Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Комп'ютеризована система відеомоніторингу вхідної зони приміщення на основі IoT-технологій*

Виконав: студент *4* курсу, групи *СІ-41*
спеціальності *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

		Бойко П.П.
	(підпис)	(прізвище та ініціали)
Керівник		*Стадник Н.Б.*
	(підпис)	(прізвище та ініціали)
Нормоконтроль		*Луцик Н.С.*
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		*Осухівська Г.М.*
	(підпис)	(прізвище та ініціали)
Рецензент		*Литвиненко Я.В.*
	(підпис)	(прізвище та ініціали)

Тернопіль
2026

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
«24» квітня 2026 р

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Бойку Павлу Павловичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Комп'ютеризована система відеомоніторингу вхідної зони приміщення на основі IoT-технологій*

Керівник роботи *Стадник Наталія Богданівна, к.т.н.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від *«24» квітня 2026 року № 4/9-188*
2. Термін подання студентом завершеної роботи *15.06.2026 р.*
3. Вихідні дані до роботи *Технічне завдання*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Аналіз технічного завдання
2. Проєктна частина
3. Практична частина
4. Безпека життєдіяльності, основи охорона праці
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Структурна схема системи
2. Схема електрична принципова
3. Блок-схема алгоритму роботи
4. Результати моделювання системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорона праці	*доц. каф. МТ Сенчишин В.С.*		

7. Дата видачі завдання *24.04.2026 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Розробка технічного завдання*	*26.01 – 02.02*	
2.	*Аналіз технічного завдання, вимог до комп'ютеризованої системи, та можливих рішень поставленого завдання*	*03.02 – 15.02*	
3.	*Розроблення структури, вибір апаратного забезпечення, проєктування комп'ютеризованої системи*	*20.04 – 25.04*	
4.	*Реалізація алгоритму, написання програмного забезпечення, моделювання комп'ютеризованої системи*	*26.04 – 05.05*	
5.	*Робота над четвертим розділом «Безпека життєдіяльності, основи охорони праці»*	*07.05 – 25.05*	
6.	*Оформлення пояснювальної записки та графічного матеріалу*	*26.05 – 07.06*	
7.	*Перевірка на академічний плагіат, перевірка керівником та консультантами*	*08.06 – 14.06*	
8.	*Попередній захист кваліфікаційної роботи бакалавра*	*15.06 – 21.06*	
9.	*Захист кваліфікаційної роботи бакалавра*	*22.06.2026*	

Студент _____ *Бойко П.П.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Стадник Н.Б.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Бойко П.П. Комп’ютеризована система відеомоніторингу вхідної зони приміщення на основі IoT-технологій : робота на здобуття освітнього ступеня бакалавра: спец. 123 — комп’ютерна інженерія. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2026.

Ключові слова: комп’ютеризована система, контроль доступу, відеофіксація подій, IoT-технології, мікроконтролер.

Кваліфікаційна робота присвячена розробці комп’ютеризованої системи відеомоніторингу вхідної зони приміщення на основі IoT-технологій. Метою роботи є створення ефективної апаратно-програмної системи, яка забезпечує підвищення рівня безпеки об’єктів за рахунок автоматизації процесів контролю доступу та віддаленого моніторингу подій.

У першому розділі проаналізовано технічне завдання на проєктування системи, сформульовано основні функціональні вимоги до її роботи, а також проведено огляд і порівняльний аналіз існуючих аналогів систем відеомоніторингу вхідної зони приміщення, що використовують IoT-технології. Це дозволило визначити їх переваги, недоліки та обґрунтувати доцільність розробки власного рішення.

Другий розділ присвячено проєктуванню апаратного забезпечення системи. Розроблено структурну схему та електричну принципову схему пристрою, а також обґрунтовано вибір елементної бази з урахуванням функціональних можливостей, енергоспоживання та вартості компонентів.

У третьому розділі розроблено алгоритм роботи системи та програмне забезпечення для мікроконтролера. Виконано інтеграцію системи з IoT-платформою для віддаленого контролю та моніторингу, а також проведено тестування розробленого рішення з метою перевірки його працездатності та відповідності заданим вимогам.

ANNOTATION

Boiko P.P. Computerized Video Monitoring System for a Building Entrance Area Based on IoT Technologies. Bachelor's Graduation Thesis: speciality 123 — Computer engineering. Ternopil: Ternopil Ivan Puluj National Technical University, 2026.

Keywords: computerized system, access control, video event recording, IoT technologies, microcontroller.

The qualification work is devoted to the development of a computerized video monitoring system for a building entrance area based on IoT technologies. The aim of the work is to design an effective hardware and software solution that improves the level of security by automating access control processes and enabling remote monitoring of events.

The first chapter analyzes the technical specifications for the system design, outlines the main functional requirements for its operation, and provides a review and comparative analysis of existing video surveillance systems for building entry areas that utilize IoT technologies. This made it possible to identify their advantages and disadvantages and justify the feasibility of developing a proprietary solution.

The second section focuses on the design of the hardware part of the system. A structural diagram and an electrical schematic diagram are developed, and the choice of the element base is substantiated considering functionality, power consumption, and cost.

The third section presents the development of the system operation algorithm and the microcontroller software. Integration with an IoT platform for remote monitoring and control is implemented, and testing of the developed system is performed to verify its operability and compliance with the specified requirements.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

API – Application Programming Interface

IoT – Internet of Things

IP – Internet Protocol

RFID – Radio Frequency Identification

SPI – Serial Peripheral Interface

TLS – Transport Layer Security

UART – Universal Asynchronous Receiver Transmitter

ГД – герконовий давач

ЕМЗ – електромагнітний замок

КДС – контроль доступу до системи

МК – мікроконтролер

МЗД – модуль зчитування даних

ПВЗ – підсистема відеозапису

СКД – система контролю доступу

СПД – система передачі даних

ВСТУП

У сучасних умовах зростання рівня урбанізації, цифровізації та автоматизації об’єктів інфраструктури питання забезпечення безпеки приміщень набуває особливої актуальності. Підвищення вимог до захисту житлових, офісних, навчальних і промислових об’єктів зумовлює необхідність використання ефективних систем відеомоніторингу, здатних не лише обмежувати несанкціонований вхід, а й забезпечувати фіксацію подій та віддалене керування об’єктом. Традиційні системи безпеки часто мають обмежену функціональність, високі витрати на впровадження або не забезпечують інтеграцію з сучасними мережевими сервісами.

Розвиток технологій Інтернету речей (IoT) відкриває нові можливості для створення гнучких, масштабованих та економічно доцільних систем відеомоніторингу вхідної зони приміщення і передавання даних у реальному часі. Використання мікроконтролерних платформ, бездротових мереж і хмарних IoT-платформ дозволяє реалізувати віддалене керування, збір та аналіз даних, а також підвищити рівень автоматизації та надійності систем безпеки. У зв’язку з цим задача розробки системи відеомоніторингу та контролю доступу до приміщення є актуальною та практично значущою.

Метою кваліфікаційної роботи є розробка та дослідження комп’ютеризованої системи відеомоніторингу вхідної зони приміщення на основі IoT-технологій, що забезпечує підвищення рівня безпеки та можливість віддаленого керування.

Для досягнення поставленої мети у кваліфікаційній роботі необхідно виконати такі задачі:

- проаналізувати технічне завдання та визначити основні вимоги до проєктованої системи;
- виконати огляд і порівняльний аналіз існуючих систем відеомоніторингу вхідної зони приміщення;
- розробити структурну схему комп’ютеризованої системи;

- спроєктувати електричну принципову схему апаратної частини системи;
- обґрунтувати вибір елементної бази та основних апаратних компонентів;
- розробити алгоритм роботи системи;
- створити програмне забезпечення для мікроконтролера;
- виконати інтеграцію системи з IoT-платформою для віддаленого моніторингу;
- провести тестування розробленої системи та оцінити її працездатність.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Огляд та аналіз сфер застосування системи відеомоніторингу вхідної зони приміщення

Сучасний етап розвитку інформаційних та комунікаційних технологій характеризується активним впровадженням комп'ютеризованих систем безпеки, що забезпечують автоматизований контроль доступу до об'єктів різного призначення. Зростання кількості інформаційних ресурсів, матеріальних цінностей та об'єктів інфраструктури, які потребують захисту, обумовлює підвищений інтерес до систем відеомоніторингу вхідної зони приміщення. Такі системи дозволяють значно підвищити рівень безпеки, зменшити вплив людського фактору та забезпечити оперативне реагування на несанкціоновані дії.

Однією з основних сфер застосування комп'ютеризованих систем відеомоніторингу є житловий сектор. У багатоквартирних будинках, приватних домоволодіннях та житлових комплексах подібні системи використовуються для обмеження доступу сторонніх людей, контролю входу до під'їздів, технічних приміщень і прибудинкових територій. Наявність функції відеофіксації дозволяє не лише ідентифікувати осіб, які здійснюють доступ, але й вести журнал подій, що підвищує рівень відповідальності користувачів та спрощує аналіз інцидентів.

Широке застосування комп'ютеризовані системи дистанційного відеомоніторингу знаходять в офісних і комерційних приміщеннях. Для підприємств, бізнес-центрів і адміністративних будівель важливим є розмежування доступу працівників і відвідувачів до різних зон об'єкта. Використання IoT-технологій у таких системах забезпечує централізоване керування, інтеграцію з корпоративними мережами та можливість віддаленого моніторингу стану безпеки. Відеофіксація подій у поєднанні з контролем

доступу дозволяє підвищити рівень захисту комерційної інформації та матеріальних ресурсів.

Не менш актуальною є сфера застосування подібних систем у навчальних закладах та установах соціальної інфраструктури. Школи, університети, лікарні та державні установи потребують підвищеного рівня контролю доступу з метою забезпечення безпеки персоналу та відвідувачів. Комп'ютеризовані системи з функцією відеофіксації дозволяють здійснювати контроль за переміщенням осіб, обмежувати доступ до службових приміщень та оперативно реагувати на надзвичайні ситуації.

У промисловій та складській сферах системи дистанційного контролю доступу використовуються для захисту виробничих зон, складів, серверних приміщень та інших об'єктів з обмеженим доступом. У таких умовах важливо забезпечити надійність, безперервність роботи та можливість інтеграції з іншими системами безпеки, зокрема системами охоронної сигналізації та відеоспостереження. Застосування IoT-технологій дозволяє реалізувати віддалений контроль стану обладнання та оперативно отримувати інформацію про події, що відбуваються на об'єкті.

Окрему увагу слід приділити використанню комп'ютеризованих систем відеомоніторингу вхідної зони приміщення в об'єктах критичної інфраструктури, таких як енергетичні підприємства, транспортні вузли та телекомунікаційні центри. Для таких об'єктів характерні підвищені вимоги до надійності, захищеності та масштабованості систем безпеки. Наявність відеофіксації подій та можливість віддаленого моніторингу дозволяють підвищити ефективність контролю та забезпечити швидке реагування на потенційні загрози.

Отже, комп'ютеризована система відеомоніторингу вхідної зони приміщення є універсальною та має практичну значущість. Поєднання засобів контролю доступу, відеофіксації та IoT-технологій забезпечує широкі можливості адаптації системи до різних умов експлуатації, що підтверджує доцільність її розробки та впровадження в межах даної кваліфікаційної роботи.

1.2 Аналіз вимог до системи відеомоніторингу вхідної зони приміщення

Коректне формулювання вимог забезпечує узгодженість між технічним завданням, архітектурою проєктованої системи та кінцевим функціональним результатом.

Передусім система повинна відповідати функціональним вимогам, які визначають її основне призначення. До таких вимог належить забезпечення контролю доступу до приміщення шляхом ідентифікації та авторизації користувачів, керування виконавчими механізмами доступу, а також відеофіксація подій біля входу та виходу. Важливою вимогою є ведення журналу подій із можливістю збереження та передавання інформації на віддалений сервер або IoT-платформу для подальшого аналізу.

Суттєве значення мають нефункціональні вимоги, серед яких ключовими є надійність, безпека та стабільність роботи системи. Система повинна забезпечувати безперервну роботу в умовах тривалої експлуатації, мати механізми захисту від збоїв та несанкціонованого доступу, а також гарантувати цілісність і конфіденційність переданих даних. У разі втрати зв’язку з мережею Інтернет система повинна зберігати базову функціональність на локальному рівні.

Вимоги до продуктивності системи визначають необхідність оперативної обробки подій у реальному часі. Затримки між моментом ідентифікації користувача, фіксацією події та керуванням доступом повинні бути мінімальними та не впливати на зручність користування системою. Відеофіксація подій має здійснюватися з достатньою якістю для ідентифікації осіб та аналізу ситуацій.

Важливим аспектом є вимоги до апаратного та ПЗ. Апаратна частина повинна базуватися на сучасних мікроконтролерних платформах, які забезпечують необхідну обчислювальну потужність, підтримку периферійних пристроїв та засобів зв’язку. Програмне забезпечення має бути модульним, масштабованим та зручним для подальшої модернізації, з можливістю оновлення без повної заміни системи.

Окремо слід виділити вимоги до інтеграції з IoT-платформою. Система повинна підтримувати надійний обмін даними з хмарним сервісом, забезпечувати віддалений моніторинг стану системи та керування її параметрами. Це дозволяє підвищити гнучкість використання системи та розширити функціональні можливості.

Проведений аналіз вимог до комп'ютеризованої системи дозволяє сформувати чітке уявлення про її функціональні та технічні характеристики, що є основою для подальшого проєктування апаратного та ПЗ в межах даної кваліфікаційної роботи.

1.3 Огляд існуючих засобів для відеомоніторингу вхідної зони приміщення

У світі сучасних технологій системи відеомоніторингу поєднують апаратні засоби, ПЗ та мережеві технології для забезпечення безпеки фізичних об'єктів та моніторингу подій, що відбуваються у контрольованих зонах. Існуючі рішення на ринку варіюються від простих автономних пристроїв до комплексних інтегрованих систем із розширеною аналітикою, відеоспостереженням та централізованим управлінням. Аналіз цих рішень демонструє як сильні сторони, так і суттєві обмеження, що мають значення для проєктування нової системи в межах даної кваліфікаційної роботи.

Серед популярних рішень на ринку – традиційні системи контролю доступу (СКД), що реалізують ідентифікацію користувачів на основі RFID-карток, кодових панелей, паролів або біометричних даних (рис. 1.1). Ці системи здебільшого забезпечують базову функціональність контролю доступу: розмежування прав, журнал подій, локальне зберігання даних та інтеграцію з охоронною сигналізацією [1]. Вони ефективні для невеликих об'єктів, де додаткові можливості системи (наприклад, аналітика відео) не є критичними. Однак у таких рішеннях часто відсутня вбудована функція відеофіксації подій, або ця функція реалізується окремо через систему відеоспостереження без тісної інтеграції з контрольно-

доступною частиною. Це означає, що відеодані та події контролю доступу не завжди пов’язані в єдине логічне ціле для автоматичного аналізу чи зберігання, що знижує ефективність розслідування інцидентів.

Рисунок 1.1 – Система контролю доступу на основі RFID-карток, кодових панелей та біометричних даних

Більш просунуті рішення пропонують комплексну інтеграцію контролю доступу з відеоспостереженням і аналітикою. Прикладом такого підходу є система ZKBio Access, яка інтегрує управління доступом із відеоаналізом, включає функції моніторингу у реальному часі, розпізнавання обличчя та побудови зв’язків між подіями контролю доступу і тригерами відеоаналітики (рис. 1.2). Така система дозволяє не лише записувати відео, а й реалізовувати інтелектуальну обробку подій (виявлення перетину зон, сповіщення про нез’ясовану активність тощо) та вести централізований контроль і налаштування доступу. Однак існують обмеження, пов’язані з її складністю, високою вартістю впровадження,

необхідністю значних обчислювальних ресурсів і складною інтеграцією з існуючою IT-інфраструктурою [2]. Для малих і середніх об’єктів це часто є недоцільним через складність адміністрування та витрати на обслуговування.

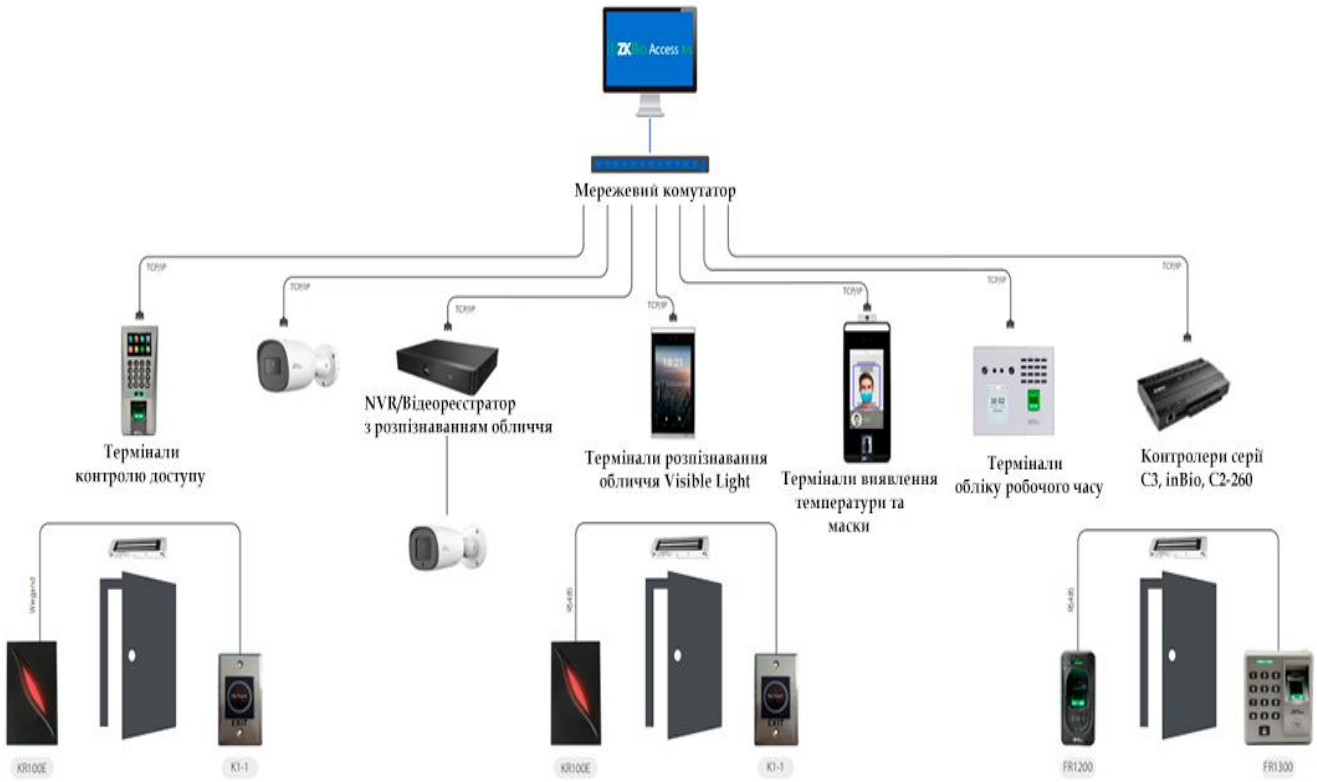

Рисунок 1.2 – Система контролю доступу з відеоспостереженням і аналітикою ZKBio Access

Виробники великого масштабу, наприклад Hikvision, пропонують широкий спектр засобів контролю доступу, що включають контролери, зчитувачі, програмне забезпечення і можливості зв’язку з системами відеоспостереження [3]. Такі комплекси дозволяють автоматизувати облік часу, формувати звіти та керувати доступом на основі заданих прав (рис. 1.3). Проте реалізація функції відеофіксації в таких системах часто покладається на інтеграцію з окремими системами відеоспостереження або реєстраторами, а не на вбудовану, повністю інтегровану архітектуру, яка забезпечує спільну обробку подій контролю доступу та відеоданих в одному модулі з кореляцією подій у реальному часі.

Рисунок 1.3 – Система віддаленого контролю доступу з можливістю відеоспостереження Hikvision

Існують також домашні або побутові рішення, які поєднують функції контролю доступу (наприклад, відеодомофони) з можливістю відеофіксації відвідувачів [4]. Такі системи достатні для приватних об’єктів, але вони не забезпечують масштабованості, централізованого управління та високого рівня безпеки, необхідних для комерційних чи промислових об’єктів.

Крім комерційних рішень, наукові й інженерні дослідження пропонують IoT-фреймворки та інтегровані платформи, де комунікація між пристроями, реєстрація подій та обробка даних здійснюються через хмарну архітектуру з аналітикою в реальному часі. Такі підходи дозволяють організувати віддалений моніторинг та аналітику, але вони здебільшого залишаються в межах прототипів або дослідницьких проєктів, що вимагають адаптації та стандартизації для промислового застосування.

Аналіз ринку показує, що існуючі комерційні системи мають певні спільні недоліки:

– відсутність повністю інтегрованого підходу до відеомоніторингу вхідної зони приміщення і контролю доступу у межах одного недорогого рішення;

– висока вартість систем корпоративного рівня та складність їхнього налаштування й обслуговування;

– обмежена гнучкість або масштабованість при розширенні системи на великі об’єкти;

– залежність від окремих компонентів (відеореєстраторів, серверів відеоаналітики), що підвищує складність архітектури та адміністративне навантаження.

Ці недоліки визначають доцільність розробки нового рішення в межах кваліфікаційної роботи, яке б поєднувало засоби відеомоніторингу вхідної зони приміщення з функціями контролю доступу, віддаленим моніторингом та IoT-зв’язком у єдиному модулі з оптимізованою архітектурою та доступною вартістю для широкого кола застосувань.

1.4 Аналіз можливих рішень поставленого завдання

Існує кілька основних напрямів реалізації систем відеомоніторингу вхідної зони приміщення, кожен з яких має свої переваги та недоліки.

Першим можливим рішенням є використання готових комерційних систем відеоспостереження з інтегрованими модулями контролю доступу. Такі системи зазвичай забезпечують високу надійність, підтримку професійного програмного забезпечення та відповідність стандартам безпеки. Водночас вони мають обмежену гнучкість щодо адаптації під конкретні вимоги об’єкта, високу вартість обладнання та ліцензій, а також залежність від виробника. Для навчальних або малобюджетних проєктів використання таких рішень є економічно недоцільним і не дозволяє повною мірою дослідити процес проєктування апаратно-програмної системи.

Іншим підходом є побудова системи на основі персонального комп’ютера або одноплатного комп’ютера з використанням зовнішніх камер, контролерів доступу та серверного програмного забезпечення. Такий варіант дозволяє реалізувати складні алгоритми обробки відеоданих і розширену аналітику, однак

супроводжується підвищеним енергоспоживанням, більшими габаритами обладнання та складністю обслуговування. Крім того, використання персонального комп’ютера як центрального вузла знижує мобільність і обмежує можливості встановлення системи в умовах обмеженого простору.

Перспективним рішенням є розробка системи на основі мікроконтролерної платформи з інтегрованими засобами зв’язку та відеофіксації. Застосування мікроконтролерів із підтримкою бездротових технологій дозволяє створити компактну, енергоефективну та відносно недорогу систему, яка може працювати автономно та забезпечувати передавання даних на IoT-платформу. Це забезпечує високу гнучкість у налаштуванні функціоналу, можливість масштабування та модернізації, а також спрощує інтеграцію з іншими IoT-пристроями.

Окрему увагу слід приділити вибору способу організації віддаленого доступу та зберігання даних. Використання хмарних IoT-платформ дозволяє реалізувати централізований моніторинг, зберігання журналів подій та відеофрагментів, а також віддалене керування системою через веб-інтерфейс або мобільний додаток. Альтернативою є локальне зберігання даних, яке зменшує залежність від мережі Інтернет, але обмежує можливості віддаленого контролю та масштабування.

Отже, найбільш доцільним для реалізації поставленого завдання в межах даної кваліфікаційної роботи є розробка комп’ютеризованої системи на основі мікроконтролерної платформи з інтеграцією IoT-технологій. Такий підхід дозволяє поєднати контроль доступу та відеофіксацію подій у єдиній системі, забезпечити віддалений моніторинг, знизити вартість реалізації та створити гнучке рішення, придатне для подальшого розвитку й адаптації до різних умов експлуатації.

РОЗДІЛ 2 ПРОЄКТНА ЧАСТИНА

2.1 Структура системи відеомоніторингу вхідної зони приміщення

На рисунку 2.1 наведено структурну схему системи відеомоніторингу вхідної зони приміщення. Центральним елементом системи є платформа EPS32-CAM, яка виконує функції обробки даних, керування периферійними пристроями та забезпечення мережевої взаємодії з хмарною IoT платформою. До складу цієї платформи входить модуль камери, який використовується для відеофіксації подій, що відбуваються під час спроб доступу до приміщення.

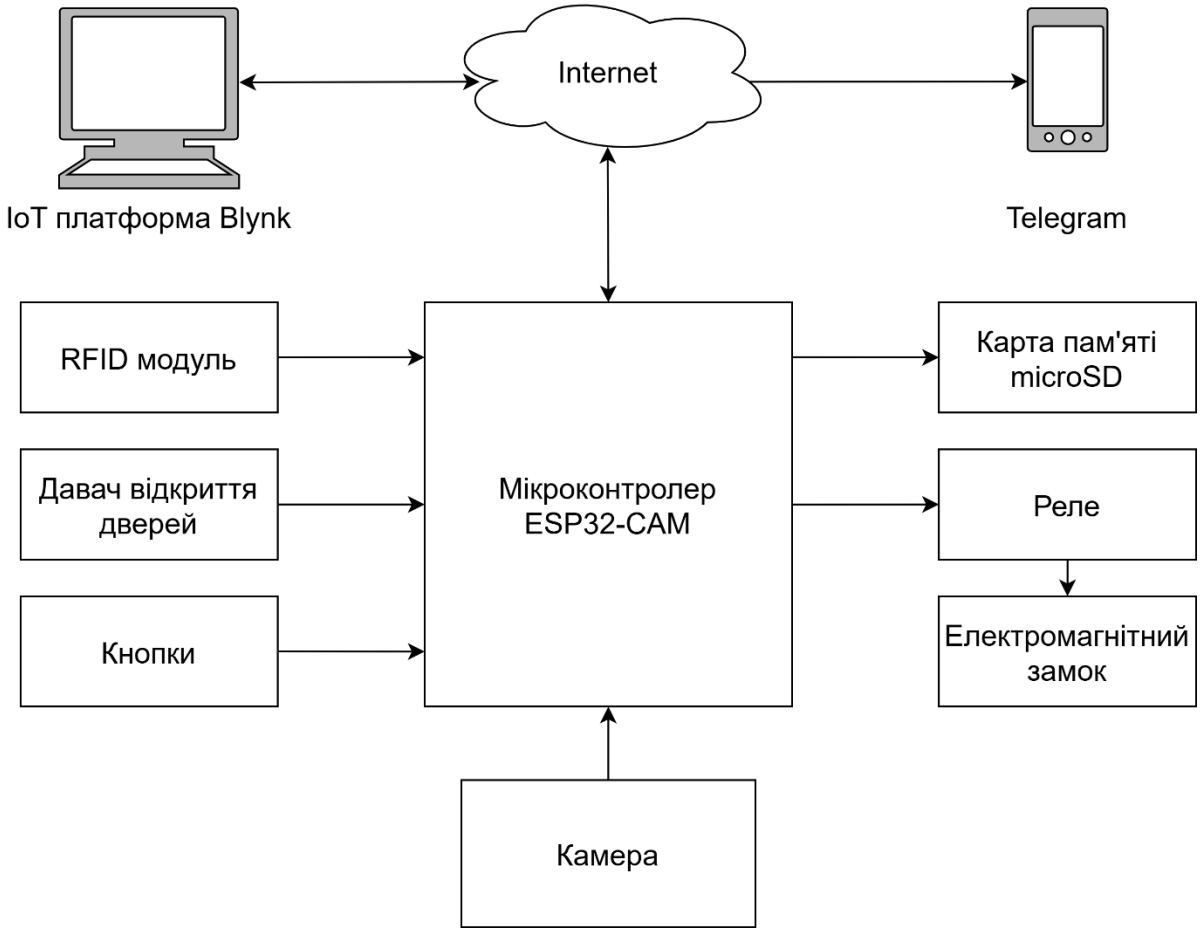

Рисунок 2.1 – Структурна схема системи відеомоніторингу вхідної зони приміщення

					КС КРБ 123.146.00.00 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Бойко П.П.			Проєктна частина	Літ.	Арк. 19 / Акрушів 18
Перевірив		Стадник Н.Б.					
Рецензент		Литвиненко Я.В.				ТНТУ, каф. КС, гр. СІ-41	
Н. Контр.		Луцик Н.С.					
Зав. каф.		Осухівська Г.М.					

До мікроконтролерної платформи підключено RFID модуль, призначений для зчитування даних з безконтактних ідентифікаційних носіїв. Отримана інформація передається до мікроконтролера, де виконується перевірка прав доступу користувача. У разі успішної ідентифікації формується команда керування виконавчим механізмом системи доступу.

Керування фізичним доступом до приміщення здійснюється за допомогою електромагнітного замка, який підключений до мікроконтролера через релейний модуль. Реле виконує функцію електричної розв’язки між керуючим сигналом мікроконтролера та силовим колом замка. У нормальному режимі замок утримує двері зачиненими, а після отримання відповідної команди від контролера відбувається його короткочасне розблокування, що дозволяє відкрити двері.

Для контролю фактичного стану дверей у системі використовується давач відкриття, який встановлюється на дверній конструкції та передає інформацію про положення дверей до мікроконтролера. Це дозволяє системі визначати, чи були двері відчинені після подання команди на надання доступу, а також виявляти можливі порушення або несанкціоноване відкриття.

Для забезпечення зручності використання системи передбачено наявність двох керуючих кнопок. Кнопка виклику використовується для подання сигналу про необхідність доступу або привернення уваги оператора системи. Кнопка виходу встановлюється з внутрішнього боку приміщення та дозволяє відкрити двері без використання засобів ідентифікації. Сигнали від цих кнопок передаються до мікроконтролера, де обробляються відповідно до заданого алгоритму роботи системи.

Важливим елементом структури системи є хмарна IoT платформа, з якою мікроконтролерна платформа взаємодіє через мережу Інтернет за допомогою бездротового зв’язку. IoT платформа забезпечує можливість віддаленого моніторингу стану системи, перегляду журналу подій, отримання повідомлень про спроби доступу та керування системою через веб-інтерфейс або мобільний додаток. Також, передбачена можливість передачі зображень з камери у месенджер Telegram, що дозволяє здійснювати візуальний контроль подій.

2.2 Розроблення апаратного забезпечення системи відеомоніторингу вхідної зони приміщення

2.2.1 Платформа ESP32-CAM

Мікроконтролерна платформа ESP32-CAM є компактним вбудованим обчислювальним модулем, що поєднує у собі функції мікроконтролера, бездротового зв’язку та відеозахоплення. Вона широко застосовується в системах Інтернету речей, зокрема у задачах відеоспостереження, контролю доступу та віддаленого моніторингу. Завдяки інтеграції камери та мережевих інтерфейсів у межах одного модуля, ESP32-CAM є ефективною основою для побудови компактних і недорогих вбудованих систем (рис. 2.2).

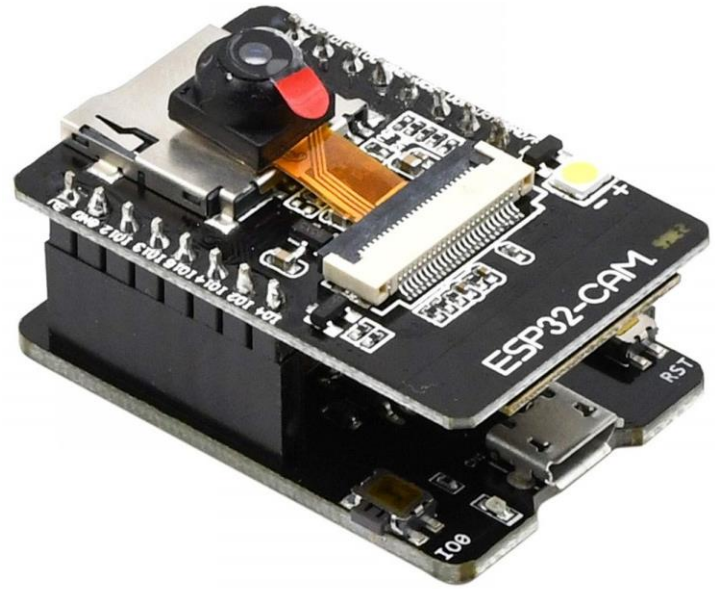

Рисунок 2.2 – Платформа ESP32-CAM

Конструктивно платформа складається з кількох функціональних блоків. Центральним елементом є мікроконтролер ESP32, побудований на базі двоядерного 32-бітного процесора. Цей мікроконтролер забезпечує виконання програмної логіки системи, обробку сигналів з периферійних пристроїв та керування виконавчими механізмами (рис. 2.3).

Рисунок 2.3 – Функції виводів платформи ESP32-CAM

До складу плати також входить модуль камери OV2640, який підключається до ESP32 через паралельний інтерфейс і забезпечує захоплення зображень або відеопотоку. Камера підтримує роздільну здатність до 1600×1200 пікселів та формати стиснення JPEG, що дозволяє ефективно передавати зображення через бездротову мережу.

Окрім цього, платформа містить модуль бездротового зв’язку, який підтримує Wi-Fi та Bluetooth, що дозволяє реалізувати пряме підключення до мережі Інтернет або взаємодію з іншими пристроями.

Важливою складовою є також підсистема пам’яті, яка включає внутрішню оперативну пам’ять SRAM обсягом близько 520 КБ, зовнішню flash-пам’ять та можливість підключення карти пам’яті microSD для зберігання даних і зображень.

Принцип роботи ESP32-CAM полягає у виконанні мікроконтролером заданої програми, яка здійснює збір даних із підключених сенсорів, обробку сигналів, керування виконавчими пристроями та обмін інформацією через мережу. У контексті системи відеомоніторингу вхідної зони приміщення процес функціонування виглядає наступним чином: після отримання сигналу про подію (наприклад, зчитування RFID-картки або натискання кнопки) мікроконтролер виконує обробку події, активує камеру для фіксації зображення та, у разі підтвердження доступу, формує сигнал керування релейним модулем для

відкриття замка. Паралельно отримані дані передаються через Wi-Fi на IoT платформу та в Telegram, де здійснюється їх збереження та віддалений моніторинг.

Ключовою особливістю платформи є можливість реалізації функцій відеофіксації без використання додаткових обчислювальних пристроїв. Це значно спрощує архітектуру системи, зменшує її вартість та підвищує надійність за рахунок зменшення кількості компонентів. Крім того, ESP32-CAM підтримує роботу з різними інтерфейсами (UART, SPI, I2C, PWM), що дозволяє легко інтегрувати її з периферійними пристроями, такими як RFID-модулі, давачі та релейні блоки. Основні характеристики платформи ESP32-CAM приведені в таблиці 2.1.

Таблиця 2.1 – Характеристики платформи ESP32-CAM

Характеристика	Значення
Мікроконтролер	ESP32 (Tensilica Xtensa LX6, 32-біт)
Кількість ядер	2
Тактова частота	до 240 МГц
Оперативна пам’ять	~520 КБ SRAM
Flash-пам’ять	4 МБ
Камера	OV2640
Роздільна здатність камери	до 1600×1200 (UXGA)
Частота кадрів	до 15 fps (UXGA)
Бездротовий зв’язок	Wi-Fi 802.11 b/g/n, Bluetooth 4.2
Інтерфейси	UART, SPI, I2C, PWM, ADC, DAC
Кількість GPIO	8–9
Підтримка microSD	є
Напруга живлення	2,2–3,6 В
Споживання струму	~160–310 мА

Вибір платформи ESP32-CAM для реалізації комп’ютеризованої системи відеомоніторингу вхідної зони приміщення є технічно обґрунтованим з кількох

причин. По-перше, модуль забезпечує поєднання функцій обчислення, зв’язку та відеофіксації в одному пристрої, що дозволяє суттєво спростити структурну схему системи. По-друге, наявність вбудованого Wi-Fi модуля забезпечує пряме підключення до IoT платформи без необхідності використання додаткових комунікаційних модулів. По-третє, достатня обчислювальна потужність мікроконтролера дозволяє реалізувати обробку подій у реальному часі, керування виконавчими механізмами та базову обробку зображень. При цьому енергоспоживання залишається значно нижчим у порівнянні з одноплатними комп’ютерами, що є важливим для вбудованих систем.

Використання ESP32-CAM дозволяє створити компактну, функціонально завершену та економічно ефективну систему відеомоніторингу вхідної зони приміщення, що повністю відповідає вимогам даної кваліфікаційної роботи.

2.2.2 RFID модуль MFRC522

RFID модуль MFRC522 є спеціалізованим пристроєм для безконтактної радіочастотної ідентифікації об’єктів. Він широко застосовується у системах контролю доступу, електронних замках, системах обліку та автоматизації. Завдяки компактності, низькій вартості та простоті інтеграції з мікроконтролерами, цей модуль є одним із найпоширеніших рішень для реалізації RFID-аутентифікації в IoT-системах (рис. 2.4).

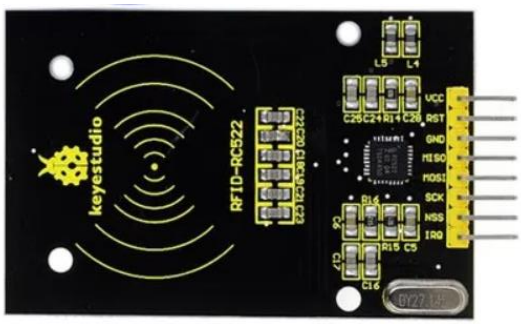

Рисунок 2.4 – RFID модуль MFRC522

Конструктивно модуль складається з інтегральної мікросхеми MFRC522, антени для прийому та передачі радіосигналів, а також допоміжних елементів.

Антена, виконана у вигляді друкованої спіралі на платі, забезпечує формування електромагнітного поля, необхідного для взаємодії з RFID-мітками. Саме ця антена визначає дальність зчитування, яка зазвичай становить до 5–6 см.

Мікросхема MFRC522 виконує функції генерації високочастотного сигналу (13,56 МГц), модуляції та демодуляції сигналів, а також обробки протоколів обміну даними відповідно до стандарту ISO/IEC 14443A.

Принцип роботи RFID модуля базується на індуктивному зв’язку між антеною зчитувача та пасивною RFID-міткою. Після піднесення картки до антени модуль генерує електромагнітне поле, яке індукує струм у мітці, активуючи її. У відповідь мітка передає свій унікальний ідентифікатор (UID) або інші дані шляхом модуляції зворотного сигналу. Отримана інформація декодується мікросхемою та передається до мікроконтролера через інтерфейс SPI для подальшої обробки.

Для взаємодії з мікроконтролером модуль MFRC522 використовує інтерфейс SPI, який забезпечує швидкий та надійний обмін даними. В таблиці 2.2 зведені технічні характеристики RFID модуля MFRC522.

Таблиця 2.2 – Характеристики RFID модуля MFRC522

Характеристика	Значення
Робоча частота	13.56 МГц
Стандарт	ISO/IEC 14443A
Напруга живлення	2,5–3,3 В
Споживаний струм	13–26 мА
Струм у режимі очікування	10–13 мА
Струм у сплячому режимі	< 80 мкА
Дальність зчитування	до 60 мм
Інтерфейс зв’язку	SPI (основний), UART, I2C
Максимальна швидкість передачі	до 10 Мбіт/с
Підтримувані карти	MIFARE S50, S70, UltraLight, DESFire
Робоча температура	приблизно −20…+80 °C

Використання RFID модуля MFRC522 у даній комп’ютеризованій системі є технічно обґрунтованим. По-перше, модуль забезпечує швидку та надійну ідентифікацію користувачів за допомогою безконтактних карт або брелоків, що є ключовою функцією системи контролю доступу. По-друге, він працює у стандартному діапазоні 13,56 МГц і підтримує широко розповсюджені типи RFID-міток, що спрощує впровадження системи та зменшує витрати на її експлуатацію. По-третє, низьке енергоспоживання та живлення від 3,3 В роблять його сумісним із платформою ESP32-CAM без необхідності додаткових перетворювачів рівнів.

Ще однією важливою перевагою є простота інтеграції: наявність готових бібліотек дозволяє швидко реалізувати функції зчитування UID, автентифікації та обробки даних. Крім того, компактні розміри модуля дозволяють легко інтегрувати його у корпус системи відеомоніторингу, а невелика дальність зчитування (до 6 см) підвищує безпеку, зменшуючи ймовірність несанкціонованого доступу.

2.2.3 Модуль реле

Модуль реле KS0011 є електромеханічним комутаційним пристроєм, призначеним для керування навантаженнями з високою напругою або струмом за допомогою низьковольтних цифрових сигналів мікроконтролера. У системах контролю доступу такі модулі виконують ключову функцію – забезпечують фізичне керування виконавчими пристроями, зокрема електромагнітними замками, освітленням або сигналізаційними системами (рис. 2.5).

Рисунок 2.5 – Модуль реле KS0011

Конструктивно модуль складається з кількох основних елементів. Центральним компонентом є електромеханічне реле типу SRD-05VDC-SL-C, яке має котушку на 5 В та групу контактів типу SPDT. До складу модуля також входить транзисторний ключ, який забезпечує керування реле від цифрового сигналу мікроконтролера, захисний діод для гасіння ЕРС самоіндукції котушки, а також світлодіодна індикація стану. Світлодіод дозволяє візуально визначити, чи активоване реле, що спрощує налагодження системи.

Модуль оснащений двома типами роз'ємів: керуючими (VCC, GND, IN) для підключення до мікроконтролера та силовими (COM, NO, NC) для підключення навантаження. Така структура дозволяє електрично розділити керуючу та силову частини системи, що підвищує безпеку експлуатації.

Принцип роботи модуля базується на перетворенні електричного сигналу у механічне перемикання контактів. При подачі логічного сигналу високого рівня (TTL) на вхід IN відбувається відкривання транзистора, через котушку реле починає протікати струм, що створює магнітне поле. Під дією цього поля рухома контактна група перемикається: нормально розімкнений контакт (NO) замикається, а нормально замкнений (NC) – розмикається. Після зняття керуючого сигналу магнітне поле зникає, і контакти повертаються у початковий стан під дією пружини.

Особливістю модуля KS0011 є активний високий рівень керування, тобто реле вмикається при подачі логічної «1» на вхід. Це спрощує програмну реалізацію керування в мікроконтролерних системах.

Модуль забезпечує комутацію значних електричних навантажень: до 10 А для нормально розімкненого контакту та до 5 А для нормально замкненого. Це дозволяє використовувати його для керування як низьковольтними, так і мережевими пристроями змінного струму. Час спрацювання реле становить близько 10 мс, що є достатнім для більшості задач автоматизації. Технічні характеристики модуля реле KS0011 наведені в таблиці 2.3.

Таблиця 2.3 – Характеристики модуля реле KS0011

Характеристика	Значення
Тип реле	Електромеханічне (SPDT)
Напруга живлення	5 В
Керуючий сигнал	TTL (активний HIGH)
Робочий струм котушки	~70 мА
Максимальний струм навантаження	10 А (NO), 5 А (NC)
Максимальна напруга комутації	до 150–250 В AC, до 24–30 В DC
Максимальна потужність	до 1200 ВА (AC), 240 Вт (DC)
Час спрацювання	~10 мс
Інтерфейс	цифровий (1 канал)
Кількість каналів	1
Наявність індикації	світлодіод

Використання модуля реле KS0011 у складі комп'ютеризованої системи відеомоніторингу вхідної зони приміщення є повністю обґрунтованим з технічної точки зору. Насамперед, модуль дозволяє безпосередньо керувати електромагнітним замком, який потребує значно більшої потужності, ніж можуть забезпечити виходи мікроконтролера. Таким чином, реле виступає як проміжний силовий ключ між ESP32-CAM та виконавчим пристроєм.

Другим важливим фактором є електрична ізоляція між керуючим та силовим колами, що підвищує надійність і безпеку системи, особливо при роботі з високою напругою. Крім того, модуль підтримує керування TTL-рівнями, що забезпечує сумісність із логічними рівнями мікроконтролера ESP32 (3,3 В), особливо завдяки наявності вбудованого транзисторного драйвера.

Ще однією перевагою є простота інтеграції: модуль підключається безпосередньо до цифрового виходу мікроконтролера та не потребує складних схем керування. Наявність гвинтових клем полегшує підключення силових кіл, що є важливим для практичної реалізації системи. Важливо також відзначити низьку вартість і широку доступність модуля.

2.2.4 Електромагнітний замок YM-280

Електромагнітний замок YM-280 є виконавчим пристроєм систем контролю доступу, який забезпечує фізичне блокування дверей за рахунок дії електромагнітного поля. Даний тип замків широко застосовується у системах безпеки, оскільки відзначається високою надійністю, відсутністю механічного зношування та простотою інтеграції з електронними системами керування (рис. 2.6).

Рисунок 2.6 – Електромагнітний замок YM-280

Конструктивно замок складається з двох частин: електромагніту (основного корпусу) та відповідної металевої пластини (якоря), яка встановлюється на дверному полотні. Електромагніт виконаний у металевому корпусі (зазвичай алюмінієвому або сталевому) з вбудованою котушкою, що генерує магнітне поле при подачі напруги. Якірна пластина виготовлена з феромагнітного матеріалу та забезпечує щільне прилягання до поверхні електромагніту.

Принцип роботи електромагнітного замка базується на явищі електромагнітної індукції. При подачі постійної напруги 12 В на котушку електромагніту виникає магнітне поле, яке притягує якірну пластину з великою силою. У випадку моделі YM-280 сила утримання становить приблизно 280 кг, що забезпечує надійне замикання дверей.

Особливістю даного типу замків є режим роботи Fail-Safe – при відсутності живлення замок автоматично розблоковується. Це важлива характеристика з точки зору пожежної безпеки, оскільки у разі аварійного відключення електроенергії забезпечується вільний вихід людей із приміщення.

При знятті напруги магнітне поле зникає, і якірна пластина відокремлюється від електромагніту, що призводить до відкриття дверей. Відсутність рухомих механічних частин (окрім незначного переміщення пластини) забезпечує високу довговічність та стійкість до зношування. Крім того, замок витримує значну кількість циклів відкривання/закривання без погіршення характеристик.

Замок YM-280 може встановлюватися на різні типи дверей: дерев'яні, металеві, скляні та протипожежні, що робить його універсальним рішенням для різних об'єктів. Його монтаж здійснюється накладним способом із використанням спеціальних кронштейнів. Характеристики електромагнітного замка YM-280 наведені таблиці 2.4.

Таблиця 2.4 – Характеристики електромагнітного замка YM-280

Характеристика	Значення
Тип замка	Електромагнітний (накладний)
Сила утримання	280 кг (≈600 lbs)
Напруга живлення	12 В DC / 24 В DC
Споживаний струм	500 мА (12 В), 250 мА (24 В)
Потужність	~6–6,6 Вт
Матеріал корпусу	Анодований алюміній / сталь
Розміри замка	~250 × 48 × 25 мм
Розміри пластини	~180 × 38 × 12 мм
Вологість	до 90–95% (без конденсації)
Тип дверей	дерев'яні, металеві, скляні
Додаткові функції	сигнал стану (NO/NC), LED
Ресурс роботи	до 1 млн циклів

Використання електромагнітного замка YM-280 у комп’ютеризованій системі відеомоніторингу вхідної зони приміщення є технічно обґрунтованим. Насамперед, замок забезпечує високу силу утримання, що гарантує надійне блокування дверей і підвищує рівень безпеки об’єкта. Другим важливим фактором є сумісність із мікроконтролерними системами. Замок керується подачею або зняттям живлення, що дозволяє легко інтегрувати його з релейним модулем, який у свою чергу керується платформою ESP32-CAM. Така схема є простою та надійною в реалізації.

Режим Fail-Safe забезпечує відповідність вимогам безпеки, особливо у громадських або навчальних приміщеннях, де важливо гарантувати можливість аварійного відкривання дверей.

Додатковою перевагою є відсутність механічного зносу, що значно збільшує термін служби замка у порівнянні з електромеханічними аналогами. Це особливо актуально для систем із великою кількістю циклів відкривання.

Також слід відзначити універсальність застосування та простоту монтажу, що дозволяє використовувати замок у різних умовах без суттєвих конструктивних змін.

Електромагнітний замок YM-280 повністю відповідає вимогам проєктованої системи за критеріями надійності, безпеки, простоти інтеграції та експлуатаційних характеристик, що обґрунтовує його використання у складі комп’ютеризованої системи відеомоніторингу вхідної зони приміщення.

2.2.5 Магнітний герконовий давач MC-38

Магнітний герконовий давач MC-38 є простим та надійним сенсорним пристроєм, призначеним для визначення стану відкриття або закриття дверей чи вікон. Він широко застосовується у системах безпеки, сигналізації та автоматизації, зокрема у системах відеомоніторингу вхідної зони приміщення, де необхідно фіксувати факт відкриття дверей після надання доступу або при несанкціонованому проникненні (рис. 2.7).

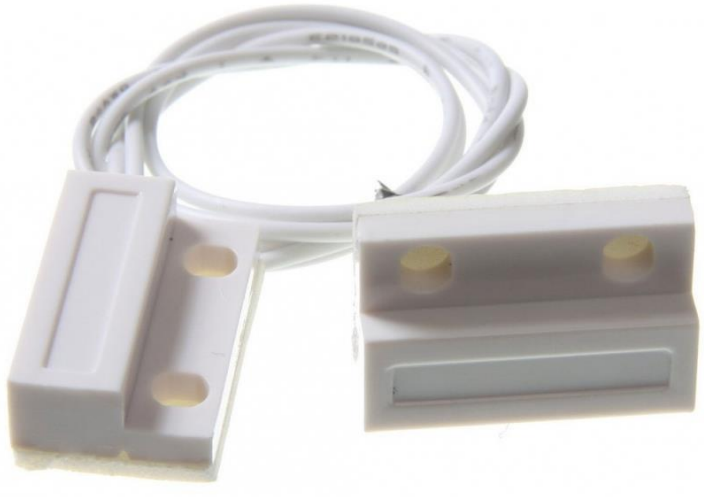

Рисунок 2.7 – Магнітний герконовий давач МС-38

Конструктивно давач складається з двох окремих частин: герконового перемикача, розміщеного у пластиковому корпусі, та постійного магніту, який встановлюється на рухомій частині (дверному полотні). Геркон містить герметичну скляну колбу, всередині якої розташовані два феромагнітні контакти. Ці контакти можуть замикатися або розмикатися під дією магнітного поля. Обидві частини давача мають компактні габарити та зазвичай виконані з ударостійкого ABS-пластику, що забезпечує їх механічну міцність і довговічність.

Давач встановлюється таким чином, щоб магніт і геркон знаходилися навпроти один одного у закритому стані дверей. Важливою особливістю є мала відстань спрацювання (10–25 мм), що забезпечує високу точність визначення стану.

Принцип роботи давача МС-38 базується на зміні стану герконового контакту під дією магнітного поля. У стандартній конфігурації використовується режим Normally Closed (NC) – нормально замкнений контакт. Це означає, що при закритих дверях контакти замкнені, і через них протікає струм. При відкритті дверей магніт віддаляється, магнітне поле зникає, і контакти розмикаються, формуючи сигнал про подію.

Такий принцип роботи є особливо важливим з точки зору безпеки: у разі обриву проводу або пошкодження датчика система також фіксує розрив кола, що інтерпретується як тривожний сигнал.

Давач МС-38 не є активним електронним пристроєм – він не генерує сигнал самостійно, а лише змінює стан електричного кола. Тому він підключається до цифрового входу мікроконтролера, де зміна стану (HIGH/LOW) інтерпретується програмою як відкриття або закриття дверей. Важливо, що давач працює з малими струмами і не призначений для комутації потужних навантажень, а лише для формування сигнальних рівнів.

Завдяки простій конструкції герконові давачі мають дуже великий ресурс роботи – до мільйонів циклів перемикання, що робить їх ефективним рішенням для довготривалих систем моніторингу. Характеристики герконового давача МС-38 наведені таблиці 2.5.

Таблиця 2.5 – Характеристики герконового давача МС-38

Характеристика	Значення
Режим роботи	Normally Closed / Normally Open
Робоча напруга	до 100–200 В DC
Максимальний струм	до 0,5 А
Потужність комутації	до 3–10 Вт
Відстань спрацювання	10–25 мм
Тип виходу	дискретний (ON/OFF)
Довжина проводу	~25–30 см
Матеріал корпусу	ABS пластик
Габарити	~27 × 14 × 8 мм
Ресурс роботи	≥ 1 000 000 спрацювань

Використання магнітного герконового давача МС-38 у даній комп’ютеризованій системі є технічно обґрунтованим з кількох причин. Насамперед, він забезпечує простий і надійний спосіб визначення фактичного стану дверей, що є критично важливим для системи відеомоніторингу вхідної зони приміщення. Це дозволяє не лише керувати відкриванням замка, але й контролювати, чи були двері дійсно відкриті або залишені відчиненими.

Другим важливим аспектом є висока надійність та довговічність давача, обумовлена відсутністю складної електроніки та мінімальною кількістю рухомих елементів.

Крім того, датчик має дуже низьке енергоспоживання (фактично пасивний елемент), що є важливим для вбудованих систем. Його інтеграція з ESP32-CAM є максимально простою і не потребує додаткових схем узгодження. Додатковою перевагою є низька вартість і доступність, що робить його економічно ефективним рішенням для масового впровадження.

Використання MC-38 дозволяє реалізувати функцію контролю стану дверей із високою надійністю, мінімальними витратами та простою інтеграцією, що повністю відповідає вимогам розроблюваної комп'ютеризованої системи відеомоніторингу вхідної зони приміщення.

2.3 Розроблення електричної схеми пристрою

На рисунку 2.8 наведено електричну принципову схему пристрою для відеомоніторингу вхідної зони приміщення.

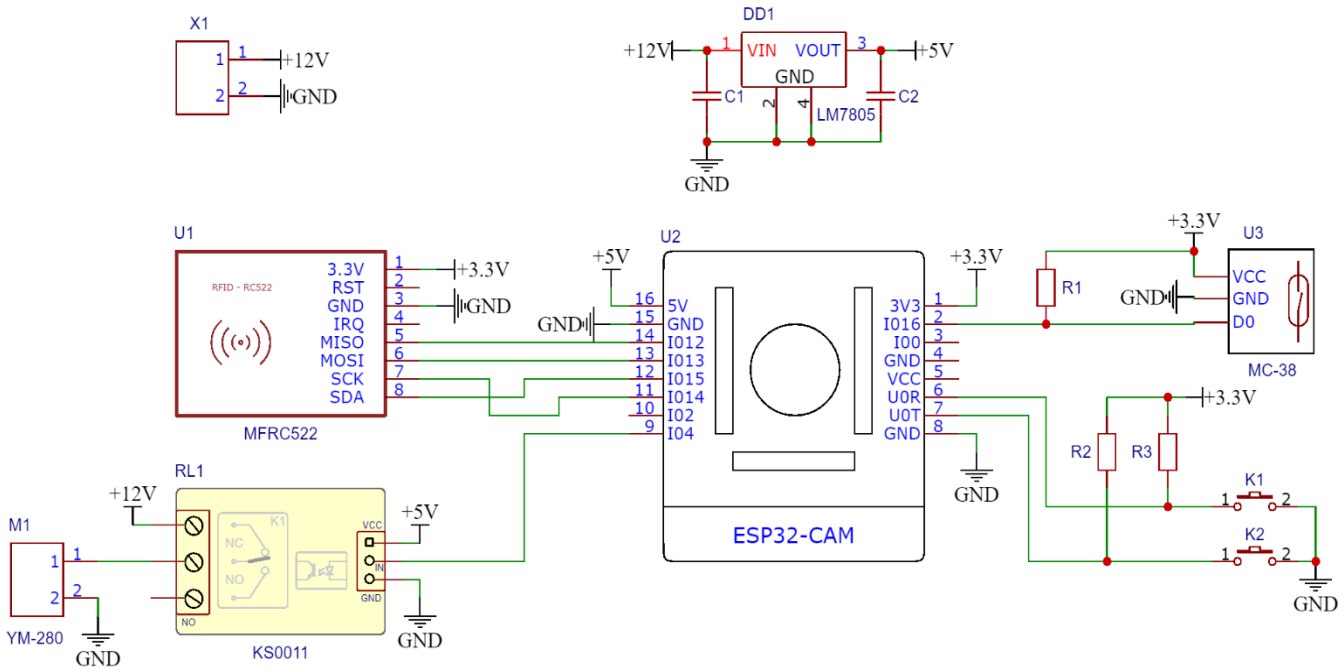

Рисунок 2.8 – Електрична принципова схема пристрою для відеомоніторингу вхідної зони приміщення

Центральним елементом схеми є мікроконтролерна платформа ESP32-CAM, яка виконує функції обробки даних, керування периферійними пристроями та передавання інформації на хмарну IoT-платформу.

Живлення системи організовано таким чином, що платформа ESP32-CAM отримує стабілізовану напругу 5 В через контакт 5V, а спільний провід підключений до контакту GND. Від цієї ж лінії живлення здійснюється живлення інших модулів системи, зокрема RFID-зчитувача та релейного модуля.

RFID модуль MFRC522, який використовується для ідентифікації користувачів за допомогою безконтактних карток або брелоків, підключається до мікроконтролера через інтерфейс SPI. Для цього контакт SDA модуля підключається до цифрового виводу GPIO15 плати ESP32-CAM, який використовується як сигнал вибору пристрою. Контакт SCK підключений до виводу GPIO14, що забезпечує передачу тактових імпульсів інтерфейсу SPI. Лінія передачі даних від мікроконтролера до RFID модуля MOSI з'єднана з виводом GPIO13, а лінія прийому даних MISO – з виводом GPIO12.

Для керування виконавчим пристроєм – електромагнітним замком YM-280 – використовується одноканальний релейний модуль KS0011. Керуючий вхід IN релейного модуля підключений до цифрового виводу GPIO4 мікроконтролера. При подачі логічного сигналу з цього виводу відбувається активація реле, що призводить до комутації силового кола замка.

Для контролю фактичного стану дверей у схемі використовується магнітний герконовий давач МС-38. Один контакт геркона підключений до входу GPIO16 мікроконтролера, а інший – до загальної землі. До цього ж входу через резистор номіналом приблизно 10 кОм підключено підтягувальний резистор до лінії живлення 3,3 В (pull-up), що дозволяє стабілізувати логічний рівень сигналу. У закритому стані дверей геркон замикає коло і на вході формується логічний нуль, тоді як при відкритті дверей контакт розмикається і на вході з'являється логічна одиниця.

Для забезпечення взаємодії користувачів із системою у схемі передбачено дві кнопки – кнопку виклику та кнопку виходу. Кнопка виклику використовується

для формування сигналу запиту доступу або виклику адміністратора. Один її контакт підключений до входу GPIO0, а інший – до загальної землі. До входу також підключений підтягувальний резистор номіналом 10 кОм до лінії живлення 3,3 В, що забезпечує стабільний логічний рівень у неактивному стані. При натисканні кнопки відбувається замикання кола і на вході формується логічний нуль.

Кнопка виходу призначена для відкривання дверей із внутрішньої сторони приміщення без використання RFID-картки. Вона підключена аналогічним чином: один контакт кнопки з’єднаний із входом GPIO3, а інший – із загальною землею. До цього входу також підключено резистор до 3,3 В, що забезпечує формування стабільного логічного сигналу.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Алгоритм роботи системи відеомоніторингу вхідної зони приміщення

Алгоритм роботи системи відеомоніторингу вхідної зони приміщення визначає послідовність дій мікроконтролерної платформи та периферійних пристроїв під час взаємодії з користувачами. Основною метою алгоритму є забезпечення надійної ідентифікації користувачів, керування електромагнітним замком дверей, контролю стану дверей та фіксації подій із передаванням інформації на IoT-платформу для віддаленого моніторингу.

Робота системи починається з етапу ініціалізації апаратних і програмних компонентів після подачі живлення на пристрій. На цьому етапі мікроконтролер платформи ESP32-CAM виконує налаштування всіх використовуваних портів введення-виведення, ініціалізацію інтерфейсу SPI для роботи з RFID-модулем MFRC522, налаштування камери OV2640, підключеної до плати, а також запуск мережевого модуля Wi-Fi. Після встановлення з’єднання з бездротовою мережею здійснюється підключення до хмарної IoT-платформи Blynk, яка використовується для віддаленого моніторингу подій та керування системою. Одночасно ініціалізуються всі периферійні пристрої: модуль реле для керування електромагнітним замком, магнітний герконовий давач стану дверей, кнопка виклику та кнопка виходу.

Після завершення ініціалізації система переходить у режим очікування подій (рис. 3.1). У цьому режимі мікроконтролер безперервно опитує RFID-модуль MFRC522 для виявлення RFID-карток у зоні зчитування. Коли користувач підносить картку або RFID-брелок до зчитувача, модуль формує сигнал про наявність мітки та передає її унікальний ідентифікатор (UID) до мікроконтролера через інтерфейс SPI. Отриманий ідентифікатор порівнюється з базою дозволених ідентифікаторів, яка зберігається у пам’яті системи або на IoT-платформі.

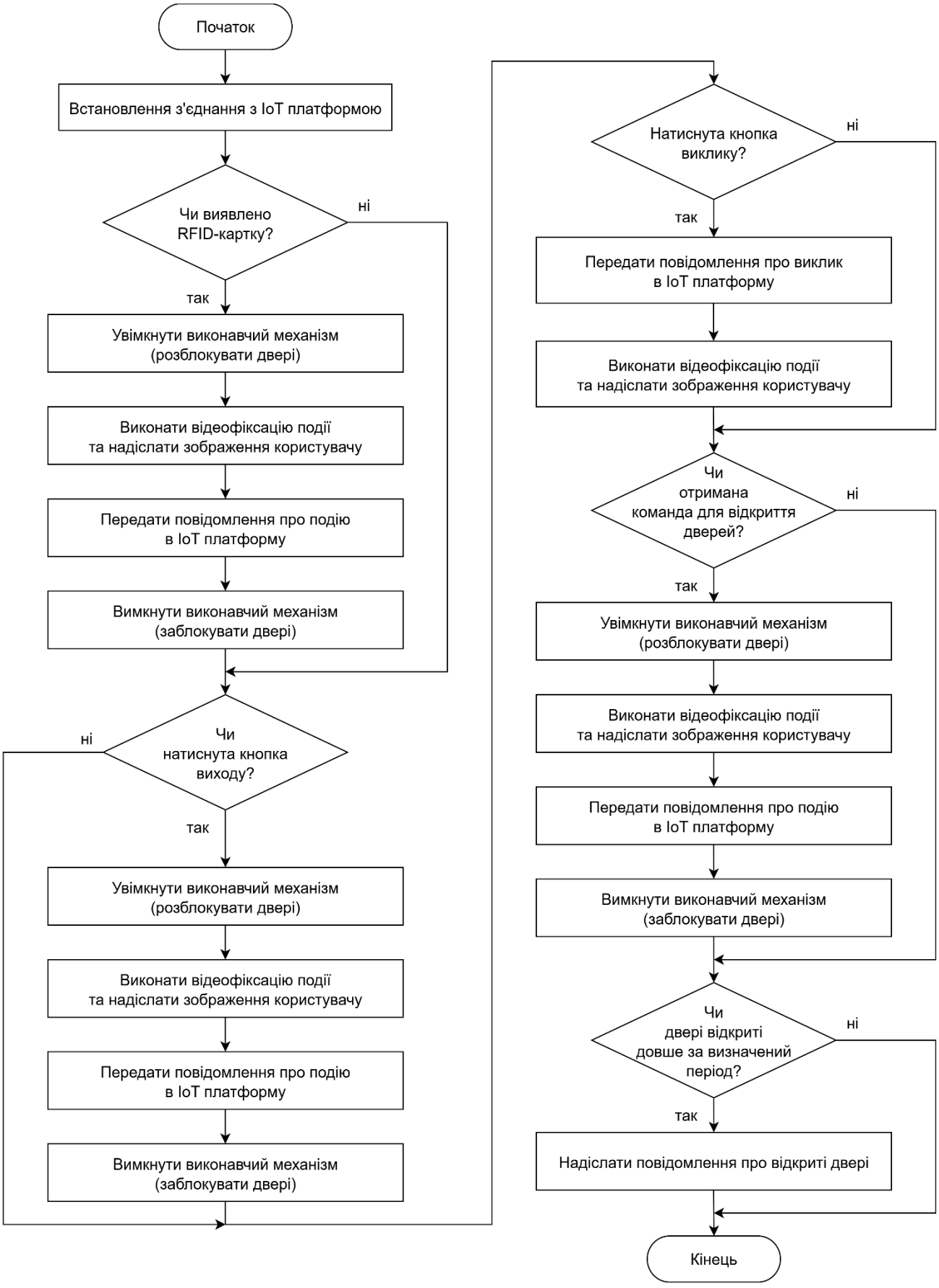

Рисунок 3.1 – Блок-схема алгоритму роботи основного циклу ПЗ системи відеомоніторингу вхідної зони приміщення

У разі, якщо ідентифікатор користувача відповідає одному із дозволених значень, система формує сигнал дозволу доступу. Мікроконтролер подає керуючий сигнал на релейний модуль KS0011, що призводить до комутації силового кола електромагнітного замка YM-280 та його розблокування. Паралельно активується камера платформи ESP32-CAM, яка виконує захоплення фотографії або короткої серії кадрів для відеофіксації події. Отримане зображення разом із інформацією про подію (час, UID картки, статус доступу) передається через мережу Wi-Fi на IoT-платформу для подальшого зберігання та відображення користувачеві.

Після розблокування дверей система переходить у режим контролю їх стану. Для цього використовується магнітний герконовий давач MC-38, який визначає факт відкриття або закриття дверей. Якщо після розблокування двері відкриваються, система фіксує цю подію та також може передавати відповідну інформацію на IoT-платформу. У разі якщо двері залишаються відкритими довше заданого часу, система може формувати попереджувальний сигнал або відправляти повідомлення користувачеві через Telegram.

Якщо зчитаний RFID-ідентифікатор відсутній у списку дозволених, система формує сигнал відмови у доступі. У цьому випадку електромагнітний замок не розблоковується. Одночасно камера також може виконувати знімок події, а інформація про невдалу спробу доступу передається на IoT-платформу для реєстрації.

Окрім доступу за RFID-карткою, система підтримує альтернативні способи керування. Зокрема, передбачено використання кнопки виходу, яка встановлюється з внутрішньої сторони приміщення. При натисканні цієї кнопки мікроконтролер формує сигнал на релейний модуль, що призводить до тимчасового розблокування електромагнітного замка та дозволяє користувачеві вийти з приміщення без використання RFID-картки.

Також у системі передбачена кнопка виклику, яка використовується для подання сигналу виклику або повідомлення адміністратора. При натисканні цієї кнопки мікроконтролер формує подію, яка передається на IoT-платформу, а камера

може виконувати знімок особи біля дверей та надсилати його через Telegram. Це дозволяє оператору віддалено оцінити ситуацію та, у разі необхідності, надати доступ до приміщення через інтерфейс IoT-платформи.

У процесі роботи система постійно підтримує зв'язок із IoT-платформою Blynk, передаючи інформацію про стан дверей, події доступу, спроби несанкціонованого входу та інші системні повідомлення. Користувач або адміністратор може віддалено переглядати ці дані через веб-інтерфейс або мобільний додаток.

Запропонований алгоритм роботи забезпечує комплексне функціонування всіх компонентів системи – RFID-ідентифікації, керування електромагнітним замком, контролю стану дверей, звукової індикації, взаємодії з користувачем через кнопки та відеофіксації подій за допомогою камери.

3.2 Розробка програмного забезпечення

3.2.1 Ініціалізація апаратних та програмних компонентів системи

Підпрограма setup() призначена для початкової ініціалізації всіх апаратних і програмних компонентів системи (рис. 3.2).

```
void setup() {
  Serial.begin(115200);
  pinMode(RELAY, OUTPUT);
  pinMode(DOOR_SENSOR, INPUT_PULLUP);
  pinMode(EXIT_BTN, INPUT_PULLUP);
  pinMode(CALL_BTN, INPUT_PULLUP);
  WiFi.begin(ssid, pass);
  while (WiFi.status() != WL_CONNECTED) delay(500);
  Blynk.begin(auth, ssid, pass);
  SPI.begin(14, 2, 15, 13);
  mfrc522.PCD_Init();
  startCamera();
  initSD();
  server.on("/stream", HTTP_GET, handleStream);
  server.begin();
}
```

Рисунок 3.2 – Лістинг коду функції setup()

На першому етапі виконується конфігурація режимів роботи цифрових виводів мікроконтролера. Зокрема, пін керування реле налаштовується як вихід, що дозволяє формувати сигнал для керування електромагнітним замком. Виводи, до яких підключені давач стану дверей, кнопка виходу та кнопка виклику, конфігуруються у режимі INPUT.

Наступним етапом є підключення до бездротової мережі Wi-Fi за допомогою функції WiFi.begin(). Після ініціалізації підключення реалізовано цикл очікування встановлення з'єднання, який перевіряє статус мережі через WiFi.status() і затримується до моменту успішного підключення. Це гарантує коректну роботу всіх мережевих сервісів у подальшому.

Після встановлення з'єднання здійснюється ініціалізація взаємодії з IoT-платформою Blynk IoT за допомогою виклику Blynk.begin(). Даний виклик забезпечує авторизацію пристрою в хмарному середовищі та підготовку до обміну даними з мобільним додатком користувача.

Особливу увагу в підпрограмі приділено ініціалізації інтерфейсу SPI, який використовується для взаємодії з RFID-модулем MFRC522. Виклик SPI.begin(14, 2, 15, 13) задає нестандартну конфігурацію виводів (SCK, MISO, MOSI, SS), що дозволяє уникнути конфліктів із іншими периферійними компонентами, зокрема камерою та картою пам'яті. Після цього виконується ініціалізація RFID-модуля за допомогою mfrc522.PCD_Init(), що переводить його у робочий режим.

Далі викликається функція startCamera(), яка відповідає за ініціалізацію камери ESP32-CAM, налаштування параметрів захоплення зображення та підготовку до передачі відеопотоку. Паралельно виконується ініціалізація карти пам'яті через функцію initSD(), що забезпечує можливість збереження зображень або послідовностей кадрів для подальшого аналізу.

На завершальному етапі виконується налаштування локального вебсервера, який використовується для трансляції відеопотоку. За допомогою виклику server.on() визначається обробник HTTP-запиту, що забезпечує передачу MJPEG-потоку клієнту. Після цього сервер запускається командою server.begin(), що переводить систему у стан готовності до обробки запитів від користувачів.

3.2.2 Основний цикл обробки подій та взаємодії компонентів системи

Підпрограма loop() реалізує безперервний цикл виконання системи та відповідає за обробку всіх подій у реальному часі. На початку кожної ітерації викликається функція Blynk.run(), яка забезпечує обслуговування з'єднання з хмарною платформою Blynk IoT та обробку вхідних і вихідних повідомлень. Це дозволяє системі оперативно реагувати на команди користувача та передавати актуальний стан пристрою (рис. 3.3).

```
void loop() {
  Blynk.run();
  server.handleClient();
  // RFID
  if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) {
    openDoor("RFID");
    mfrc522.PICC_HaltA();
  }
  // вихід
  if (digitalRead(EXIT_BTN) == LOW) {
    openDoor("exit");
    delay(500);
  }
  // виклик
  if (digitalRead(CALL_BTN) == LOW) {
    Blynk.virtualWrite(V1, "CALL!");
    Blynk.virtualWrite(V2, "http://" + WiFi.localIP().toString() + "/stream");
    recordEvent("call");
    sendPhotoTelegram();
    delay(500);
  }
  checkDoorState();
}
```

Рисунок 3.3 – Лістинг коду функції loop()

Паралельно виконується обробка HTTP-запитів локального вебсервера за допомогою функції server.handleClient(). Даний виклик забезпечує підтримку клієнтських підключень і, зокрема, передачу відеопотоку з камери через попередньо налаштований маршрут /stream. Таким чином реалізується можливість віддаленого перегляду відео.

Наступний блок коду відповідає за обробку RFID-ідентифікації користувачів. За допомогою умовного оператора перевіряється наявність нової

картки та успішність зчитування її серійного номера. У разі виконання цих умов викликається функція openDoor(), яка ініціює відкриття електромагнітного замка. Після цього виконується команда PICC_HaltA(), що переводить RFID-картку у стан очікування та запобігає повторному зчитуванню того самого ідентифікатора.

Окремий блок відповідає за обробку кнопки виходу. При виявленні логічного нуля на відповідному вході (натискання кнопки) викликається функція openDoor("exit"), яка забезпечує відкриття дверей без необхідності RFID-авторизації. Після цього реалізовано коротку затримку, що запобігає багаторазовому спрацюванню.

Наступний функціональний блок реалізує обробку кнопки виклику. У разі її натискання система формує повідомлення для користувача, передаючи у хмарну платформу текст "CALL!" через віртуальний пін V1. Одночасно формується та передається посилання на відеопотік, яке містить локальну IP-адресу пристрою та шлях до ресурсу /stream. Це дозволяє користувачеві отримати доступ до відео з камери.

Крім передачі повідомлень, при натисканні кнопки виклику виконується виклик функції recordEvent("call"), яка відповідає за фіксацію події, зокрема запис серії кадрів на карту пам’яті. Додатково викликається функція sendPhotoTelegram(), що забезпечує надсилання зображення через месенджер Telegram, підвищуючи інформативність і оперативність реагування.

3.2.3 Ініціалізація карти пам’яті та реалізація відеофіксації подій

У межах програмної реалізації системи було розроблено підпрограми initSD() та recordEvent(), які забезпечують роботу з картою пам’яті microSD та реалізацію функції відеофіксації подій шляхом збереження послідовності зображень. Дані підпрограми є ключовими для забезпечення локального збереження візуальної інформації, що дозволяє здійснювати подальший аналіз подій доступу.

Підпрограма initSD() виконує ініціалізацію файлової системи карти пам’яті з використанням інтерфейсу SD_MMC. На початку роботи викликається функція

SD_MMC.begin(), яка здійснює спробу монтування файлової системи. У разі невдалого підключення виводиться діагностичне повідомлення через послідовний інтерфейс, що дозволяє оперативно виявити проблему. Якщо ж ініціалізація проходить успішно, система повідомляє про готовність карти пам'яті до роботи. Такий підхід забезпечує базовий контроль працездатності підсистеми збереження даних (рис. 3.4).

```
void initSD() {
  if (!SD_MMC.begin()) {
    Serial.println("SD Card Mount Failed");
    return;
  }
  Serial.println("SD Card OK");
}
```

Рисунок 3.4 – Лістинг коду функції initSD()

Основна функціональність відеофіксації реалізована у підпрограмі recordEvent(). Її принцип роботи базується на послідовному захопленні та збереженні серії кадрів із камери, що фактично формує короткий відеофрагмент у вигляді набору JPEG-зображень. На вході підпрограма приймає параметр prefix, який використовується для ідентифікації типу події (наприклад, виклик або доступ), що дозволяє структурувати збережені файли (рис. 3.5).

```
void recordEvent(String prefix) {
  for (int i = 0; i < 20; i++) {
    camera_fb_t * fb = esp_camera_fb_get();
    if (!fb) continue;
    String path = "/event_" + prefix + "_" + String(i) + ".jpg";
    File file = SD_MMC.open(path.c_str(), FILE_WRITE);
    if (file) {
      file.write(fb->buf, fb->len);
      file.close();
    }
    esp_camera_fb_return(fb);
    delay(150);
  }
}
```

Рисунок 3.5 – Лістинг коду функції recordEvent()

У тілі підпрограми реалізовано цикл, який виконується 20 разів, забезпечуючи захоплення відповідної кількості кадрів. На кожній ітерації викликається функція esp_camera_fb_get(), яка повертає буфер із зображенням. У разі, якщо отримання кадру не вдалося, ітерація пропускається, що підвищує стійкість системи до можливих збоїв.

Для кожного отриманого кадру формується унікальний шлях до файлу, який включає префікс події та порядковий номер кадру. Далі виконується відкриття файлу на карті пам’яті у режимі запису (FILE_WRITE). Якщо файл успішно відкрито, відбувається запис бінарних даних зображення (fb->buf) відповідної довжини (fb->len), після чого файл закривається. Це гарантує цілісність збережених даних.

Після завершення запису виконується повернення буфера кадру за допомогою esp_camera_fb_return(fb), що є необхідним для звільнення пам’яті та коректної роботи камери. Між ітераціями реалізовано затримку, яка визначає інтервал між кадрами та впливає на тривалість і «плавність» сформованого відеофрагмента.

3.2.4 Передача зображень у месенджер Telegram

Підпрограма sendPhotoTelegram() призначена для надсилання зображень, отриманих із камери, до користувача через месенджер Telegram. Дана функція реалізує взаємодію з API сервісу Telegram за допомогою HTTPS-запитів і забезпечує оперативне інформування користувача про події, що відбуваються в системі (рис. 3.6).

На початковому етапі створюється об’єкт класу WiFiClientSecure, який використовується для встановлення захищеного з’єднання з сервером. Виклик методу setInsecure() дозволяє спростити процес встановлення TLS-з’єднання шляхом ігнорування перевірки сертифіката сервера, що є допустимим для вбудованих систем із обмеженими ресурсами, хоча й знижує рівень криптографічної безпеки.

```
void sendPhotoTelegram() {
  WiFiClientSecure client;
  client.setInsecure();
  camera_fb_t * fb = esp_camera_fb_get();
  if (!fb) return;
  if (client.connect("api.telegram.org", 443)) {
    String head = "--123\r\nContent-Disposition: form-data;
                  name=\"chat_id\";\r\n\r\n" + chatID + "\r\n";
    String tail = "\r\n--123--\r\n";
    client.println("POST /bot" + botToken + "/sendPhoto HTTP/1.1");
    client.println("Host: api.telegram.org");
    client.println("Content-Type: multipart/form-data; boundary=123");
    client.print("Content-Length: ");
    client.println(head.length() + fb->len + tail.length());
    client.println();
    client.print(head);
    client.write(fb->buf, fb->len);
    client.print(tail);
  }
  esp_camera_fb_return(fb);
}
```

Рисунок 3.6 – Лістинг коду функції sendPhotoTelegram()

Далі здійснюється отримання поточного кадру з камери за допомогою функції esp_camera_fb_get(). У разі невдалого отримання зображення підпрограма завершує виконання, що запобігає виникненню помилок при передачі даних. Отриманий буфер містить JPEG-зображення, готове до передавання мережею.

Наступним кроком є встановлення з’єднання з сервером Telegram через порт 443, який використовується для HTTPS-трафіку. У разі успішного підключення формується HTTP POST-запит із типом вмісту multipart/form-data, що дозволяє передавати бінарні дані зображення. Заголовок запиту містить службову інформацію, включаючи ідентифікатор чату (chat_id), у який буде надіслано повідомлення.

Формування тіла запиту здійснюється шляхом конкатенації трьох частин: заголовка (head), безпосередньо бінарних даних зображення (fb->buf) та завершальної частини (tail). При цьому обчислюється загальна довжина повідомлення, яка передається у полі Content-Length. Після цього дані послідовно передаються на сервер за допомогою методів print() і write().

Після завершення передачі обов'язково виконується виклик esp_camera_fb_return(fb), який звільняє буфер кадру та забезпечує стабільну роботу камери в подальшому. Відсутність цього виклику могла б призвести до витоку пам'яті та збоїв у роботі системи.

3.2.5 Реалізація потокової відеотрансляції через вебсервер

Підпрограма handleStream() призначена для організації передачі відеопотоку з камери мікроконтролера клієнтському пристрою через локальний вебсервер. Вона реалізує механізм потокової трансляції у форматі MJPEG, що дозволяє відображати послідовність кадрів у браузері в реальному часі без необхідності складної обробки відео (рис. 3.7).

```
void handleStream() {
  WiFiClient client = server.client();
  server.sendContent("HTTP/1.1 200 OK\r\n");
  server.sendContent("Content-Type: multipart/x-mixed-replace;
                      boundary=frame\r\n\r\n");
  while (client.connected()) {
    camera_fb_t * fb = esp_camera_fb_get();
    server.sendContent("--frame\r\n");
    server.sendContent("Content-Type: image/jpeg\r\n\r\n");
    client.write(fb->buf, fb->len);
    server.sendContent("\r\n");
    esp_camera_fb_return(fb);
  }
}
```

Рисунок 3.7 – Лістинг коду функції handleStream()

На початку виконання підпрограми формується об'єкт клієнта WiFiClient, який представляє активне підключення користувача до вебсерверу. Далі сервер надсилає HTTP-відповідь із кодом успішного запиту (200 OK) та заголовок Content-Type, який визначає тип переданих даних як multipart/x-mixed-replace. Даний формат дозволяє передавати безперервний потік окремих JPEG-зображень, розділених спеціальними маркерами (boundary), що інтерпретуються браузером як відео.

Основна логіка підпрограми реалізована у циклі, який виконується доти, доки клієнт залишається підключеним до сервера. У кожній ітерації циклу відбувається отримання поточного кадру з камери за допомогою функції esp_camera_fb_get(). Отриманий буфер містить JPEG-зображення, яке буде передано клієнту.

Після отримання кадру сервер формує службову частину відповіді, яка включає розділювач кадрів (--frame) та заголовок із зазначенням типу даних (image/jpeg). Далі бінарні дані зображення передаються безпосередньо клієнту за допомогою методу client.write(fb->buf, fb->len). Після цього додається символ переходу на новий рядок, що сигналізує про завершення поточного кадру.

Обов'язковим етапом є виклик функції esp_camera_fb_return(fb), яка звільняє буфер кадру та повертає його у пул пам'яті. Це забезпечує безперервну роботу камери та запобігає переповненню оперативної пам'яті мікроконтролера.

3.2.6 Реалізація керування доступом та дистанційного відкриття дверей

У даній системі реалізовано функціональність відкриття дверей, а також забезпечено можливість дистанційного керування доступом через хмарну IoT-платформу Blynk. Основною підпрограмою є openDoor(), яка виконує комплекс дій у відповідь на подію доступу незалежно від її джерела (рис. 3.8).

```
void openDoor(String source) {
  digitalWrite(RELAY, HIGH);
  recordEvent(source);
  sendPhotoTelegram();
  Blynk.virtualWrite(V0, "Door opened: " + source);
  delay(3000);
  digitalWrite(RELAY, LOW);
}

// ===== Blynk remote =====
BLYNK_WRITE(V10) {
  if (param.asInt()) openDoor("remote");
}
```

Рисунок 3.8 – Лістинг коду для віддаленого відкриття дверей

На початку виконання підпрограми формується керуючий сигнал для реле шляхом встановлення високого логічного рівня на відповідному виводі. Це призводить до активації електромагнітного замка та фізичного відкриття дверей. Параметр source, який передається у функцію, використовується для ідентифікації джерела події, наприклад RFID-авторизація, натискання кнопки виходу або дистанційна команда.

Після відкриття дверей викликається підпрограма recordEvent(), яка забезпечує відеофіксацію події шляхом збереження серії кадрів на карту пам’яті. Додатково виконується виклик sendPhotoTelegram(), що дозволяє миттєво передати зображення користувачу через месенджер, підвищуючи рівень інформованості та безпеки.

Наступним етапом є передача інформації про подію у хмарну платформу за допомогою функції Blynk.virtualWrite(). Це дозволяє відобразити відповідне повідомлення у мобільному додатку та вести журнал подій у реальному часі. Таким чином користувач отримує чітке розуміння того, яким саме способом було відкрито двері.

Після виконання основних дій реалізовано затримку тривалістю 3 секунди, протягом якої замок залишається відкритим, що забезпечує достатній час для проходу користувача. По завершенні цього інтервалу подається сигнал на вимкнення реле, що призводить до повернення замка у закритий стан.

Додатково у наведеному коді реалізовано обробник подій платформи Blynk — BLYNK_WRITE(). Даний механізм забезпечує прийом команд від користувача через мобільний додаток. У разі, якщо значення віртуального піна V10 є активним, викликається підпрограма openDoor("remote"), що ініціює відкриття дверей у дистанційному режимі.

Наведений фрагмент коду реалізує централізований механізм керування доступом із підтримкою локальних і віддалених сценаріїв. Поєднання фізичного керування, відеофіксації та інтеграції з хмарними сервісами забезпечує високий рівень функціональності та безпеки розробленої системи.

3.3 Налаштування хмарної IoT платформи Blynk

У межах реалізації системи відеомоніторингу вхідної зони приміщення було виконано налаштування хмарної IoT-платформи Blynk для забезпечення віддаленого моніторингу та керування системою. Налаштування виконувалося з урахуванням необхідності інтеграції з мікроконтролерною платформою ESP32-CAM, передачі подій у реальному часі, а також забезпечення можливості віддаленого доступу до відеопотоку та керування електромагнітним замком.

На початковому етапі було створено новий проєкт у середовищі Blynk із використанням шаблонного підходу (Template). У параметрах шаблону було задано тип пристрою (ESP32), а також визначено набір віртуальних каналів, які використовувалися для обміну даними між пристроєм та хмарною платформою. Для кожного функціонального елемента системи було виділено окремий віртуальний пін: для відображення статусу доступу (V0), сигналу виклику (V1), передачі посилання на відеострім (V2), повідомлення про стан дверей (V3), а також для дистанційного керування замком (V10). Така структура дозволила розділити функціональні потоки даних і спростити подальшу інтеграцію (рис. 3.9).

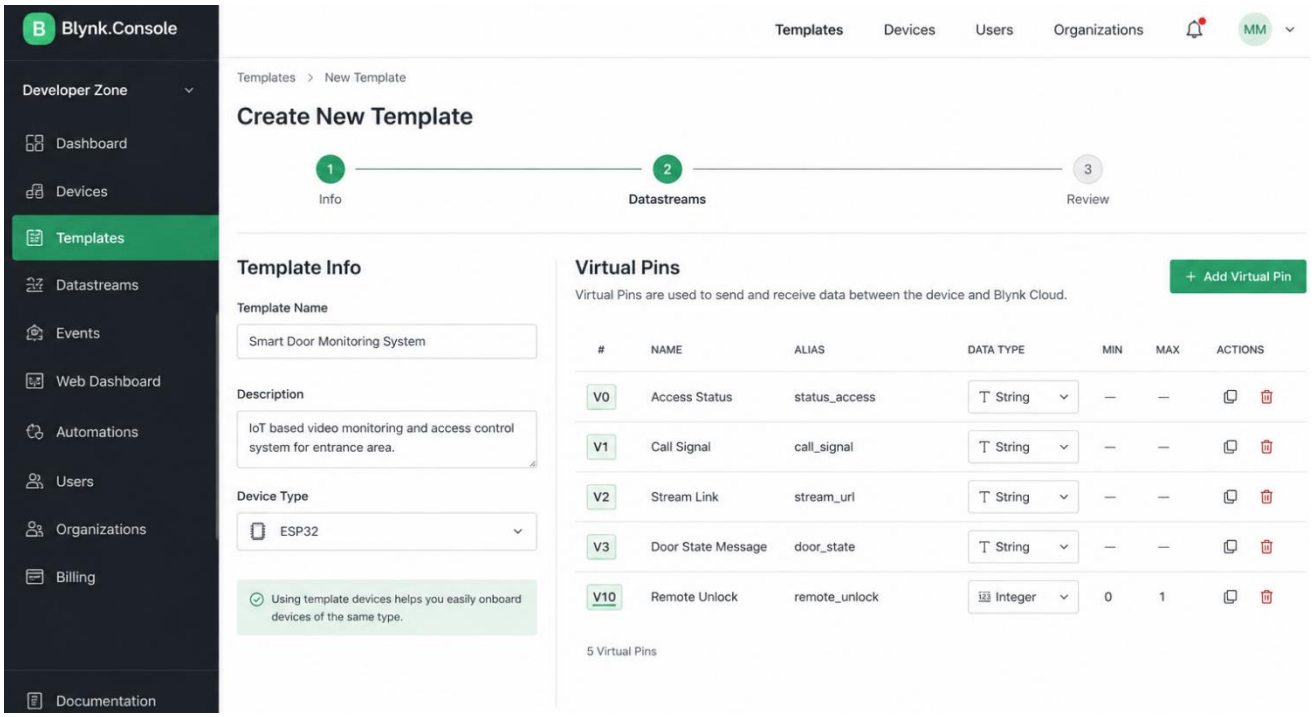

Рисунок 3.9 – Процес створення віртуальних пінів в Blynk

Далі було виконано налаштування інформаційної панелі (Dashboard) у мобільному додатку Blynk. Для відображення стану системи було додано текстові та індикаторні віджети, які відображали події доступу, спроби несанкціонованого входу та стан дверей. Для реалізації функції виклику було використано віджет сповіщень, який активувався при натисканні відповідної кнопки на пристрої. Окремо було додано віджет для відображення URL-адреси відеопотоку, який формувався мікроконтролером у вигляді посилання на локальний вебсервер (MJPEG-стрім). Це дозволило користувачу переходити за посиланням та переглядати відео в режимі реального часу.

Для реалізації дистанційного керування електромагнітним замком було налаштовано кнопку (Button), прив'язану до віртуального піна V10. Кнопка працювала у режимі перемикача (switch), що дозволяло надсилати команду на відкриття дверей безпосередньо з мобільного додатку. У програмному коді мікроконтролера було реалізовано обробку цієї команди через функцію BLYNK_WRITE, що забезпечувало негайну реакцію системи на дії користувача.

Особливу увагу було приділено налаштуванню системи сповіщень. У середовищі Blynk було активовано механізм push-повідомлень, які надсилалися у випадках: натискання кнопки виклику, спроби несанкціонованого доступу, тривалого перебування дверей у відкритому стані, а також при кожному успішному відкритті дверей. Це забезпечило оперативне інформування користувача про всі критичні події в системі.

Інтеграція з відеофункціоналом була реалізована шляхом передачі у Blynk текстового повідомлення з посиланням на локальний вебсервер ESP32-CAM, який забезпечував трансляцію MJPEG-потоку. При виникненні події виклику або доступу система формувала відповідне повідомлення та передавала IP-адресу пристрою разом із шляхом до стріму. Таким чином користувач отримував можливість оперативно переглянути відео з камери у браузері.

Додатково було реалізовано взаємодію з іншими сервісами через Blynk шляхом передачі інформаційних повідомлень, що дублювалися у месенджері Telegram. Це підвищило надійність системи оповіщення та дозволило зберігати фотодокази подій поза межами самої IoT-платформи.

3.4 Моделювання та тестування системи

На першому етапі дослідження було виконано моделювання розроблюваної системи відеомоніторингу вхідної зони приміщення в середовищі Cirkit Designer, що дозволило перевірити коректність електричної принципової схеми та логіку взаємодії компонентів без необхідності негайного створення фізичного прототипу. У процесі моделювання було сформовано віртуальну схему, яка включала мікроконтролерну платформу ESP32-CAM, RFID-модуль MFRC522, модуль реле, герконовий давач, кнопки керування та допоміжні елементи. Особливу увагу було приділено правильності підключення інтерфейсу SPI для RFID-модуля, а також узгодженню рівнів сигналів і живлення для всіх компонентів (рис. 3.10).

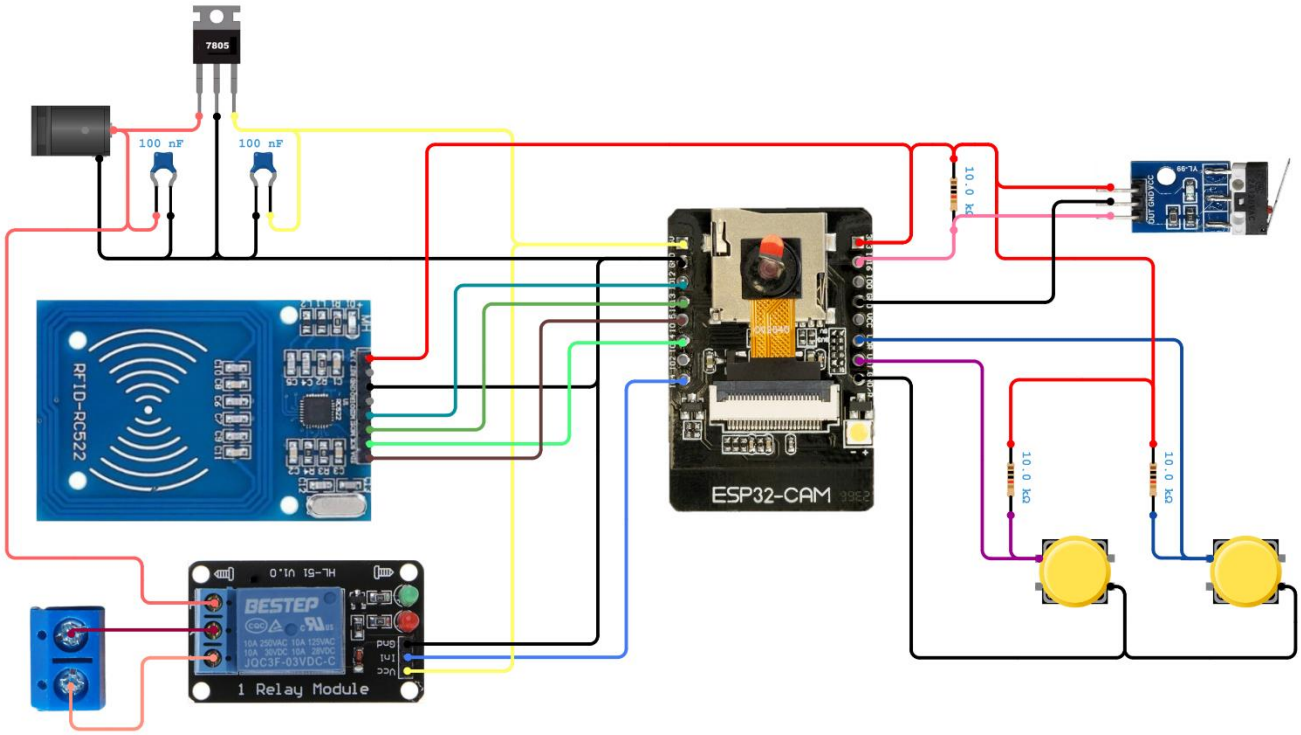

Рисунок 3.10 – Модель системи відеомоніторингу вхідної зони приміщення

У середовищі моделювання було реалізовано базову логіку роботи системи, що включала ідентифікацію користувача за RFID-карткою, керування реле та обробку сигналів від датчиків і кнопок. Проведене моделювання дозволило перевірити правильність роботи алгоритму обробки подій, зокрема сценарії

успішної та неуспішної авторизації, реакцію системи на натискання кнопки виходу та кнопки виклику, а також контроль стану дверей. У результаті було встановлено, що обрана структура системи забезпечує коректну взаємодію всіх компонентів, а затримки в обробці сигналів знаходяться в допустимих межах.

Після завершення етапу моделювання було виконано перехід до створення фізичного прототипу системи. На цьому етапі здійснювалося поетапне підключення всіх апаратних компонентів відповідно до розробленої електричної схеми. Спочатку було реалізовано базове підключення ESP32-CAM із налаштуванням живлення та перевіркою працездатності мікроконтролера і камери. Було перевірено коректність ініціалізації камери та можливість отримання зображень, а також стабільність роботи при підключенні до бездротової мережі Wi-Fi.

На наступному етапі було підключено RFID-модуль MFRC522. Проведено тестування зчитування ідентифікаторів RFID-карток, у ході якого підтверджено коректність обміну даними між модулем і мікроконтролером. Було перевірено стабільність роботи при багаторазових спробах зчитування, а також відсутність конфліктів із іншими периферійними пристроями.

Далі було інтегровано релейний модуль та електромагнітний замок. У процесі тестування перевірено правильність формування керуючих сигналів, а також швидкодію системи при відкритті та закритті замка. Встановлено, що затримка між підтвердженням доступу та розблокуванням замка є мінімальною та не перевищує часток секунди, що забезпечує комфортне використання системи.

Окремо було проведено тестування магнітного герконового давача МС-38, який використовується для контролю стану дверей. У ході випробувань перевірено коректність визначення станів «відкрито» та «закрито», а також реакцію системи на тривале перебування дверей у відкритому стані. Підтверджено, що система здатна своєчасно формувати відповідні повідомлення та передавати їх на IoT-платформу.

Наступним етапом стало тестування функціоналу кнопок виходу та виклику. При натисканні кнопки виходу система коректно виконувала розблокування замка

без необхідності використання RFID-картки. При натисканні кнопки виклику формувалося повідомлення для користувача, а також активувався відеопотік із камери, що дозволяло віддалено оцінити ситуацію перед наданням доступу.

Особливу увагу було приділено тестуванню функцій відеофіксації. Було перевірено роботу камери ESP32-CAM у режимі формування JPEG-кадрів, а також передачу відеопотоку через локальний вебсервер у форматі MJPEG. Додатково було реалізовано запис серії зображень на карту пам’яті microSD при виникненні подій доступу або виклику, що фактично дозволяє відтворити короткий відеофрагмент. Проведені випробування показали, що система стабільно зберігає послідовність кадрів без втрати даних.

Також було протестовано інтеграцію з IoT-платформою Blynk та Telegram. Перевірено коректність передачі повідомлень про події, отримання сповіщень у мобільному додатку, а також можливість дистанційного керування замком. Окремо було перевірено передачу посилання на відеопотік, що дозволяє користувачеві переглядати зображення з камери.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Аварії з викидом радіоактивних речовин

Найнебезпечнішими за наслідками є аварії на АЕС з викидом в атмосферу радіоактивних речовин, внаслідок яких має місце довгострокове радіоактивне забруднення місцевості на величезних площах.

На підприємствах атомної енергетики відбулися такі значні аварії:

− 1957 рік — аварія в Віндскейлі (Північна Англія) на заводі по виробництву плутонію (зона радіоактивного забруднення становила 500 км^2);

− 1957 рік — вибух сховища радіоактивних відходів біля Челябінська, СРСР (радіаційне забруднення переважно стронцієм-90 території, на якій мешкало 0,5 млн. осіб);

− 1961 рік — аварія на АЕС в Айдахо-Фолсі, США (в реакторі стався вибух);

− 1979 рік — аварія на АЕС «Тримайл-Айленд» у Гарисберзі, США (сталося зараження великих територій короткоживучими радіонуклідами, що призвело до необхідності евакуювати населення з прилеглої зони).

− 1986 рік — аварія на Чорнобильській АЕС;

− 2011 рік — аварія на Фукусімській АЕС.

Найбільша за масштабами забруднення навколишнього середовища аварія сталася 26 квітня 1986 р. Внаслідок грубих порушень правил експлуатації та помилкових дій персоналу 1986 рік став для людства роком вступу в епоху ядерної біди. Історія людства ще не знала такої аварії, яка була б настільки згубною за своїми наслідками для довкілля, здоров'я та життя людей. Радіаційне забруднення територій та водоймищ, міст та сіл, вплив радіонуклідів на мільйони людей, які тривало проживають на забруднених територіях, дозволяє назвати масштаби цієї катастрофи глобальними, а ситуацію — надзвичайною.

Грубі порушення правил експлуатації АЕС, скоєні персоналом ЧАЕС, полягали в наступному [32]:

- проведення експерименту будь-якою ціною, незважаючи на зміну стану реактора;
- вивід з роботи справного технологічного захисту, який просто зупинив би реактор ще до того як він потрапив би в небезпечний режим;
- замовчання масштабу аварії в перші дні керівництвом ЧАЕС.

У сучасному викладі, причини аварії такі:

- реактор був неправильно спроєктований і небезпечний;
- персонал не був проінформований про небезпеки;
- персонал допустив ряд помилок і ненавмисно порушив існуючі інструкції, частково через відсутність інформації про небезпеки реактора;
- відключення захисту або не вплинуло на розвиток аварії, або не суперечило нормативним документам.

В результаті аварії з сільськогосподарського користування було виведено близько 5 млн га земель, довкола АЕС створена 30-кілометрова зона відчуження, знищені і поховані (закопані важкою технікою) сотні дрібних населених пунктів.

Перед аварією в реакторі четвертого блоку знаходилося 180–190 тон ядерного палива (діоксиду урану). За оцінками, які в наш час вважаються найбільш достовірними, в навколишнє середовище було викинуто від 5 до 30 % від цієї кількості. Деякі дослідники ставлять під сумнів ці дані, посилаючись на наявні фотографії і спостереження очевидців, які показують, що реактор практично порожній. Слід, проте, враховувати, що об'єм 180 тон діоксиду урану становить лише незначну частину від об'єму реактора. Реактор в основному був заповнений графітом, вважається, що він згорів в перші дні після аварії [32].

Ґрінпіс і міжнародна організація «Лікарі проти ядерної війни» стверджують, що в результаті аварії лише серед ліквідаторів померли десятки тисяч чоловік, в Європі зафіксовано 10 000 випадків вроджених патологій в новонароджених, 10 000 випадків раку щитоподібної залози і очікується ще 50 тисяч. За даними організації Союз «Чорнобиль», з 600 000 ліквідаторів 10 % померло і 165 000 стало інвалідами.

Кількість постраждалих від Чорнобильської аварії можна визначити лише приблизно. Окрім загиблих працівників АЕС і пожежників, до них слід віднести хворих військовослужбовців і цивільних осіб, що брали участь в ліквідації наслідків аварії, і мешканців районів, що піддалися радіоактивному забрудненню. Визначення того, яка частина захворювань з'явилася наслідком аварії — вельми складне завдання для медицини і статистики. Вважається, що більша частина смертельних випадків, пов'язаних з дією радіації, була або буде викликана онкологічними захворюваннями.

2011 рік — аварія на Фукусімській АЕС. У результаті найсильнішого в історії Японії землетрусу силою 8,8 балів за шкалою Ріхтера, що стався 11 березня 2011 р. на північно-східному узбережжі Японії і викликаного ним цунамі на першому блоці атомної електростанції [32].

«Фукусіма-1» стався вибух, що привів до руйнування залізобетонної оболонки реактора і викиду в атмосферу радіоактивних речовин. Це привело до загибелі 5178 людей і зникнення безвісті 8606 осіб як безпосередньо від руйнувань, так і викликаного ним цунамі висотою до 12 метрів. Близько 100300 будинків у країні були зруйновані стихією повністю або частково.

З 15 по 18 березня вибухи відбулися ще на двох блоках, 3-й та 4-й енергоблоки охопила пожежа, що привело до викиду радіоактивних речовин у атмосферу. До 27 березня на чотирьох постраждалих енергоблоках вдалось відновити роботу приладів управління і деякі робочі функції. 4 квітня для вирішення завдання екстреного відкачування високо радіоактивної води з підземних споруд енергоблоків було здійснене скидання у море приблизно 10 000 тон радіоактивно зараженої води.

11 квітня стався 7-бальний землетрус, але ніхто з ліквідаторів не постраждав і всі аварійні операції були продовжені. З 17 квітня почалось спорудження системи з насосів, що відкачували б забруднену воду з підземних споруд, а також фільтрів, установлених зовні енергоблоків, для очищення води і теплообмінників для її охолодження.

У середині грудня всі проблемні реактори АЕС були приведені в стан холодної зупинки. Ситуацію на АЕС «Фукусіма-1» вдалося стабілізувати. Наступний, більш складний, етап ліквідації наслідків аварії – витяг розплавленого ядерного палива з реакторів – японські фахівці почнуть проводити не раніше, ніж через 10 років.

4.2 Розробка захисту від пожеж та вибухів в системах опалення, вентиляції, освітлення та кондиціонування повітря

Перед початком опалювального сезону теплові мережі, які розміщені у приміщеннях, калориферні й теплогенераторні установки, котельні, печі та інші опалювальні прилади повинні бути перевірені й відремонтовані. Несправні опалювальні прилади не повинні допускатися до експлуатації.

Гарячі поверхні тепломереж, що розташовані у приміщеннях, у яких вони можуть створити небезпеку спалахування парів, газів, пилу або аерозолів, потрібно ізолювати таким способом, щоб температура на поверхні теплоізольованої конструкції була не менш ніж на 20 % нижчою за температуру самоспалахування речовин [33].

Усі гарячі ділянки поверхонь трубопроводів і обладнання, яке розташоване в зоні можливого потрапляння на них вибухонебезпечних, горючих або легкозаймистих речовин, необхідно покрити металевою обшивкою. Не дозволяється експлуатація теплових мереж з просоченою вибухонебезпечними, горючими або легкозаймистими речовинами теплоізоляцією. Очищення печей та димоходів від сажі необхідно проводити перед початком, а також впродовж усього опалювального сезону, а саме [33]:

– кухонних кип’ятильників та плит – один раз на місяць;

– печей безперервної дії – не рідше одного разу на два місяці;

– опалювальних печей періодичної дії на рідкому та твердому паливі – не рідше одного разу на три місяці.

У приміщеннях котелень та інших теплогенеруючих установок населених пунктів і підприємств забороняється [33]:

– сушити взуття, спецодяг та інші матеріали на паропроводах та котлах;

– працювати при відключених або зіпсованих приладах регулювання і контролю, а також за їх відсутності;

– розпалювати установки без їх попередньої продувки;

– подавати паливо, коли газові пальники або форсунки згасли;

– експлуатувати установки у випадку витікання газу із системи паливоподачі або підтікання рідкого палива;

– допускати до роботи працівників, які не пройшли навчання з пожежно-технічного мінімуму та не отримали відповідних кваліфікаційних посвідчень, а також залишати без догляду працюючі нагрівники і котли.

Забороняється вносити зміни до елементів системи кондиціонування, вентиляції повітря і опалення, які перешкоджають поширенню пожежі. Не дозволяється робота технологічного обладнання у пожежонебезпечних та вибухопожежонебезпечних приміщеннях при відключених або несправних сухих фільтрах, гідрофільтрах, пиловловлювальних, пиловсмоктувальних та інших приладах вентиляційних систем.

Усі металеві фільтри, трубопроводи, повітроводи та інше обладнання витяжних установок, які транспортують вибухонебезпечні та горючі речовини, повинні бути захищені від статичної електрики та заземлені, а також мати пристрої для очищення.

При розміщенні вибухозахищених вентиляторів за межами приміщень для них необхідно влаштовувати спеціальне укриття з негорючих матеріалів. Під час експлуатації вентиляційних систем забороняється [34]:

– експлуатувати переповнені циклони;

– видаляти за допомогою однієї системи відсосів пил, пару, різні гази та інші речовини, які при змішуванні можуть викликати вибух, горіння або спалахи;

– складувати впритул (на відстані менше половини метра) до устаткування і повітроводів негорючі матеріали в горючій упаковці або горючі матеріали;

– застосовувати припливно-витяжні повітроводи й канали для відведення газів від кип'ятильників, газових колонок, приладів опалення та інших нагрівальних приладів;

– залишати двері вентиляційних камер відчиненими, зберігати в камерах різне устаткування та матеріали;

– знімати або відключати вогнезатримувальні пристрої;

– закривати решітки, отвори і витяжні канали.

Автономні моноблочні кондиціонери, а також автономні кондиціонери роздільного типу можна розміщувати у будівлях та приміщеннях різного призначення, крім приміщень, у яких не допускається рециркуляція. Зовнішні блоки автономних кондиціонерів роздільного типу потужністю по холоду до 12 кВт допускається розміщувати у критих переходах, відкритих сходових клітках, на незасклених лоджіях.

Холодильне обладнання з аміаковмісним холодоагентом можна використовувати при реконструкції для холодопостачання систем кондиціонування виробничих приміщень, розміщуючи обладнання в окремих прибудовах, будинках або окремих приміщеннях одноповерхових виробничих будинків. Випарники та конденсатори можна розміщувати на відкритих майданчиках на відстані не менше ніж два метри від стіни будівлі. Використання поверхневих повітроохолоджувачів з аміаковмісним холодоагентом не допускається.

Під час експлуатації калориферів потрібно дотримуватися таких вимог [34]:

– слідкувати за тим, щоб транзитні канали, через які подається нагріте в калорифері повітря, не мали отворів, крім каналів, призначених для подавання повітря у приміщення;

– систематично проводити гідравлічним або пневматичним способом очищення калориферів від забруднень;

– не допускати виникнення зазорів між калориферами, а також між будівельними і калориферними конструкціями камер, а виявлені зазори зашпаровувати негорючими матеріалами;

– тримати в справному стані контрольно-вимірювальні прилади;

– відстань між конструкціями з важкогорючих та горючих матеріалів і калориферами повинна бути не меншою за півтора метра за наявності електричного або вогневого підігріву і не меншою за 0,1 метр, коли теплоносієм є пара або вода.

Прокладання, підключення, монтаж мереж, влаштування електричного захисту на лініях, які живлять побутові кондиціонери, повинні виконуватись відповідно до вимог інструкції виробника. Лінії живлення до кожного побутового кондиціонера чи групи кондиціонерів потрібно забезпечувати автономним пристроєм електричного захисту незалежно від наявності захисту на загальній лінії, яка відповідає за живлення групи кондиціонерів.

Поперечний переріз електропровідників, які живлять одинично встановлені побутові кондиціонери, повинен відповідати допустимому навантаженню по струму, яке визначається паспортом на виріб. Зовнішній простір та стіни будинків навколо кондиціонерів повинні бути розчищені від витких рослин, гілок дерев та інших конструкцій і предметів із горючих матеріалів у радіусі не менше ніж півтора метра.

Під час експлуатації побутових кондиціонерів заборонено [34]:

– перетинати протипожежні перешкоди інженерними системами кондиціонера без влаштування проходок, які відповідають нормованій межі вогнестійкості протипожежної перешкоди;

– замінювати наявні триполюсні штепсельні роз'єднувачі на двополюсні;

– вносити в конструкцію кондиціонерів зміни, не передбачені заводом-виробником;

– використовувати в якості опорних конструкцій горючі елементи конструкцій рам замість монтажних кріплень заводського виготовлення або інших металевих конструкцій у випадку встановлення кондиціонера у віконному отворі.

Систему відеомоніторингу вхідної зони приміщення на основі IoT-технологій розроблено з дотриманням вимог щодо захисту від пожеж та вибухів в системах опалення, вентиляції, освітлення та кондиціонування повітря.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було розроблено комп’ютеризовану систему відеомоніторингу вхідної зони приміщення на основі IoT-технологій.

У ході роботи було проаналізовано сучасні підходи до побудови систем відеомоніторингу та обґрунтовано вибір апаратно-програмної платформи ESP32-CAM як базового елемента системи, що забезпечує поєднання функцій обробки даних, бездротового зв’язку та відеозахоплення.

Розроблено структурну та електричну принципову схеми системи, у яких передбачено інтеграцію RFID-модуля, керування електромагнітним замком, давача стану дверей, кнопок керування та підсистеми відеофіксації, що забезпечує комплексну реалізацію функцій доступу.

Розроблено алгоритм роботи системи, який охоплює процеси ідентифікації користувачів, обробки подій, керування виконавчими пристроями, формування відеоданих та їх передавання на віддалені сервіси.

У програмній частині реалізовано прошивку мікроконтролера з підтримкою взаємодії з IoT-платформою Blynk, організовано відеопотік, запис серії кадрів на карту пам’яті та інтеграцію з сервісом Telegram для надсилання сповіщень і зображень.

Проведено моделювання системи в середовищі Cirkit Designer, що дозволило перевірити коректність схеми та алгоритмів роботи до етапу фізичної реалізації.

Створено та протестовано фізичний прототип системи, у ході чого підтверджено стабільність роботи всіх компонентів, коректність ідентифікації користувачів, надійність керування замком і ефективність відеофіксації подій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зубко І., Купрій В. Автоматизовані системи контролю доступу на основі біометричних даних. In The 13th International scientific and practical conference “Implementation of modern technologies in science”. Varna, Bulgaria. International Science Group. 2022. P. 514-515.
2. Sadique M.F., Alam K.M. Enhancing security measures in student housing through advanced access control systems. Khulna University Studies, 2024. P. 238-254.
3. Dragonas E., Lambrinoudakis C., Kotsis M. IoT forensics: Exploiting unexplored log records from the HIKVISION file system. Journal of Forensic Sciences, 2023. 68(6). P. 2002-2011.
4. Чашницька Т.Г. Аналіз зарубіжного досвіду у сфері використання систем відеоспостереження. Нове українське право, 2022 (2). P. 207-214.
5. Жаровський Р.О., Луцик Н.С., Осухівська Г.М., Паламар А.М., Тиш Є.В. Методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 123 «Комп’ютерна інженерія» усіх форм навчання. Тернопіль: ТНТУ, 2024. 39 с.
6. Лупенко С.А., Пасічник В.В., Тиш Є.В. Комп’ютерна логіка. Навчальний посібник. Львів: Видавництво «Магнолія 2006», 2024. 354 с.
7. Буров Є., Митник М. Комп’ютерні мережі. (у 2-х томах). Львів, Магнолія, 2018. 740 с.
8. Лупенко С.А., Луцик Н.С., Лупенко А.М., Стадник Н.Б. Лінійний циклічний випадковий процес як математична модель тестових коливних сигналів у інформаційних системах діагностики, аутентифікації та прогнозування. Вісник Національного університету Львівська політехніка. Інформаційні системи та мережі, 2014 (783), С. 145-153.
9. Yatsyshyn V., Pastukh O., Kukharska V., Palamar A., Kulikov S. Method and tool of detecting software architecture patterns in the process of computer systems development. CEUR Workshop Proceedings, 4th International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2024), Ternopil, Ukraine, Opole, Poland, October 23-25, 2024. Vol. 3896. P. 12-24.

10. Лупенко С.А., Литвиненко Я.В., Осухівська Г.М., Стадник Н.Б., Сверстюк А.С. Модифікація програмного комплексу для автоматизованого визначення морфологічних та ритмічних діагностичних ознак за електрокардіосигналами. Вісник Хмельницького національного університету. Технічні науки, 2020 (1), С. 137-146.

11. Palamar M., Nakonetchnyi Y., Palamar A., Strembitskyi M., Apostol Y. Modernization of the azimuth drive design for the antenna system. Scientific Journal of TNTU, Ternopil, Ukraine, 2025. Vol. 117, No 1, P. 54–61.

12. Palamar M., Yavorska M., Palamar A., Strembitskyi M. Modeling and Research of Satellite Antenna Adjustment Process for Earth Remote Sensing. 2022 IEEE 2nd Ukrainian Microwave Week, Kharkiv, Ukraine, November 14-18, 2022. P. 317-320.

13. Strembitskyi M., Yavorska M., Palamar A., Kochan R., Yeromenko V. A comparative study of bug algorithms for robot navigation. CEUR Workshop Proceedings, 3rd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2025), Ternopil, Ukraine, June 11-12, 2025. Vol. 4057 P. 312-321.

14. Palamar A., Voloskyi V., Kramar O., Kramar T., Stankevych O., Yatsyshyn V. Information computer system with a virtual tour for cultural heritage preservation of the Zbarazh Castle Museum's exhibition hall. CEUR Workshop Proceedings, The 3rd International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA 2024), Lviv, Ukraine, October 31, 2024. Vol. 3851.

15. Романов Д.В., Осухівська Г.М., Паламар А.М. Система управління зовнішнім освітленням на основі Інтернету речей. Актуальні задачі сучасних технологій : збірник тез доповідей X міжнародної науково-практичної конференції молодих учених та студентів (Тернопіль, 24-25 листопада 2021 року), Тернопіль: ТНТУ, 2021. С. 120.

16. Palamar A., Pettai E. Microgrid for the Department of Electrical Drives and Power Electronics. 8th International Symposium "Topical Problems in the Field of Electrical and Power Engineering" and "Doctoral School of Energy and Geotechnology II" (January 11-16, 2010), Pärnu, Estonia, 2010. P. 54-61.

17. Palamar A. Methods and means of increasing the reliability of computerized modular uninterruptible power supply system. Scientific Journal of TNTU, Ternopil, Ukraine, 2020. Vol. 99, No 3. P. 133–141.

18. Оконський М.В., Лупенко С.А., Паламар А.М. Інформаційно-вимірювальна система для контролю метеорологічних параметрів на основі Інтернету речей. Матеріали IX науково-технічної конференції "Інформаційні моделі, системи та технології" Тернопільського національного технічного університету імені Івана Пулюя (Тернопіль, 8–9 грудня 2021 року), Тернопіль: ТНТУ, 2021. С. 118.

19. Palamar A., Stadnyk M., Palamar M. Adaptive PID regulation method of uninterruptible power supply battery charge current based on artificial neural network. Scientific Journal of TNTU, Ternopil, Ukraine, 2022. Vol. 107, No 3. P. 5–13.

20. Оконський М.В., Лупенко С.А., Паламар А.М. Комп'ютерна система для моніторингу метеорологічних параметрів на основі IoT. Актуальні задачі сучасних технологій : збірник тез доповідей X міжнародної науково-практичної конференції молодих учених та студентів (Тернопіль, 24–25 листопада 2021 року), Тернопіль: ТНТУ, 2021. С. 112.

21. Palamar M., Horyn T., Palamar A., Batuk V. Method of calibration MEMS accelerometer and magnetometer for increasing the accuracy determination angular orientation of satellite antenna reflector. Scientific Journal of TNTU, Ternopil, Ukraine, 2022. Vol. 108, No 4. P. 79–88.

22. Palamar M., Pasternak Y., Palamar A., Poikhalo A. Precision tracking of the trajectory LEO satellite by antenna with induction motors in the control system. Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2017), Bucharest, Romania, September 21–23, 2017. Vol. 2. P. 1051–1055.

23. Паламар М., Пастернак Ю., Паламар А. Дослідження динамічних похибок системи прецизійного керування антеною з асинхронним електроприводом. Вісник ТНТУ, Тернопіль: ТНТУ, 2014. Вип. 76, № 4. С. 164–173.

24. Palamar A., Karpinskyy M. Control of an Uninterruptible Power Supply in a DC Microgrid System. 10th International Symposium Symposium "Topical Problems in the Field of Electrical and Power Engineering" and "Doctoral School of Energy and Geotechnology II" (January 10-15, 2011), Pärnu, Estonia, 2011. P. 80-84.

25. Stadnyk M., Palamar A. Project management features in the cybersecurity area. Scientific Journal of TNTU, Ternopil, Ukraine, 2022. Vol. 106, No 2. P. 54–62.

26. Voloskyi V., Leshchyshyn Y., Romanyshyn N., Palamar A., Tarasenko L. Method and algorithm for efficient cell balancing in the lithium-ion battery control system. CEUR Workshop Proceedings, The 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024), Zboriv, Ukraine, October 02-04, 2024. Vol. 3842. P. 258-267.

27. Palamar A., Karpinskyy M., Vodovozov V. Design and Implementation of a Digital Control and Monitoring System for an AC/DC UPS. 7th International Conference-Workshop «Compatibility and Power Electronics» (CPE 2011), June 1-3, 2011. P. 173–177.

28. Palamar A., Palamar M. Fire Safety Monitoring System Based on Internet of Things. CEUR Workshop Proceedings, 2023. 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), Ternopil, Ukraine, June 14-16, 2023. Vol. 3468. P. 164-172.

29. Погребенник В.Д., Клим Г.І., Бордун І.М., Пташник В.В., Паламар А.М. Системи оперативного контролю інтегральних параметрів водного середовища. Т. 2. Елементи комп'ютерних систем оперативного контролю: колективна монографія. Житомир: Видавничий дім «Бук-Друк», 2021. 180 с.

30. Voloshchuk A., Velychko D., Osukhivska H., Palamar A. Computer system for energy distribution in conditions of electricity shortage using artificial intelligence. CEUR Workshop Proceedings, 2nd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2024), Ternopil, Ukraine, June 12-14, 2024. Vol. 3742 P. 66-75.

31. Palamar A. Control system simulation by modular uninterruptible power supply unit with adaptive regulation function. Scientific Journal of TNTU, Ternopil, Ukraine, 2020. Vol. 98, No 2. P. 129–136.

32. Сокуренко В.В., Бандурка О.М. Безпека життєдіяльності та охорона праці : підруч. Харків : ХНУВС, 2021. 308 с.

33. Мохняк С.М. Безпека життєдіяльності. Навчальний посібник. Львів: вид. НУ „Львівська політехніка", 2009. 264 с.

34. Гандзюк М.П., Желібо Є.П., Халімовський М.О. Основи охорони праці. К.: Каравела, 2007. 408 с.

Додаток А

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Кафедра комп’ютерних систем та мереж

«ЗАТВЕРДЖУЮ»
Завідувач кафедрою КС
_____ Осухівська Г.М.
“ 2 ” лютого 2026 р.

КОМП’ЮТЕРИЗОВАНА СИСТЕМА ВІДЕОМОНІТОРИНГУ ВХІДНОЇ ЗОНИ ПРИМІЩЕННЯ НА ОСНОВІ ІОТ-ТЕХНОЛОГІЙ

ТЕХНІЧНЕ ЗАВДАННЯ

на 8 листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

«УЗГОДЖЕНО»
Керівник кваліфікаційної роботи
_____ к.т.н. Стадник Н.Б.
“ 2 ” лютого 2026 р.

«ВИКОНАВЕЦЬ»
Студент групи СІ–41
_____ Бойко П.П.
“ 2 ” лютого 2026 р.

Тернопіль 2026

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи бакалавра: «Комп’ютеризована система відеомоніторингу вхідної зони приміщення на основі IoT-технологій».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.146.00.00.

1.2 Виконавець

Студент групи СІ-41, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Бойко Павло Павлович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи бакалавра є наказ по університету № 4/9-188 від «24» квітня 2026 року.

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи бакалавра – 26.01.2026 р.

Плановий термін завершення виконання кваліфікаційної роботи бакалавра – 21.06.2026 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Оформлення технічної документації до кваліфікаційної роботи бакалавра здійснюється згідно діючих вимог вітчизняних та міжнародних стандартів. Технічна документація до кваліфікаційної роботи бакалавра включає в себе текст пояснювальної записки та креслення, які максимально інформативно та стисло відображають основні результати розробки комп’ютеризованої системи відеомоніторингу вхідної зони приміщення на основі IoT-технологій. Основними регламентними документами при оформленні та пред’явлені результатів проєктування є групи діючих стандартів ДСТУ, ISO, ЄСКД та ЕСПД. Пред’явлення результатів кваліфікаційної роботи бакалавра відбувається шляхом захисту роботи на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Комп’ютеризована система відеомоніторингу вхідної зони приміщення призначена для автоматизованого обмеження та контролю доступу осіб до об’єктів різного призначення. Система забезпечує ідентифікацію користувачів, керування виконавчими механізмами доступу, відеофіксацію подій, збереження та передавання даних на віддалений сервер або IoT-платформу.

Система може застосовуватися у житлових будинках, офісних приміщеннях, навчальних закладах, складських та виробничих об’єктах, де існує потреба в підвищенні рівня безпеки та централізованому контролі доступу.

2.2 Мета створення системи

Метою створення системи є розробка ефективного апаратно-програмного комплексу, який забезпечує дистанційний контроль доступу до приміщення з можливістю відеофіксації подій та інтеграції з IoT-інфраструктурою. Реалізація системи повинна забезпечити підвищення рівня безпеки, зменшення впливу людського фактору та можливість віддаленого моніторингу і керування.

2.3 Характеристика об'єкту

Об’єктом автоматизації є приміщення з контрольованими точками доступу, оснащене електромеханічними або електромагнітними замками, пристроями ідентифікації користувачів та засобами відеоспостереження. Об’єкт може мати обмежений або відкритий доступ до мережі Інтернет, а умови експлуатації передбачають безперервну або періодичну роботу системи.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Система повинна функціонувати як єдиний апаратно-програмний комплекс, що забезпечує безперервний контроль доступу, збір і передавання даних, відеофіксацію подій та віддалене керування. Робота системи повинна бути стабільною, безпечною та відповідати вимогам інформаційної безпеки.

3.1.1 Вимоги до структури та функціонування системи

Структурно система повинна складатися з таких основних компонентів:

- мікроконтролерного вузла керування;
- модулів ідентифікації користувачів;

– відеомодуля для фіксації подій;
– виконавчих пристроїв керування доступом;
– засобів зв’язку з IoT-платформою.

Функціонування системи має ґрунтуватися на обробці подій доступу в реальному часі з можливістю локального та віддаленого керування.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Обмін даними між компонентами системи повинен здійснюватися з використанням стандартних цифрових інтерфейсів та протоколів зв’язку. Для віддаленого передавання даних доцільно використовувати бездротові технології зв’язку з підтримкою мережі Інтернет. Передавання інформації повинно бути захищеним від несанкціонованого доступу.

3.1.3 Вимоги до режимів функціонування системи

Система повинна підтримувати такі режими роботи:
– автоматичний режим відеомоніторингу вхідної зони приміщення;
– ручний режим керування;
– аварійний режим у разі збоїв або втрати зв’язку;
– режим технічного обслуговування та налаштування.

Перемикання між режимами має здійснюватися програмно або через інтерфейс керування.

3.1.4 Перспективи розвитку та модернізації системи

Архітектура системи повинна передбачати можливість подальшої модернізації, зокрема:
– розширення кількості точок доступу;
– підключення додаткових давачів і камер;

- інтеграцію з іншими системами безпеки;
- оновлення програмного забезпечення без заміни апаратної частини.

3.1.5 Вимоги до надійності системи

Система повинна забезпечувати безперервну роботу протягом заданого часу експлуатації. У разі виникнення збоїв повинні застосовуватися механізми відновлення працездатності та збереження даних. Компоненти системи повинні мати достатній рівень відмовостійкості.

Показники надійності системи відеомоніторингу вхідної зони приміщення на основі IoT-технологій повинні відповідати вимогам ДСТУ 50136-1. Ймовірність безвідмовної роботи системи повинна складати не менше 99,7 %.

3.1.6 Вимоги до функцій та задач, які виконує система

Система повинна виконувати такі основні функції:

- ідентифікація та авторизація користувачів;
- керування доступом до приміщення;
- відеофіксація подій доступу;
- передавання даних на IoT-платформу;
- віддалений моніторинг та керування;
- збереження журналу подій.

3.1.7 Вимоги до апаратного забезпечення

Апаратне забезпечення системи повинно базуватися на сучасних енергоефективних компонентах. Обрані елементи мають забезпечувати необхідну продуктивність, стабільність роботи та можливість інтеграції з

периферійними пристроями. Конструкція повинна бути зручною для монтажу та експлуатації.

Вимоги до елементної бази розробки:

– режими роботи і умови експлуатації вибраних елементів повинні відповідати вказаним в ТЗ;

– вибрана елементна база має забезпечувати необхідні режими роботи системи;

– елементна база по можливості має бути широковживаною, доступною і дешевою. Необхідно також враховувати можливість заміни вибраних елементів на аналогічні (вітчизняні чи імпортного виробництва).

Вимоги до мікроконтролера:

– мікроконтролер має підтримувати RISC архітектуру команд;

– мікроконтролер повинен містити необхідний набір вбудованих периферійних пристроїв (таймери, АЦП і т.п.) та потрібну кількість керованих портів введення /виведення.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ.

Комплект конструкторської документації повинен складатись з:

– пояснювальної записки;

– графічного матеріалу:

1. структурна схема системи;
2. схема електрична принципова;
3. блок-схема алгоритму роботи;
4. результати моделювання системи.

*Примітка: В комплект конструкторської документації можуть вноситися зміни та доповнення в процесі розробки.

5 Стадії та етапи проєктування

Таблиця 1 – Стадії та етапи виконання КРБ

№ етапу	Назва етапу виконання КРБ	Термін виконання
1.	Розробка технічного завдання	26.01 – 02.02
2.	Аналіз технічного завдання, вимог до комп'ютеризованої системи, та можливих рішень поставленого завдання	03.02 – 15.02
3.	Розроблення структури, вибір апаратного забезпечення, проєктування комп’ютеризованої системи	20.04 – 25.04
4.	Реалізація алгоритму, написання програмного забезпечення, моделювання комп’ютеризованої системи	26.04 – 05.05
5.	Робота над четвертим розділом «Безпека життєдіяльності, основи охорони праці»	07.05 – 25.05
6.	Оформлення пояснювальної записки та графічного матеріалу	26.05 – 07.06
7.	Перевірка на академічний плагіат, перевірка керівником та консультантами	08.06 – 14.06
8.	Попередній захист кваліфікаційної роботи бакалавра	15.06 – 21.06
9.	Захист кваліфікаційної роботи бакалавра	22.06.2026

6 Додаткові умови виконання кваліфікаційної роботи бакалавра

Під час виконання кваліфікаційної роботи в дане технічне завдання можуть вноситися зміни та доповнення.

Додаток Б

Перелік елементів

Поз. позначення	*Найменування*	*Кіл.*	*Примітка*
	Конденсатори		
C1, C2	0805-X7R-50V-100 нФ±20%	2	
	Мікросхема		
DD1	Стабілізатор напруги LM7805	1	
	Перемикачі		
K1, K2	Вимикач кнопковий КЕ-011	2	
	Виконавчі механізми		
M1	Електромагнітний замок YM-280	1	
	Резистори		
R1	0805-0,125-10 кОм±5%	1	
R2, R3	0805-0,125-4,7 кОм±5%	2	
	Реле		
RL1	Модуль реле 5VDC KS0011	1	
	Модулі		
U1	RFID модуль MFRC522	1	
U2	Модуль Wi-Fi ESP32-CAM з камерою 2MP	1	
U3	Магнітний герконовий давач МС-38	1	
	Роз’єми		
X1	Роз’єм XH2.54-3P 2-х контактний	1	

					КС КРБ 123.146.00.00 ПЕ	
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*		
Розробив		*Бойко П.П.*			*Пристрій для відеомоніторингу вхідної зони приміщення на основі IoT-технологій* *Перелік елементів*	*Літ.* / *Арк.* 77 / *Акрушів* 1
Перевірив		*Стадник Н.Б.*				
Рецензент		*Литвиненко Я.В.*				*ТНТУ, каф. КС, гр. СІ-41*
Н. Контр.		*Луцик Н.С.*				
Зав. каф.		*Осухівська Г.М.*				

Додаток В

Лістинг програми

Лістинг В.1 – Код програми мікроконтролера для реалізації системи відеомоніторингу вхідної зони приміщення на основі IoT-технологій.

```
#include "esp_camera.h"
#include <WiFi.h>
#include <BlynkSimpleEsp32.h>
#include <SPI.h>
#include <MFRC522.h>
#include "FS.h"
#include "SD_MMC.h"
#include <WebServer.h>
#include <WiFiClientSecure.h>
#include "secret.h"

// ===== RFID =====
#define SS_PIN 13
#define RST_PIN 12
MFRC522 mfrc522(SS_PIN, RST_PIN);

// ===== Піни =====
#define RELAY 4
#define DOOR_SENSOR 16
#define EXIT_BTN 3
#define CALL_BTN 1

unsigned long doorOpenTime = 0;
bool doorPreviouslyOpen = false;
const unsigned long DOOR_TIMEOUT = 10000; // 10 секунд
bool alertSent = false;

WebServer server(80);

// ===== Setup =====
void setup() {
  Serial.begin(115200);
  pinMode(RELAY, OUTPUT);
  pinMode(DOOR_SENSOR, INPUT_PULLUP);
  pinMode(EXIT_BTN, INPUT_PULLUP);
  pinMode(CALL_BTN, INPUT_PULLUP);
  WiFi.begin(ssid, pass);
  while (WiFi.status() != WL_CONNECTED) delay(500);
  Blynk.begin(auth, ssid, pass);
  SPI.begin(14, 2, 15, 13);
  mfrc522.PCD_Init();
  startCamera();
  initSD();
```

```
  server.on("/stream", HTTP_GET, handleStream);
  server.begin();
}

// ===== Loop =====
void loop() {
  Blynk.run();
  server.handleClient();
  // RFID
  if (mfrc522.PICC_IsNewCardPresent() &&
mfrc522.PICC_ReadCardSerial()) {
    openDoor("RFID");
    mfrc522.PICC_HaltA();
  }
  // вихід
  if (digitalRead(EXIT_BTN) == LOW) {
    openDoor("exit");
    delay(500);
  }
  // виклик
  if (digitalRead(CALL_BTN) == LOW) {
    Blynk.virtualWrite(V1, "CALL!");
    Blynk.virtualWrite(V2, "http://" + WiFi.localIP().toString() +
"/stream");
    recordEvent("call");
    sendPhotoTelegram();
    delay(500);
  }
  checkDoorState();
}

// ===== Камера =====
void startCamera() {
  camera_config_t config;
  config.ledc_channel = LEDC_CHANNEL_0;
  config.ledc_timer = LEDC_TIMER_0;
  config.pin_d0 = 5; config.pin_d1 = 18;
  config.pin_d2 = 19; config.pin_d3 = 21;
  config.pin_d4 = 36; config.pin_d5 = 39;
  config.pin_d6 = 34; config.pin_d7 = 35;
  config.pin_xclk = 0;
  config.pin_pclk = 22;
  config.pin_vsync = 25;
  config.pin_href = 23;
  config.pin_sccb_sda = 26;
  config.pin_sccb_scl = 27;
  config.pin_pwdn = 32;
  config.pin_reset = -1;
  config.xclk_freq_hz = 20000000;
  config.pixel_format = PIXFORMAT_JPEG;
  config.frame_size = FRAMESIZE_QVGA;
  config.jpeg_quality = 12;
  config.fb_count = 1;
```

```
  esp_camera_init(&config);
}

// ===== SD =====
void initSD() {
  if (!SD_MMC.begin()) {
    Serial.println("SD Card Mount Failed");
    return;
  }
  Serial.println("SD Card OK");
}

// ===== Запис події =====
void recordEvent(String prefix) {
  for (int i = 0; i < 20; i++) {
    camera_fb_t * fb = esp_camera_fb_get();
    if (!fb) continue;
    String path = "/event_" + prefix + "_" + String(i) + ".jpg";
    File file = SD_MMC.open(path.c_str(), FILE_WRITE);
    if (file) {
      file.write(fb->buf, fb->len);
      file.close();
    }
    esp_camera_fb_return(fb);
    delay(150);
  }
}

// ===== Telegram фото =====
void sendPhotoTelegram() {
  WiFiClientSecure client;
  client.setInsecure();
  camera_fb_t * fb = esp_camera_fb_get();
  if (!fb) return;
  if (client.connect("api.telegram.org", 443)) {
    String head = "--123\r\nContent-Disposition: form-data;
                  name=\"chat_id\";\r\n\r\n" + chatID + "\r\n";
    String tail = "\r\n--123--\r\n";
    client.println("POST /bot" + botToken + "/sendPhoto HTTP/1.1");
    client.println("Host: api.telegram.org");
    client.println("Content-Type: multipart/form-data;
boundary=123");
    client.print("Content-Length: ");
    client.println(head.length() + fb->len + tail.length());
    client.println();
    client.print(head);
    client.write(fb->buf, fb->len);
    client.print(tail);
  }
  esp_camera_fb_return(fb);
}

// ===== Стрім =====
```

```
void handleStream() {
  WiFiClient client = server.client();
  server.sendContent("HTTP/1.1 200 OK\r\n");
  server.sendContent("Content-Type: multipart/x-mixed-replace;
                      boundary=frame\r\n\r\n");
  while (client.connected()) {
    camera_fb_t * fb = esp_camera_fb_get();
    server.sendContent("--frame\r\n");
    server.sendContent("Content-Type: image/jpeg\r\n\r\n");
    client.write(fb->buf, fb->len);
    server.sendContent("\r\n");
    esp_camera_fb_return(fb);
  }
}

// ===== Відкрити двері =====
void openDoor(String source) {
  digitalWrite(RELAY, HIGH);
  recordEvent(source);
  sendPhotoTelegram();
  Blynk.virtualWrite(V0, "Door opened: " + source);
  delay(3000);
  digitalWrite(RELAY, LOW);
}

void checkDoorState() {
  bool doorOpen = (digitalRead(DOOR_SENSOR) == LOW); // LOW =
відкрито (типово для геркона)
  // Двері щойно відкрились
  if (doorOpen && !doorPreviouslyOpen) {
    doorOpenTime = millis();
    alertSent = false;
    doorPreviouslyOpen = true;
  }
  // Двері відкриті занадто довго
  if (doorOpen && !alertSent && (millis() - doorOpenTime >
DOOR_TIMEOUT)) {
    Blynk.virtualWrite(V3, "WARNING: Door open too long!");
    alertSent = true;
  }
  // Двері закрились
  if (!doorOpen && doorPreviouslyOpen) {
    doorPreviouslyOpen = false;
    alertSent = false;
  }
}

// ===== Blynk remote =====
BLYNK_WRITE(V10) {
  if (param.asInt()) openDoor("remote");
}
```