НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.42:628.92:681.3.067.7:004.032.26

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	Завідувач кафедри
Інформаційних технологій	Комп'ютерних систем, мереж та кібербезпеки
_____ Болбот І.М., д.т.н, проф.	_____ Касаткін Д.Ю., к.п.н., доц.
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2024 р.	«___»_____2024 р.

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

На тему: «Розробка комп'ютерної системи управління інженерними комунікаціями для приватного будинку з використанням інтелектуальних алгоритмів»

Спеціальність «123 «Комп'ютерна інженерія»

Освітня програма: Комп'ютерні системи і мережі

Орієнтація освітньої програми: Освітньо-професійна

Гарант освітньої програми

_____ _____ _____

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник дипломного проекту

_____ _____ _____

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав _____ _____

(підпис) (ПІБ студента)

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____ / Касаткін Д.Ю., к.п.н., доц. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ МАГІСТЕРСЬКОЇ СТУДЕНТУ

Крижанівський Микола Сергійович
(прізвище, ім'я, по батькові)
Спеціальність (напрям підготовки): комп'ютерна інженерія_____

Тема кваліфікаційної бакалаврської роботи: «розробка комп'ютерної системи управління інженерними комунікаціями для приватного будинку з використанням інтелектуальних алгоритмів»_____
_____
_____
затверджена наказом ректора НУБіП України від "____" _____20___р. №_____
Термін подання завершеної роботи на кафедру _____
Вихідні дані до кваліфікаційної бакалаврської роботи _____
_____
_____
_____
_____
Перелік питань, що підлягають розробці:
1. _____
2. _____
3. _____
Перелік графічного матеріалу (за потреби) _____
_____

Дата видачі завдання "_____"_____2024 р.

Керівник магістерської роботи _____ _Місюра М. Д., к.т.н., доцент.__
(підпис) (прізвище та ініціали)
Завдання прийняв до виконання _____ ____Крижанівський М. С._____
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області		Виконано
2	Проектування системи		Виконано
3	Реалізація системи		Виконано
4	Тестування системи		Виконано
5	Оформлення пояснювальної записки		Виконано
6	Оформлення графічного матеріалу		Виконано

Студент _____ _____
(підпис) (ініціали та прізвище)

Керівник роботи _____ _____
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 89 сторінок, 30 рисунків, 5 додатки, 16 джерел.

Тема: Розробка комп'ютерної системи управління комунікаціями з використанням інтелектуальних алгоритмів

Предмет дослідження: Технології розроблення комп'ютерних систем управління комунікаціями.

Об’єкт дослідження: Процес управління комунікаціями в рамках комп’ютерних мереж, що забезпечують зв’язок та обмін інформацією.

Мета дипломного проекту: Проектування та розробка комп'ютерної системи управління комунікаціями, яка використовує інтелектуальні алгоритми для оптимізації процесів обміну інформацією та підвищення їх безпеки.

Завдання дипломного проекту:

Розробка алгоритмів для виявлення аномалій у комунікаційних потоках, що дозволяє запобігти несанкціонованому доступу.

Створення системи оповіщення про можливі загрози та втручання в комунікаційні мережі.

Апаратні та програмні засоби, що використовувалися при проектуванні: draw.io, Microsoft Visio, Cisco Packet Tracer, Tinkercad, java script.

Результати, досягнуті в процесі роботи: Було розроблено автоматизовану комп’ютерну систему управління комунікаціями з використанням інтелектуальних алгоритмів, проведено тестування системи, яке підтвердило її працездатність та ефективність у виконанні всіх заявлених функцій.

Одержані результати можуть бути використані для покращення безпеки комунікацій у різних сферах, що потребують захисту даних та підвищення рівня управління інформаційними потоками.

ЗМІСТ

No table of contents entries found.**СКОРОЧЕНІ ТА УМОВНІ ПОЗНАЧЕННЯ**

DC – Постійна напруга.

ПЗП – Постійний запам'ятовувальний пристрій

MCU – Мікроконтролер, інтегральна схема для управління електронними пристроями.

МОП – Технологія виготовлення електронних схем.

IC – Інтегральна схема.

NOR – Тип логічної схеми або пам'яті, де бітові комірки з'єднуються логічною операцією.

OTP – Одноразово програмована пам'ять, дані записуються один раз.

GPU – Графічний процесор, обробляє зображення для виведення на екран.

KNX – Відкрита система для автоматизації будівель.

IoT – Інтернет речей, мережа підключених пристроїв, що обмінюються даними.

RFID – Радіочастотна ідентифікація, технологія передачі даних за допомогою радіохвиль.

HD – Високоякісне зображення.

HD-TVI – Інтерфейс передачі відео високої роздільної здатності.

PIR – Пасивний інфрачервоний сенсор для виявлення теплових об'єктів.

ІЧ – Випромінювання в інфрачервоному діапазоні, використовується в сенсорах.

ВСТУП

У сучасному світі технології стрімко розвиваються, і з кожним роком все більше людей усвідомлюють важливість автоматизації та інтеграції різних систем у повсякденному житті. Однією з найбільш актуальних тем у цій сфері є розробка комп'ютерних систем управління комунікаціями, які використовують інтелектуальні алгоритми для оптимізації процесів управління в умовах "розумного дому". Концепція "розумного дому" передбачає інтеграцію різноманітних пристроїв і систем, що дозволяє забезпечити комфорт, безпеку та енергоефективність житлових приміщень.

Системи управління комунікаціями в "розумному домі" охоплюють широкий спектр функцій, таких як управління освітленням, опаленням, безпекою, а також моніторингом енергоспоживання. Використання інтелектуальних алгоритмів у цих системах дозволяє не лише автоматизувати рутинні процеси, але й адаптувати їх до потреб користувачів, забезпечуючи індивідуальний підхід та підвищуючи загальний рівень комфорту.

Однією з ключових переваг впровадження таких систем є можливість інтеграції різних технологій, що дозволяє створити єдину екосистему, яка реагує на зміни в навколишньому середовищі та поведінці мешканців. Наприклад, система може автоматично регулювати температуру в приміщенні в залежності від часу доби або присутності людей, а також забезпечувати безпеку шляхом моніторингу та управління сигналізацією.

Важливим аспектом розробки комп'ютерних систем управління комунікаціями є використання інтелектуальних алгоритмів, які дозволяють системі навчатися на основі даних, що збираються з різних сенсорів та пристроїв. Це відкриває нові можливості для оптимізації роботи системи, зменшення витрат на енергоспоживання та підвищення рівня безпеки. Наприклад, алгоритми машинного навчання можуть аналізувати поведінку користувачів і пропонувати оптимальні сценарії використання ресурсів, що, в свою чергу, сприяє зниженню витрат на комунальні послуги.

У рамках даної магістерської роботи буде розглянуто процес розробки комп'ютерної системи управління комунікаціями, що використовує інтелектуальні алгоритми для реалізації функцій "розумного дому" та сигналізації. Буде проведено аналіз існуючих рішень на ринку, вивчено вимоги до системи, а також розроблено концепцію та архітектуру системи. Основна увага буде приділена інтеграції різних компонентів, таких як сенсори, контролери та програмне забезпечення, а також розробці алгоритмів, які забезпечать ефективну взаємодію між ними.

Таким чином, метою даної роботи є створення ефективної та надійної комп'ютерної системи управління комунікаціями, яка не лише відповідатиме сучасним вимогам, але й забезпечить високий рівень зручності та безпеки для користувачів. Важливою частиною дослідження стане оцінка ефективності запропонованих рішень, що дозволить виявити сильні та слабкі сторони системи, а також можливості для подальшого вдосконалення.

У процесі роботи буде проведено детальний аналіз існуючих технологій, які використовуються в системах "розумного дому" та сигналізації. Це включатиме вивчення різних типів сенсорів, пристроїв управління, а також програмних рішень, які можуть бути інтегровані в єдину систему. Особливу увагу буде приділено інтелектуальним алгоритмам, які здатні адаптуватися до змін у середовищі та поведінці користувачів, що є критично важливим для забезпечення ефективності та зручності використання системи.

Крім того, в рамках дослідження буде розглянуто питання безпеки даних та конфіденційності, оскільки інтеграція різних технологій вимагає забезпечення надійного захисту інформації, що передається між пристроями. Це стане важливим аспектом для користувачів, які прагнуть забезпечити безпеку свого житла та особистих даних.

На завершення, результати даної магістерської роботи можуть стати основою для подальших досліджень у сфері автоматизації житлових приміщень, а також сприяти розвитку нових технологій, які забезпечать ще

більшу інтеграцію та автоматизацію в повсякденному житті. Впровадження таких систем не лише підвищить комфорт і безпеку, але й сприятиме зниженню витрат на енергоспоживання, що є актуальним у сучасному світі, де питання екології та раціонального використання ресурсів стають дедалі важливішими.

Таким чином, дана робота має на меті не лише розробку конкретної комп'ютерної системи, але й внесення свого внеску в розвиток інтелектуальних технологій, які можуть змінити наше уявлення про комфорт і безпеку

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА ОЦІНКА ІСНУЮЧИХ ВПРОВАДЖЕНЬ В СФЕРІ КОМП'ЮТЕРНОЇ СИСТЕМИ УПРАВЛІННЯ КОМУНІКАЦІЯМИ

1.1 Сучасні тенденції в розробці систем розумного дому

Сьогодні автоматизація процесів розвивається дуже швидко, спрощуючи життя людям. Вона охоплює всі сфери, від роботи до управління житловими будинками. Технології розумних будинків стають все популярнішими, оскільки допомагають полегшити побутові завдання, особливо для тих, хто має обмежені фізичні можливості.

Дослідження показало, що існуючі рішення для розумних будинків не завжди відповідають потребам людей з обмеженими можливостями. Було виявлено, що необхідно розробити спеціалізоване рішення, яке б повністю задовольняло їхні потреби. Це рішення має враховувати специфічні вимоги та адаптувати технології розумного будинку до особливостей життя таких людей. [25]

Порівняння функціональних вимог до адаптованих систем і можливостей сучасних рішень на ринку показало, що більшість з них не враховують потреби людей з обмеженими фізичними можливостями. Тому важливо створити технології, які б дійсно допомагали цій категорії населення.

Технологічний прогрес у сучасному світі розвивається дуже швидко і охоплює всі аспекти нашого життя. Технології оточують нас щодня, починаючи від смартфонів і годинників до розумних будинків. Головне питання, яке потребує дослідження, – це адаптація сучасних технологій розумних будинків до потреб людей з обмеженими фізичними можливостями.

Більшість авторитетних публікацій у цій галузі належить закордонним експертам, таким як Чері Превілль, Мухаммед Асадулла, Ларс Бергер та Андреас Швагер, які займаються дослідженням і вдосконаленням технологій розумних будинків і мають значний вплив у цій сфері.[25]

Основна частина матеріалу стосується апаратних систем, які базуються на мікроконтролерах. Мікроконтролер (MCU) – це компактний комп'ютер на одній мікросхемі, що складається з одного або кількох процесорів, пам'яті та програмованих периферійних пристроїв вводу/виводу. Він часто включає сегнетоелектричну оперативну пам'ять, флеш-пам'ять або ПЗП. Мікроконтролери призначені для вбудованих програм, на відміну від мікропроцесорів, які використовуються в персональних комп'ютерах. [17]

Сучасні мікроконтролери подібні до систем на чіпі (SoC), але є менш складними. SoC може містити компоненти мікроконтролера, але зазвичай інтегрує їх з більш просунутими периферійними пристроями, такими як графічні процесори або модулі Wi-Fi. Мікроконтролери широко використовуються в сфері розумних будинків. [17]

Усі рішення, пов’язані з апаратними системами, базуються на мікроконтролерах. Мікроконтролер (MCU – мікроконтролерний блок) є компактним комп’ютером, що розміщується на одній мікросхемі інтегральної схеми (IC) з оксиду напівпровідників металу (МОП). Він містить один або кілька процесорів (ядр), а також пам’ять і програмовані периферійні пристрої вводу/виводу. До складу мікросхеми часто входять пам’ять програм у вигляді сегнетоелектричної оперативної пам’яті, флеш-пам’яті NOR або ПЗП OTP, а також обмежена кількість оперативної пам’яті. Мікроконтролери призначені для вбудованих програм, на відміну від мікропроцесорів, які використовуються в персональних комп’ютерах або інших рішеннях, що орієнтовані на загальні потреби і складаються з різних дискретних мікросхем.

У сучасному контексті мікроконтролер можна порівняти з системою на чіпі (SoC), хоча він є менш складним. SoC може містити елементи мікроконтролера, але зазвичай об'єднує їх з більш розвиненими периферійними пристроями, такими як графічний процесор (GPU), модуль Wi-Fi або кілька співпроцесорів. Однією з галузей, де мікроконтролери знаходять широке застосування, є сфера розумних будинків. Якщо брати

розумні будинки або охоронні системи частіше за все використовують плату ATmega2661 (показано на рисунку 1.1)

Рисунок 1.1 - Плата ATmega2561

Тема розумних будинків стає все більш актуальною серед молоді, яка прагне автоматизувати та спростити різноманітні процеси, додаючи інтелект навіть до таких речей, як пилосос. [17]

Сучасний "smart-home" є апаратно-програмною системою, що об'єднує електронні та механічні компоненти будинку для полегшення керування ними через один пристрій. Такі системи можуть бути підключені до комп'ютерної мережі, що дозволяє користувачам дистанційно керувати ними через інтернет. Інтеграція інформаційних технологій допомагає синхронізувати роботу всіх систем і пристроїв у будинку на основі аналізу зовнішніх умов. [25]

Розумний будинок сприяє підвищенню ефективності у веденні справ, автоматизації побутових процесів та створює нові можливості для дозвілля. Незважаючи на те, що це дорога технологія, яка потребує планування під час будівництва і встановлення якісного обладнання, існують доступніші варіанти. Навіть стандартний будинок можна оснастити сучасними пристроями, що розширять функціональність та покращать мобільність.

Наприклад, завдяки розумній техніці, піч може нагадати про потребу в очищенні, а холодильник повідомить про необхідність ремонту. Якщо в будинку з’явиться незнайомий гість, сигналізація автоматично викличе охорону та попередить власника. Також система може налаштовувати освітлення, температуру або музику відповідно до присутності конкретної особи. "Розумний замок" на основі Bluetooth фіксує, коли хтось виходить із

кімнати, та дозволяє надавати доступ друзям чи родичам, з одночасним повідомленням власника про відкриття дверей.[12]

Розумний будинок розробляється спеціалізованими компаніями, які створюють унікальні проєкти з професійним підходом до дизайну та програмування. Алгоритми багатокімнатних систем адаптовані для виконання індивідуальних потреб мешканців і враховують зміни у навколишньому середовищі чи питання безпеки. Однією з ключових функцій є дистанційне управління, коли користувач може одним натисканням кнопки змінити атмосферу в будинку, а сама система автоматично аналізує умови та виконує необхідні налаштування. Крім того, пристрої в розумному будинку можуть бути об'єднані в мережу «plug and play», що підключається до інтернету.[7]

Окремої уваги заслуговують рішення для людей з обмеженими фізичними можливостями, які дозволяють їм значно полегшити виконання побутових завдань, таких як контроль за світлом, водою чи жалюзі, зменшуючи необхідність фізичних зусиль.[8]

Сучасні рішення розумних будинків дозволяють керувати ними за допомогою голосових команд, що усуває необхідність використовувати кнопки, смартфони чи комп’ютери. Це значно спрощує життя людей з повною паралізацією, для яких навіть прості дії, такі як вимкнення телевізора або світла, можуть бути проблемними. Така автоматизація полегшує щоденні завдання та іноді може врятувати життя, особливо якщо система включає функції безпеки або можливість виклику швидкої допомоги.

Автоматизація будинку охоплює різні сфери. Наприклад, керування системами опалення, вентиляції та кондиціонування повітря дозволяє дистанційно контролювати енергоефективність через інтернет завдяки простому інтерфейсу. Системи освітлення інтегруються в єдину мережу, що забезпечує зв’язок між різними елементами освітлення та централізованими обчислювальними пристроями. Крім того, за допомогою датчиків навколишнього середовища та розумних лічильників будинок може автоматично реагувати на зміни у використанні енергії.[25]

Інтеграція побутової техніки з інтелектуальними мережами дозволяє використовувати, наприклад, енергію сонячних панелей для роботи приладів у час пікової продуктивності. Системи безпеки також можна інтегрувати з домашньою автоматизацією, що дає можливість дистанційно контролювати відеоспостереження, блокувати двері та вікна по всьому будинку. .[25]

До того ж, такі системи допомагають виявляти витоки, реагувати на задимлення або підвищений рівень вуглекислого газу. Вони також підтримують автоматизацію для людей похилого віку та людей з інвалідністю, полегшуючи їхній побут. Окремі системи призначені для догляду за домашніми тваринами та дітьми, контролюючи їхні рухи та доступ до певних зон. Контроль якості повітря всередині і зовні приміщення, зокрема через датчики, допомагає моніторити рівень забруднення і навіть створювати мапи забруднення. [12]

Крім цього, розумна кухня може бути оснащена інвентарем для холодильників, програмами приготування їжі та системами стеження за процесом приготування, що робить цей аспект життя ще більш зручним і ефективним.[18]

Пристрої з голосовим управлінням, такі як Amazon Alexa або Google Home, часто використовуються для контролю побутової техніки та систем у розумному будинку. Існує кілька варіантів таких систем.

Провідні системи автоматизації базуються на з’єднанні всіх компонентів, таких як датчики, вимикачі, системи клімат-контролю та панелі управління, через одну дротову мережу, яка управляється з центрального щита. Основні переваги таких систем – висока надійність сигналу, легка інтеграція з іншими системами, довговічність через відсутність акумуляторних пристроїв та підвищена безпека завдяки низькому струму в вимикачах. Однак основним недоліком є необхідність у центральному щиті, що може ускладнювати доступ для людей з обмеженими фізичними можливостями.

Децентралізовані системи автоматизації функціонують так, що кожен пристрій має власний мікропроцесор і пам'ять, що не залежить від живлення. Якщо один пристрій виходить з ладу, інші продовжують працювати. Наприклад, система KNX дозволяє використовувати незалежні блоки, які забезпечують високу надійність і підтримку спеціальних сценаріїв управління. Попри це, такі системи також не завжди підходять для людей з обмеженими можливостями. .[25]

Відкриті протоколи автоматизації, як KNX, дозволяють різним виробникам створювати сумісні між собою пристрої, забезпечуючи широкий вибір обладнання та постійне оновлення. Відкрита система дає можливість обирати з різних варіантів дизайну та функціональності. Проте для людей з інвалідністю така система може бути складною через необхідність сертифікації кожного пристрою. [12]

Системи із закритими протоколами розробляються виробниками для зниження вартості та прискорення розробки. Вони пропонують цікаві рішення за нижчою ціною, проте обмежені в можливості модернізації та не завжди можуть бути адаптовані під потреби людей з обмеженими фізичними можливостями.

З огляду на проведений аналіз, можна зробити висновок, що на ринку відсутні універсальні рішення, адаптовані для людей з інвалідністю. Існують індивідуальні замовні системи, але вони часто вимагають значних фінансових витрат. Це свідчить про потребу в розробці нових систем, які будуть доступними, швидкими у виготовленні та налаштуванні. [18]

Основні вимоги до таких кастомних систем включають низьку вартість, можливість швидкого додавання нових компонентів, сумісність зі сторонніми модулями, повністю голосове управління, відсутність складних щитків та вимикачів, інтеграцію з функцією екстреного виклику та можливість зв'язку з контактами з "швидкого доступу". Якщо система відповідатиме цим критеріям, вона зможе вважатися адаптованою для людей з обмеженими можливостями, враховуючи їхні особливі потреби та повсякденні виклики.

1.2 Інтелектуальні алгоритми в управлінні комунікаціями

Інтелектуальні алгоритми відіграють важливу роль у системах управління комунікаціями, сприяючи ефективній взаємодії між пристроями, системами та користувачами. Вони автоматизують процеси передачі даних, прийняття рішень та адаптації систем до змінних умов, підвищуючи загальну продуктивність і точність операцій. Такі алгоритми широко використовуються в телекомунікаціях, комп'ютерних мережах, мобільних пристроях, розумних будинках та промислових системах автоматизації.

Однією з важливих галузей, де застосовуються інтелектуальні алгоритми, є маршрутизація в комп'ютерних мережах. Цей процес полягає у виборі найбільш оптимального маршруту для передачі даних між різними вузлами мережі. Для цього використовуються різні методи, такі як пошук найкоротшого шляху, заснований на алгоритмі Дейкстри, або векторні алгоритми відстаней, де кожен вузол обмінюється інформацією про відстань до інших вузлів. Інший підхід ґрунтується на інформації про стан з’єднань, що дозволяє кожному вузлу обчислювати оптимальний маршрут на основі даних від інших вузлів. Сучасні алгоритми маршрутизації все частіше використовують штучний інтелект і машинне навчання для прогнозування заторів, адаптації маршрутів під навантаження та автоматичного виявлення несправностей.

Мобільні мережі, зокрема 4G, 5G та мережі Інтернету речей (IoT), також активно використовують інтелектуальні алгоритми для оптимізації роботи. Вони допомагають ефективно розподіляти частотний спектр між користувачами, що є ключовим завданням у радіозв'язку. Алгоритми керування потоками даних дозволяють підтримувати баланс між якістю обслуговування та швидкістю передачі даних. У свою чергу, алгоритми керування трафіком можуть адаптуватися до змінних умов, таких як переміщення користувачів або зміни в навантаженні мережі, забезпечуючи постійне обслуговування.

Інтернет речей (IoT) постійно розширюється, і кількість підключених до мережі пристроїв стрімко зростає. Це вимагає інтелектуальних алгоритмів для управління трафіком, що забезпечують надійну передачу даних і оптимальне використання ресурсів. Наприклад, алгоритми класифікації трафіку дозволяють сортувати дані за їхньою важливістю та терміновістю, забезпечуючи першочергову обробку критичних повідомлень. Крім того, алгоритми, що оптимізують енергоспоживання, допомагають зберігати заряд батарей IoT-пристроїв шляхом мінімізації кількості переданих даних або вибору оптимальних маршрутів передачі. Також використовуються мультиагентні системи, де кожен пристрій може працювати як автономний агент, що приймає рішення на основі поточних умов, що робить мережі IoT більш гнучкими та адаптивними. .[25]

Безпека комунікацій також є важливою сферою для застосування інтелектуальних алгоритмів. Алгоритми для виявлення вторгнень аналізують трафік, шукаючи аномалії або підозрілі активності, які можуть вказувати на кібератаки. Використання машинного навчання дозволяє постійно вдосконалювати методи розпізнавання нових загроз. Алгоритми шифрування даних допомагають забезпечити захищеність інформації, водночас мінімізуючи вплив на продуктивність систем. Автоматизація процесів автентифікації та авторизації через інтелектуальні алгоритми значно підвищує безпеку мереж і допомагає ефективно керувати доступом до ресурсів.

Системи "розумного будинку" також активно використовують інтелектуальні алгоритми для автоматизації побутових процесів і підвищення енергоефективності. Завдяки алгоритмам штучного інтелекту, такі системи можуть адаптувати свою роботу до потреб мешканців, аналізуючи їхні звички та поведінкові моделі. Наприклад, система може автоматично регулювати опалення, освітлення або роботу побутової техніки, забезпечуючи зручність та економію ресурсів. Алгоритми керування енергоспоживанням аналізують поведінку користувачів, щоб мінімізувати споживання енергії, коли це можливо.

Таким чином, інтелектуальні алгоритми у сфері управління комунікаціями є важливим інструментом для підвищення ефективності мереж, їхньої гнучкості та надійності. Вони застосовуються у багатьох галузях, від маршрутизації в комп'ютерних мережах до керування трафіком у мобільних мережах і IoT, а також забезпечують підвищений рівень безпеки та автоматизації в сучасних технологіях "розумного будинку". Штучний інтелект та машинне навчання відкривають нові можливості для покращення управління комунікаціями, роблячи їх більш адаптивними та відповідними до сучасних вимог.

1.3 Аналіз існуючих рішень у сфері сигналізації

Охоронні сигналізації можуть бути різних типів: від простих систем зі звуковим сповіщенням до більш сучасних варіантів з використанням GSM, Wi-Fi або складніших систем з радіосповіщенням.

Щоб вибрати оптимальне рішення для виконання завдання, важливо ознайомитися з наявними варіантами, оцінити їхні переваги та недоліки.

Далі буде розглянуто кілька охоронних систем, представлених на ринку. Оскільки більшість з них є закритими, їхні робочі схеми не доступні для детального аналізу.

Загалом, ринок систем безпеки характеризується високою конкуренцією та інвестиційною привабливістю. Постійне впровадження новітніх технологій та зростання попиту на охоронні рішення сприяють динамічному розвитку цього сектора. Для прикладу було проаналізовано три найпопулярніші системи:

- Ajax
- Satel
- U-Prox

Ajax (показано на рисунку 1.2) є однією з найпопулярніших охоронних систем в Україні. Ця система пропонує надійний захист проти зламу та пожежі, а також має широкі можливості зв'язку, включаючи зв'язок з центром

безпеки через мобільний додаток. Ajax працює через бездротовий зв’язок, що робить її легкою в монтажі та обслуговуванні.

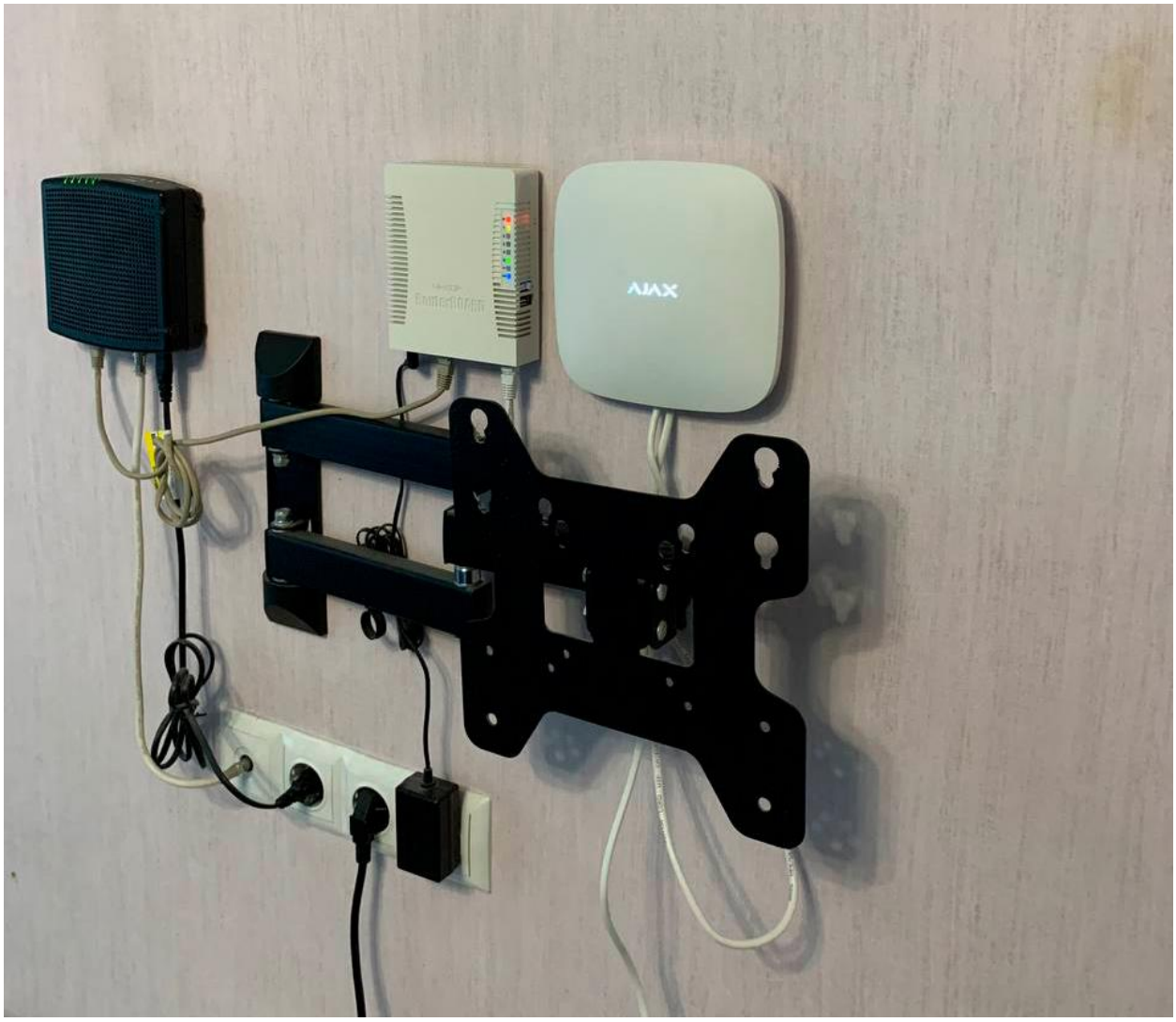


Рисунок 1.2 - Система охорони Ajax

Основними перевагами Ajax є простий у використанні мобільний додаток для керування, висока чутливість датчиків і швидка реакція системи. Також вона легко інтегрується з іншими розумними пристроями, забезпечуючи зручність користувачів та вимагаючи мінімального обслуговування. Завдяки цьому Ajax особливо приваблює тих, хто шукає інноваційні та практичні рішення для безпеки дому або бізнесу.

Система охорони включає такі основні елементи, як датчики руху, датчики відкривання дверей і вікон, а також датчики виявлення витоків газу, диму та води, доповнені внутрішніми та зовнішніми сиренами. Керування

здійснюється через спеціальний додаток на смартфоні, що дозволяє дистанційно контролювати стан системи і отримувати повідомлення про події в будинку.

Однією з ключових переваг є багаторівневий захист, що дає змогу налаштувати систему під конкретні потреби дому або офісу. Крім того, Ajax підтримує інтеграцію з системами відеоспостереження та контролю доступу.

Система має багато переваг над конкурентами, включно з високою надійністю та стійкістю до вторгнень, широкими функціями безпеки, такими як виявлення руху, захист від витоків газу, диму та води. Інтуїтивно зрозумілий інтерфейс забезпечує зручність у використанні. [4]

Однак недоліком Ajax є висока вартість компонентів, що може бути перешкодою для деяких користувачів.

Satel (як показано на рисунку 1.3) – це ще одна популярна охоронна система в Україні, яка забезпечує повний захист оселі за допомогою датчиків руху, а також вікон і дверей. Окрім цього, Satel підтримує можливість віддаленого керування та моніторингу через мобільний додаток.

Рисунок 1.3 - Система охорони SATEL

Ця система охорони створена польською компанією, яка спеціалізується на виробництві безпечних рішень для дому та комерційних об'єктів. Асортимент продукції включає системи контролю доступу, відеоспостереження, сигналізації, протипожежний захист та багато інших рішень. Satel можна встановити на будь-який тип будівлі, зокрема житлові будинки, офіси, магазини, склади та інші приміщення.

Satel пропонує широкий вибір пристроїв для охорони, таких як датчики руху, відкриття дверей і вікон, димові детектори, пульти керування та сирени. Усі компоненти використовують бездротову технологію, що спрощує налаштування та управління системою.

Окрім базових функцій, система Satel підтримує віддалене керування через мобільний додаток або веб-інтерфейс. Також вона дозволяє автоматизувати керування освітленням, опаленням та іншими пристроями в будинку.

Систему Satel відзначають високою надійністю, безпекою та можливістю легкої модернізації та розширення. Вона проста у використанні та не вимагає складного встановлення також вирізняється високою стабільністю роботи та відповідністю міжнародним стандартам безпеки. Вона надає можливість налаштовувати індивідуальні конфігурації для різних типів об'єктів, що робить її гнучкою для різних сценаріїв використання. Широкий асортимент обладнання дозволяє адаптувати систему під конкретні потреби, а також інтегрувати її з відеоспостереженням, пожежною безпекою та системами автоматизації будівель. Керування може здійснюватися як локально, так і через віддалені інтернет-інтерфейси, що забезпечує максимальну зручність.

Однак система має і свої недоліки. Процес встановлення та налаштування може бути досить складним і часто вимагає допомоги професійного інсталятора. Дротові версії системи потребують розгалуженої інфраструктури для прокладання кабелів, що може стати проблемою для вже облаштованих приміщень. Крім того, вартість Satel може бути вищою

порівняно з простішими рішеннями, особливо коли мова йде про охоплення великих об'єктів.[11]

Система охорони U-Prox (показано на рисунку 1.4) є однією з популярних охоронних рішень в Україні, забезпечуючи ефективний захист як для житлових приміщень, так і для офісів. Її ключовим елементом є центральна панель керування, яка здійснює контроль за всіма підключеними датчиками. Підключення системи до сигналізаційної централі дозволяє швидко реагувати на будь-які надзвичайні ситуації.

Рисунок 1.4 - Система охорони U-Prox

Серед переваг U-Prox варто виділити можливість додаткового розширення функціоналу завдяки підключенню модулів для контролю доступу, відеоспостереження, пожежної сигналізації та інших систем. Окрім того, система здатна працювати автономно, що гарантує охорону навіть у разі відсутності електропостачання.

Система U-Prox використовує різноманітні типи датчиків, включаючи датчики відкриття вікон і дверей, датчики руху, а також сенсори для виявлення витоку газу, диму та інших небезпек. Всі ці датчики відзначаються високою надійністю і забезпечують точне виявлення загроз.

Окрім звичних способів оповіщення, таких як звукова і світлова сигналізація, U-Prox може надсилати сповіщення про стан системи через SMS або повідомлення на мобільний телефон.

U-Prox пропонує простоту встановлення та налаштування завдяки бездротовим технологіям. Користувачі можуть здійснювати безконтактний контроль доступу за допомогою мобільних пристроїв, що забезпечує зручність. Система підтримує масштабованість, що дозволяє адаптувати її до різних об’єктів, і може інтегруватися з іншими системами безпеки та автоматизації. Віддалене керування через мобільний додаток робить процес ще зручнішим.

Однак, важливо врахувати деякі недоліки: система має високу залежність від надійності бездротового зв’язку, що може викликати проблеми. Користувачі, які не знайомі з мобільними рішеннями для контролю доступу, можуть потребувати додаткового навчання. Для великих чи складних систем можуть знадобитися додаткові модулі, що підвищить загальну вартість.

U-Prox є відмінним вибором для тих, хто шукає сучасне та інноваційне рішення для контролю доступу та охорони, особливо для комерційних приміщень і офісів. [30]

1.4 Аналіз характеристик та можливостей існуючих систем

Ajax є системою охоронної сигналізації, яка застосовує сучасні технології, включаючи бездротові комунікації та шифрування, для забезпечення підвищеного рівня безпеки. Зазвичай комплект охоронної системи Ajax містить датчик руху, датчик відкриття, пульт керування системою та центральний шлюз.

Шлюз Ajax є центральним пристроєм системи і має наступні характеристики:

- Максимальна кількість підключених бездротових пристроїв (датчиків, брелоків, клавіатур і т.д.) до 100 штук;
- Частота бездротових датчиків: 868/915 МГц;

- Потужність радіопередавача датчиків: 20 мВт;
- Канали зв'язку: GSM (850/900/1800/1900 Мгц) , Ethernet;
- Час роботи без електроживлення: 10 годин;
- Живлення: 110 - 250 В АС.

Шлюз Ajax має інтуїтивно зрозумілий і зручний інтерфейс, доступний через мобільні додатки для iOS та Android, що дозволяє віддалено управляти системою, перевіряти статус датчиків та налаштовувати сповіщення. Компанія Ajax використовує бездротові засоби зв'язку в маршрутизаторах, такі як Wi-Fi та двочастотні радіоканали (868/915 МГц), що забезпечує швидкий і надійний обмін даними між датчиками та шлюзом. Маршрутизатори Ajax оснащені надійним шифруванням, що гарантує безпечну передачу даних та захищає систему від злому. Крім того, шлюз Ajax має вбудовану панель управління, яка дозволяє зручно контролювати статуси датчиків і охоронних пристроїв, підключених до системи.

Додаткові функції шлюзу Ajax включають можливості відеоспостереження, контролю доступу, автоматичного включення та вимкнення системи, а також підтримку резервного живлення. Це модульна система, що дозволяє розширювати її, додаючи нові датчики та обладнання безпеки.

Ajax забезпечує віддалений доступ до системи з будь-якої точки світу через мобільні додатки або веб-інтерфейс, що дозволяє власникам контролювати та адмініструвати систему на відстані, а також отримувати сповіщення про її стан. Доступ до системи можна надати іншим користувачам, таким як члени родини або співробітники. Ці апаратні параметри охоронної системи дозволяють створювати досить масштабні та складні системи безпеки для великих підприємств, приватних будинків, парків тощо. [4]

Шлюз SATEL (або SATEL Integra) – це контрольно-приймальний пристрій (КПП), який виконує функцію основного засобу для збору даних та

управління охоронними системами в рамках безпеки приміщень або територій. Основні характеристики шлюзу SATEL:

- Максимальна кількість підключених бездротових пристроїв (датчиків, брелоків, клавіатур і т.д.) до 48 штук;
- Частота бездротових датчиків: 868 МГц – 4 канала;
- Потужність радіопередавача датчиків: 20 мВт;
- Канали зв'язку: GSM (850/900/1800/1900 Мгц) , Ethernet;
- Час роботи без електроживлення: 11 годин;
- Живлення: DC 12 В.

Шлюз SATEL має модульну конструкцію, що дозволяє додавати додаткові модулі відповідно до потреб системи безпеки. Він також є багатофункціональним пристроєм, здатним виконувати різні ролі в системі безпеки, такі як контролер доступу, пристрій для вимірювання параметрів приміщення (температури, вологості), система пожежної сигналізації та відеонагляд. Крім того, управління SATEL здійснюється за допомогою спеціального програмного забезпечення, що дозволяє налаштовувати параметри системи безпеки, моніторити стан пристроїв і записувати відеоінформацію.

SATEL сумісний з різними пристроями безпеки, що робить його універсальним рішенням для охорони. Він здатний працювати в широкому діапазоні температур, що дозволяє використовувати його в різних кліматичних умовах. Крім того, SATEL має можливість резервування за допомогою додаткового блоку, що підвищує надійність системи безпеки. Програмне забезпечення шлюзу підтримує кілька мов, що робить його доступним для користувачів з різних країн і регіонів.

SATEL є надійним і функціональним засобом охорони для приміщень і територій. Його модульна конструкція дозволяє легко додавати додаткові модулі для виконання різних функцій системи безпеки, а програмне забезпечення забезпечує простий і зручний процес налаштування та

управління системою. Широкий діапазон робочих температур і можливість резервування гарантують стабільну та надійну роботу системи охорони в будь-яких умовах. [11]

Охоронна компанія U-Prox пропонує широкий асортимент продуктів для забезпечення безпеки в будівлях і на територіях. Одним із основних компонентів цих систем безпеки є шлюзи, які забезпечують взаємодію між датчиками і контролерами системи. Система охорони U-Prox є комплексним рішенням для захисту будівель і територій. Серед характеристик цієї системи можна виділити:

- Максимальна кількість підключених бездротових пристроїв (датчиків, брелоків, клавіатур і т.д.) до 99 штук;
- Частота бездротових датчиків: 868 МГц – 6 канала;
- Потужність радіопередавача датчиків: 20 мВт;
- Канали зв'язку: GSM (850/900/1800/1900 Мгц) , Ethernet;
- Час роботи без електроживлення: 8 годин;
- Живлення: AC 220 В.

U-Prox використовує технологію RFID для ідентифікації користувачів, що дозволяє запобігати несанкціонованому доступу та контролювати переміщення персоналу і відвідувачів. Система підключається до Інтернету за допомогою бездротових технологій, що забезпечує швидкий доступ до даних про стан системи та розширює охоплюючий радіус.

U-Prox має вбудовану систему моніторингу, яка дозволяє відслідковувати стан системи в режимі реального часу і оперативно реагувати на будь-які відхилення. Вона може інтегруватися з іншими системами безпеки, такими як контроль доступу, відеоспостереження та пожежна сигналізація, що сприяє створенню єдиної інтегрованої системи безпеки.

Система відзначається високою надійністю та захищеністю від злому, що забезпечує безпеку будівлі або території. Інтерфейс управління є простим, що дозволяє легко налаштовувати та керувати всіма функціями. Користувач

має можливість отримати доступ до системи з будь-якого місця та в будь-який час за допомогою Інтернету та спеціального додатка на смартфоні чи комп'ютері.

Цей набір характеристик, представлених шлюзом U-Prox, дозволяє проектувати великі охоронні системи як для промисловості, так і для приватних будинків. [30]

1.5 Висновки до розділу

У даному розділі були розглянуті ключові аспекти розвитку комп'ютерних систем управління комунікаціями, зокрема сучасні тенденції в розробці систем розумного дому, впровадження інтелектуальних алгоритмів, а також аналіз існуючих рішень у сфері сигналізації, включаючи характеристики відомих систем, таких як Ajax, SATEL та U-Prox.

Сучасні тенденції в розробці систем розумного дому свідчать про активний розвиток технологій, які покликані підвищити комфорт, безпеку та енергоефективність житлових і комерційних приміщень. Інноваційні рішення забезпечують інтеграцію різноманітних пристроїв і систем, що дозволяє користувачам управляти ними з одного центру. Важливим аспектом є орієнтація на користувача, що проявляється в розробці інтуїтивно зрозумілих інтерфейсів та зручних мобільних додатків, які дозволяють контролювати всі елементи системи з будь-якої точки світу.

Інтелектуальні алгоритми, які використовуються в управлінні комунікаціями, грають критично важливу роль у забезпеченні адаптивності та ефективності систем. Завдяки використанню штучного інтелекту та машинного навчання, ці системи можуть самостійно приймати рішення, адаптуватися до змінних умов і навчатися на основі зібраних даних. Це не лише підвищує їхню продуктивність, але й значно полегшує управління.

Аналіз існуючих рішень у сфері сигналізації показав, що сучасні системи охорони пропонують широкий спектр функцій, включаючи можливість інтеграції з іншими елементами розумного дому, такими як системи відеоспостереження, контролю доступу та пожежної сигналізації. Це

дозволяє створювати єдину інтегровану систему безпеки, яка забезпечує комплексний захист.

Дослідження характеристик і можливостей систем Ajax, SATEL та U-Prox підтвердило їхню високу надійність, функціональність та гнучкість. Кожна з цих систем має унікальні особливості, які роблять їх привабливими для користувачів з різними потребами. Зокрема, модульна конструкція, підтримка різних протоколів та можливість резервування роботи створюють умови для їх ефективного використання в різних сферах.

Таким чином, проведений аналіз демонструє, що комп'ютерні системи управління комунікаціями перебувають на стадії активного розвитку. Вони впроваджують новітні технології та інновації, що підвищують їхню ефективність і зручність використання. Це відкриває нові перспективи для подальших досліджень та впроваджень у цій динамічній галузі, надаючи можливості для створення ще більш інтегрованих і адаптивних рішень для забезпечення безпеки і комфорту.

Цей набір характеристик, представлених шлюзом U-Prox, дозволяє проектувати великі охоронні системи як для промисловості, так і для приватних будинків.

2 ВИМОГИ ДО РОЗРОБКИ ТА РЕАЛІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ КОМУНІКАЦІЯМИ: ТЕХНОЛОГІЇ ТА ІНТЕГРАЦІЯ КОМПОНЕНТІВ

2.1 Вимоги до системи.

Система безпеки не має права на помилку, адже від цього залежить не тільки збереження майна, але й життя людей. При таких високих ставках кожен елемент системи має значення. Обладнання повинне бути надійним, а комплект підібраний правильно. Монтаж і налаштування повинні враховувати особливості об’єкта та вимоги користувача. Пропуск одного аспекту може зробити всю систему неефективною. Безпекова система повинна функціонувати бездоганно, оскільки від цього залежить не тільки захист майна, а й життя людей. При таких високих ризиках кожен елемент системи є важливим. Обладнання повинно бути надійним, а всі пристрої правильно підібрані. Монтаж і налаштування необхідно виконувати з урахуванням особливостей об'єкта та вимог клієнта. Пропустити хоча б один етап – означає створити ілюзію безпеки.

Сучасні системи безпеки на перший погляд здаються простими: пристрої підключаються за кілька хвилин, а налаштування відбувається через зручний мобільний додаток. Проте це лише видимість. Процес встановлення охоронної системи включає багато важливих етапів: огляд об’єкта, визначення можливих зон перешкод для сигналу, вибір обладнання, розробка проекту, монтаж приладів, тестування зон виявлення, налаштування системи, підключення до моніторингової станції, підготовка документації та передача готового проекту клієнту. Лише професіонал здатний швидко й ефективно виконати всі ці завдання.

Для ефективного захисту житла, робочого місця чи інших об’єктів сучасна система безпеки зазвичай складається з кількох компонентів та функцій. Характерними особливостями таких систем є:

Для ефективного моніторингу та фіксації подій на території необхідні камери спостереження високої якості з чітким зображенням. Важливо, щоб

вони мали функції перегляду в реальному часі, виявлення руху та режим нічного бачення.

Сигналізаційні системи: У разі несанкціонованого доступу вони негайно інформують користувача та діють як засіб стримування. Окрім основної панелі керування і сигналізації, такі системи мають включати датчики для виявлення руху, відкриття дверей і вікон. Бажано інтегрувати їх з мобільними повідомленнями або службами моніторингу.

Система контролю доступу регулює вхід і вихід із приміщень за допомогою електронних замків, безключового доступу, біометричних сканерів (відбитків пальців чи розпізнавання обличчя) або карток доступу. Можна також поєднати її із системами обліку робочого часу.

Сучасна система безпеки може включати бар'єри, такі як паркани, ворота або інші засоби для обмеження несанкціонованого доступу. Безпеку можна підвищити за допомогою інтеграції цих елементів із камерами спостереження та системами сигналізації.

Правильно організоване освітлення допомагає відлякувати зловмисників. Ліхтарі з датчиками руху або системи програмованого освітлення забезпечують додатковий захист у нічний час чи в темних зонах.

Для ефективного нагляду і фіксації подій на об'єкті необхідні високоякісні камери з високою роздільною здатністю. Вони повинні мати функції, такі як перегляд у реальному часі, детекція руху та можливість роботи в умовах слабкого освітлення.

Охоронні системи у випадку порушення система негайно сповіщає власника і служить засобом відлякування. Окрім центральної панелі та сигналізації, важливо мати датчики для виявлення руху, відкриття дверей і вікон. Оптимально, коли система підключена до мобільних сповіщень або служб моніторингу.

Система доступу регулює контроль входу та виходу з будівлі. Прикладами є електронні замки, безключовий доступ, біометричні зчитувачі або картки. Також можливе інтегрування із системою обліку робочого часу.

Периметральна охорона: сучасна система безпеки може включати різні засоби обмеження доступу, такі як огорожі, ворота або бар'єри. Додаткову

безпеку можна забезпечити, поєднавши ці компоненти з камерами і сигналізацією.

Охоронне освітлення: якісне освітлення відіграє ключову роль у запобіганні порушенням. Ліхтарі з датчиками руху або програмовані системи освітлення можуть значно підвищити рівень безпеки в темний час або на слабко освітлених ділянках.

2.2 •Функціональна схема системи

С початку було розроблено макет креслення приватного будинку, а також подвір’я та гаражу, для подальшого розміщення датчиків та іншого обладнання. (показано на рисунку 2.1)

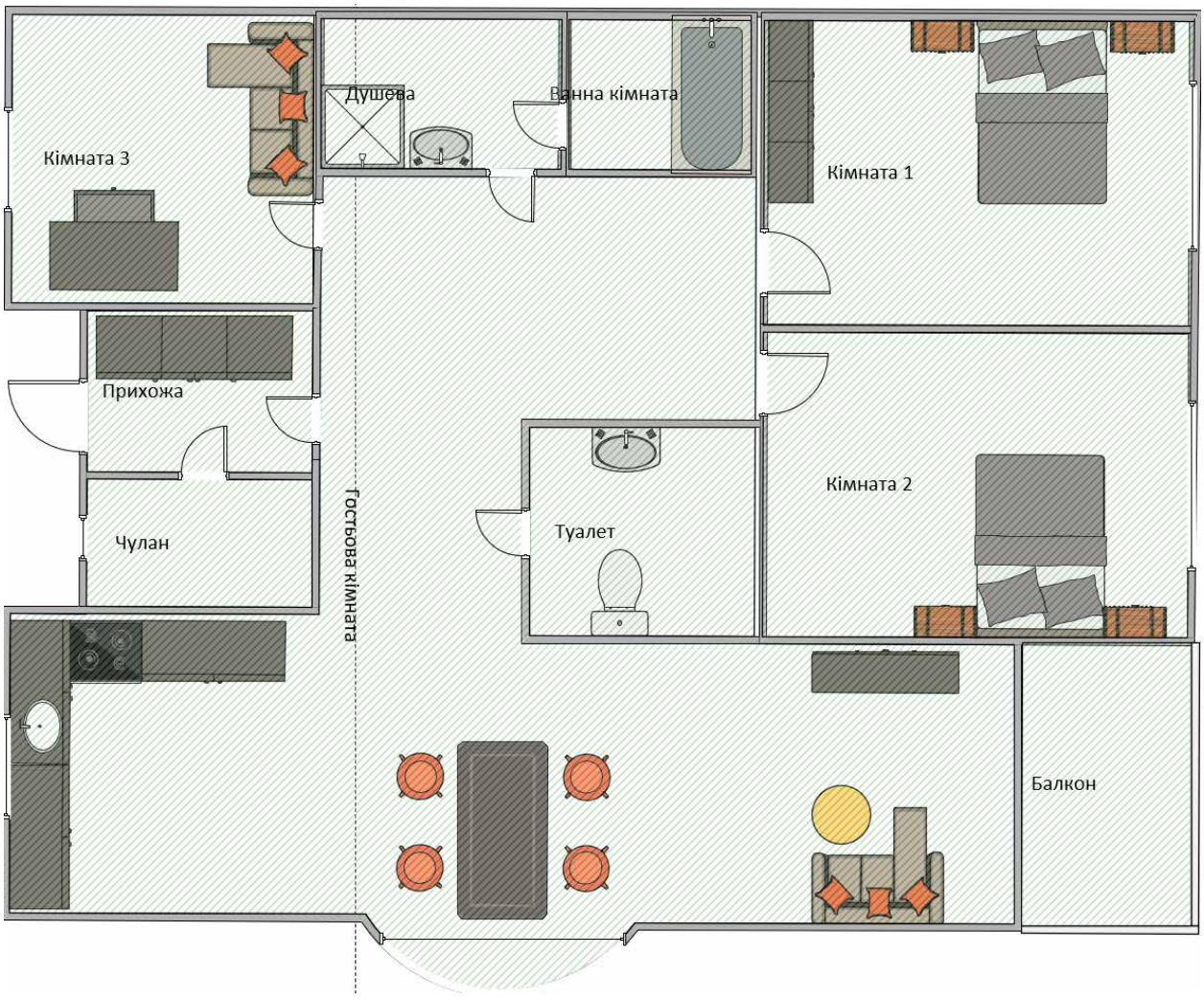


Рисунок 2.1 - Макет креслення приватного будинку

На представленому макеті, як зображено на рисунку 2.2, було розміщено всі пристрої та датчики, що складають систему охорони будинку. Було

прийнято рішення встановити інфрачервоні датчики руху на всіх можливих проходах для виявлення пересування і фіксації відкривання дверей. Ці датчики будуть інтегровані з системою сигналізації, щоб забезпечити своєчасне реагування на будь-які спроби несанкціонованого доступу.

Важливим аспектом є встановлення камер відеоспостереження. У кожній кімнаті, включно з гаражем, передбачено одну камеру, спарену з датчиком руху, що дозволяє ефективно відслідковувати події у режимі реального часу. Таке поєднання гарантує автоматичне ввімкнення відеозапису при виявленні руху. Для зовнішнього спостереження на подвір'ї було встановлено камери в кожному куті території, що забезпечує повний контроль над периметром будинку. Це рішення підвищує рівень безпеки, дозволяючи виявляти потенційні загрози на ранніх стадіях.

Окрім цього, на всіх вікнах встановлено датчики руху, які спрацьовують при спробах відчинення. Додатково, для забезпечення пожежної безпеки, вікна обладнані розумними сервоприводами, що автоматично спрацьовуватимуть у випадку пожежі, відкриваючи шляхи для евакуації або вентиляції приміщень.

У кожній кімнаті також встановлено датчики диму та спринклери. Ці елементи є частиною комплексної системи пожежної охорони, яка забезпечує швидке реагування на виявлене займання. Поєднання всіх датчиків в єдину систему дозволяє ефективно захищати будинок від пожеж.

На головному вході до будинку було встановлено RFID-зчитувач та магнітний замок, що надає можливість безконтактного входу до приміщення за допомогою ключ-картки або іншого ідентифікатора. Таке рішення покращує безпеку доступу та забезпечує зручність для мешканців будинку.

У коморі було розміщено всі плати Arduino, які використовуються для контролю роботи охоронної системи. Важливі компоненти, такі як сервер, шлюз та комутатор, розташовано в кімнаті власника, що дозволяє забезпечити централізоване управління всіма системами та підтримку стабільного з'єднання між пристроями. Така організація дозволяє максимально ефективно

контролювати всі процеси, пов’язані з безпекою будинку, і своєчасно реагувати на будь-які зміни чи загрози.

Таким чином, загальна структура охоронної системи забезпечує не лише захист від зовнішніх загроз, але й підвищує рівень безпеки внутрішніх приміщень завдяки впровадженню пожежної сигналізації та розумних технологій, що сприяють захисту майна та життя мешканців.

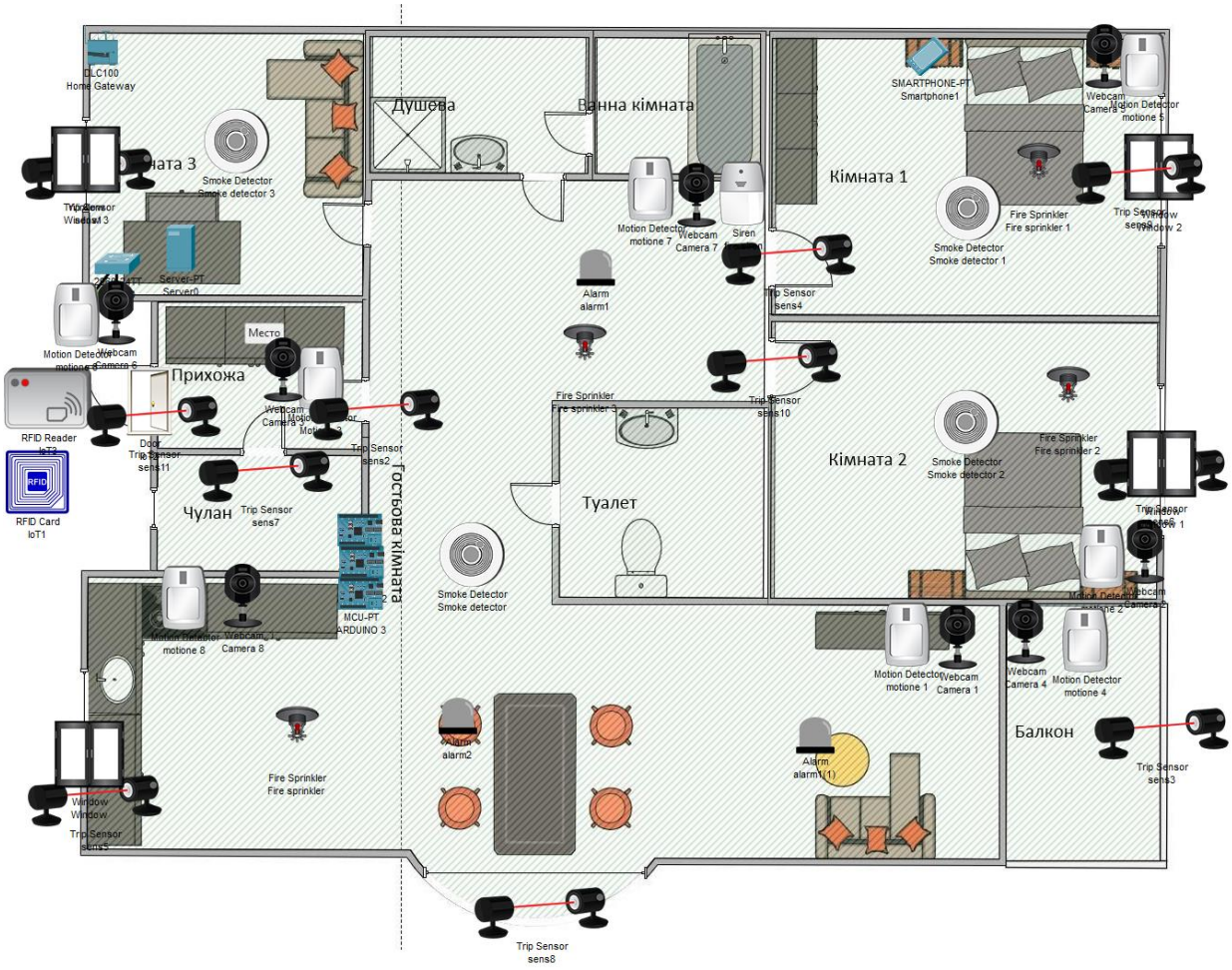


Рисунок 2.2 - Розміщення елементів на макеті

Таким Таким чином, система була розподілена на п'ять окремих секторів. Три з них являють собою незалежні один від одного блоки, побудовані на платах Arduino, до яких під'єднано різноманітне обладнання. Кожен з цих блоків підключений до головного шлюзу через бездротовий зв'язок, що забезпечує їх інтеграцію у загальну систему безпеки.

Перший сектор відповідає за роботу платформи відеоспостереження. Він об'єднує всі камери спостереження, забезпечуючи їхню синхронну роботу

з іншими компонентами системи. Цей сектор контролює запис відео та його передачу на центральний сервер, а також взаємодію з датчиками руху, що активують камери.

Другий сектор – бездротовий, який відповідає за управління різними допоміжними елементами системи, такими як сповіщення або інтеграція з іншими пристроями для автоматизації процесів охорони. Це може включати віддалене керування замками, сиренами або іншими пристроями.

Перший сектор, який отримав назву головний сектор (показаний на рисунку 2.3), є одним із найважливіших компонентів системи безпеки. Його склад включає плату Arduino, RFID-зчитувач, три інфрачервоні датчики руху та сигналізацію. Основне завдання цього сектора - забезпечення контролю доступу до будинку, а також моніторинг руху в ключових зонах.Інфрачервоні датчики реагують на будь-яке пересування в межах своїх зон дії, негайно активуючи сигналізацію у разі виявлення небажаної активності. Це значно підвищує рівень захисту приміщень, особливо під час відсутності власників. RFID-зчитувач, у свою чергу, забезпечує зручний і безпечний доступ до будинку за допомогою безконтактних ключів або карток, що також мінімізує ризик несанкціонованого проникнення.

Особливістю сектора головного сектору безпеки є його інтеграція з іншими частинами системи через бездротовий зв'язок, що забезпечує синхронізовану роботу всіх компонентів безпеки. Завдяки цьому досягається безперебійний обмін даними між секторами, що дозволяє швидко реагувати на загрози та контролювати всі аспекти системи.

Загалом, така структура сектора дозволяє не лише стежити за безпекою в режимі реального часу, але й оперативно вживати заходів у разі будь-яких порушень. Це рішення забезпечує комплексний підхід до охорони, поєднуючи автоматизовані технології з надійністю ручного управління, що робить систему безпеки максимально ефективною та зручною у використанні.

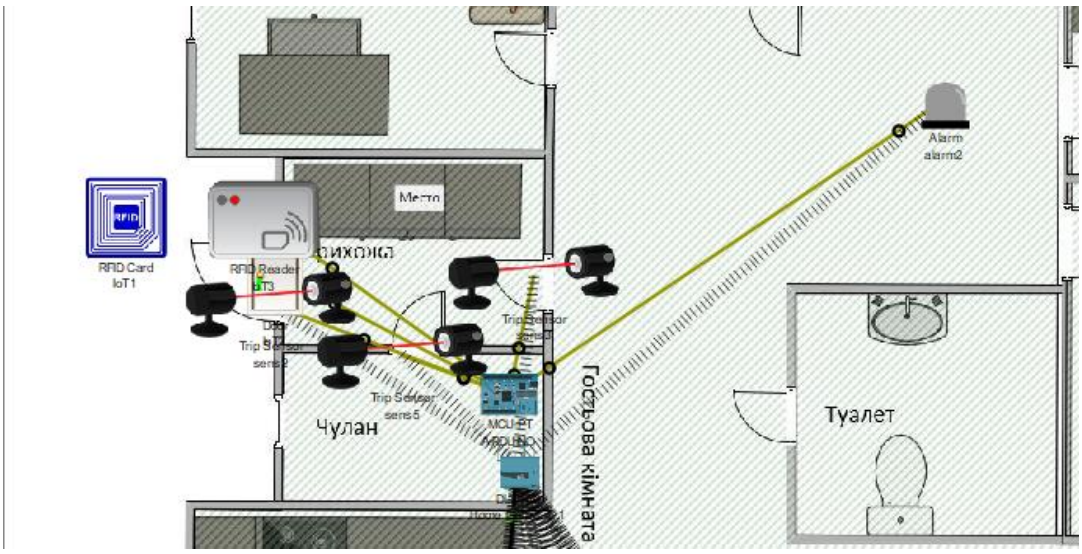


Рисунок 2.3 – Головний сектор безпеки

Другий та третій сектори також є важливими елементами системи безпеки, кожен з яких включає в себе плату Arduino, чотири інфрачервоні датчики руху та сигналізацію (показано на рисунку 2.4). Ці сектори отримали назви сектор безпеки периметру 1 та 2. Вони відповідають за моніторинг та захист периметру об’єкта, забезпечуючи постійний контроль та швидке реагування на будь-які спроби несанкціонованого проникнення.

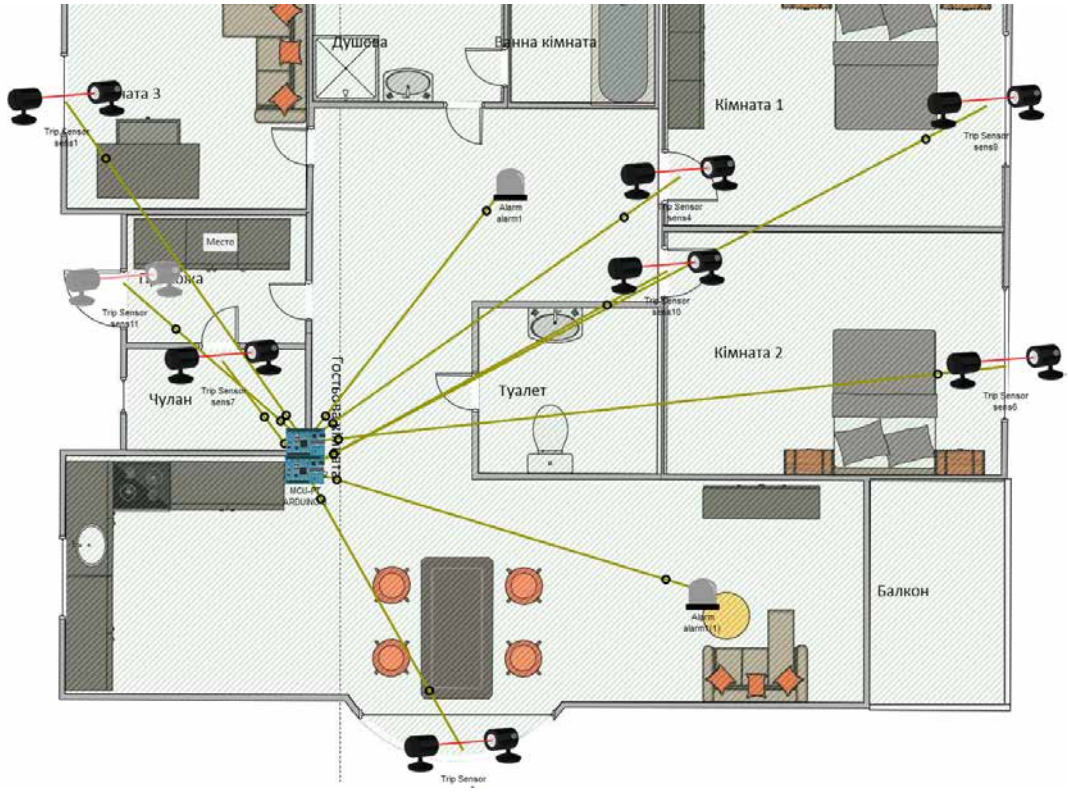


Рисунок 2.4 – Сектора безпеки периметру 1 та 2

Інфрачервоні датчики, встановлені по периметру, забезпечують своєчасне виявлення будь-якого руху, що дозволяє миттєво активувати сигналізацію у випадку порушення меж безпеки. Це особливо важливо для запобігання проникненню зловмисників на територію об’єкта, що охороняється, забезпечуючи додатковий рівень захисту до системи внутрішнього нагляду.

Сектор безпеки периметру 1 та 2 інтегровані з іншими компонентами системи безпеки, що дозволяє не тільки оперативно сповіщати власника або службу охорони про порушення, але й забезпечувати комплексний захист будинку або об'єкта. Завдяки бездротовому зв'язку ці сектори можуть швидко передавати інформацію на центральний шлюз та взаємодіяти з іншими секторами системи.

Таким чином, другий і третій сектори не лише підвищують загальний рівень безпеки, але й забезпечують надійну охорону зовнішнього периметру, створюючи багаторівневу систему захисту, здатну своєчасно реагувати на будь-які загрози.

Система пожежної безпеки (показано на рисунку 2.5) є ключовим елементом захисту будинку, що гарантує своєчасне реагування на загрози, пов'язані з вогнем. До складу цієї системи входять датчики диму, спринклери, пожежна сигналізація, а також сервоприводи, встановлені на вікнах. Усі ці компоненти взаємодіють між собою та керуються через центральний шлюз, що забезпечує централізований контроль і управління.

Датчики диму виконують функцію постійного моніторингу повітря на наявність диму або небезпечних часток, які можуть свідчити про початок пожежі. У разі виявлення загрози, датчики автоматично активують пожежну сигналізацію, яка негайно сповіщає мешканців будинку або охоронну службу про небезпеку.

Спринклери, які також є частиною системи, миттєво реагують на сигнали від датчиків диму. Вони автоматично активуються у разі підтвердженого займання і починають розпилювати воду або інші вогнегасні

речовини, щоб загасити вогонь або мінімізувати його поширення. Це дозволяє знизити шкоду, завдану майну, та дає додатковий час для евакуації мешканців.

Сервоприводи на вікнах грають важливу роль у забезпеченні безпеки під час пожежі. У випадку пожежної тривоги ці приводи автоматично відкривають вікна, забезпечуючи доступ свіжого повітря або димовідведення. Це не тільки допомагає уникнути накопичення диму в приміщеннях, але й створює додаткові евакуаційні шляхи для мешканців будинку.

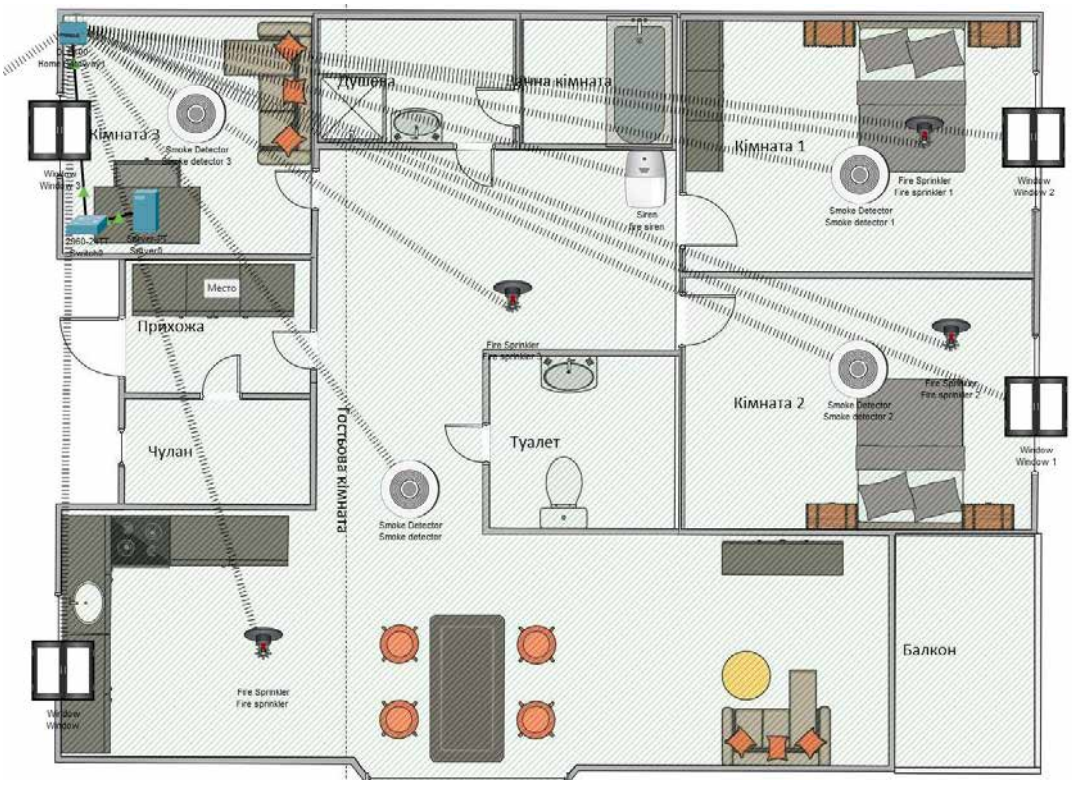


Рисунок 2.5 - система пожежної системи

Вся система пожежної безпеки працює в тісній інтеграції через центральний шлюз, який координує роботу всіх її компонентів. Шлюз забезпечує безперебійний зв'язок між датчиками, спринклерами, сигналізацією та сервоприводами, дозволяючи швидко реагувати на будь-які зміни у стані безпеки. Крім того, центральний шлюз може бути підключений до зовнішніх систем моніторингу або мобільних додатків, що дозволяє власникам отримувати сповіщення в реальному часі та віддалено контролювати систему.

Загалом, система пожежної безпеки, побудована на такій інтегрованій основі, забезпечує надійний захист від пожежних загроз, мінімізуючи ризики для життя мешканців та зберігаючи майно від пошкоджень.

Останній сектор системи, названий Сектором відеоспостереження, складається із восьми камер відеоспостереження, восьми датчиків руху та головного сервера (показано на рисунку 2.6). Основне завдання цього сектора – забезпечення резервного контролю за всією системою безпеки, управління її налаштуваннями, а також постійний моніторинг стану системи в реальному часі.

Кожна з восьми камер відеоспостереження забезпечує повний огляд території, а датчики руху активують камери, коли фіксують будь-які підозрілі дії. Цей механізм дозволяє не тільки записувати події, але й оперативно реагувати на потенційні загрози, активуючи інші елементи системи безпеки при необхідності.

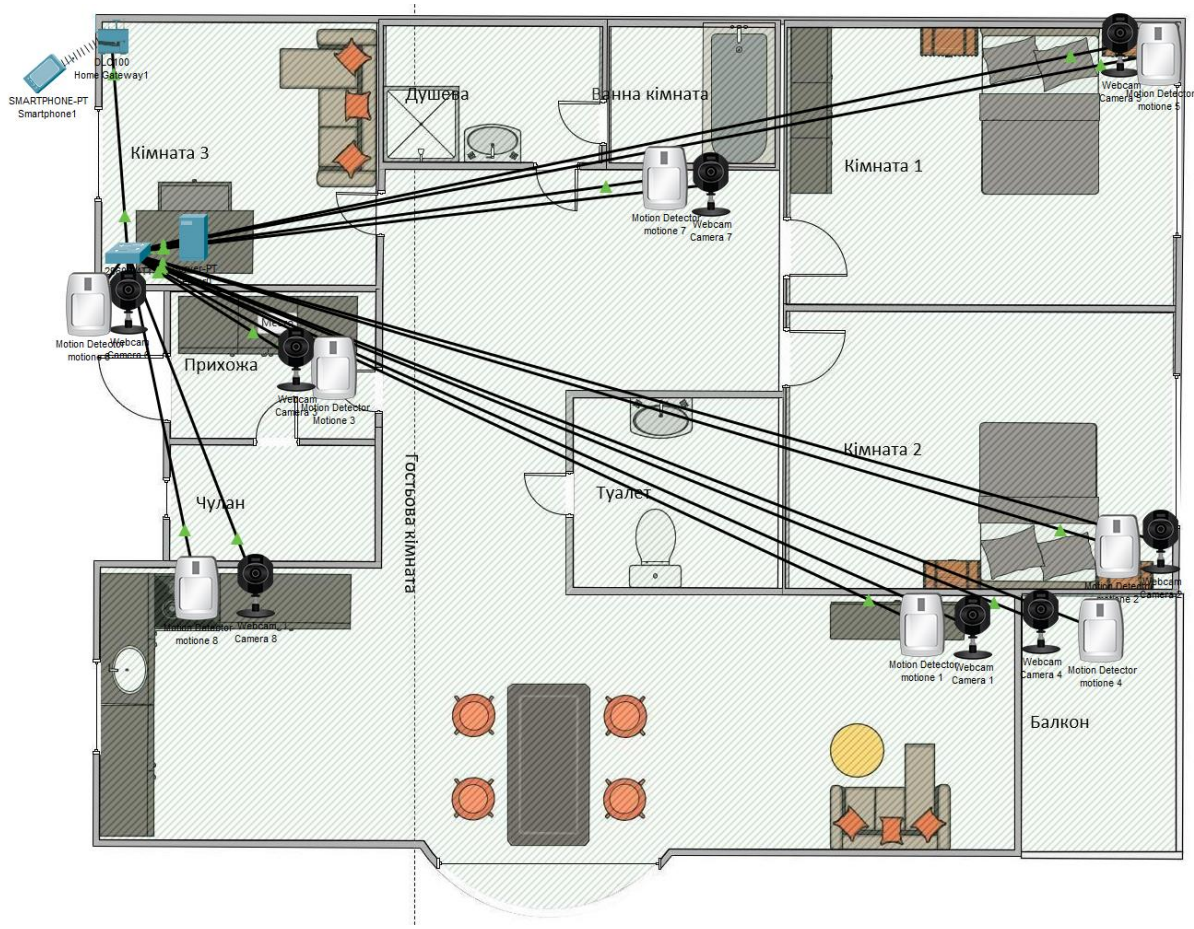


Рисунок 2.6 - Сектор відеоспостереження

Даний сектор буде відповідати за резервний контроль системи, за її налаштування та моніторингом за її станом в реальному часі, даний сектор також буде проводити збір всіх даних, а на додаток даний сектор буде керувати всіма камерами відеоспостереження.

Після розміщення всіх компонентів на макеті було виконано їх підключення до основної системи (як показано на рисунку 2.7). Обладнання, таке як інфрачервоні датчики руху, сигналізація, RFID-зчитувач і магнітний замок, було під'єднано до плати Arduino. Крім того, зазначені пристрої, за винятком магнітного замка та RFID-зчитувача, були підключені до головного шлюзу через бездротовий зв'язок, що підвищило загальну відмовостійкість системи.

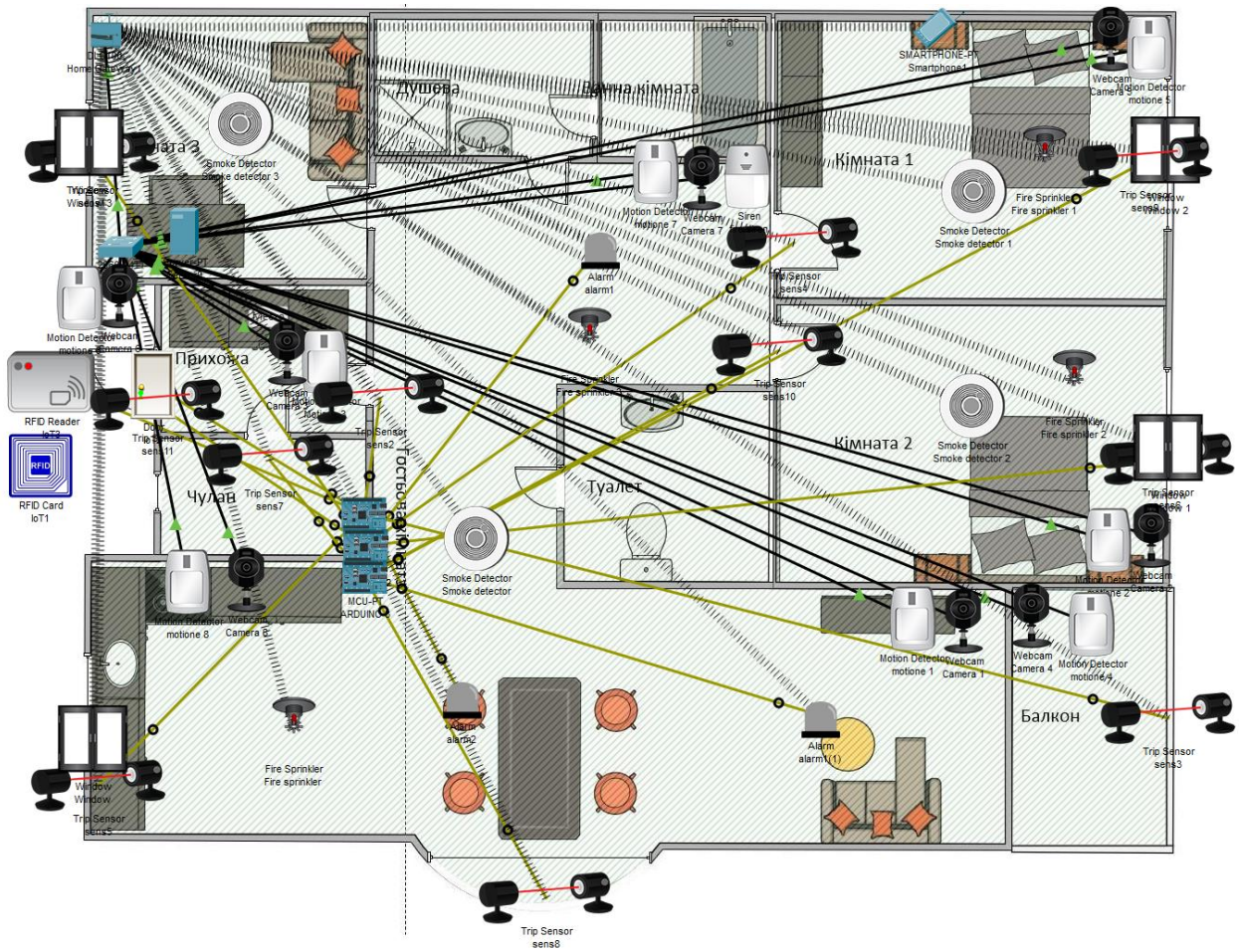


Рисунок 2.7 Функціональна схема

Всі камери відеоспостереження та датчики руху було підключено до комутатора за допомогою витої пари, а комутатор, у свою чергу, під'єднаний

до головного шлюзу також через виту пару. Це рішення було обрано для забезпечення максимальної надійності з'єднання та мінімізації можливих збоїв.

Інші елементи системи, такі як датчики диму, спринклери та розумні сервоприводи для вікон, були під'єднані до головного шлюзу через бездротове підключення. У цьому сегменті охоронної системи не передбачалося використання резервної системи керування, оскільки бездротове рішення забезпечує достатню стабільність для цих компонентів.

2.3 •Створення коду та опис алгоритмів та для управління комунікаціями

Розробка почалась зі створення коду для плати Arduino 1 які присутня на схемі.

2.1 Лістинг коду Arduino 1

```
// Призначення пінів
const DOORS_PIN = 4; // Кількість дверей
const READER_PIN = A1; // Пін зчитувача карт
const TRIP_SENSORS = [1, 2, 3, 4]; // Масив тригерних датчиків
const LED_PIN = 5; // Пін для світлодіода
function setup() {
    pinMode(DOORS_PIN, OUTPUT);// Встановлюємо пін дверей як вихід
    pinMode(READER_PIN, INPUT); // Встановлюємо пін зчитувача як
вхід
    // Встановлюємо тригерні датчики як входи
    TRIP_SENSORS.forEach(sensor => pinMode(sensor, INPUT));

    pinMode(LED_PIN, OUTPUT); // Встановлюємо пін світлодіода як
вихід
}
function loop() {
    // Перевіряємо наявність картки
    const isCardPresent = (analogRead(READER_PIN) === 0);
    // Керуємо дверима в залежності від наявності картки
    customWrite(DOORS_PIN, isCardPresent ? 1 : 0);
    // Перевіряємо, чи активовано хоча б один тригерний датчик
    const isAnySensorActive = TRIP_SENSORS.some(sensor =>
digitalRead(sensor) > 0);
    // Керуємо світлодіодом в залежності від статусу датчиків
    digitalWrite(LED_PIN, isAnySensorActive ? HIGH : LOW);
}
```

Код починається з визначення пінів, які використовуються для підключення компонентів.

- DOORS_PIN` (4) – пін для керування дверима.
- READER_PIN` (A1) – пін для зчитувача карт.
- TRIP_SENSORS` – масив, що містить номери пінів (1, 2, 3, 4) для чотирьох тригерних датчиків, які будуть перевірятися на активність.
- LED_PIN` (5) – пін для світлодіода, який інформує про статус тригерних датчиків.

Далі була створена функція setup() яка встановлює налаштування для всіх пінів

- pinMode(DOORS_PIN, OUTPUT)` – встановлює пін дверей як вихід, що дозволяє контролювати їх відкриття або закриття.
- pinMode(READER_PIN, INPUT)` – встановлює пін зчитувача карт як вхід, щоб отримувати дані про наявність картки.
- Використовується цикл `forEach` для масиву `TRIP_SENSORS`, щоб встановити кожен з тригерних датчиків як вхід.
- pinMode(LED_PIN, OUTPUT)` – встановлює пін світлодіода як вихід для індикації активності датчиків.

Далі встановлювалась функція loop(): дана функція виконується безперервно в циклі, щоб постійно перевіряти статус компонентів.

- const isCardPresent = (analogRead(READER_PIN) === 0)` – перевіряє, чи картка присутня. Якщо зчитувач карт виявляє картку (значення 0), то змінна `isCardPresent` стає істинною.
- customWrite(DOORS_PIN, isCardPresent ? 1 : 0)` – контролює двері на основі наявності картки. Якщо картка присутня, двері відкриваються (значення 1), якщо ні – закриваються (значення 0).
- const isAnySensorActive = TRIP_SENSORS.some(sensor => digitalRead(sensor) > 0)` – перевіряє, чи активовано хоча б один з тригерних

датчиків. Якщо будь-який з датчиків виявляє об’єкт (значення більше 0), то змінна `isAnySensorActive` стає істинною.

- digitalWrite(LED_PIN, isAnySensorActive ? HIGH : LOW)` – контролює світлодіод. Якщо активовано хоча б один тригерний датчик, світлодіод світиться (значення HIGH), інакше – вимикається (значення LOW).

Цей код реалізує систему, в якій двері відкриваються лише у присутності картки (зчитуваній З піну `READER_PIN`). Світлодіод (сигналізація) інформує про активність тригерних датчиків: якщо хоча б один з датчиків активний, світлодіод світиться, в іншому випадку – не працює. Код працює в циклі, постійно перевіряючи стан компонентів, забезпечуючи безперервний контроль над системою. Нижче на рисунку 2.8 та 2.9 зображено блок схему роботи даного коду

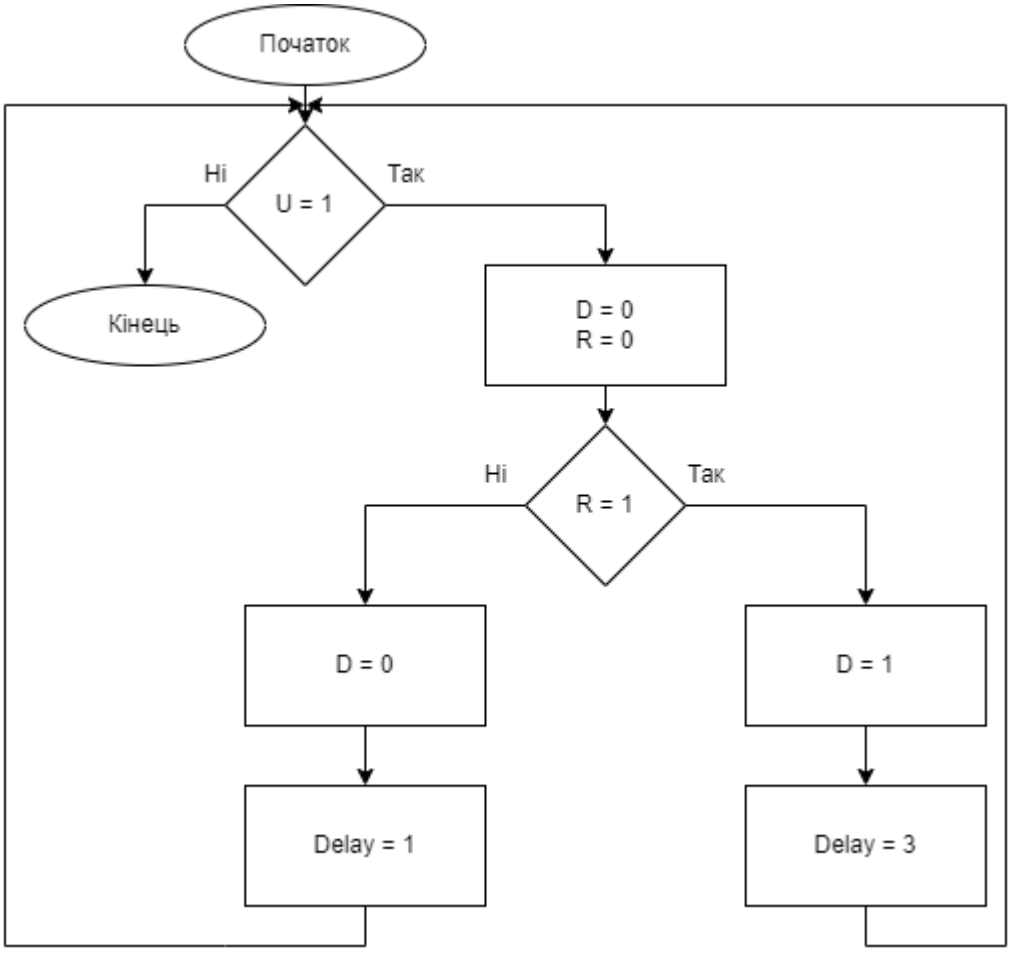


Рисунок 2.8 Блок-схема роботи зчитувача карток та кард рідеру

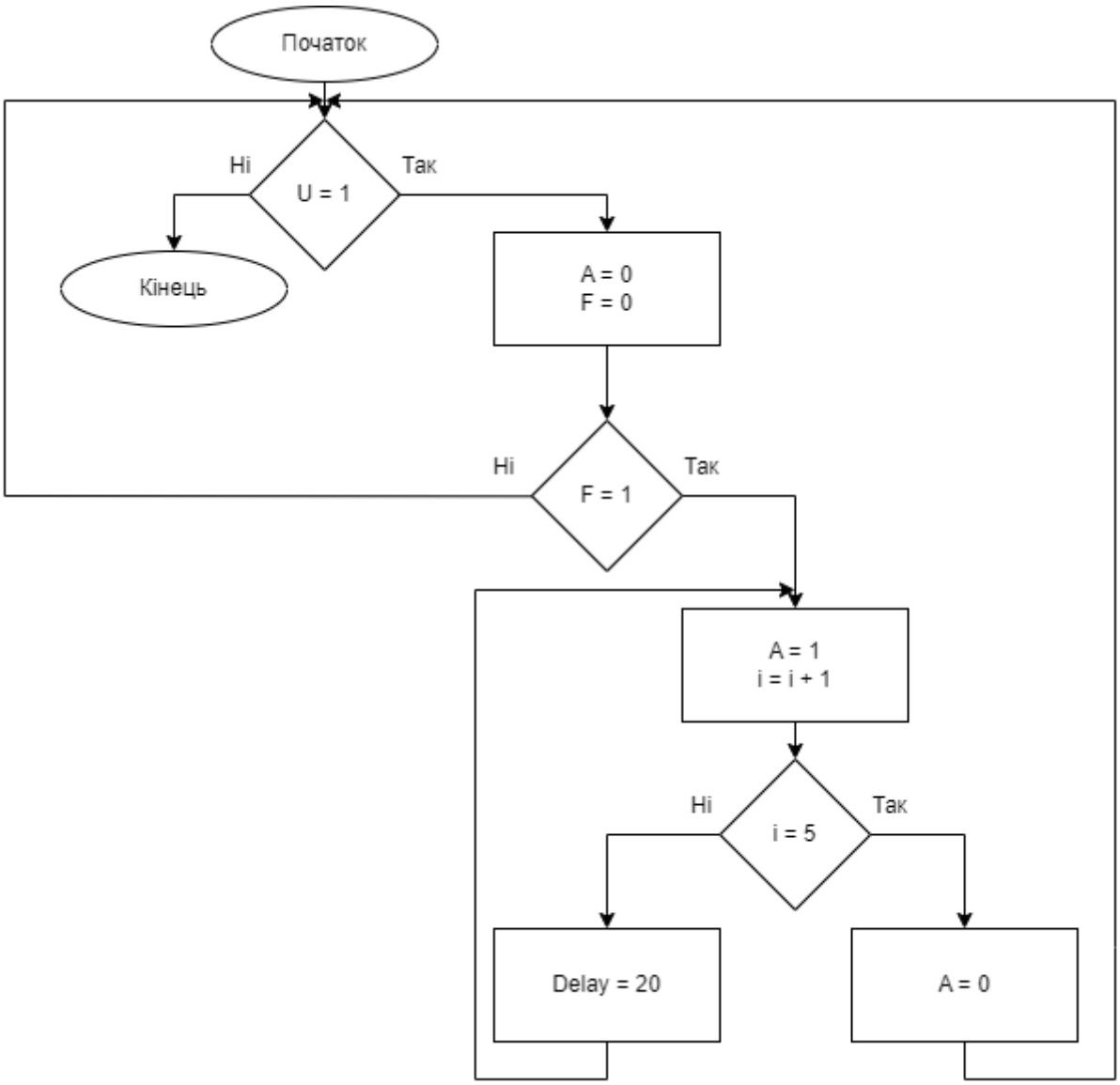


Рисунок 2.9 Блок-схема роботи системи сигналізації

Далі було написано код для Arduino 2 та Arduino 3, даний код повинен буде відповідати за безпеку периметру.

2.2 Лістинг коду Arduino 2 та 3

```
// Призначення пінів
const TRIP_SENSORS = [1, 2, 3, 4]; // Масив тригерних датчиків
const LED_PIN = 5; // Пін для світлодіода

function setup() {
    // Встановлюємо тригерні датчики як входи
    TRIP_SENSORS.forEach(sensor => pinMode(sensor, INPUT));

    pinMode(LED_PIN, OUTPUT); // Встановлюємо пін світлодіода як
вихід
}

function loop() {
```

```
    // Читання значень з тригерних датчиків
    const sensorsActive = TRIP_SENSORS.map(sensor => 
digitalRead(sensor));

    // Перевіряємо, чи активовано хоча б один тригерний датчик
    const isAnySensorActive = sensorsActive.some(value => value > 
0);
    // Керуємо світлодіодом в залежності від статусу датчиків
    digitalWrite(LED_PIN, isAnySensorActive ? HIGH : LOW);
}
```

Призначення пінів:

Код починається з визначення пінів, які використовуються для підключення компонентів

- TRIP_SENSORS – масив, що містить номери пінів (1, 2, 3, 4) для чотирьох тригерних датчиків, які будуть перевірятися на активність.
- LED_PIN (5) – пін для світлодіода, який інформує про активність тригерних датчиків.

Далі була прописана функція setup():, яка встановлює початкові налаштування для всіх пінів.

- Цикл forEach перебирає масив TRIP_SENSORS і встановлює кожен з тригерних датчиків як вхід (INPUT).
- pinMode(LED_PIN, OUTPUT) – встановлює пін світлодіода як вихід, щоб його можна було вмикати і вимикати.

Далі була прописана функція функція loop():, ця функція виконується безперервно в циклі.

- Використовується метод map, щоб зчитати значення з усіх тригерних датчиків, результати зберігаються в масиві sensorsActive.
- const isAnySensorActive = sensorsActive.some(value => value > 0) – перевіряє, чи активовано хоча б один з тригерних датчиків. Якщо будь-який з датчиків виявляє об’єкт (значення більше 0), змінна isAnySensorActive стає істинною.
- digitalWrite(LED_PIN, isAnySensorActive ? HIGH : LOW) – контролює світлодіод. Якщо активовано хоча б один тригерний датчик,

світлодіод світиться (значення HIGH), в іншому випадку – вимикається (значення LOW).

Код реалізує систему виявлення об'єктів за допомогою чотирьох тригерних датчиків, які можуть виявляти об’єкти в певній зоні. Світлодіод служить візуальним індикатором, що вказує на активність датчиків. Якщо хоча б один з датчиків виявляє об’єкт, світлодіод світиться, що сигналізує про наявність об’єкта в зоні виявлення. Код працює в циклі, постійно перевіряючи стан датчиків і забезпечуючи безперервний контроль за середовищем.

Після написання коду для платформи Arduino було розроблено алгоритми роботи для таких пристроїв, як камери відеоспостереження та датчиків руху(Зображено на рисунку 2.10).

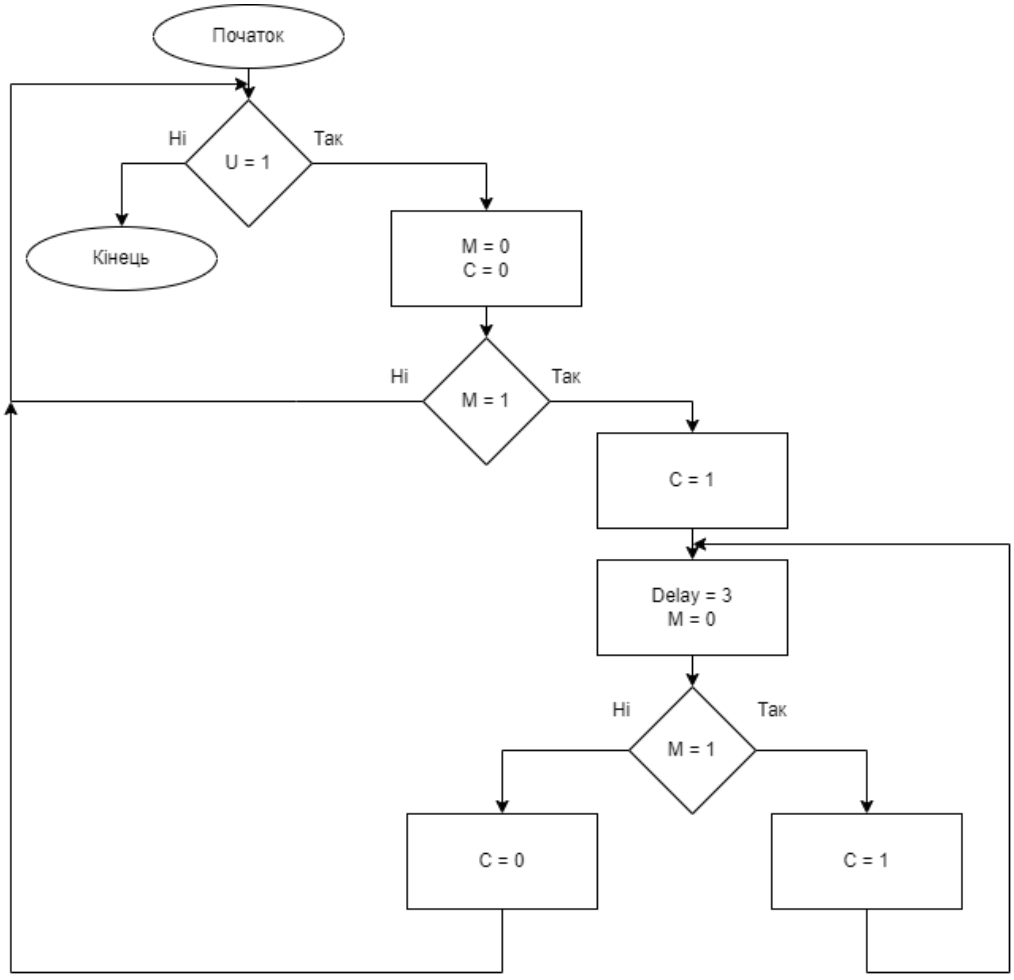


Рисунок 2.10 – Блок-схема роботи системи відеоспостереження

Алгоритм для камер та датчиків руху функціонує наступним чином: Спочатку здійснюється перевірка наявності живлення. Якщо живлення немає, алгоритм припиняє роботу. У разі наявності живлення статус камери та датчика руху присвоюється як 0 (режим сну). Після цього алгоритм перевіряє, чи активувався датчик руху. Якщо датчик переходить у статус 1 (активний), то камері присвоюється статус 1 (ввімкнена). Потім відбувається повторна перевірка стану датчика руху: якщо він залишається активним, система продовжує роботу в циклі до моменту, поки статус датчика не повернеться до 0. У разі неактивності датчика алгоритм повторюється спочатку.

Далі було розроблено алгоритм для системи пожежної безпеки, що зображений на рисунку 2.11.

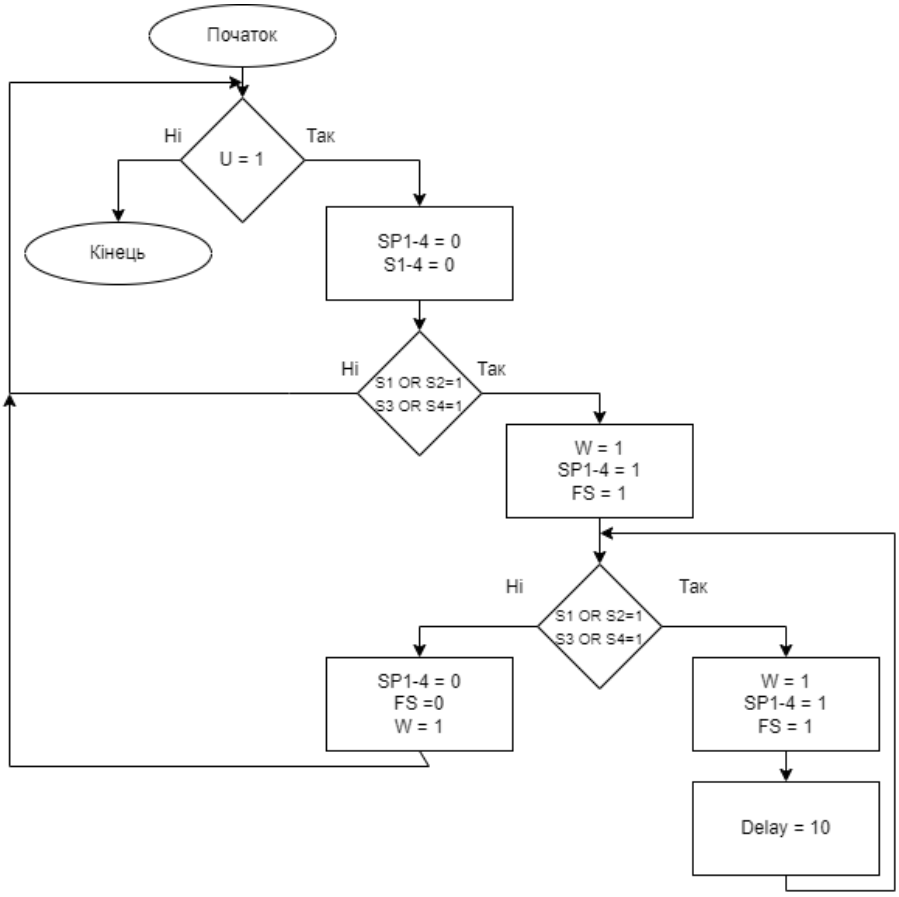


Рисунок 2.10 – Блок-схема роботи системи пожежо гасіння

Алгоритм для пожежної системи працює так: Спершу перевіряється наявність живлення. Якщо живлення немає, система автоматично припиняє роботу. Якщо живлення є, всім датчикам диму присвоюється статус 0

(неактивні). Далі система перевіряє, чи хоча б один із датчиків не перейшов у статус 1 (виявлено дим). Якщо виявлено дим, всі спринклери активуються (статус 1), а розумні сервоприводи на вікнах відчиняються (статус 1) для проникненню повітря в середину.

Після цього виконується повторна перевірка: якщо хоча б один датчик диму залишається активним (статус 1), спринклери продовжують працювати до моменту, коли всі датчики диму повернуться до статусу 0. Для запобігання перевантаженню системи між перевірками вводиться10-секундна затримка. Після того, як усі датчики диму повертаються до статусу 0, алгоритм починає виконуватися знову.

2.4 Вибір та опис апаратного забезпечення

Вибір компонентів безпосередньо впливає на вартість і ефективність роботи системи. У цьому розділі буде сформовано перелік елементів, які відповідають вимогам поставленого завдання.

Для забезпечення базової комплектації системи охорони приватного будинку необхідні такі компоненти:

- Розумний шлюз;
- Маршрутизатор;
- Сервер;
- Інфрачервоні датчики;
- Сигналізація;
- Датчики диму;
- Спринклери;
- Камери відеоспостереження;
- RFID-зчитувач;
- Магнітний замок для дверей;
- Розумні приводи для вікон.

Першим елементом, який слід розглянути, є шлюз, оскільки він є "мозком" системи і відіграє одну з ключових ролей у її функціонуванні.

При виборі шлюзу для системи охорони приватного будинку важливо враховувати його сумісність із комп'ютерною системою. Необхідно перевірити, які протоколи зв'язку використовуються у вашій системі (наприклад, TCP/IP, Zigbee, Z-Wave тощо), і переконатися, що шлюз підтримує ці протоколи. Також важливо звернути увагу на функціональні можливості шлюзу. Якщо шлюз не буде досить функціональним, можуть виникнути проблеми з підключенням до нього таких пристроїв, як плата Arduino, камери відеоспостереження та датчики руху, оскільки шлюз може виявитися з ними несумісним.

Ще одним критичним фактором є можливість масштабування системи, оскільки в майбутньому може виникнути потреба у її розширенні. Крім того, шлюз повинен бути зручним у використанні, щоб звичайний користувач міг легко його налаштовувати та керувати системою.

Під дані характеристики найбільш підходящим буде шлюз від компанії Livolo (показано на рисунку 2.11)

Рисунок 2.11 Шлюз Zigbee 3.0 Livolo (VL-XG002)

Шлюз Zigbee 3.0 Livolo (VL-XG002) забезпечує інтеграцію між різними пристроями стандарту Zigbee та центральною системою управління через мобільний додаток. Його основне завдання полягає у формуванні стабільного бездротового зв'язку між пристроями, такими як сенсори, вимикачі та інші елементи автоматизації, для забезпечення зручності керування з єдиного інтерфейсу.

Пристрій використовує протокол Zigbee 3.0, який є одним з найбільш поширених стандартів для смарт-пристроїв. Цей стандарт забезпечує високий рівень безпеки завдяки шифруванню даних і надійності зв'язку, що особливо важливо для інтеграції великої кількості пристроїв в одну систему. Завдяки своїм технічним характеристикам шлюз може забезпечити стабільний зв'язок навіть на значних відстанях, що дозволяє використовувати його в приміщеннях різної площі та конфігурації.

Ключовою перевагою шлюзу Livolo є його енергоефективність, оскільки Zigbee-пристрої споживають значно менше енергії порівняно з Wi-Fi-пристроями. Крім того, він підтримує роботу з голосовими помічниками, такими як Google Assistant і Amazon Alexa, що розширює можливості інтеграції в різні сценарії використання смарт-будинків. Це робить пристрій особливо зручним для тих користувачів, які прагнуть автоматизувати щоденні процеси через голосові команди або віддалене управління.

Загалом, шлюз Livolo VL-XG002 є ефективним рішенням для створення надійної смарт-інфраструктури. Його використання дозволяє забезпечити гнучкість системи управління, легкість інтеграції нових пристроїв та зниження енергоспоживання, що особливо важливо в умовах сучасних вимог до енергоефективності та безпеки житлових приміщень.

Характеристики даного шлюзу

За допомогою мобільного додатку Livolo користувачі можуть управляти освітленням та іншими підключеними пристроями дистанційно, незалежно від свого місцезнаходження. Це дозволяє здійснювати контроль з будь-якого мобільного пристрою з доступом до Інтернету.

Додаток Livolo Home надає зворотний зв'язок про поточний стан підключених пристроїв, таких як освітлювальні прилади (увімкнені чи вимкнені). Це дозволяє уникнути потреби фізично перевіряти, чи вимкнене світло, забезпечуючи додатковий комфорт та спокій.

Шлюз використовує хмарний сервер Amazon AWS, що гарантує високий рівень безпеки для зберігання та обробки даних. Це надає користувачам впевненість у захисті їх інформації та стабільності роботи пристрою.

Шлюз здатний напряму підтримувати з'єднання до 112 різних пристроїв. До них входять 20 бездротових маршрутизаторів, 32 бездротові пристрої та до 60 інших смарт-пристроїв, що робить його ідеальним для великих домашніх або офісних смарт-систем.

У випадку тимчасової втрати Інтернет-зв'язку, смарт-сценарії, налаштовані в системі, продовжують працювати в локальній мережі. Це забезпечує безперервну роботу підключених пристроїв, навіть коли зовнішній доступ обмежений.

Завдяки інтеграції з Google Assistant і Amazon Alexa, користувачі можуть керувати освітленням та іншими пристроями за допомогою голосових команд. Це значно полегшує взаємодію з системою, дозволяючи управляти нею через смартфон або розумну колонку від Google чи Amazon.

Наступним компонентом, який було розглянуто, є комутатор. Під час його вибору слід звернути увагу на кілька важливих аспектів. Перш за все, необхідно визначити кількість портів, яка знадобиться для підключення всіх пристроїв. Важливим параметром є також швидкість передачі даних, оскільки для системи безпеки будь-які затримки є неприпустимими. Ще один ключовий аспект - це рівень безпеки, який повинен забезпечувати комутатор.

Оптимальним варіантом для цієї системи є комутатор TP-Link TL-SF1024D (TL-SF1024D), як показано на рисунку 2.12.

Основні характеристики цього комутатора:

Кількість портів: Комутатор оснащений 24 портами Ethernet зі швидкістю 10/100 Mbps, що дозволяє підключити велику кількість пристроїв до мережі.

Швидкість передачі даних: Підтримує швидкість до 100 Mbps, що забезпечує швидкий обмін даними між підключеними пристроями, що особливо важливо для безперервної роботи системи охорони.

Рисунок 2.12 - Комутатор TP-Link TL-SF1024D.

Завдяки підтримці Plug and Play, підключення пристроїв до мережі відбувається без складних налаштувань, що значно спрощує процес інтеграції.

Комутатор комплектується зовнішнім блоком живлення, який забезпечує стабільне енергопостачання.

Фізичні параметри пристрою становлять 294 x 180 x 44 мм, що робить його компактним і зручним для встановлення.

Пристрій автоматично регулює споживання енергії в залежності від активності портів, що сприяє економії електроенергії.

Комутатор підтримує функцію контролю потоку (IEEE 802.3x), що дозволяє запобігти втратам даних під час передавання, забезпечуючи надійність мережевих з'єднань.

При виборі камер відеоспостереження для комп'ютерної системи охорони, слід враховувати конкретні потреби і характеристики, а саме якість зображення, кут який буде охоплювати дана камера, а також чи встановлено в камеру модуль нічного бачення, для задоволення даних потреб підходить камера Hikvision DS-2CE56H0T-IRMMF(показано на рисунку 2.13) - це високоякісна відеокамера типу "купольна" від відомого виробника Hikvision, яка належить до серії Turbo HD. Вона призначена для відеоспостереження в умовах високої чіткості (HD), з підтримкою технології HD-TVI, яка дозволяє передавати відео по коаксіальних кабелях без значних втрат якості на великі відстані.

Рисунок 2.13 - Камера Hikvision DS-2CE56H0T-IRMMF.

Роздільна здатність 5 Мп: Камера забезпечує високу роздільну здатність 2560×1944 пікселів, що дозволяє отримувати деталізоване зображення, яке добре підходить для розпізнавання об'єктів і осіб. Вона пропонує чітке зображення навіть на великій відстані.

Фіксований об'єктив 3.6 мм: Фіксований об'єктив із фокусною відстанню 3.6 мм забезпечує широкий кут огляду, що підходить для спостереження за більшими площами, як-от парковки, склади або територія перед будівлею.

Інфрачервона підсвітка (IR): Камера оснащена інфрачервоною підсвіткою для зйомки в умовах низької освітленості або повної темряви. Дальність підсвічування становить до 20 метрів, що дозволяє отримувати чітке зображення навіть вночі.

Технологія EXIR 2.0: Використання передової технології EXIR забезпечує рівномірне інфрачервоне освітлення та усуває проблеми засвічення в центрі кадру, що покращує якість зображення в темну пору доби.

Захист IP67: Камера має високий ступінь захисту від пилу та вологи (IP67), що робить її придатною для використання на відкритих просторах або в складних погодних умовах. Це забезпечує довговічність і надійну роботу на вулиці.

Технологія відео стиснення H.265: Завдяки підтримці H.265+, камера ефективно зменшує обсяг збережених даних, що дозволяє економити місце на носіях без втрати якості зображення.

Технологія 4-в-1: Камера підтримує кілька відео стандартів (HD-TVI, AHD, CVI та аналог), що дозволяє легко інтегрувати її у вже існуючі системи відеоспостереження або розширювати мережу з новими пристроями.

Переваги:

- Висока якість зображення завдяки роздільній здатності 5 Мп.
- Надійна робота в нічний час завдяки інфрачервоному підсвічуванню до 20 метрів.
- Широкі можливості підключення та сумісність із різними стандартами відеоспостереження.
- Високий ступінь захисту від пилу та вологи (IP67), що робить камеру ідеальною для зовнішнього використання.

Недоліки:

- Фіксований об'єктив (3.6 мм) може бути менш гнучким у налаштуванні для специфічних потреб огляду.
- Для запису відео у форматі високої чіткості може знадобитися більше місця на носіях для зберігання даних, хоча технологія H.265 частково вирішує це питання.

Під час вибору інфрачервоного датчика руху для комп'ютеризованої системи охорони слід зважати на специфічні вимоги та характеристики пристрою, такі як: Дальність дії, Кут огляду, Зона ігнорування та Надійність. Оскільки датчик планується підключити до плати Arduino, було обрано ІЧ-датчик руху HC-SR505 для Arduino, даний датчик показано на рисунку 2.13.

Рисунок 2.13 – Інфрачервоний датчик руху HC-SR505

Модуль з інфрачервоним датчиком руху PIR HC-SR505 - це компактний і недорогий датчик руху, який використовує пасивну інфрачервону технологію для виявлення теплового випромінювання об’єктів. Завдяки своїм компактним розмірам і енергоефективності, він широко

застосовується в системах автоматизації, зокрема в освітленні, сигналізації, проєктах "розумного дому" та в DIY-проєктах.

Тип датчика: PIR (пасивний інфрачервоний датчик), який реагує на зміни інфрачервоного випромінювання в зоні дії. Це означає, що датчик визначає наявність теплового об’єкта, наприклад людини, але не випромінює власного інфрачервоного сигналу.

Основні характеристики модуля з інфрачервоним датчиком руху PIR HC-SR505:

- Тип датчика: Пасивний інфрачервоний (PIR)
- Напруга живлення: 4.5–20 В постійного струму (DC)
- Споживання струму: < 60 мкА (у режимі очікування)
- Діапазон виявлення руху: до 3 метрів
- Кут огляду: приблизно 100°
- Час затримки спрацювання: 8 секунд (незмінний)
- Робоча температура: від -20°C до +80°C
- Розміри: близько 10x23 мм

Сумісність: Підходить для роботи з мікроконтролерами, такими як Arduino, Raspberry Pi, ESP8266

Модуль має радіус дії до 3 метрів, що достатньо для автоматизованих систем невеликого розміру. Датчик розрахований на виявлення руху в межах кута огляду близько 100°.

Час затримки спрацювання датчика становить близько 8 секунд, що дозволяє швидко реагувати на виявлений рух і викликати відповідну дію (вмикання світла, запуск сигналізації тощо).

Датчик працює від низької напруги - від 4.5 до 20 В, що робить його сумісним із широким колом електронних пристроїв, включаючи батарейне живлення або системи з мікроконтролерами (наприклад, Arduino або Raspberry Pi).

Завдяки низькому споживанню енергії цей модуль ідеально підходить для автономних пристроїв, де важлива тривала робота від батареї.

Переваги:

- Компактність і легкість інтеграції в різні проєкти завдяки малим розмірам.
- Низьке енергоспоживання, що робить його економічним рішенням для батарейних пристроїв.
- Сумісність з популярними платформами для DIY-проєктів (Arduino, Raspberry Pi), завдяки чому модуль підходить для широкого кола автоматизованих рішень.
- Простота налаштування: Датчик поставляється практично готовим до використання і не потребує складних налаштувань.

Недоліки:

- Обмежена дальність виявлення (до 3 метрів), що може бути недостатньо для деяких великих або зовнішніх застосувань.
- Фіксована затримка спрацювання (8 секунд), що не дозволяє змінювати тривалість сигналу за необхідності.
- Чутливість до зовнішніх факторів: PIR-датчики можуть реагувати на зміну температури або теплове випромінювання інших об'єктів, що може спричинити випадкові спрацювання в нестабільних умовах.

Під час вибору розумного сервопривода для вікон у системі охорони необхідно звернути увагу на кілька важливих параметрів: Сумісність із системою, Потужність приводу, Швидкість відкриття/закриття, Надійність у роботі, а також Можливість бездротового підключення для інтеграції з центральною системою управління. Розумний сервопривід XYDHB12 (Показано на рисунку 2.14)забезпечує швидке й надійне закривання та відкривання вікон у разі активації тривоги або для інших автоматизованих сценаріїв, таких як контроль вентиляції та димовидалення. Завдяки своїй міцності та надійності, цей актуатор підходить для використання в

автоматизації, промисловому обладнанні, системах керування положенням, а також у проєктах «розумного дому».

Рисунок 2.14 - Розумний сервопривід XYDHB12

Хід даного сервоприводу 300 мм, цей показник визначає максимальну довжину, на яку шток може висуватися, що дозволяє використовувати пристрій для завдань, де потрібна відносно велика амплітуда переміщення.

Сила натискання: 1500 Н даного сервоприводу така сила дозволяє актуатору переміщати важкі об'єкти, що робить його ефективним для роботи з масивними конструкціями та механізмами.

Швидкість руху приводу 4 мм/с забезпечує досить повільний, але стабільний рух штока, що підходить для додатків, де важлива контрольованість та точність.

напруга в 12 В постійного струму (DC) є стандартною для багатьох джерел живлення, що полегшує інтеграцію актуатора в різні системи.

Зазвичай актуатори цієї моделі мають рівень захисту IP65, що означає стійкість до пилу і бризок води. Це дозволяє використовувати його в умовах підвищеної вологості або в зовнішньому середовищі.

Матеріал і конструкція: Металевий корпус і шток забезпечують довговічність та зносостійкість. Це особливо важливо для важких умов експлуатації, таких як виробничі приміщення або зовнішні монтажі.

Переваги:

- Висока сила натискання (1500 Н) дозволяє використовувати актуатор для роботи з важкими об’єктами.
- Надійність і довговічність завдяки металевій конструкції та рівню захисту IP65.
- Сумісність з широким спектром систем, що працюють на 12 В DC.
- Контрольованість і плавність руху через низьку швидкість, що підходить для застосувань, де потрібна точність.

Недоліки:

- Невелика швидкість руху (4 мм/с), що може бути обмеженням для додатків, де потрібен швидкий лінійний рух.
- Відносно висока енергоспоживання для живлення на 12 В при навантаженні, що може потребувати потужного джерела живлення.

Під час вибору датчика диму для системи охорони варто врахувати кілька ключових аспектів: Чутливість до диму, Швидкість реагування, Сумісність із системою безпеки, Надійність у різних умовах середовища та Можливість бездротового підключення. Обраний датчик має забезпечувати миттєве виявлення диму та швидке оповіщення системи про загрозу пожежі. Важливо також, щоб він був стійким до хибних спрацювань, що гарантує стабільну роботу навіть за змінних умов температури та вологості.

Під дані умови підходить датчик диму CoVi Security HM-200 що зображений на рисунку 2.15

Рисунок 2.15 - Датчик диму CoVi Security HM-200

Бездротовий автономний датчик диму CoVi Security HM-200 з підтримкою Tuya Smart є сучасним пристроєм, призначеним для забезпечення безпеки в житлових та комерційних приміщеннях. Його основна функція полягає у швидкому виявленні диму та своєчасному попередженні про загрозу пожежі. Завдяки інтеграції з платформою Tuya Smart, цей датчик забезпечує простоту використання та ефективний контроль за пожежонебезпечними ситуаціями в рамках системи розумного будинку.

Датчик HM-200 обладнано чутливим сенсором, який швидко реагує на появу диму і миттєво активує сигналізацію, що дозволяє оперативно вжити необхідних заходів у разі загрози. Використання бездротової технології істотно спрощує процес установки та інтеграції в існуючу систему безпеки. Можливість підключення до смартфона або інших пристроїв через мобільні додатки та голосових помічників, що підтримуються Tuya Smart, дозволяє користувачам зручно управляти датчиком і отримувати актуальні сповіщення про виявлення диму, навіть якщо вони знаходяться далеко від дому.

Крім того, датчик НМ-200 має гучну звукову сигналізацію та світлодіодні індикатори, які ефективно сповіщають про небезпеку. Це особливо важливо в ситуаціях, коли користувача немає вдома або під час сну, адже сигналізація залишається чутною та помітною. Живлення пристрою здійснюється від вбудованого акумулятора, що забезпечує автономну роботу без залежності від електромережі. Це гарантує надійний контроль за ситуацією навіть під час тимчасових відключень електроенергії.

Таким чином, бездротовий датчик диму НМ-200 із підтримкою Tuya Smart є незамінним елементом безпеки для будь-якого дому чи офісу. Він не лише виявляє дим, а й надає можливість віддаленого управління та оперативного отримання сповіщень. Це надійне рішення для забезпечення захисту майна та життя від ризиків, пов'язаних із пожежами. При виборі електроприводу для кульового крана хомут необхідно врахувати кілька критично важливих аспектів, які впливають на ефективність та надійність системи управління. Першочерговою характеристикою є потужність приводу, яка повинна відповідати технічним вимогам крана та специфікаціям системи, щоб забезпечити належну продуктивність.

Наступним важливим фактором є швидкість реакції електроприводу. Він має забезпечувати оперативне відкриття та закриття клапана, що є ключовим для ефективного управління потоком рідини чи газу. Це дозволяє оптимізувати процеси, що вимагають точного контролю над розподілом ресурсів.

Сумісність з системою автоматизації є ще одним важливим аспектом, оскільки привід повинен легко інтегруватися з наявними контролерами та датчиками. Це забезпечує безперебійну роботу всієї системи, що сприяє підвищенню її ефективності.

Надійність у різних умовах середовища є важливим критерієм, оскільки електропривід повинен бути здатним витримувати температурні коливання, вологість та інші впливи навколишнього середовища. Ця

характеристика забезпечує стабільну роботу пристрою в умовах, що змінюються, запобігаючи можливим збоїв.

Крім того, можливість бездротового підключення значно полегшує процес установки та управління, надаючи гнучкість у налаштуванні системи. Вибраний електропривід повинен гарантувати стабільну роботу без збоїв і бути стійким до хибних спрацьовувань. Це є запорукою надійного функціонування системи управління у змінних умовах експлуатації.

Під дані умови підходить електронний контролер для клапанів води Aqara Smart Valve Controller T1(Зображено на рисунку 2.16), що дозволяє здійснювати дистанційне управління. Основна функція цього пристрою полягає в автоматичному відкритті та закритті клапанів, що підвищує зручність і безпеку в домашньому середовищі.

Рисунок 2.16 - Електронний контролер для клапанів води Aqara Smart Valve Controller T1

Контролер має широкий спектр сумісності з популярними екосистемами, такими як Apple HomeKit, Amazon Alexa, Google Assistant і IFTTT. Це забезпечує безперешкодну інтеграцію в уже існуючі системи

розумного дому. Завдяки бездротовій технології та підтримці стандарту Zigbee 3.0, установка пристрою не потребує проведення додаткових проводів або внесення змін до вже існуючих трубопроводів.

Однією з ключових можливостей контролера є автоматичне виявлення витоків. У випадку підключення до спеціалізованих датчиків, що реагують на витік води або газу, пристрій здатний самостійно закривати відповідні клапани, що зменшує ризики аварійних ситуацій. Заявлена підтримка протоколу Matter також відкриває нові можливості для інтеграції з іншими розумними пристроями в майбутньому.

Цей контролер відрізняється підвищеним рівнем безпеки, адже можливість автоматичного закриття клапанів у разі виявлення витоку здатна запобігти затопленню або витоку газу. Дистанційне управління через мобільний додаток або за допомогою голосових асистентів робить процес моніторингу стану клапанів простим і зручним. Крім того, інтеграція з іншими елементами розумного дому дозволяє створювати сценарії для оптимізації використання ресурсів.

Проте для функціонування пристрою необхідний хаб Aqara Zigbee 3.0, який продається окремо. Незважаючи на підтримку основних екосистем, функціональність пристрою може бути обмежена в деяких випадках.

Для реалізації системи карткового доступу було вибрано RFID-модуль MFRC522 даний пристрій зображено на рисунку,

RFID-модуль MFRC522 — це популярний безконтактний зчитувач, що працює на частоті 13.56 МГц. Він широко використовується в проектах, пов’язаних з ідентифікацією, контролем доступу, трекінгом товарів та іншими застосуваннями RFID-технології. Розглянемо деякі ключові аспекти аналізу цього модуля.

MFRC522 працює на частоті 13.56 МГц, що дозволяє йому взаємодіяти з картами стандарту ISO/IEC 14443 A/MIFARE. Зазвичай відстань зчитування становить до 10 см, проте це може змінюватися в залежності від розміру та типу RFID-мітки. Модуль живиться від напруги в діапазоні від 2.5 до 3.6 В, що

робить його сумісним із різними мікроконтролерами, такими як Arduino. MFRC522 використовує SPI, I2C або UART для з’єднання з мікроконтролерами, що забезпечує гнучкість в реалізації проектів. Принцип роботи MFRC522 базується на використанні електромагнітного поля для передачі даних між зчитувачем і RFID-міткою. Коли мітка наближається до зчитувача, вона отримує енергію з його поля, що дозволяє їй передавати дані назад.

Рисунок 2.17 - RFID-модуль MFRC522

В цілому, RFID-модуль MFRC522 є надійним і економічно вигідним рішенням для багатьох проектів, пов’язаних із безконтактною ідентифікацією. Його простота в інтеграції та функціональність роблять його популярним вибором серед розробників.

Для реалізації системи сигналізації на базі Arduino було вибрано rduino UNO R3 (MCU - ATMega328P + CH340G) який зображено на рисунку 2.18

Arduino UNO R3 — це популярна плата для розробки, яка базується на мікроконтролері ATMega328P. Вона має 32 Кб флеш-пам'яті для зберігання коду, з яких 0,5 Кб зарезервовано для завантажувача. Також плата має 2 Кб статичної оперативної пам'яті (SRAM) та 1 Кб пам'яті для зберігання даних (EEPROM). Плата оснащена 14 цифровими виходами, з яких 6 можуть використовуватися як аналогові виходи (PWM). Вона має 6 аналогових входів,

що дозволяє підключати різноманітні сенсори. Arduino UNO R3 підтримує різні інтерфейси зв'язку, включаючи I2C та SPI, а також має один серійний порт.

Рисунок 2.18 - Плата Arduino UNO R3

Для живлення плати можна використовувати USB-кабель або зовнішнє джерело живлення в діапазоні від 7 до 12 В. Плата має вбудований стабілізатор напруги, що забезпечує стабільну роботу навіть при варіаціях вхідної напруги. Arduino UNO R3 також включає в себе мікросхему CH340G для USB-інтерфейсу, що забезпечує простий підключення до комп'ютера для програмування та комунікації.

Для побудови ефективної системи охорони будинку з інтегрованою пожежною сигналізацією необхідний сервер із високою надійністю та достатньою потужністю для обробки відео- та сенсорних даних у режимі реального часу. Основними функціями цього сервера є зберігання, обробка та передача даних, які надходять від охоронних і пожежних датчиків, забезпечуючи оперативне реагування на загрози безпеці.

Процесор сервера повинен відповідати вимогам багатопотокової обробки, що дозволяє одночасно керувати кількома завданнями, такими як обробка відеопотоків, обробка сигналів від датчиків і передача даних. Для

цього підходять процесори типу Intel Xeon або AMD Ryzen Threadripper з 6–12 ядрами, що підтримують одночасну обробку декількох потоків даних, що забезпечує стабільність і надійність системи навіть під значним навантаженням.

Оперативна пам'ять обсягом 16–32 ГБ (DDR4 або DDR5) дозволяє зберігати великі обсяги даних у буфері для швидкого доступу, що необхідно для одночасної обробки відеопотоків з камер спостереження, повідомлень про тривогу і сигналів від різних сенсорів. Такий обсяг пам’яті забезпечує ефективну роботу системи без затримок.

Для зберігання даних рекомендується використовувати комбіноване рішення з жорстких дисків і твердотільних накопичувачів. Жорсткий диск обсягом не менше 2 ТБ забезпечує зберігання відеозаписів та журналів на тривалий період, дозволяючи зберігати записи з кількох камер протягом 2–4 тижнів. Твердотільний накопичувач (SSD) обсягом 256–512 ГБ рекомендується для зберігання операційної системи та основних програм, що підвищує швидкість доступу до даних і загальну продуктивність системи. Рекомендується використовувати конфігурацію RAID (RAID 1 або RAID 5) для підвищення надійності зберігання і забезпечення безперебійного функціонування системи навіть у разі виходу одного з накопичувачів з ладу.

Для обробки відеопотоків, особливо якщо передбачається використання технологій розпізнавання облич або виявлення руху, бажано встановити графічний процесор (GPU), наприклад, NVIDIA GTX 1660 або серії Quadro з підтримкою обробки відео за допомогою технології CUDA. Це дозволяє оптимізувати обробку відеоданих, знижуючи навантаження на центральний процесор і підвищуючи загальну продуктивність системи.

Мережева карта гігабітного класу (Gigabit Ethernet) забезпечує стабільне з’єднання і високу швидкість передачі даних, що особливо важливо для своєчасної обробки і передачі інформації з камер і датчиків до центрального сервера. У випадку використання PoE (Power over Ethernet),

мережевий комутатор повинен підтримувати живлення через Ethernet, що значно спрощує монтаж і підключення пристроїв.

Операційна система сервера вибирається залежно від вимог програмного забезпечення для моніторингу. Найбільш популярні рішення включають Windows Server або Linux (Ubuntu Server, CentOS), які забезпечують високу стабільність роботи і сумісність з більшістю охоронних програм, а також дозволяють налаштувати додаткові функції безпеки.

Система охорони і пожежної сигналізації вимагає наявності певних компонентів, таких як IP-камери відеоспостереження високої роздільної здатності (1080p або вище), PIR-датчики руху для виявлення несанкціонованих вторгнень, датчики відкриття дверей і вікон, а також пожежні сенсори (димові та теплові датчики) для вчасного реагування на небезпеку. Крім того, для оповіщення при спрацюванні сигналізації використовуються сирени та світлові сигналізатори.

Додаткові опції включають встановлення джерела безперебійного живлення (UPS) для забезпечення роботи сервера, камер і датчиків у разі перебоїв з електропостачанням. Використання хмарного зберігання даних може бути корисним для забезпечення резервного копіювання важливих записів і віддаленого доступу до них. Інтеграція GSM або LTE-модулів дозволить відправляти повідомлення про тривогу при відсутності інтернет-з’єднання.

Таким чином, сервер для охоронної системи з пожежною сигналізацією повинен мати достатню обчислювальну потужність, великий обсяг оперативної пам’яті і сховища для безперебійного обслуговування системи, а також стабільне підключення до мережі. Така архітектура забезпечить надійний рівень безпеки і дасть змогу оперативно реагувати на можливі загрози.

2.5 Висновки до розділу

У цьому розділі детально розглянуто вимоги до розробки та реалізації сучасної системи управління комунікаціями, з особливим акцентом на

інтеграцію компонентів для забезпечення високої ефективності та надійності функціонування. У контексті системи було створено функціональну схему, що ілюструє основні компоненти та їх взаємозв'язки, а також описано специфікації, які повинна відповідати сучасна система такого роду.

Серед вимог до системи були визначені ключові аспекти, такі як надійність, швидкість реагування на загрози, легкість у використанні та масштабованість для подальшого вдосконалення. Приділено увагу безпеці даних і захисту від несанкціонованого доступу, що є критично важливим для систем, які обробляють чутливу інформацію.

У процесі розробки були прописані алгоритми для основних функцій системи, що включали управління системою пожежогасіння, відеонаглядом та сигналізацією. Створено блок-схеми, які детально ілюструють роботу зазначених компонентів. Зокрема, розроблено алгоритми для системи сигналізації, що базується на платформі Arduino з використанням датчиків ІЧ-випромінювання, які забезпечують своєчасне виявлення загроз.

Також розроблено блок-схему для роботи головного входу в будинок через картку, що дозволяє інтегрувати рішення для контролю доступу. Ця схема включає в себе різні етапи процесу авторизації, а також механізми управління станом замка на основі успішної або неуспішної спроби доступу.

Крім того, було підібрано відповідні компоненти для реалізації системи, що включають апаратні засоби, програмне забезпечення та датчики, що забезпечують злагоджену роботу всієї системи. У результаті було створено комплексну структуру, яка забезпечить не лише ефективну охорону об’єкта, а й високий рівень автоматизації процесів.

Таким чином, цей розділ підкреслює важливість комплексного підходу до проектування системи управління комунікаціями, де враховані всі етапи - від розробки вимог до вибору компонентів. Успішна інтеграція всіх елементів сприятиме підвищенню ефективності комунікаційних процесів, забезпечить надійність і безпеку системи, а також відкриє можливості для подальшого розвитку та модернізації.

3 ОЦІНКА ЕФЕКТИВНОСТІ ТА РЕЗУЛЬТАТИ ТЕСТУВАННЯ СИСТЕМИ

3.1 Методи тестування

Для перевірки функціональності та надійності мережевої системи, що об’єднує численні елементи безпеки, було застосовано програмне забезпечення Cisco Packet Tracer(Показано на рисунку 3.1). Це потужний інструмент для моделювання мережевих з’єднань та обладнання, який дозволяє створювати віртуальні структури мережі та тестувати їх у максимально наближених до реальних умовах. Основною метою тестування стала перевірка здатності системи обробляти дані, забезпечувати своєчасне реагування на сигнали від датчиків і гарантувати безперервність роботи за умов підвищеного навантаження. Це особливо актуально для таких компонентів системи, як інфрачервоні датчики, камери відеоспостереження, сигналізація та інші пристрої, інтегровані з центральним шлюзом для роботи в режимі реального часу.

У Cisco Packet Tracer було змодельовано мережеву топологію, що включає маршрутизатор, комутатор, сервер і ключові елементи безпеки. Програмне забезпечення дозволило симулювати різні з’єднання, необхідні для датчиків руху, камер, сигналізації та інших пристроїв, що складають систему. Першочерговим завданням цього етапу стала перевірка коректності налаштувань IP-адрес і інших параметрів підключення, а також ефективності передачі даних комутатором між пристроями. Окремим етапом стала оцінка швидкості передачі даних, оскільки для системи безпеки будь-які затримки є критичними. Cisco Packet Tracer дозволив створити різноманітні сценарії із змінною інтенсивністю трафіку, завдяки чому вдалося оцінити швидкість реакції системи та затримки під час передачі сигналів від датчиків до камер. Особливу увагу приділили забезпеченню швидкої обробки даних для своєчасного спрацювання системи охорони.

Для належного функціонування важливою є коректна маршрутизація даних між компонентами системи. Cisco Packet Tracer дозволив змоделювати маршрутизацію та проаналізувати її ефективність. Було протестовано, як сервер обробляє дані від камер і сигналізаційної системи з урахуванням можливих затримок і їх впливу на сповіщення про загрози.

Крім того, для забезпечення стабільності системи було проведено тестування надійності з'єднань. Усі пристрої - датчики диму, спринклери, сервоприводи для вікон - мають стабільно працювати, особливо у разі загрози пожежі. Cisco Packet Tracer дозволив провести стрес-тести, імітуючи підвищене навантаження, і оцінити, чи система зберігає безперервний зв'язок під час збоїв або навантаження, та чи відновлює його автоматично.

Під час тестування було також оцінено максимальну пропускну здатність мережі, зокрема у сценаріях, коли сигнали надходять одночасно від декількох пристроїв. Cisco Packet Tracer дозволив визначити, як система справляється з високим рівнем трафіку і чи уникнуто пакетних затримок, що є важливим для стабільності мережі при активації кількох елементів охоронної системи.

Сигналізаційна система була окремо протестована на здатність швидко реагувати на сигнали від датчиків руху та диму. У Cisco Packet Tracer змоделювали ситуації спрацьовування датчиків та перевірили своєчасність обробки цих сигналів. Важливим етапом стала перевірка на можливість віддаленого доступу через додаток, який забезпечує сповіщення в реальному часі.

Враховуючи необхідність захищеного з'єднання між пристроями, було також протестовано налаштування безпеки мережі. Cisco Packet Tracer дозволив оцінити стійкість системи до можливих загроз, таких як несанкціонований доступ до шлюзу або спроби порушення з'єднання. Було перевірено, чи забезпечується захист від потенційних загроз для підтримки безпеки даних у мережі.

Завершальний етап включав комплексний аналіз результатів тестування, що дозволив оцінити ефективність роботи кожного компонента системи. Завдяки моделюванню у Cisco Packet Tracer вдалося виявити потенційні недоліки та провести необхідні оптимізації, що підвищили надійність і ефективність мережевої інфраструктури, створивши стабільну і безпечну систему для захисту приміщення.

3.2 Результати тестування

Першим етапом тестування було перевірено роботу системи порушення периметру, яка є важливим елементом комплексної охорони об’єкта. Ця система побудована на базі плати Arduino, до якої під’єднані такі елементи, як сигналізація, інфрачервоні датчики руху, RFID-зчитувач та магнітний замок. Після завершення налаштувань та завантаження коду, було проведено серію тестів, щоб переконатися у правильній роботі всіх компонентів. Результати цього тесту представлені на рисунку 3.1, що ілюструє успішну роботу системи

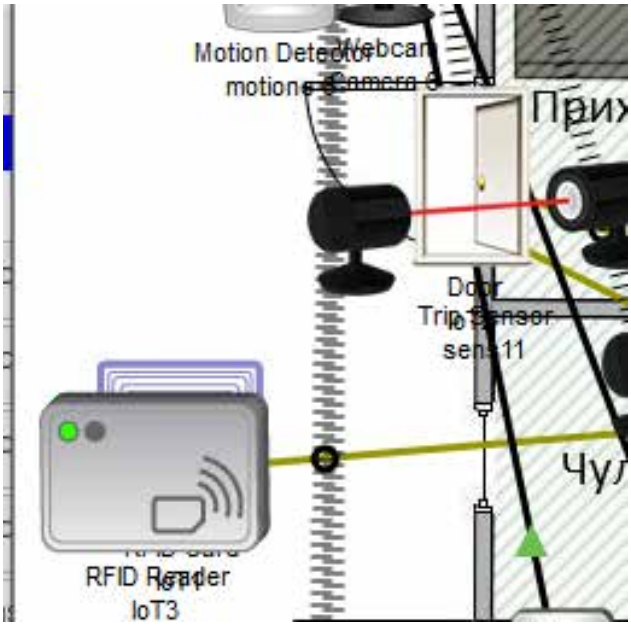


Рисунок 3.1 Тестування системи порушення периметру

За підсумками тестування стало очевидно, що код функціонує відповідно до заданих параметрів. Карта доступу, створена та налаштована спеціально для RFID-зчитувача, працює коректно: при використанні карти

замок відкрився, що підтверджує правильність налаштувань. Це свідчить про те, що всі компоненти системи - від зчитувача до сигналізації - взаємодіють належним чином, забезпечуючи заплановану функціональність охорони.

Тестування також дозволило оцінити швидкість реакції системи на виявлення руху, адже будь-які затримки або некоректна робота датчиків могли б знизити рівень безпеки. Результати показали, що сигнал від інфрачервоних датчиків руху миттєво передається на плату Arduino, яка активує сигналізацію без жодних затримок. Це надзвичайно важливо, оскільки своєчасне спрацювання сигналізації може відіграти вирішальну роль у запобіганні несанкціонованому доступу.

Таким чином, результати тестування підтвердили, що інтеграція всіх компонентів системи порушення периметру була виконана успішно, а система налаштована правильно і готова до подальшого використання.

Наступним кроком було тестування системи сигналізації, яка включає інфрачервоні датчики руху та безпосередньо сигналізаційний блок. Ця перевірка мала на меті оцінити швидкість реакції та загальну надійність роботи компонентів у різних умовах. Всі результати тестування відображено на рисунку 3.2, де видно, як швидко система реагує на зміни в навколишньому середовищі.

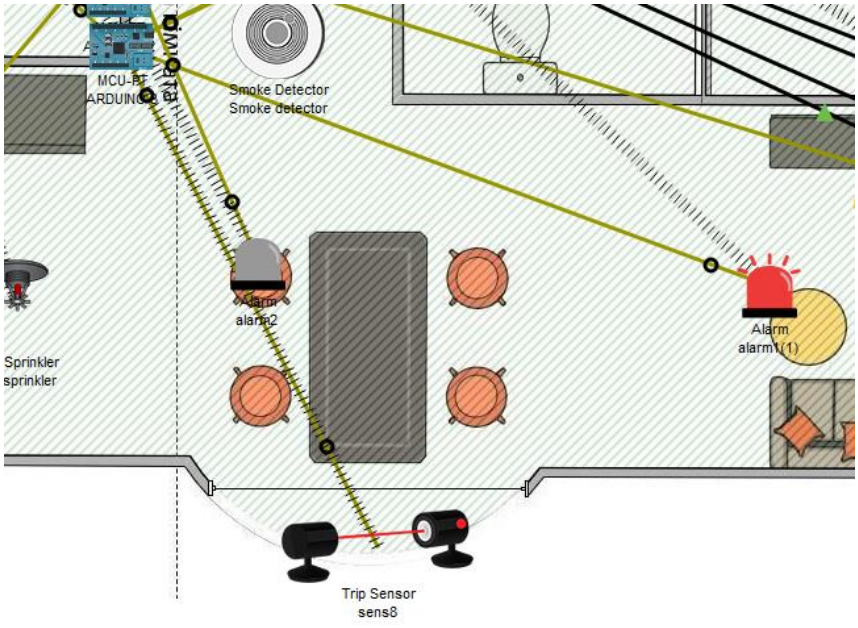


Рисунок 3.2 Тестування системи сигналізації

Результати показали, що після активації інфрачервоного датчика руху сигналізація спрацьовує практично миттєво. Така швидка реакція є ключовою характеристикою якісної охоронної системи, яка дозволяє забезпечити максимальний рівень захисту та швидкість сповіщення про небезпеку. Це також свідчить про стабільну інтеграцію всіх елементів, що дозволяє системі працювати безперебійно й відповідати вимогам користувача.

Підсумовуючи результати тестів першого, другого та третього секторів, можна з упевненістю стверджувати, що система повністю виконує свій функціонал і відповідає усім вимогам до сучасних систем безпеки. Кожен компонент, починаючи від датчиків руху та закінчуючи системою сигналізації, працює злагоджено, забезпечуючи високу ефективність і надійність системи в цілому. Такий результат дає впевненість у тому, що система відповідає сучасним стандартам безпеки й здатна виконувати свої завдання в реальних умовах.

Наступним етапом нашого дослідження стало тестування системи пожежної охорони. Для цього була проведена симуляція пожежі в контрольованому приміщенні з використанням вихлопних газів автомобіля. Результати цього тестування детально представлені на рисунку 3.3 та 3.4.

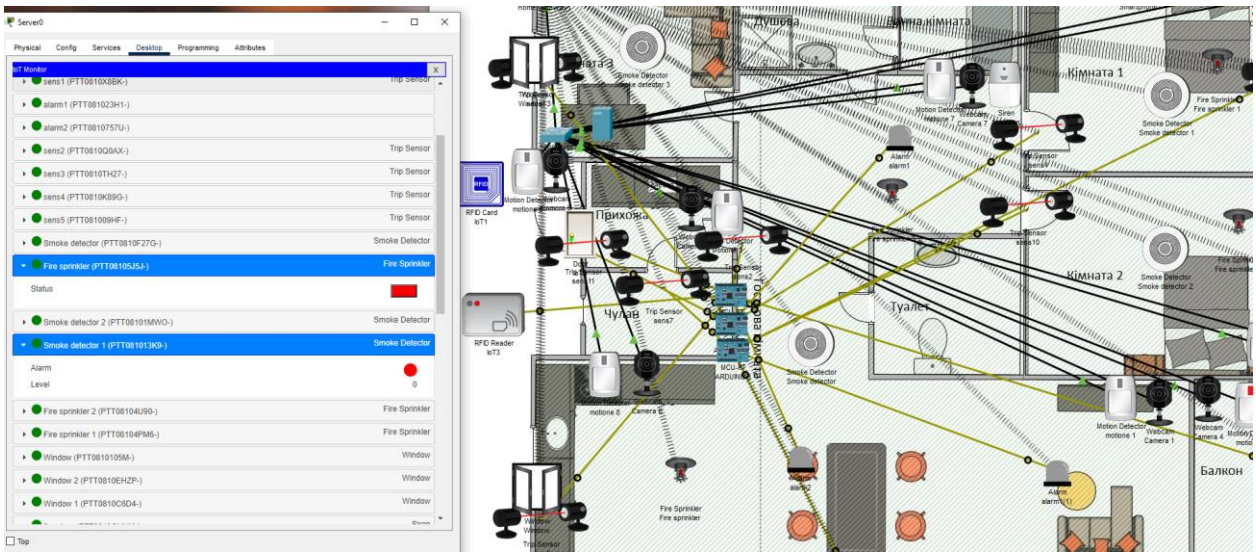


Рисунок 3.3 - Тестування системи пожежної безпеки до спрацювання

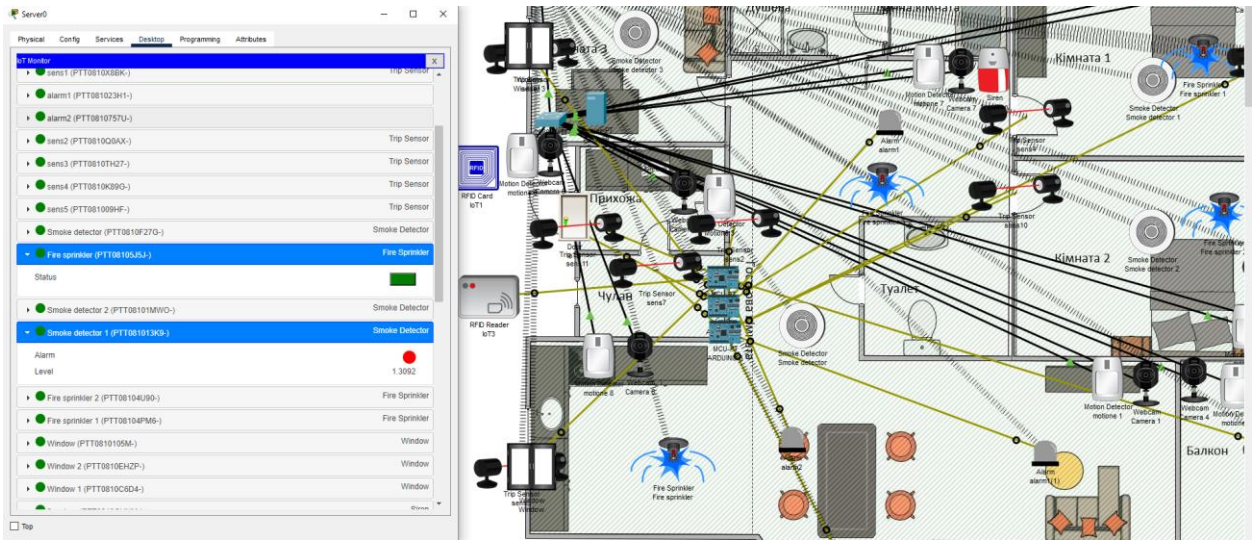


Рисунок 3.4 - Тестування системи пожежної безпеки після спрацювання

Аналізуючи результати тесту, можна відзначити, що одразу після появи джерела диму датчики спрацювали, активуючи спринклери. Це запобігло подальшому поширенню вогню. У відповідь на цю небезпечну ситуацію всі розумні сервоприводи, встановлені на вікнах, закрились. Це було зроблено для того, щоб уникнути проникнення свіжого повітря в приміщення, яке могло б підтримати горіння.

Коли джерело диму буде успішно нейтралізовано, система автоматично вимикається і переходить у режим очікування. Важливо зазначити, що сигналізація залишається увімкненою, і її можна вимкнути лише в ручному режимі. Це зроблено для привернення уваги оточуючих, адже доступ спринклерів до води може бути нестабільним, і існує ймовірність повторної пожежі. Крім того, власник отримує сповіщення про спрацювання датчика як на свій мобільний телефон, так і на сервер, що підкреслює важливість своєчасної реакції в таких критичних ситуаціях.

Останнім етапом тестування системи стало оцінювання роботи сегмента з камерами відеоспостереження, яке ілюструється на рисунку 3.5. У процесі тестування було виявлено, що як тільки датчик руху фіксує активність, камера автоматично вмикається і починає записувати відео. Це особливо корисно для

забезпечення безпеки в різних умовах, адже дає змогу оперативно реагувати на потенційні загрози.

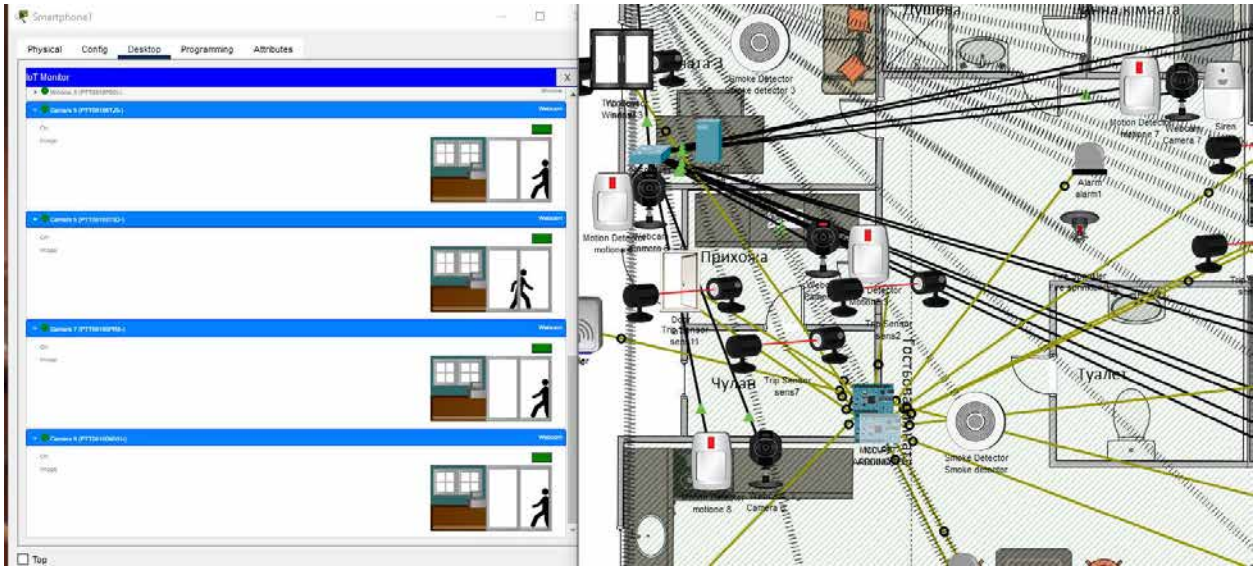


Рисунок 3.5 - Тестування системи камер відеоспостереження

Крім того, важливим аспектом є те, що після завершення спостереження - коли джерело руху більше не зафіксоване - камера вимикається з невеликою затримкою. Ця функція не лише зберігає електроенергію, але й оптимізує використання сховища, адже записи ведуться лише в момент активності. Таке рішення суттєво підвищує ефективність системи спостереження, дозволяючи користувачам зосередитися на важливих моментах і зменшуючи ризик перевантаження інформації. У цілому, цей сегмент відіграє ключову роль у забезпеченні надійності та функціональності всієї системи відеоспостереження.

На завершальному етапі тестування було проведено стрес-тест для оцінки відмовостійкості всієї системи безпеки. Метою цього тестування було перевірити, як система впорається з одночасною активацією кількох ключових компонентів, що забезпечують безпеку об'єкта. Даний стрес тест зображено на рисунку 3.6

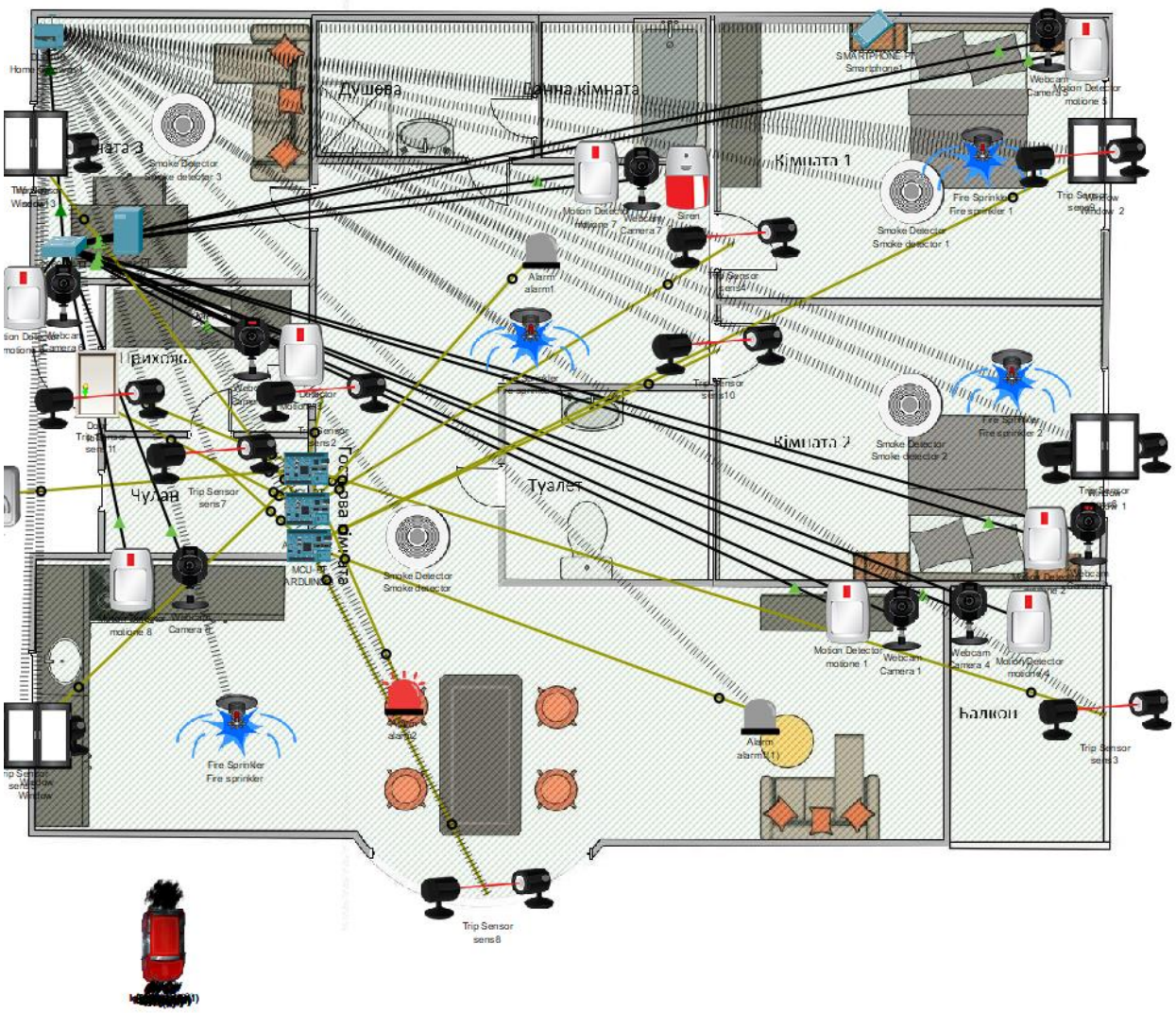


Рисунок 3.6 – Стрес тестування системи

Було активовано систему відеоспостереження, включаючи камери та датчики руху. Це дозволило оцінити їхню здатність оперативно реагувати на події: при фіксації руху камери автоматично вмикалися і починали запис, забезпечуючи візуальний моніторинг ситуації.

Крім того, була активована пожежна безпека, включаючи пожежну тривогу, спринклери та датчики диму. Цей етап тестування дав змогу перевірити, як система реагує на виявлення диму або тепла, а також оцінити швидкість активації спринклерів у разі виявлення пожежі. Така інтеграція є критично важливою для миттєвого реагування на надзвичайні ситуації та захисту життя і майна.

Додатково, для перевірки захисту території була активована система порушення периметру, яка включала сигналізацію та інфрачервоні датчики на базі Arduino. Ця система дозволяє своєчасно виявляти будь-які спроби несанкціонованого доступу, активуючи сигналізацію при фіксації порушень.

Під час стрес-тесту проводився моніторинг роботи всіх систем, що дало змогу оцінити їхню здатність функціонувати паралельно без збоїв. Важливо було перевірити, як взаємодіють різні елементи системи, чи не виникають конфлікти в їхній роботі, і чи забезпечується надійне реагування на різні загрози. Результати цього тестування підтвердили стійкість системи до стресових умов і виявили можливі слабкі місця, які потребують вдосконалення для подальшого підвищення загального рівня безпеки.

Завдяки цим комплексним перевіркам була забезпечена впевненість у тому, що система готова до будь-яких надзвичайних ситуацій і здатна ефективно захищати об'єкт

3.3 Аналіз ефективності системи

Завдяки цим комплексним перевіркам була забезпечена впевненість у тому, що система готова до будь-яких надзвичайних ситуацій і здатна ефективно захищати об'єкт

В умовах зростаючої кількості загроз, зокрема ризиків несанкціонованого проникнення та пожежної небезпеки, подібні комплексні рішення є вкрай важливими для забезпечення як приватних, так і комерційних об'єктів. Дана система базується на інтеграції різних компонентів, здатних працювати синхронізовано, що дозволяє досягти максимальної ефективності та миттєвої реакції на будь-які потенційні загрози.

Центральним елементом системи є її модульна структура, яка забезпечує гнучкість, масштабованість і зручність адаптації під різні потреби. До її складу входять такі важливі компоненти, як плата Arduino, до якої підключені інфрачервоні датчики руху, сигналізація, RFID-зчитувач, магнітний замок, а також додаткові елементи - камери відеоспостереження, датчики диму, спринклери та розумні сервоприводи для вікон. Таке поєднання дає змогу

комплексно захищати об'єкт на всіх рівнях: контролювати периметр, реагувати на наявність руху та забезпечувати автоматичну протидію загрозам, зокрема пожежі.

Актуальність цієї системи полягає в здатності реагувати на виклики сучасної безпеки. На першому етапі тестування, що проводилося у середовищі Cisco Packet Tracer, було перевірено систему порушення периметру, яка показала високу ефективність у фіксації спроб несанкціонованого доступу. Завдяки інфрачервоним датчикам руху, які миттєво передають сигнал на плату Arduino, сигналізація активується без затримок, що є важливим критерієм для сучасних охоронних систем. Крім того, налаштування RFID-зчитувача та магнітного замка дозволяють точно контролювати доступ до приміщень, що забезпечує додатковий рівень безпеки.

Система сигналізації показала не лише швидку, а й надійну реакцію. За результатами тестування було підтверджено, що при виявленні руху інфрачервоним датчиком сигналізація активується негайно. Це вказує на високу якість взаємодії всіх компонентів та відсутність затримок у передачі сигналу, що є критичним для забезпечення своєчасного реагування на загрози. Така оперативність дає змогу створити додатковий захисний бар’єр, що значно ускладнює несанкціоноване проникнення та підвищує рівень безпеки для користувача.

Ще одним вагомим аспектом системи є її здатність до віддаленого керування за допомогою технології Tuya Smart. Завдяки цій функції користувач може отримувати повідомлення про стан системи, її активацію або тривоги на мобільний додаток, незалежно від свого місця перебування. Це не тільки забезпечує постійний контроль над безпекою об'єкта, але й надає можливість швидко реагувати на будь-які зміни у разі необхідності, що є важливою перевагою у сучасних умовах.

Система пожежної безпеки є ще одним надзвичайно важливим компонентом, який забезпечує додатковий захист у разі виникнення пожежонебезпечних ситуацій. Під час тестування цієї частини було проведено

симуляцію появи диму за допомогою вихлопних газів автомобіля. У результаті тестування датчики диму оперативно виявили дим, активувавши спринклери, що почали подавати воду для гасіння потенційного вогню. Крім того, сервоприводи на вікнах автоматично закрили вікна, запобігаючи надходженню свіжого повітря, яке могло б підживлювати вогонь. Це рішення є критичним для безпеки, оскільки відсутність кисню уповільнює поширення пожежі, що дає час для гасіння або евакуації.

Додатковою перевагою є функція ручного вимкнення сигналізації лише після активації пожежної системи, що дає змогу привернути увагу оточуючих до можливого ризику, навіть після того, як пожежу було ліквідовано. Така логіка роботи особливо корисна, якщо доступ до води для спринклерів обмежений або існує можливість повторного загоряння. Також автоматичне надсилання сповіщень власнику на мобільний телефон і сервер дозволяє не тільки бути проінформованим, але й мати можливість віддалено контролювати ситуацію в будь-який момент.

Підсумовуючи всі результати тестування і функціональні можливості системи, можна зробити висновок, що вона повністю відповідає сучасним вимогам до охоронних систем і забезпечує комплексний підхід до безпеки об’єкта. Надійність і функціональність кожного компонента, інтеграція з мобільними додатками та висока чутливість до змін у навколишньому середовищі гарантують, що ця система буде затребуваною для різних типів користувачів. Здатність до автоматизованої роботи і віддаленого контролю робить її оптимальним вибором для забезпечення захисту житлових та комерційних об'єктів.

Таким чином, система демонструє комплексний і сучасний підхід до охорони, який базується на новітніх технологіях і ефективній інтеграції обладнання, що забезпечує не лише захист від несанкціонованого проникнення, а й пожежну безпеку. Така система не тільки задовольняє потреби користувачів, але й створює новий стандарт безпеки, що відповідає усім вимогам до надійності та швидкості реагування.

3.4 Економічні розрахунки та висновки

Аналіз побудови системи охорони, що складається з компонентів шлюз Zigbee 3.0 Livolo, комутатор TP-Link TL-SF1024D, камера Hikvision DS-2CE56H0T-IRMMF, ІЧ-датчик руху HC-SR505, розумний сервопривід XYDHB12, плата Arduino UNO R3 (CH340), датчик диму CoVi Security HM-200, контролер для клапанів води Aqara Smart Valve Controller T1 та RFID модуль MFRC522, дозволяє порівняти її з готовими охоронними рішеннями, такими як Ajax та Satel. Для детальної оцінки доцільності було розглянуто ціни, складність встановлення та функціональні можливості всіх трьох систем.

Вартість компонентів для системи на основі Zigbee та Arduino

Загальна вартість побудови системи з компонентами на базі Zigbee та Arduino є досить конкурентоспроможною та може бути налаштована відповідно до конкретних потреб об’єкта. Основний шлюз Zigbee 3.0 Livolo забезпечує централізоване управління системою, що легко розширюється за рахунок компонентів, які підтримують Zigbee-протокол.

Приблизна вартість окремих компонентів системи:

- Zigbee 3.0 шлюз Livolo - 1 200 грн
- Комутатор TP-Link TL-SF1024D - 2 500 грн
- Камера Hikvision DS-2CE56H0T-IRMMF - 3 000 грн
- ІЧ-датчик руху HC-SR505 (5 шт.) - по 200 грн, разом 1 000 грн
- Розумний сервопривід XYDHB12 (2 шт.) - по 1 500 грн, разом 3 000 грн
- Arduino UNO R3 (CH340) - 500 грн
- Датчик диму CoVi Security HM-200 - 1 500 грн
- Контролер клапанів Aqara Smart Valve Controller T1 - 2 000 грн
- RFID модуль MFRC522 - 300 грн

Таким чином, загальна вартість обладнання становить приблизно 15 000–18 000 грн. Це робить систему на базі Zigbee та Arduino доступною в порівнянні з іншими готовими рішеннями.

Оцінка витрат на систему Ajax

Система Ajax є бездротовою і має вищу загальну вартість через закриту екосистему та необхідність придбання компонентів лише цього бренду. Вартість складових для повного захисту середнього приватного будинку виглядає так:

- Ajax StarterKit (хаб, датчик руху, датчик відкриття дверей, брелок) - 5 500–8 000 грн
- Датчики диму (2 шт.) - 1 500 грн за кожен, загалом 3 000 грн
- Зовнішня сирена - 2 500 грн
- Додаткові датчики руху (2 шт.) - 1 500 грн за датчик, разом 3 000 грн
- Датчики відкриття вікон (5 шт.) - 700 грн за датчик, загалом 3 500 грн
- Камери відеоспостереження (2 шт.) - 3 500 грн за камеру, загалом 7 000 грн
- Розумний контролер для електромережі - 2 000 грн

При самостійному встановленні витрати на монтаж мінімальні, однак послуги спеціалістів можуть коштувати приблизно 2 000 грн. Загальна вартість системи Ajax становить 26 000–28 500 грн, що є значно дорожчим варіантом порівняно з Zigbee-системою на базі Arduino.

Оцінка витрат на систему Satel

Satel - це дротова або комбінована система, яка є більш надійною та стабільною, але вимагає більш складного монтажу і професійного налаштування. Вартість компонентів для середнього приватного будинку:

- Центральний блок, дротові датчики руху, контролер доступу - 6 000–9 000 грн
- Датчики диму (2 шт.) - 1 200 грн за датчик, загалом 2 400 грн
- Зовнішня сирена - 2 000 грн
- Додаткові датчики руху (2 шт.) - 1 200 грн за датчик, разом 2 400 грн
- Датчики відкриття вікон (5 шт.) - 500 грн за датчик, загалом 2 500 грн

- Камери відеоспостереження (2 шт.) - 3 000 грн за камеру, загалом 6 000 грн
- Додатковий блок живлення та резервна батарея - 1 500 грн
- Плата розширення для додаткових датчиків - 2 500 грн
- Вартість монтажу Satel, враховуючи потребу в прокладці проводів і підключенні компонентів, становить близько 4 000 грн.

Загальна вартість системи Satel знаходиться в межах 28 000–30 800 грн, що, як і у випадку з Ajax, є вищим показником порівняно з системою на базі Zigbee та Arduino.

Складність встановлення створеної системи є прийнятною для користувачів з базовими технічними знаннями, що дозволяє проводити монтаж самостійно. Плата Arduino потребує мінімальних навичок програмування, однак надає широкі можливості для кастомізації. Інші компоненти, такі як камера Hikvision та датчики, легко інтегруються в загальну систему через Zigbee-шлюз, що спрощує процес налаштування. У порівнянні, встановлення системи Ajax простіше завдяки бездротовій архітектурі та інтуїтивно зрозумілому мобільному додатку, тоді як Satel вимагає професійного монтажу через переважно дротову архітектуру, що збільшує витрати на обслуговування і налаштування.

Актуальність і перспектива даної системи зумовлені можливістю легкої інтеграції з розумними пристроями через Zigbee та підтримкою сучасних платформ автоматизації, таких як Tuya або Google Home. Це забезпечує додаткові функції, як-от дистанційне керування та моніторинг, а також розширення системи новими елементами. Здатність оновлювати та розширювати систему робить її інвестиційно привабливою у довготривалій перспективі, оскільки можна інтегрувати нові технології без потреби в повній модернізації.

Отже, побудова системи на основі таких компонентів є виправданим рішенням як з точки зору вартості, так і з погляду функціональності. Вона

забезпечує високий рівень безпеки, простоту в налаштуванні та обслуговуванні, а також можливість створення індивідуальних сценаріїв роботи, що підходить для середніх і великих об’єктів. Ця система відповідає сучасним стандартам безпеки і є перспективною платформою для забезпечення комплексного захисту об’єктів різного призначення.

3.5 Висновки до розділу

У цьому розділі було здійснено комплексну оцінку ефективності системи реалізованої для захисту будинку. Процес оцінки складався з кількох ключових етапів, включаючи методи тестування, результати, аналіз ефективності та економічні розрахунки.

На етапі тестування було застосовано різноманітні методи, які дозволили об'єктивно оцінити функціональність системи в реальних умовах. Основні акценти були зроблені на тестуванні чутливості датчиків, швидкості реагування сигналізації та ефективності системи відеонагляду. Всі методи тестування сприяли виявленню як сильних, так і слабких сторін системи, що є важливим для її подальшого вдосконалення.

Результати тестування показали, що система демонструє високий рівень надійності та швидкості реагування на потенційні загрози. Усі компоненти - від системи сигналізації до відеонагляду - функціонують синергічно, забезпечуючи цілісну та ефективну систему охорони. Однак, виявлені незначні недоліки були враховані і стали основою для рекомендацій щодо подальшого поліпшення.

Аналіз ефективності системи підтвердив її здатність до своєчасного виявлення загроз і швидкої реакції на них. Оцінка показників, таких як час сповіщення, відсоток успішних спроб виявлення загроз та рівень помилок, засвідчила, що система відповідає сучасним вимогам безпеки.

Крім того, економічні розрахунки продемонстрували, що інвестиції в розробку та впровадження системи є виправданими. Проведений аналіз витрат і вигод вказує на високий потенціал рентабельності та доцільність використання даної системи для забезпечення безпеки житла.

Таким чином, результати оцінки ефективності та тестування системи підтверджують її готовність до реального застосування. Вона не лише відповідає вимогам сучасного захисту, а й демонструє високі показники ефективності, що робить її цінним інструментом для забезпечення безпеки будинку. Подальші вдосконалення системи, виходячи з отриманих результатів, сприятимуть підвищенню її ефективності та надійності в умовах змінного середовища.

ВИСНОВКИ

У рамках даної магістерської роботи було проведено комплексне дослідження, присвячене розробці комп'ютерної системи управління комунікаціями з використанням інтелектуальних алгоритмів. Дослідження почалося з визначення актуальності теми, яка стала особливо важливою в умовах швидкого розвитку технологій і потреби в автоматизації різних аспектів життєдіяльності людини. У роботі було сформульовано мету і завдання дослідження, об'єктом якого стали системи управління комунікаціями, а предметом — інтелектуальні алгоритми, що забезпечують їх функціонування.

Згідно з методологією дослідження, був проведений огляд літератури, який дозволив виявити сучасні тенденції в розробці систем розумного дому. Особливу увагу було приділено аналізу інтелектуальних алгоритмів, які здатні покращити управління комунікаціями, а також вивченню існуючих рішень у сфері сигналізації. Це дало змогу зрозуміти сучасні підходи до проектування таких систем і їх інтеграції у повсякденне життя.

Теоретичні основи розробки комп'ютерних систем були представлені через призму системного підходу, архітектури комп'ютерних систем і принципів роботи інтелектуальних алгоритмів. Було обґрунтовано вибір технологій і інструментів для реалізації проекту, що стало основою для подальшого проектування системи управління комунікаціями. Вимоги до системи, функціональна схема та методи інтеграції компонентів системи дозволили створити чітку структуру, яка відповідає сучасним стандартам і потребам користувачів.

У процесі розробки інтелектуальних алгоритмів були описані їх функції та можливості. Зокрема, алгоритми обробки даних та прийняття рішень, які забезпечують ефективність управління комунікаціями, інтегрувалися в загальну структуру системи. Це дало можливість оптимізувати процеси та підвищити їх продуктивність.

Реалізація системи включала в себе опис програмного забезпечення, вибір апаратного забезпечення та інтеграцію всіх компонентів у єдину систему. Цей етап був критично важливим для забезпечення коректної роботи всіх елементів системи, що в свою чергу відобразилося на результатах тестування.

Тестування та оцінка ефективності системи стали завершальним етапом дослідження. Було застосовано різноманітні методи тестування, результати яких підтвердили високу ефективність та надійність розробленої системи. Аналіз показників ефективності системи засвідчив, що вона відповідає заявленим вимогам і має значний потенціал для подальшого вдосконалення.

У висновках даної роботи були підведені основні результати дослідження. Система управління комунікаціями з використанням інтелектуальних алгоритмів показала свою готовність до реального застосування в умовах сучасного життя. Відзначено також, що для подальшого розвитку системи слід врахувати рекомендації, спрямовані на оптимізацію алгоритмів, підвищення інтеграції з іншими системами, а також розширення функціональних можливостей.

Перспективи розвитку системи охоплюють не лише її удосконалення, а й адаптацію до нових технологій та інновацій, що з'являються на ринку. Таким чином, результати даної магістерської роботи можуть стати основою для подальших досліджень у сфері автоматизації та управління комунікаціями, а також для створення нових, більш досконалих систем, які відповідатимуть вимогам часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Встановлення системи захисту Ajax в трикімнатній квартирі [Електронний ресурс] // Ajax. – 2011. – Режим доступу до ресурсу: https://alarm.bezpeka.systems/ua/portfolio/ustanovka-sistemy-zashhity-ajax-v-trehkomnatnoj-kvartire/.

2. 7 Key Components in Security Architecture to Protect Company Assets [Електронний ресурс] // Rogue logics. – 2023. – Режим доступу до ресурсу: https://www.roguelogics.com/7-key-components-in-security-architecture-to-protect-company-assets/

3. Analysing Smart Home Security Using Packet Tracer Simulation Software [Електронний ресурс] // IEEE Xplore logo - Link to home. – 2023. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/9431781.

4. Комплект сигналізації Ajax StarterKit Cam Plus White [Електронний ресурс] // Ohrana ua. – 2014. – Режим доступу до ресурсу: https://ohrana.ua/komplekt-signalizatsii-ajax-starterkit-cam-plus-beliy.html.

5. Рябчун Ю. В. Управління розвитком складних систем [Електронний ресурс] / Ю. В. Рябчун, Д. Е. Середа, В. Р. Кохан // МОЖЛИВОСТІ ТА ПЕРЕВАГИ УКРАЇНСЬКОГО РИНКУ ТЕХНОЛОГІЙ «РОЗУМНИЙ БУДИНОК». – 2019. – Режим доступу до ресурсу: file:///D:/Загрузки/299962-Текст%20статті-692307-1-10-20240315.pdf.

6. Joseph J. Types of Arduino Boards – Quick Comparison on Specification and Features [Електронний ресурс] / Jobit Joseph // circut digest. – 2022. – Режим доступу до ресурсу: https://circuitdigest.com/article/different-types-of-arduino-boards.

7. ФРИЗ М. Р. Інтернет речей та смарт технології [Електронний ресурс] / МАРІАННА РОМАНІВНА ФРИЗ. – 2024. – Режим доступу до ресурсу: https://sites.google.com/view/bezpecnyj-internet/можливості-інтернету/інтернет-речей-та-смарт-технології.

8. Савицький Т. Використання штучного інтелекту для системи розумного будинку [Електронний ресурс] / Т. Савицький, М. Орлова // reasearchGate. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/342064185_Vikoristanna_stucnogo_intelektu_dla_sistemi_rozumnogo_budinku.

9. Програмування електронних систем обробки даних [Електронний ресурс] // МІХ.СумДУ. – 2021. – Режим доступу до ресурсу: https://mix.sumdu.edu.ua/textbooks/36685/1104879/index.html.

10. . Simar S. A Comprehensive Review of Smart Home Automation Systems July 2023 [Електронний ресурс] / S. Simar, A. Sourabh // ResearchGate. – 2023. – Режим доступу до ресурсу: https://www.researchgate.net/publication/372406470_A_Comprehensive_Review_of_Smart_Home_Automation_Systems.

11. Контроллер бездротовоїі системи Satel ABAX 2 ACU-220 [Електронний ресурс] // Ohrana ua. – 2014. – Режим доступу до ресурсу: https://ohrana.ua/kontroller-besprovodnoy-sistemi-satel-abax-2-acu-220.html.

12. How Data Analysis can be used for Smart Home Automation [Електронний ресурс] // articulecube. – 2024. – Режим доступу до ресурсу: https://www.articlecube.com/how-data-analysis-can-be-used-smart-home-automation.

13. Розумна централь Ajax Hub біла [Електронний ресурс] // Ajax. – 2023. – Режим доступу до ресурсу: https://sheriff.promo/tproduct/1-780262643301-rozumna-tsentral-ajax-hub-bla.

14. 3Dyi [Електронний ресурс] // GSM-сигнализация на Arduino. – 2023. – Режим доступу до ресурсу: https://3d-diy.ru/wiki/projects/gsm-signalizatsiya-na-arduino/.

15. КОМУТАТОР TP-LINK TL-SF1024D [Електронний ресурс] // Secur. – 2023. – Режим доступу до ресурсу: http://surl.li/hgcrq

16. What Is a Security System and How Does it Work? [Електронний ресурс] // SafeWise. – 2023. – Режим доступу до ресурсу: https://www.safewise.com/home-security-faq/how-do-security-systems-work/.

17. Smart home technology saves money and helps protect the planet [Електронний ресурс] // IoTNOW. – 2024. – Режим доступу до ресурсу: https://www.iot-now.com/2024/04/22/144080-smart-home-technology-saves-money-and-helps-protect-the-planet/.

18. What Is A Home Security System and How Does It Work? [Електронний ресурс] // security.org. – 2023. – Режим доступу до ресурсу: https://www.security.org/home-security-systems/what-is-a-home-security-system/.

19. Kingston U. SMART HOME USING CISCO PACKET TRACER [Електронний ресурс] / University Kingston // studocu. – 2021. – Режим доступу до ресурсу: https://www.studocu.com/en-gb/document/kingston-university/network-security/smart-home-using-cisco-packet-tracer/14467719.

20. Які є види сигналізацій та їх принцип роботи [Електронний ресурс] // Gaziknet. – 2023. – Режим доступу до ресурсу: https://www.gazik.com.ua/avtomatychni-vorota.html.

21. Мережеве обладнання [Електронний ресурс] // Comtrade. – 2023. – Режим доступу до ресурсу: http://surl.li/hgcrg.

22. Intelligent Communication System [Електронний ресурс] // SilentDirect. – 2018. – Режим доступу до ресурсу: https://www.sciencedirect.com/topics/engineering/intelligent-communication-system.

23. Кеньо Г. В. Моделювання розумного будинку в середовищі Cisco Packet Tracer / Г. В. Кеньо, В. В. Хома. – Львів: Львівська політехніка, 2022. – 104 с.

24. Vaishnavi S. G. Smart Home Automation: A Literature Review [Електронний ресурс] / S. G. Vaishnavi, S. Y. Pratibha // International Journal of Computer Applications. – 2016. – Режим доступу до ресурсу: https://research.ijcaonline.org/rtdm2016/number1/rtdm2568.pdf.

25. Гнедюк В. Л. ТЕНДЕНЦІЇ РОЗВИТКУ ТЕХНОЛОГІЙ РОЗУМНИХ БУДИНКІВ І ЇХ ВИКОРИСТАННЯ ЛЮДЬМИ З ОБМЕЖЕНИМИ МОЖЛИВОСТЯМИ В СУЧАСНОМУ СОЦІУМІ [Електронний ресурс] / В. Л. Гнедюк // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2023. – Режим доступу до ресурсу: 25.

26. Ланде Д. В. ОСНОВИ ТЕОРІЇ І ПРАКТИКИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У СФЕРІ КІБЕРБЕЗПЕКИ [Електронний ресурс] / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова. – 2018. – Режим доступу до ресурсу: https://ela.kpi.ua/server/api/core/bitstreams/5eb4cb50-3ef0-44d1-b35f-a80eade1554b/content.

27. Оксентюк Р. А. УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ЗВ'ЯЗКАМИ [Електронний ресурс] / Р. А. Оксентюк. – 2016. – Режим доступу до ресурсу: https://elartu.tntu.edu.ua/bitstream/lib/21268/1/Конспект%20лекцій.pdf.

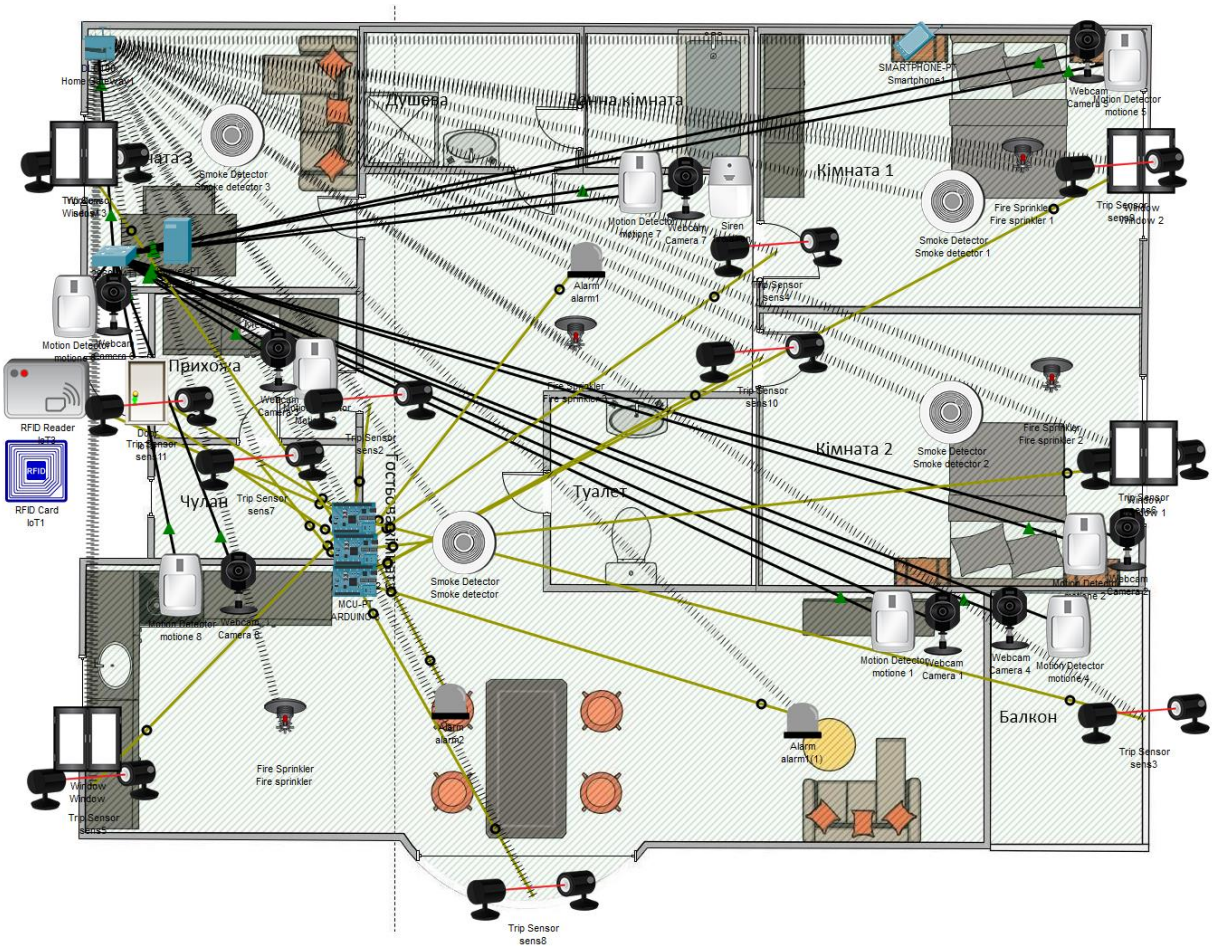
28. Аврунін О. ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ АВТОМАТИЗАЦІЇ [Електронний ресурс] / О. Аврунін, С. Владов, М. Петченко. – 2016. – Режим доступу до ресурсу: https://openarchive.nure.ua/server/api/core/bitstreams/d7217c7f-e0c7-4dc8-9076-eb3f2c445191/content.

29. Ринок «розумного будинку» в Україні: комфорт і безпека коштує своїх грошей [Електронний ресурс] // Pro consalting. – 2023. – Режим доступу до ресурсу: https://pro-consulting.ua/ua/pressroom/rynok-umnogo-doma-v-ukraine-komfort-i-bezopasnost-stoit-svoih-deneg.

30. Контроллер бездротовоїі системи U-Prox ABAX 2 ACU-220 [Електронний ресурс] // Ohrana ua. – 2014. – Режим доступу до ресурсу: https://ohrana.ua/komplekti-signalizacij/pultovaya-ohrana/maks-pro-wifi-komplekt.html

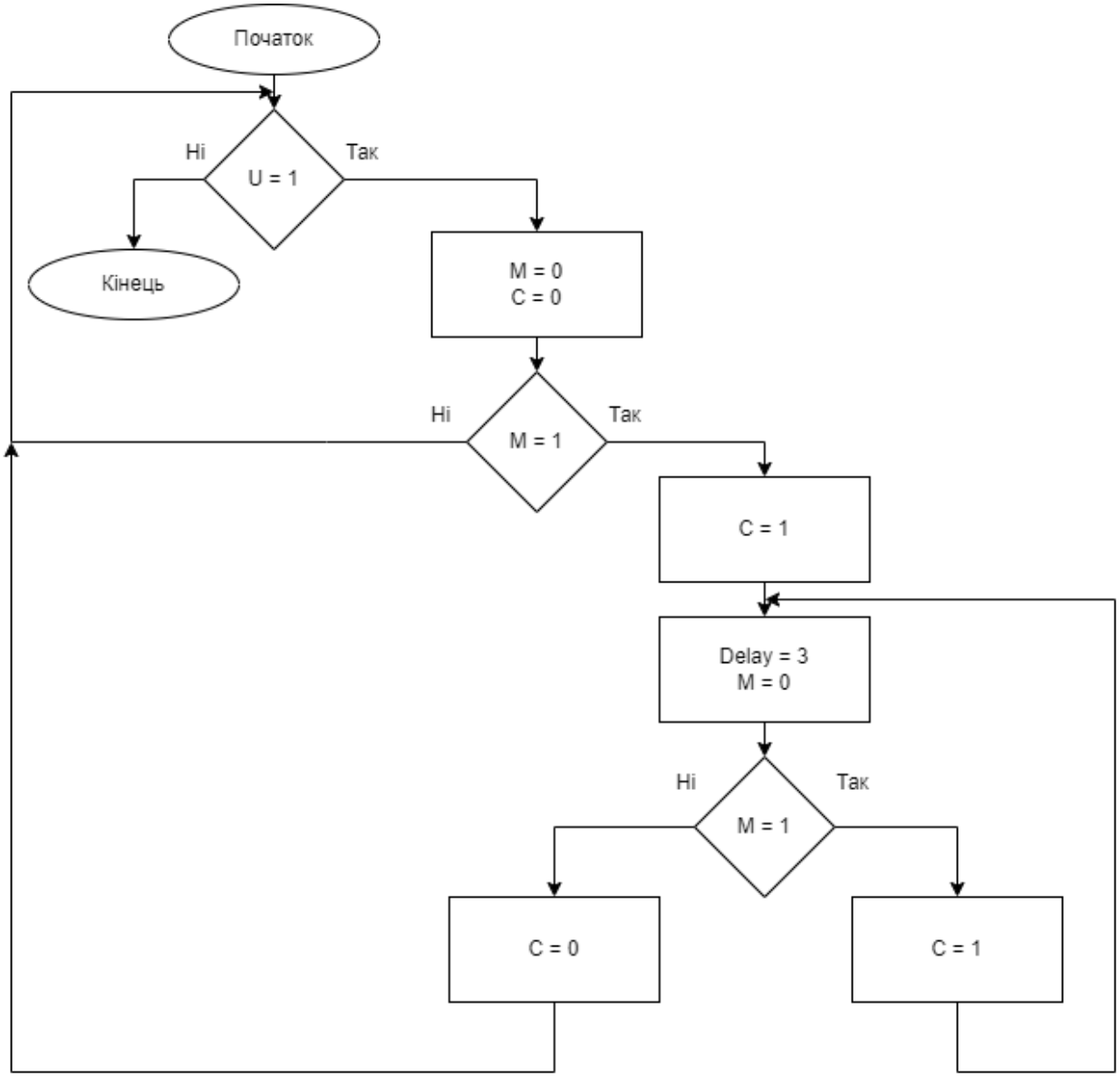
ДОДАТОК А

Схема системи



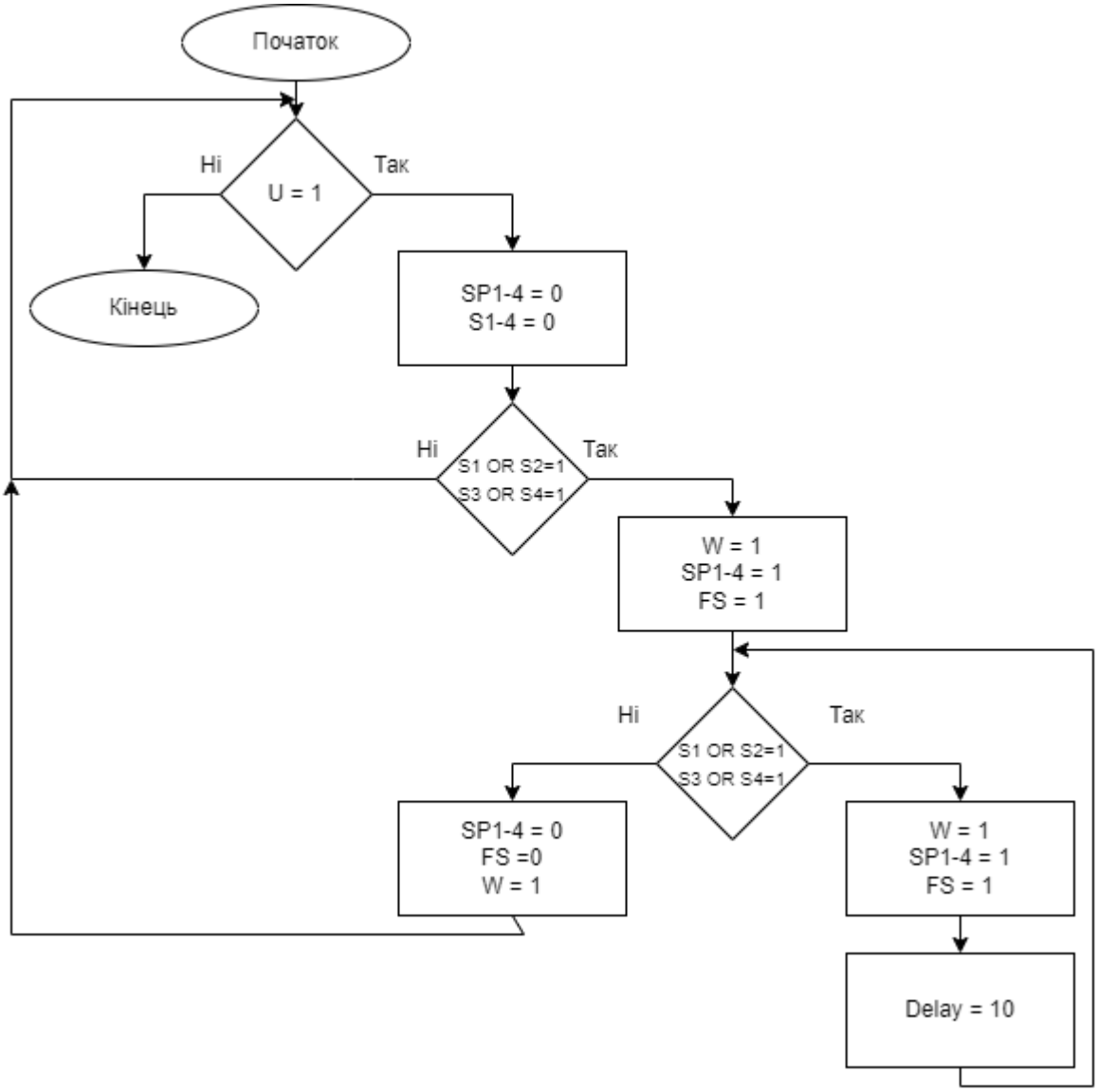
ДОДАТОК Б

Блок схема роботи системи відеоспостереження



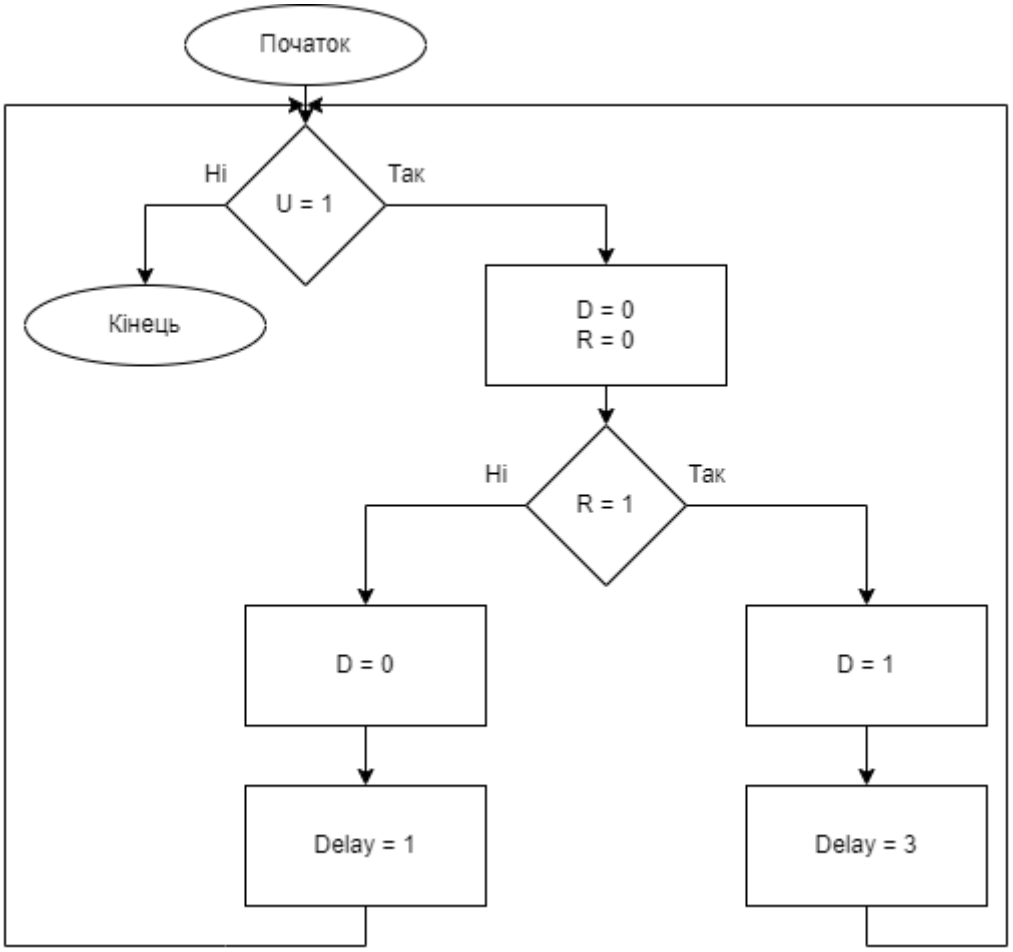
ДОДАТОК В

Блок схема роботи системи пожежної безпеки



ДОДАТОК Г

Блок схема роботи системи карткового доступу



ДОДАТОК Д

Блок схема роботи системи сигналізації