методу введення та обробки даних:

- Визначення, як будуть збиратися дані (наприклад, через тестування, відгуки від користувачів, технічні специфікації).
- Встановлення формули для визначення загальної оцінки кожної системи на основі вагових коефіцієнтів для кожного критерію.

4. Тестування та калібрування алгоритму:

- Проведення пілотного тестування алгоритму з використанням відомих даних для перевірки його точності та об'єктивності.
- Калібрування параметрів алгоритму згідно отриманих результатів для забезпечення найбільшої точності оцінок.

Після розробки, алгоритм може бути використаний для оцінки поточних або нових систем захисту, дозволяючи керівництву компаній або охоронним агенціям обирати найбільш ефективні рішення на основі об'єктивних даних. Це

забезпечує зменшення витрат та підвищення загальної безпеки об'єктів.

За допомогою цього алгоритму можна також проводити регулярні перевірки існуючих систем для забезпечення їх актуальності та ефективності в умовах змінних загроз та технологічного розвитку.

3.3 Моделювання та симуляція

Для моделювання систем захисту, особливо коли стандартне програмне забезпечення не може бути використане через обмеження нерозголошення, можна використовувати альтернативні методи. У цьому випадку було обрано використання програми Sweet Home 3D для створення макетів будинків, а також Adobe After Effects для демонстрації симуляційного процесу.

Sweet Home 3D дозволяє створювати детальні 3D моделі будівель з можливістю розміщення віртуальних камер та інших компонентів систем безпеки для візуалізації їх розташування та оглядових зон.

1. Створення плану будинку: На першому етапі розробляється докладний план приміщень, в якому визначаються основні зони для моніторингу.

2. Розміщення компонентів безпеки: Камери, датчики руху, та інші сенсори розміщуються у стратегічних місцях відповідно до розробленої схеми безпеки.

3. Візуалізація зон охоплення: Програма дозволяє візуалізувати зони охоплення камер та сенсорів, що є корисним для аналізу "мертвих зон".

Adobe After Effects використовується для створення відеовізуалізації, яка імітує реальний процес моніторингу та відповіді системи на зовнішні подразники або загрози. Це включає анімацію шляхів можливого проникнення та відповіді системи сигналізації.

1. Сценарії відповіді: Різні сценарії безпекових порушень моделюються для демонстрації, як система реагуватиме на реальні інциденти.

2. Демонстрація взаємодії систем: Показується, як різні компоненти системи взаємодіють для забезпечення комплексної відповіді.

Цей підхід до моделювання має свої обмеження, оскільки він не завжди може точно відтворити реальні фізичні та технічні характеристики систем захисту. Такі моделі можуть бути корисні для первинної візуалізації та

розуміння потенційної функціональності, але вони мають використовуватись у поєднанні з більш точним спеціалізованим програмним забезпеченням від охоронних компаній для детального аналізу та точної оцінки ефективності систем.

Такий підхід дозволяє більш ефективно використовувати доступні ресурси та демонструвати потенційні можливості системи безпеки, що може бути особливо корисним на етапах планування та розробки проектів.

3.4 3D моделювання будинку

Sweet Home 3D є ефективним інструментом для 3D моделювання будинків, що дозволяє створювати детальні плани приміщень і розміщувати меблі та інші елементи інтер'єру, а також моделювати системи безпеки.

Процес створення 3D моделей у Sweet Home 3D

1. Початок роботи:

Створення нового проекту в Sweet Home 3D починається з розробки плану поверху.

2. Моделювання внутрішнього простору:

Після створення структури будинку можна розміщувати меблі, побутову техніку та інші елементи інтер'єру з обширної бібліотеки, що включена в програму. Кожен елемент був мною бути точно відрегульований за розміром та орієнтацією для точного планування простору, для демонстрації – рисунок 3.3 та рисунок 3.4, на них видно що інтер’єр та екстер’єр був розроблений детально, що може допомогти при візуальній оцінці ризиків в майбутньому.

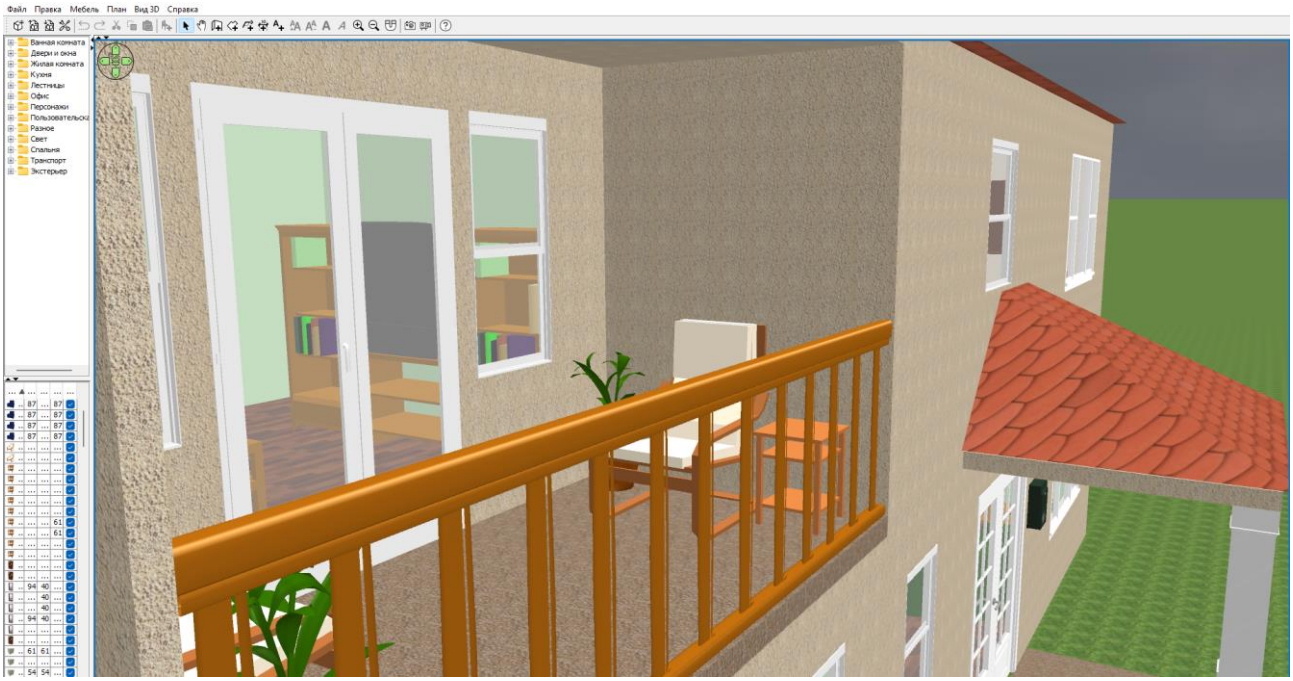

Рисунок 3.3 – Передній фасад з інтер’єром розробленої моделі

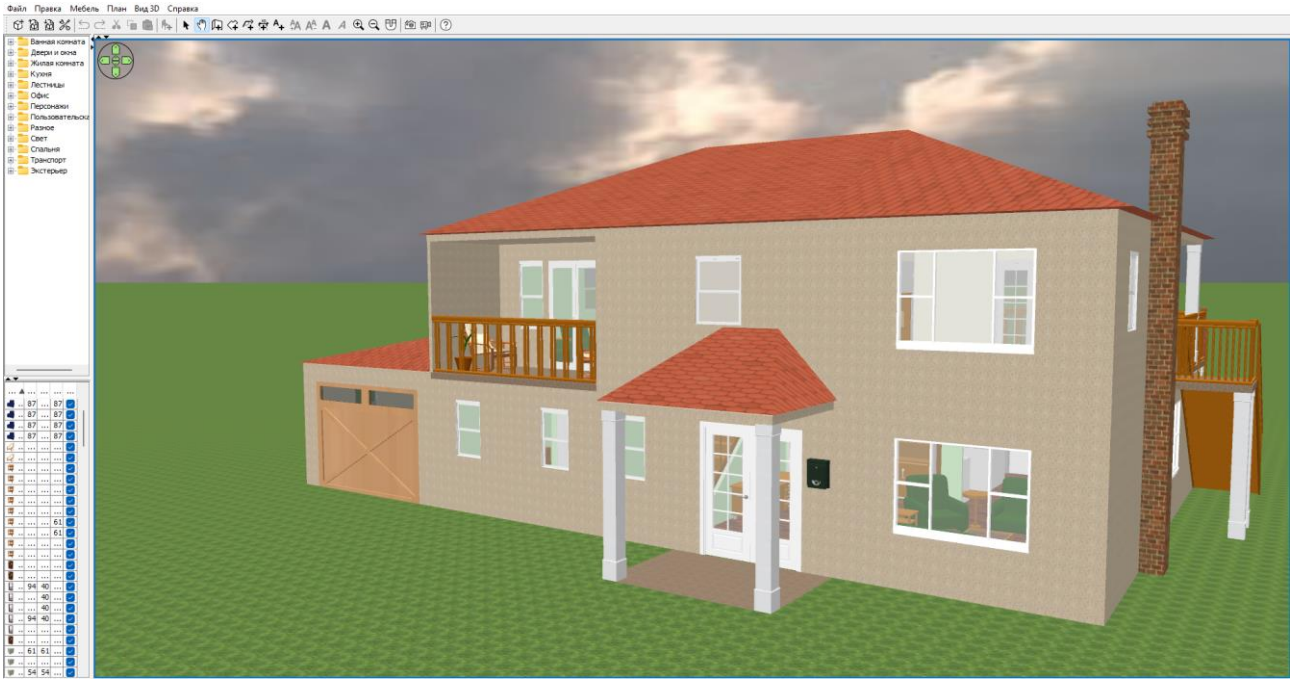

Рисунок 3.4 – Загальний план розробленої моделі

3. Візуалізація та перегляд:

Sweet Home 3D дозволяє переглядати створену 3D модель у реальному часі з різних точок зору. Віртуальний візит дає можливість "пройтися" по моделі будинку, що сприяє кращому уявленню про кінцевий результат.

4. Моделювання систем безпеки:

Для інтеграції систем безпеки, таких як камери відеоспостереження та датчики, Sweet Home 3D дозволяє моделювати їх розташування і покриття, допомагаючи аналізувати ефективність розміщення з точки зору забезпечення безпеки об'єкта.

Для об'єкту (будинку) я обрав СРП U-Prox MP WiFi S, що зображена на рисунку 3.5, та знайшов найбільш відповідні 3D моделі для демонстрації. Також я вже відразу інтегрував розширення для того аби показати можливості до масштабування системи. Частина елементів зображена на рисунку 3.6

Рисунок 3.5 – Охоронна система U-Prox MP WiFi S

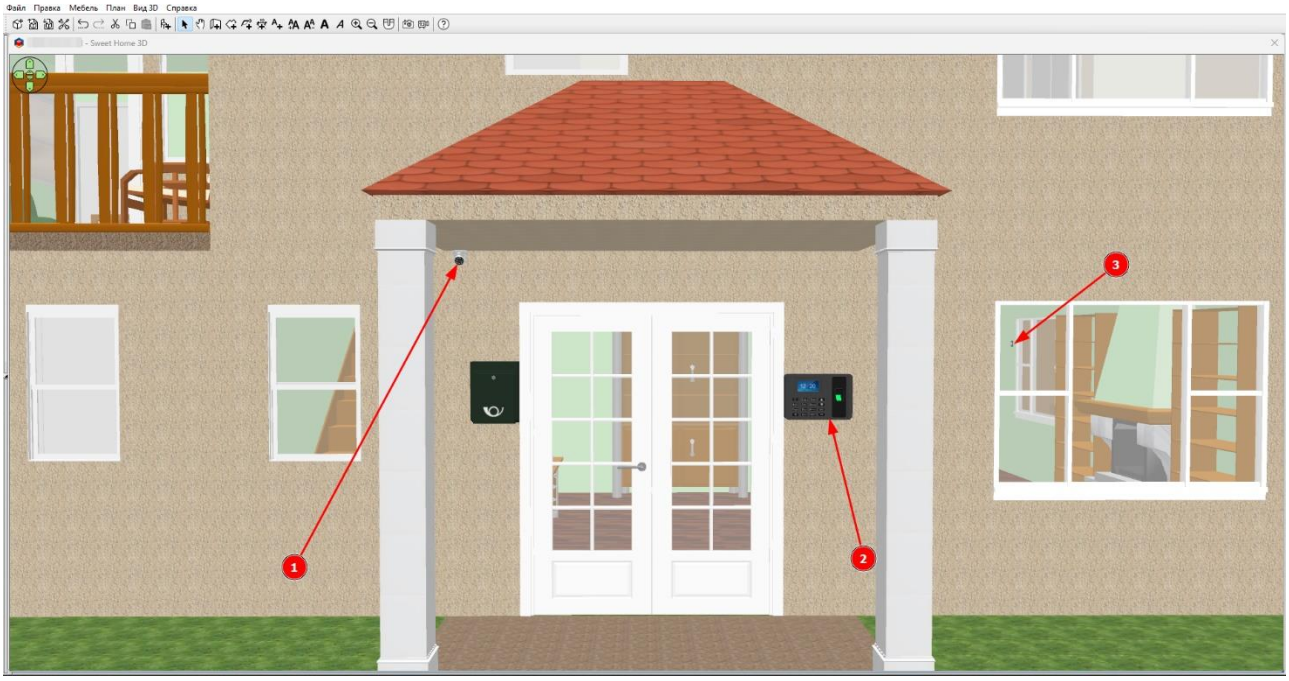

Рисунок 3.6 – Розміщення елементів СРП на 3D моделі

На рисунку видно 3 елементи:

1) IP камера TC-C32HS з вбудованим мікрофоном, турельним форм фактором та кутами огляду: Горизонтальні: 99.7°, Вертикальні: 55.1° що дозволяє охопити всю територію будівлі спереду.
2) 3D аналог терміналу з сенсорною панеллю і сканером відбитків пальців для безключового доступу до дверей
3) Магнітоконтактний сповіщувач MAKS WDC mini, що слугує для детекції відкривання вікна

Чому Sweet Home 3D?

Основною причиною стала неможливість використати пропрієтарне ПЗ компанії в якій я проходив практику через договір про нерозголошення комерційної таємниці, тому довелось імітувати процеси проектування в інших програмах. При цьому я знайшов багато плюсів у використанні саме цієї програми:

Доступність та відкритість: Програма є безкоштовною та відкритою, що робить її доступною широкому колу користувачів, включаючи студентів, дизайнерів інтер'єру та архітекторів.

Незалежність від обмежень на російське ПЗ: Важливим аспектом вибору Sweet Home 3D є його відповідність законодавчим обмеженням України щодо

використання російського програмного забезпечення, що гарантує легальність і безпечність використання програми в освітніх та комерційних проектах.

Основною виграшною особливістю є те що програма розповсюджується за моделлю «Open Source» («Відкрите Джерело»), що означає легкість модифікації та підтримку сторонніми розробниками і повністю прозорість коду програми.

Цей інструмент є ефективним рішенням для візуалізації і планування не тільки звичайних будинків, але й складних систем безпеки, забезпечуючи важливе поєднання функціональності, доступності та законності.

Sweet Home 3D стоїть серед популярних програм для 3D моделювання, таких як SketchUp, AutoCAD, і Revit. Кожна з цих програм має свої особливості та відмінності, які роблять їх більш або менш підходящими для конкретних завдань.

Плюси Sweet Home 3D:

- Sweet Home 3D має інтуїтивно зрозумілий інтерфейс, який дозволяє користувачам без досвіду швидко освоїти основи 3D моделювання.
- Програма є повністю безкоштовною, що робить її доступною для студентів, неприбуткових організацій, а також для особистого використання.
- Включає велику кількість меблів, фіксованих елементів і обладнання, яке можна легко імпортувати та використовувати в проектах.
- Sweet Home 3D є відкритим програмним забезпеченням, що дозволяє спільноті розробників вносити свої поліпшення та розширення.

Мінуси Sweet Home 3D:

Хоча програма досить зручна для базового моделювання, вона не має деяких складних інструментів, які пропонуються в професійних CAD програмах. Sweet Home 3D може не забезпечувати необхідну точність в моделюванні для деяких складних архітектурних або інженерних проектів.

Альтернативи Sweet Home 3D та їх особливості:

1. SketchUp:

Хоча SketchUp відомий своїми потужними інструментами для 3D моделювання і широко використовується професіоналами, він вимагає платної

підписки для доступу до всіх функцій.

2. AutoCAD:

AutoCAD є лідером в галузі професійного CAD проектування, але його висока вартість і складність можуть бути недоцільними для користувачів, які шукають простіше рішення для базового 3D моделювання.

3. Revit:

Revit відмінно підходить для складних архітектурних проектів і інтеграції з BIM (Building Information Modeling), але його складність і вартість роблять його менш доступним для некомерційного використання.

Обравши Sweet Home 3D, я отримав доступ до простого, але ефективного інструменту для 3D моделювання, який добре підходить для освітніх проектів і невеликих архітектурних практик. Його доступність простота використання роблять його особливо привабливим вибором у порівнянні з комерційними програмами, що вимагають значних фінансових інвестицій.

4. ПРАКТИЧНЕ ВПРОВАДЖЕННЯ ТА ОБГОВОРЕННЯ ПЕРСПЕКТИВ

У цьому розділі моєї дипломної роботи я розглядаю практичні аспекти впровадження систем безпеки та дискутую можливі майбутні розвитки в області технологій захисту. Завдяки алгоритмічному підходу до оцінки і вибору оптимальних систем, ми можемо забезпечити ефективну безпеку для конкретних об'єктів.

4.1 Вибір оптимальної системи захисту для конкретного будинку

На основі розробленого алгоритму оцінки було вибрано оптимальну систему безпеки для демонстраційного житлового будинку. Система включає відеокамери з високою роздільною здатністю, сучасні датчики руху, інтегровані сигналізації та смарт-домові технології. Важливою частиною системи є її здатність до інтеграції з мобільними пристроями, що дозволяє власникам контролювати стан безпеки в реальному часі з будь-якої точки світу.

4.2 Налаштування систем

Налаштування системи виражається в написанні топ-скрипту для управління і відладки параметрами охоронної системи. Програмування системи вимагало детальної настройки для забезпечення злагодженої роботи всіх компонентів і мінімізації помилкових спрацьовувань.

4.3 Обговорення результатів дослідження

Після встановлення та тестування системи, я проаналізував її ефективність. Результати показали, що сучасні технології значно підвищують рівень безпеки. Виявлено, що інтеграція різних компонентів значно покращує час реакції на потенційні загрози та дозволяє власникам більш ефективно керувати системою.

4.4 Перспективи розвитку технологій захисту

Подальші дослідження будуть спрямовані на вдосконалення алгоритмів машинного навчання для прогнозування потенційних загроз та підвищення точності системи. Також має місце розробка спеціалізованого програмного забезпечення для емуляції різних навантажень на пристрої за заданими характеристиками, що дозволить ще точніше моделювати та оцінювати

ефективність систем безпеки.

Розроблений алгоритм дозволяє швидко і точно розробляти плани з облаштування захисними системами різноманітні типи будівель, з урахуванням специфічних вимог та умов. Інтеграція сучасних технологій підвищує рівень безпеки та зручності для користувачів, забезпечуючи економію витрат на розробку та експлуатацію систем. Подальший розвиток технологій та методів оцінки відкриває нові можливості для вдосконалення систем захисту і забезпечення безпеки об'єктів різного призначення.

На завершення, важливо зазначити, що технології в області систем безпеки стрімко розвиваються. В майбутньому можна очікувати появи ще більш розумних систем з штучним інтелектом, які зможуть не тільки реагувати на загрози, але й прогнозувати їх. Це включає вдосконалення алгоритмів машинного навчання для аналізу поведінки та визначення незвичайних паттернів, що можуть вказувати на потенційні загрози.

Ці перспективи вимагають подальших досліджень і інновацій, і я планую продовжувати працювати в цьому напрямку, аби забезпечити не тільки захист, але й передбачуваність у системах безпеки для житлових та комерційних об'єктів.

ВИСНОВКИ

У процесі виконання даної дипломної роботи було досягнуто поставленої мети – розроблено алгоритм встановлення та модернізації охоронних систем для житлових та нежитлових об'єктів, базуючись на сучасних технологіях та методах інтеграції в системи «Розумний Простір».

Створено алгоритм, що дозволяє оцінювати ефективність різних систем захисту, враховуючи такі параметри, як надійність, масштабованість, вартість, взаємодія з іншими системами та зручність використання.

Алгоритм представлений у вигляді таблиці Microsoft Excel, що забезпечує простий і зрозумілий спосіб порівняння різних систем та вибору найбільш оптимального варіанту.

Впроваджено методи інтеграції IoT, біометричних систем, бездротових технологій та штучного інтелекту для підвищення рівня безпеки та зручності користування.

Розроблено візуалізацію роботи охоронної системи на базі 3D моделі будівлі, створеної у Sweet Home 3D, та відеовізуалізацію у Adobe After Effects.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Zainab A., Amina I., Muhammad A., Baballe M., Sani S. Contribution of the IoT to the Security System – July 2023. – Vol. 3. – P. 2-3.
2. Bebis, G., Gyaourova, A., Singh, S., Pavlidis, I. Face recognition by fusing thermal infrared and visible imagery. Image Vis. Comput. – July 2006 – Vol. 24. №7, 727–742.
3. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / Rivest R.L., Shamir A., Adleman L. // Communications of the ACM. – February 1978. – Vol. 21. № 2. – P. 120-126.
4. Jain A.K., Flynn P., Ross A.A. Handbook of Biometrics / Jain A.K., Flynn P., Ross A.A. – New York: Springer, 2008. – 556 p.
5. Li S., Xu L.D., Zhao S. The Internet of Things: A Survey. – April 2015. – Vol. 17. № 2. – P. 243-259.
6. Stallings W. Cryptography and Network Security: Principles and Practice / Stallings W. – 7th ed., 2016. – 768 p.
7. National Institute of Standards and Technology (NIST) - Security and Privacy Controls for Information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 8 травня 2024 р.)
8. International Journal of Smart Home (IJSH). URL: https://gvpress.com/journals/IJSH/ (дата звернення 15 травня 2024 р.)
9. Journal of Visual Communication and Image Representation (JVCIR). URL: https://www.sciencedirect.com/journal/journal-of-visual-communication-and-image-representation (дата звернення 15 травня 2024 р.)
10. Journal of Network and Computer Applications (JNCA). URL: https://www.sciencedirect.com/journal/journal-of-network-and-computer-applications (дата звернення 15 травня 2024 р.)

11. A Journal of Research and Innovation. Information Systems Frontiers (ISF). URL: https://link.springer.com/journal/10796 (дата звернення 16 травня 2024 р.)

12. Exploding Topics: 80+ Amazing IoT Statistics (2024-2030). URL: https://explodingtopics.com/blog/iot-stats (дата звернення 10 червня 2024 р.)

ДОДАТОК А
ЛІСТИНГ ТОП-СКРИПТУ ДЛЯ КЕРУВАННЯ СИСТЕМОЮ БЕЗПЕКИ

Топ-скрипт для керування системою безпеки U-Prox MP WiFi, збору інформації з датчиків у файли, написаний мовою Python та припускає що за наданою адресою розміщується сервер і відкритий порт охоронної компанії який слугує приймачем реквестів та каналом підключення оператора до системи датчиків

```
import logging
from logging.handlers import RotatingFileHandler
import datetime
import time
import threading
import requests
log_filename_detailed = 'full_log.log'
log_formatter_detailed = logging.Formatter('%(asctime)s - %(levelname)s - %(message)s')
log_handler_detailed = RotatingFileHandler(log_filename_detailed, maxBytes=5*1024*1024, backupCount=5)
log_handler_detailed.setFormatter(log_formatter_detailed)
log_filename_simple = 'mini_log.txt'
log_formatter_simple = logging.Formatter('%(message)s')
log_handler_simple = RotatingFileHandler(log_filename_simple, maxBytes=5*1024*1024, backupCount=5)
log_handler_simple.setFormatter(log_formatter_simple)
logger_detailed = logging.getLogger('detailed')
logger_detailed.addHandler(log_handler_detailed)
logger_detailed.setLevel(logging.INFO)
logger_simple = logging.getLogger('simple')
logger_simple.addHandler(log_handler_simple)
```

```
logger_simple.setLevel(logging.INFO)
logger_detailed.info("Ініціалізована система детального логування")
logger_simple.info("Ініціалізована система короткого логування")
SECURE_AGENCY_URL = "http://127.0.0.1:8000/report"

class SecuritySystem:
    def __init__(self):
        self.sensors = {'двері': False, 'вікно': False, 'датчик руху': False}
        self.alarm_status = False
        logger_detailed.info("Систему безпеки Ініціалізовано")
    def update_sensor_status(self, sensor, status):
        self.sensors[sensor] = status
        simple_log_message = f"{datetime.datetime.now()} - статус сенсора
{sensor.capitalize()} змінено на {status}"
        if status:
            logger_simple.warning(f"УВАГА!!! {simple_log_message}")
        else:
            logger_simple.info(simple_log_message)
        detailed_log_message = f"статус сенсора {sensor.capitalize()} змінено на
{status}"
        if status:
            logger_detailed.warning(f"УВАГА!!! {detailed_log_message}")
        else:
            logger_detailed.info(detailed_log_message)
        if status:
            self.send_alert_to_secure_agency(sensor, status)
    def send_alert_to_secure_agency(self, sensor, status):
        try:
            data = {
                "timestamp": str(datetime.datetime.now()),
                "sensor": sensor,
```

```
            "status": status
        }
        response = requests.post(SECURE_AGENCY_URL, json=data)
        if response.status_code == 200:
            logger_detailed.info(f"Надіслано запит до охоронної службі: {data}")
        else:
            logger_detailed.error(f"Не вдалося відправити запит охоронній
службі: {response.status_code}")
    except Exception as e:
        logger_detailed.error(f"Помилка надсилання запиту охоронній службі:
{e}")
  def activate_alarm(self):
    if not self.alarm_status:
        self.alarm_status = True
        logger_detailed.warning("Сигналізацію активовано!")
  def deactivate_alarm(self):
    if self.alarm_status:
        self.alarm_status = False
        logger_detailed.info("Сигналізацію деактивовано")
  def receive_check_request_from_agency(self):
    logger_detailed.info("Оператор охоронної служби встановив з'єднання
для перевірки датчиків.")
security_system = SecuritySystem()
def handle_event(sensor, status):
  security_system.update_sensor_status(sensor, status)
  if status:
    logger_detailed.warning(f"Подію зафіксована на сенсорі: {sensor}.")
    security_system.activate_alarm()
  else:
    logger_detailed.info(f"Подію зафіксована на сенсорі: {sensor}.")
def monitor_sensors(real_time_data):
```

```
    for sensor, status in real_time_data.items():
        handle_event(sensor, status)
def check_time_and_adjust_settings():
    current_time = datetime.datetime.now()
    current_hour = current_time.hour
    if 22 <= current_hour or current_hour < 6:
        logger_detailed.info("Нічний режим активовано. Збільшено чутливість сенсорів.")
        security_system.update_sensor_status('датчик руху', True)
        security_system.update_sensor_status('двері', True)
        security_system.update_sensor_status('вікно', True)
    else:
        logger_detailed.info("Денний режим активовано. Встановлена стандартна чутливість сенсорів.")
        security_system.update_sensor_status('датчик руху', False)
        security_system.update_sensor_status('двері', False)
        security_system.update_sensor_status('вікно', False)
def update_sensor_status_periodically():
    try:
        while True:
            real_time_data = {'двері': True, 'вікно': True, 'датчик руху': True}
            for sensor, status in real_time_data.items():
                security_system.update_sensor_status(sensor, status)
            logger_detailed.info("Стан сенсорів оновлено.")
            time.sleep(30)
    except Exception as e:
        logger_detailed.error(f"Помилка при черговому оновлені стану сенсорів: {e}")
def announce_mode_periodically():
    try:
        while True:
```

```
            current_time = datetime.datetime.now()
            current_hour = current_time.hour
            if 22 <= current_hour or current_hour < 6:
                logger_detailed.info("Нагадування. Поточний режим: нічний.")
            else:
                logger_detailed.info("Нагадування. Поточний режим: денний.")
            time.sleep(300)
    except Exception as e:
        logger_detailed.error(f"Помилка при ініціалізації періодичного
сповіщення режиму роботи {e}")
def day_night_cycle_control():
    try:
        while True:
            check_time_and_adjust_settings()
            time.sleep(3600)
    except KeyboardInterrupt:
        logger_detailed.info("Контроль циклів День/Ніч зупинений
користувачем.")
def shutdown_system():
    try:
        logger_detailed.info("Ініціалізація завершення роботи системи.")
        security_system.deactivate_alarm()
        for sensor in security_system.sensors.keys():
            security_system.update_sensor_status(sensor, False)
        logger_detailed.info("Всі сенсори та сигналізацію було деактивовано.")
    except Exception as e:
        logger_detailed.error(f"Помилка при процесі завершення системи: {e}")
if __name__ == "__main__":
    update_thread = threading.Thread(target=update_sensor_status_periodically)
    update_thread.start()
```

```
    announce_mode_thread =
threading.Thread(target=announce_mode_periodically)
    announce_mode_thread.start()
    day_night_cycle_thread = threading.Thread(target=day_night_cycle_control)
    day_night_cycle_thread.start()
```

ДОДАТОК Б
ЛІСТИНГ ПРОГРАМИ ІМІТУВАННЯ СЕРВЕРУ ПРИЙМАННЯ ЗАПИТІВ

Програма імітування серверу слугує для тимчасової емуляції реагування на реквести від системи захисту. В справжніх умовах використовується такий самий метод але на стороні сервера відповідальної охоронної компанії.

```
from flask import Flask, request, jsonify
app = Flask(__name__)
@app.route('/report', methods=['POST'])
def handle_report():
    data = request.json
    print(f"Received report: {data}")
    return jsonify({"message": "Data received successfully"}), 200
if __name__ == "__main__":
    app.run(host='127.0.0.1', port=8000, debug=True)
```