Міністерство освіти і науки України Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно–інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

перший (бакалаврський)
(рівень вищої освіти)

Розроблення системи автоматизації доступу у виробниче приміщення з використанням технологій IIoT

(тема)

Виконав:
здобувач 4 року навчання,
групи АКТАКІТ–21–1
Олексій МАРТИНЮК
(власне ім'я, прізвище)

Спеціальність 151 – Автоматизація та комп'ютерно–інтегровані технології
(код і повна назва спеціальності)
Тип програми: освітньо–професійна
Освітня програма: Автоматизація та комп'ютерно–інтегровані технології
(повна назва освітньої програми)

Керівник: доц. Микола СТАРОДУБЦЕВ
(посада, власне ім'я, прізвище)

Допускається до захисту
Зав. кафедри КІТАР _____ Ігор НЕВЛЮДОВ
(підпис) (власне ім'я, прізвище)

2025 р.

Я, Мартинюк Олексій Валерійович, як здобувач вищої освіти ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Я не використовував штучний інтелект для підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

12 червня 2025 р. Олексій МАРТИНЮК

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Факультет АКТ
Кафедра КІТАР
Рівень вищої освіти перший (бакалаврський)
Спеціальність 151 Автоматизація та комп'ютерно–інтегровані технології
(код і повна назва)
Тип програми Освітньо–професійна
Освітня програма Автоматизація та комп'ютерно–інтегровані технології
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
« ___»_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Здобувачеві Мартинюку Олексію Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення системи автоматизації доступу у виробниче приміщення з використанням технологій IIoT

Затверджена наказом по університету від 19.05.2025 р. №391 Ст
2. Термін подання здобувачем роботи до екзаменаційної комісії 27.06.2025 р.
3. Вихідні дані до роботи
3.1 Технічне завдання – Розробити систему автоматизованого контролю доступу до виробничого приміщення з використанням мікроконтролера ESP32–CAM , модуля RFID RC522, сервоприводу SG90, кнопки, датчика руху та п'єзодинаміка.
3.2 Бібліотеки: ESP32Servo, UniversalTelegramBot, MFRC522, EEPROM, WiFi, SPI, esp_camera;
3.3 Telegram Bot Token та Chat ID
3.4 Середа програмування – Arduino IDE

4. Перелік питань, що потрібно опрацювати в роботі
   4.1 Аналіз області застосування
   4.2 Розробка апаратної частини системи доступу
   4.3 Розробка функціональної схеми та алгоритму роботи системи доступу
   4.4 Розрахунки з теорії автоматичного управління
   4.5 Реалізація прототипу та тестування системи доступу
   4.6 Охорона праці

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри)

Демонстраційний матеріал в форматі (*.ppt), А4 –9 сторінок)

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Приміт–ка
1	Вибір теми, погодження з науковим керівником	01.03.2025 – 03.03.2025	Виконано
2	Аналіз предметної області та постановка задачі	04.04.2025 – 10.04.2025	Виконано
3	Розробка структурної схеми та вибір апаратної платформи	11.04.2025 – 17.04.2025	Виконано
4	Реалізація програмного забезпечення системи доступу	18.05.2025 – 01.06.2025	Виконано
5	Тестування, налагодження системи	03.06.2025 – 10.06.2025	Виконано
6	Оформлення пояснювальної записки	11.06.2025	Виконано
7	Подання роботи на перевірку Інтернет–сервісом StrikePlagiarism	19.06.2025	
8	Подання роботи на рецензію	21.06.2025	
9	Подання роботи на підпис зав. кафедри	22.06.2025	
11	Подання кваліфікаційної роботи в ЕК	26.06.2025	

Дата видачі завдання 19.05.2025 р.

Здобувач _____ Олексій МАРТИНЮК
(підпис) (власне ім'я, прізвище)

Керівник роботи _____ доц. Микола СТАРОДУБЦЕВ
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 85 с., 5 табл., 21 рис., 2 дот., 29 джерела.

СИСТЕМА ДОСТУПУ, ІНДУСТРІАЛЬНИЙ ІНТЕРНЕТ РЕЧЕЙ, МІКРОКОНТРОЛЕР, КОНТРОЛЬ ДОСТУПУ, RFID.

Об'єкт розробки – процес автоматизованого контролю доступу до виробничого приміщення.

Предмет робробки – інтелектуальна система доступу на базі технологіı IIoT и використанням мікроконтролера ESP32–CAM.

Методи розробки – аналітичний огляд технічної літератури, моделювання структури системи, експериментальна перевірка роботи програмно–апаратних засобів, тестування у реальних умовах.

З використанням технологій Інтернету речей та реалізацією взаємодії и розробка прототипу системи доступу до виробничого приміщення.

У роботі проаналізовано сучасні методи організації доступу, досліджено проблематику безпеки в умовах промислового середовища, обґрунтовано вибір апаратних компонентів, побудовано алгоритм роботи системи та розроблено скетч для ESP32–CAM. Система реалізує RFID–ідентифікацію, обробку руху, фіксацію подій камерою та відправлення повідомлень адміністратору через бот.

ABSTRACT

Explanatory note: 85 pages, 5 tables, 21 figures, 2 supplements, 29 sources.

ACCESS SYSTEM, INDUSTRIAL INTERNET OF THINGS, MICROCONTROLLER, ACCESS CONTROL, RFID.

The work object is the process of automated control of access to the production premises.

The subject of robot is an intellectual access system based on technology–using ESP32–CAM microcontroller.

Development methods–analytical review of technical literature, modeling of system structure, experimental checking of the operation of software and hardware, testing in real conditions.

Using Internet technologies and interaction implementation and developing a prototype of a production room.

Modern access organization methods are analyzed, safety issues in the industrial environment are investigated, the selection of hardware components is substantiated, the system algorithm is built and a sketch for ESP32–CAM is developed. The system sells RFID IDENTIZATION, movement processing, fixation of events with a camera and sending messages to the administrator through a bot.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ІЧ – датчик руху;

API – Application Programming Interface (інтерфейс програмування застосунків);

ESP32–CAM – мікроконтролер з вбудованою камерою;

GPIO – General Purpose Input/Output (універсальні входи/виходи);

ID – ідентифікатор;

IoT – Internet of Things (інтернет речей);

IIoT – Industrial Internet of Things (промисловий інтернет речей);

JSON – JavaScript Object Notation (формат обміну даними);

LED – Light Emitting Diode (світлодіод);

PCB – Printed Circuit Board (друкована плата);

RFID – Radio Frequency Identification (радіочастотна ідентифікація);

UART – Universal Asynchronous Receiver–Transmitter (універсальний асинхронний приймач–передавач);

UI – User Interface (інтерфейс користувача);

Wi–Fi – Wireless Fidelity (бездротова передача даних).

ВСТУП

У сучасних умовах розвитку промисловості, зростаючої потреби у безпеці та цифровізації виробничих процесів, питання контролю доступу до технічних приміщень набуває особливої актуальності. Забезпечення надійного, гнучкого та централізованого управління доступом є ключовим елементом у структурі сучасного підприємства. Застарілі системи, що базуються на механічних замках або автономних електронних зчитувачах, часто не відповідають вимогам часу – зокрема, не дозволяють вести журнал подій, здійснювати віддалений моніторинг або швидко масштабуватись під змінені умови.

Індустріальний Інтернет речей (IIoT), як окремий напрям технологій Інтернету речей, надає широкі можливості для побудови інтелектуальних систем доступу. Завдяки поєднанню мікроконтролерної техніки, безконтактної ідентифікації, датчиків середовища, модулів бездротової передачі даних, стає можливим створення розумних рішень, які здатні не лише виконувати локальні дії, а й аналізувати події, фіксувати спроби доступу, реагувати на загрози у режимі реального часу.

Мета даної роботи полягає у розробці прототипу IIoT–системи доступу до виробничого приміщення з можливістю автоматичного виявлення присутності, авторизації користувача за допомогою RFID–картки, керування виконавчим пристроєм (електрозамком) та фіксації подій за допомогою вбудованої камери. Також передбачено надсилання повідомлень до адміністратора через бот у месенджері, що забезпечує інтерактивну взаємодію з системою у віддаленому режимі.

Реалізація проєкту здійснюється на основі відкритих апаратних і програмних рішень, зокрема модуля ESP32–CAM, який об’єднує мікроконтролер, модуль Wi–Fi та камеру, а також додаткових сенсорів і виконавчих елементів, таких як RFID–зчитувач RC522, інфрачервоний датчик руху, сервомотор SG90 та кнопка аварійного відкриття. Важливою

особливістю реалізації є підтримка енергоощадного режиму та використання логіки переходу в режим сну при відсутності активності.

Дана тема була обрана не лише через свою актуальність у контексті безпеки на підприємствах, але й з практичної точки зору – як можливість створити реальне рішення, що може бути впроваджене на об’єкті або використане як базова платформа для подальших розробок у сфері автоматизованих IIoT–систем. У процесі реалізації здобувач набув практичних навичок зі схемотехніки, мікроконтролерного програмування, налаштування бездротових мереж, кібербезпеки, роботи з API Telegram та основ теорії автоматичного управління.

Таким чином, виконання цієї кваліфікаційної роботи дозволяє не лише вирішити прикладну інженерну задачу, а й продемонструвати фахову підготовку до подальшої професійної діяльності у сфері комп’ютерно–інтегрованих технологій, систем керування та автоматизації..

Кваліфікаційну роботу оформити згідно ДСТУ 3008:2015 [1], а також з методичними вказівками з підготовки й оформлення кваліфікаційної роботи здобувачами першого (бакалаврського) рівня вищої освіти спеціальності 151 Автоматизація та комп’ютерно–інтегровані технології освітньої програми «Системна інженерія» [2].

Також отримані результати відповідають переліку Цілей сталого розвитку, зокрема Цілі 9 «Промисловість, інновації та інфраструктура» (п. 9.1 та 9.4).

1 АНАЛІЗ ОБЛАСТІ ЗАСТОСУВАННЯ

1.1 Проблематика організації доступу на виробничих об’єктах

Сучасні виробничі підприємства стикаються з численними викликами у сфері організації ефективного контролю доступу до приміщень, що мають стратегічне або обмежене призначення. Забезпечення безпеки виробничих процесів, конфіденційної інформації, обладнання та персоналу стало однією з ключових задач, від вирішення якої залежить не лише стабільність роботи підприємства, але й його конкурентоспроможність на ринку. Однією з найбільш актуальних проблем у цій сфері є застарілість багатьох існуючих систем контролю доступу, їх низька інтегрованість, недостатня автоматизація та слабкий рівень захисту від несанкціонованих дій.

Багато виробничих об’єктів сьогодні все ще покладаються на механічні або аналогові засоби контролю – наприклад, ключі, магнітні картки або обмеження у вигляді охорони. Подібні системи мають низку суттєвих недоліків. По–перше, вони не забезпечують достатнього рівня безпеки, адже ключі можуть бути скопійовані, втрачені або передані іншим особам. По–друге, у таких системах відсутня можливість централізованого або дистанційного моніторингу подій, немає аналітики щодо руху персоналу, що створює ризики як для безпеки підприємства, так і для ефективного управління робочими процесами [1].

Зокрема, для підприємств, які працюють з потенційно небезпечними матеріалами, технікою, автоматизованими виробничими лініями або у режимі підвищеної конфіденційності, ризики проникнення сторонніх осіб або помилкового доступу працівників до критичних зон можуть мати фатальні наслідки – як у вигляді травмування персоналу, так і в контексті техногенних аварій, витоків даних або зриву виробничих циклів. Відсутність можливості оперативно реагувати на подібні інциденти або

відстежити їх причину погіршує ситуацію. Як наслідок, актуальною стає потреба у впровадженні більш сучасних, надійних і гнучких систем контролю доступу. Важливо врахувати, що більшість існуючих систем не мають адаптивної логіки, яка дозволяє змінювати рівень доступу в реальному часі залежно від змін у структурі персоналу, розкладу змін, аварійної ситуації тощо. Також типові системи рідко передбачають багатофакторну ідентифікацію користувачів – тобто одночасне використання кількох способів підтвердження особи: RFID–карти, біометрії (наприклад, розпізнавання обличчя), PIN–коду або віддаленого підтвердження через мобільний додаток. Саме багатофакторна аутентифікація дозволяє значно підвищити рівень захисту, що особливо актуально у випадках, коли доступ до окремих приміщень мають не лише штатні працівники, але й тимчасовий персонал, підрядники або представники контролюючих органів [2].

Окремої уваги заслуговує питання реєстрації та логування подій входу і виходу. У багатьох виробничих системах облік ведеться вручну або взагалі відсутній. Це створює труднощі у розслідуванні інцидентів, аналізі часу перебування персоналу на об’єкті, а також у роботі з трудовими спорами чи перевірках служби безпеки. Сучасні системи доступу мають інтегруватися з внутрішніми IT–системами підприємства, включаючи бази даних кадрів, аналітичні модулі та системи автоматизації виробництва, що дозволяє формувати повну картину подій у режимі реального часу.

Проблематичним є й питання масштабованості та вартості існуючих систем. Багато рішень, які пропонуються на ринку, не враховують специфіку малого або середнього виробництва, мають складну архітектуру та вимагають серйозних інвестицій в обладнання, програмне забезпечення, навчання персоналу. Для підприємств, що працюють в умовах обмежених бюджетів, подібні витрати є неприпустимими, що змушує залишатися на застарілому рівні безпеки. Таким чином, виникає потреба у створенні систем, що базуються на доступних технологіях, є відкритими, гнучкими та

мають можливість адаптації до потреб конкретного виробництва.

У контексті розширення концепції Інтернету речей (IoT) з'являється новий напрям – Industrial Internet of Things (IIoT), який відкриває широкі можливості для побудови інтелектуальних систем контролю доступу. Завдяки використанню мікроконтролерів, модулів зв'язку, сенсорів і алгоритмів обробки даних можна реалізувати систему, яка не лише фіксує події доступу, але й здатна аналізувати контекст ситуації – наприклад, активність датчиків руху, рівень освітлення, температуру, час доби, сигнали з інших пристроїв. Такі можливості дають змогу приймати складніші рішення на основі логіки подій, підвищуючи загальний рівень інтелектуальної безпеки підприємства.

Таким чином, аналіз проблем у сфері забезпечення доступу до виробничих приміщень демонструє актуальність переходу до нової архітектури рішень, що включають в себе доступні апаратні компоненти, розумні алгоритми контролю, адаптивну взаємодію з користувачем і повну інтеграцію в цифрову інфраструктуру підприємства. Саме такий підхід дозволяє сформувати новий рівень безпеки, який не лише зменшує ризики несанкціонованого доступу, а й підтримує гнучкість у керуванні доступом, надає інструменти для аналізу ефективності персоналу та дозволяє масштабувати систему в майбутньому.

1.2 Актуальність застосування технологій IIoT

У сучасних умовах стрімкого розвитку цифрових технологій промислові підприємства стикаються з новими викликами, пов'язаними з необхідністю підвищення ефективності виробництва, зменшення витрат, підвищення рівня автоматизації та безпеки, а також з адаптацією до концепції індустрії 4.0. У цьому контексті особливої актуальності набувають технології Інтернету речей для промислового застосування, відомі як IIoT (Industrial Internet of Things). Ці технології забезпечують інтеграцію

фізичних пристроїв, датчиків, контролерів і програмного забезпечення в єдину мережу, що дозволяє здійснювати автоматизований збір, обробку, передавання та аналіз даних у реальному часі. У свою чергу, це відкриває нові можливості для моніторингу та керування виробничими процесами, у тому числі й системами контролю доступу до виробничих приміщень.

Питання актуальності впровадження IIoT особливо загострюється в умовах зростаючого попиту на інтелектуальні системи безпеки, які здатні не лише фіксувати факти доступу або несанкціонованого проникнення, але й здійснювати аналітичну обробку інформації, виявляти аномалії в поведінці персоналу або обладнання, адаптуватися до змін у режимах роботи підприємства. Традиційні системи контролю доступу, які базуються на простих механізмах авторизації за допомогою магнітних карток чи кодових замків, втрачають свою ефективність через обмежену функціональність, відсутність гнучкості та неспроможність до інтеграції з іншими виробничими системами. Технології IIoT, навпаки, дозволяють створити розумну мережу пристроїв, у якій кожен елемент системи доступу –від RFID–модуля до відеокамери –може взаємодіяти з хмарними сервісами, базами даних, системами відеоспостереження або штучного інтелекту для прийняття рішень.

Ще одним ключовим аспектом актуальності є забезпечення безперервного моніторингу та обліку робочого часу, переміщення працівників та доступу до критично важливих зон підприємства. Завдяки технологіям IIoT з’являється можливість не лише відстежувати події в реальному часі, а й здійснювати аналітику на основі зібраних даних. Наприклад, система може виявити тенденцію запізнень, перевищення часу перебування в заборонених зонах, або розпізнати обличчя працівника через камеру ESP32–CAM і дозволити доступ тільки після успішної ідентифікації. Інтеграція датчиків руху, RFID–модулів та відеоспостереження дозволяє створити багаторівневу систему безпеки, яка адаптується до умов конкретного виробництва.

Також слід зазначити, що IIoT відіграє важливу роль у досягненні енергоефективності та оптимізації ресурсів. Наприклад, система може вимикати освітлення чи обладнання в приміщенні, якщо датчик руху не фіксує присутність працівників, або надсилати сповіщення про несанкціоноване проникнення в неробочий час. Це сприяє зменшенню витрат на електроенергію та підвищенню дисципліни персоналу. Більше того, можливість дистанційного доступу до даних та керування системою через Wi–Fi або Bluetooth відкриває нові горизонти в адмініструванні – технічний персонал або служба безпеки може миттєво реагувати на події навіть без фізичної присутності на об'єкті.

Перевагою IIoT також є висока масштабованість: систему можна поступово доповнювати новими модулями, сенсорами чи сервоприводами без необхідності повної перебудови інфраструктури. Це особливо важливо для малих і середніх підприємств, які не можуть дозволити собі повномасштабні інвестиції в дорогі системи автоматизації. Простота інтеграції IIoT–компонентів з такими платами, як ESP32, робить технології доступними для широкого кола розробників, студентів, інженерів та техніків. Вони мають змогу самостійно створювати та модифікувати системи доступу з урахуванням специфіки конкретного об'єкта, що суттєво підвищує ефективність охоронних заходів.

Крім того, не можна залишити поза увагою роль IIoT у підвищенні рівня кібербезпеки. Завдяки використанню сучасних протоколів шифрування даних, систем аутентифікації, хмарного зберігання журналів подій та інтеграції з Telegram–ботами або іншими засобами повідомлення, система доступу стає не тільки більш функціональною, але й безпечнішою. Це дозволяє уникнути випадків фальсифікації доступу або маніпуляцій із традиційними засобами контролю. Актуальність цих функцій значно зросла з урахуванням останніх кіберзагроз, з якими стикаються підприємства у всьому світі.

Таким чином, впровадження технологій IIoT у систему контролю

доступу до виробничого приміщення є надзвичайно актуальним кроком, який відповідає сучасним вимогам до цифрової трансформації виробництва, забезпечення безпеки, ефективності, гнучкості та адаптивності до змін у зовнішньому середовищі. IIoT формує нову парадигму у сфері охорони, де замість реактивного підходу (реакція на факт порушення) реалізується проактивний підхід (виявлення ризику та запобігання порушенню). Усе це свідчить про високий потенціал IIoT у розробці та впровадженні інтелектуальних систем контролю доступу, які стають не лише інструментом охорони, а й елементом стратегічного управління підприємством в умовах індустрії 4.0.

1.3 Причини створення нової системи доступу

Попри наявність ряду готових рішень на ринку систем контролю доступу, багато з них мають обмеження у гнучкості конфігурації, високій вартості впровадження, складності інтеграції в існуючу інфраструктуру або недостатній захист персональних даних. Крім того, більшість таких систем не враховують специфіку саме виробничих приміщень, де важливо забезпечити стійкість обладнання до пилу, вібрацій, електромагнітних перешкод, а також передбачити наявність аварійного режиму роботи при перебоях з електропостачанням або мережею.

Створення власної системи на базі доступних мікроконтролерів, таких як ESP32–CAM, та інших модулів дозволяє розробити рішення, яке буде максимально адаптоване до конкретних умов підприємства. Власна розробка забезпечує більший контроль над функціоналом, можливість масштабування, гнучке налаштування сценаріїв доступу та мінімізацію витрат на обслуговування [5].

У таблиці 1.1 нижче наведено порівняння основних характеристик готових рішень і запропонованої розробки.

Таблиця 1.1 – Порівняння основних характеристик готових рішень і запропонованої розробки

Характеристика	Готова система (ринкова)	Власна розробка (на базі IIoT)
Вартість впровадження	Висока	Низька
Можливість кастомізації	Обмежена	Висока
Інтеграція з іншими системами	Потребує окремих рішень	Відкрита архітектура
Віддалене управління	Частково	Повністю реалізується
Реакція на спробу вторгнення	Стандартна	Гнучка, з адаптивними сценаріями
Потреба в охоронному персоналі	Так	Мінімізується
Витрати на обслуговування	Високі	Низькі

1.4 Сфера застосування розроблюваної системи

Система автоматизованого контролю доступу у виробниче приміщення, створена на основі технологій IIoT (Industrial Internet of Things), має широкий спектр потенційного застосування у сучасному промисловому середовищі. Така система дозволяє підвищити рівень безпеки, забезпечити персоніфікований доступ, вести облік переміщень працівників, а також інтегруватися з іншими елементами розумного виробництва, створюючи єдину цифрову екосистему підприємства. Основною сферою її використання виступають підприємства, де існує

потреба обмежити або регламентувати фізичний доступ до окремих зон виробництва, складів, лабораторій, серверних або адміністративних приміщень. Це можуть бути як великі заводи, так і невеликі майстерні, де працюють кваліфіковані спеціалісти, що мають різні рівні допуску.

Класичним прикладом такої сфери є підприємства з підвищеним рівнем техногенної небезпеки, де несанкціоноване потрапляння у зону з небезпечними механізмами або матеріалами може призвести до аварій, пошкодження обладнання або загрози життю людей. На таких об’єктах впровадження інтелектуальної системи доступу дозволяє чітко розмежувати права персоналу, автоматично реєструвати час входу та виходу, та інтегрувати ці дані до загальної системи безпеки. Наприклад, при виникненні аварійної ситуації відповідальні особи можуть швидко отримати інформацію, хто перебував у приміщенні, а за допомогою розумного алгоритму доступ може бути тимчасово заблокований або обмежений лише для аварійних служб.

Ще однією перспективною сферою використання розробленої системи є високотехнологічні виробництва, де застосовується обладнання, яке потребує спеціальної кваліфікації. У таких умовах важливо, щоб доступ до техніки мали лише сертифіковані працівники, проходження яких фіксується системою і за необхідності може бути проаналізовано. Крім того, система може виконувати функцію присутності – фіксуючи час прибуття та вибуття працівників, що корисно для ведення табелів обліку робочого часу. У деяких випадках така система здатна замінити або доповнити традиційні методи контролю, наприклад, журнали реєстрації чи ручне відкривання дверей охоронцем.

У контексті Індустрії 4.0, де все більше підприємств переходять до повної автоматизації процесів, розроблювана система ідеально вписується у концепцію "цифрового подвійника" виробництва, де кожна дія має цифрове відображення. Інтеграція через Wi–Fi та протоколи IoT дозволяє об'єднувати її з іншими системами: відеоспостереженням, пожежною

сигналізацією, системами енергоменеджменту, внутрішніми ERP–системами тощо. Завдяки такому підходу підприємство отримує можливість не лише автоматизувати контроль доступу, а й створити аналітику щодо ефективності використання ресурсів, безпеки, відповідності регламентам доступу.

Важливо зазначити, що сфера застосування розширюється і поза межі суто виробничих потреб. Подібну систему можна адаптувати для офісних приміщень, навчальних закладів, лабораторій, банківських установ, логістичних компаній, дата–центрів або навіть об’єктів критичної інфраструктури. Наприклад, у навчальних корпусах університетів система може використовуватись для обмеження доступу до лабораторій, де зберігається коштовне або небезпечне обладнання, а у дата–центрах – для контролю доступу до серверних кімнат. У таких умовах важливо забезпечити як фізичну безпеку обладнання, так і збереження конфіденційних даних, що можуть оброблятись в окремих зонах.

Розроблена система може бути особливо цінною для малих та середніх підприємств, які не мають змоги впроваджувати дорогі комерційні рішення, але прагнуть дотримуватись високих стандартів безпеки. Завдяки використанню недорогих, але функціональних апаратних компонентів, таких як ESP32–CAM, RFID RC522 та інших, вона залишається доступною, при цьому забезпечуючи високу надійність та функціональність. Гнучкість архітектури дозволяє доповнювати систему новими модулями, наприклад, додати розпізнавання облич, логування в хмару, керування з мобільного застосунку, а також реалізувати багаторівневу аутентифікацію – наприклад, комбінацію RFID та розпізнавання обличчя.

У контексті кіберфізичних систем, які дедалі активніше впроваджуються у виробничих процесах, запропонована система є прикладом фізичного інтерфейсу до цифрового середовища підприємства. Через неї реалізується зв’язок між реальним світом (персоналом, дверима, приміщенням) і цифровою логікою контролю та аналітики. Це дозволяє

будувати більш складні системи – наприклад, запуск обладнання лише після підтвердження входу уповноваженої особи або автоматичне вмикання вентиляції/освітлення при вході в приміщення.

Загалом, сфера застосування розроблюваної системи дуже широка і охоплює різні галузі, де безпека, контроль доступу та облік руху людей відіграють важливу роль. Вона є гнучким, масштабованим і доступним рішенням для підприємств різного рівня, що робить її актуальною і конкурентоспроможною на ринку сучасних систем безпеки.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ ДОСТУПУ

2.1 Вибір апаратних компонентів

У процесі розробки системи доступу до виробничого приміщення з використанням технологій IIoT особливу увагу необхідно приділити правильному вибору апаратних компонентів, які забезпечать необхідну функціональність, надійність та взаємодію між усіма модулями системи. Урахування технічних характеристик, енергоспоживання, підтримки бездротового зв’язку, можливостей розширення та зручності інтеграції є критично важливим для досягнення ефективної роботи системи. Нижче наведено докладний опис основних апаратних компонентів, що були обрані для реалізації проєкту. Модуль камери ESP32–CAM Wi–Fi ESP32 Bluetooth з камерою OV2640.

Цей модуль є центральним елементом системи, оскільки виконує функції контролера, камери для розпізнавання облич або фіксації відео/зображень, а також забезпечує бездротове підключення через Wi–Fi та Bluetooth. ESP32–CAM побудований на основі потужного мікроконтролера ESP32, що має двоядерний процесор Tensilica LX6, частотою до 240 МГц. Він оснащений 4 МБ вбудованої пам'яті PSRAM, що дозволяє зберігати зображення високої якості.

Модуль підтримує зйомку у форматі JPEG, а також потокове відео через локальну мережу. Камера OV2640 має роздільну здатність до 2 мегапікселів і забезпечує якісне зображення навіть при поганому освітленні, що є важливим для умов виробничих приміщень (рис. 2.1).

Рисунок 2.1 – Зовнішній вигляд ESP32–CAM з камерою OV2640

Плата адаптер ESP32 є допоміжним елементом, що полегшує підключення модуля ESP32–CAM до комп’ютера або іншого пристрою для програмування. Вона включає інтерфейс USB–to–TTL (зазвичай на базі чіпа CP2102 або CH340G), який необхідний для прошивки модуля. Також адаптер дозволяє легко подавати живлення на ESP32–CAM і забезпечує стабільне з’єднання (рис. 2.2).

Рисунок 2.2 – Плата адаптер ESP32 з micro–USB

Сервопривід SG90 буде використано для управління фізичним механізмом відкривання або закривання дверей. Цей компонент відзначається компактністю, низьким енергоспоживанням та простою інтеграцією з мікроконтролерами. Сервомотор здатен повертатися на кут до 180°, що цілком достатньо для активації замка, повороту засувки або відкривання защіпки.

SG90 має зворотній зв’язок за положенням, що дозволяє точно визначати його стан. Працює від напруги 4.8–6.0 В і має стандартний інтерфейс управління за допомогою широтно–імпульсної модуляції (PWM) (рис. 2.3).

Рисунок 2.3 – Сервопривод TowerPro SG90

Buzzer буде використано для звукової індикації подій: успішного входу, помилки при авторизації, активації датчика руху тощо. Активний динамік є автономним пристроєм, який генерує звуковий сигнал при подачі живлення. Це дозволяє керувати ним без генерації PWM–сигналу, що зменшує навантаження на контролер.

Buzzer забезпечує просту зворотну реакцію користувачу і підвищує рівень зручності використання системи. Його компактні розміри і низька споживана потужність роблять його ідеальним для вбудованих систем (рис.2.4).

Рисунок 2.4 – Активний пьезодинамік (buzzer)

Ця кнопка виконує функцію ручного виклику – наприклад, відкриття дверей зсередини приміщення або подачі сигналу на зчитування RFID чи запуск сканування обличчя. Вона має міцний пластиковий корпус і надійну контактну групу, що забезпечує довготривале використання. Тактильний відгук дозволяє зрозуміти користувачу, що натискання було виконане.

Використання модульної версії спрощує підключення на макетній платі без пайки, що зручно на етапі тестування (рис. 2.5).

Рисунок 2.5 – Модульна кнопка

HC–SR501 використовується для виявлення присутності людини в зоні доступу. Він заснований на піросенсорі, який реагує на зміну інфрачервоного випромінювання. Датчик має регульовану дальність виявлення (до 7 метрів) та час затримки, що дозволяє адаптувати його до умов конкретного об’єкта.

У системі доступу його можна використати як активатор відеозапису або як додаткову перевірку перед зчитуванням ідентифікатора (рис. 2.6).

Рисунок 2.6 – ІЧ–датчик руху HC–SR501

Цей модуль відповідає за ідентифікацію користувачів за допомогою RFID– карток або брелоків. Працює на частоті 13,56 МГц, підтримує стандарт ISO/IEC 14443, широко використовується в системах контролю доступу. Він підключається через інтерфейс SPI, що забезпечує високу швидкість обміну з мікроконтролером.

RC522 дозволяє зчитувати унікальний ID картки та порівнювати його з базою даних користувачів. При успішному збігу ініціюється відкривання дверей. Даний спосіб є надійним, дешевим і простим у реалізації (рис. 2.7).

Рисунок 2.7 – RFID модуль RC522 з картою

Макетна плата використовується для збирання схеми без пайки. Вона дозволяє швидко протестувати з’єднання між компонентами, змінювати схему в реальному часі та додавати нові модулі без порушення цілісності всієї системи. Плата MB–102 має дві бічні шини живлення і 400 отворів для підключення.

Використання макетної плати особливо актуальне на етапі прототипування, коли система активно модифікується (рис. 2.8).

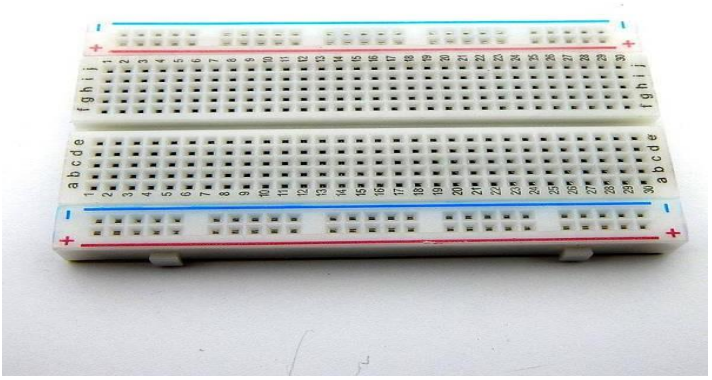

Рисунок 2.8 – Макетна плата MB–102

Модуль HW використовується для подання живлення на схему без пайки. Він дозволяє розповсюдити живлення на 5 В та 3,3 В завдяки заглушкам що є в комплекті (рис. 2.9).

Рисунок 2.9 – Модуль HW

2.2 Схема з’єднання апаратної частини

Усі компоненти з'єднані відповідно до логічної схеми, яка враховує необхідні інтерфейси та напруги живлення. Камера ESP32–CAM підключена до адаптера, який живиться від 5 В через USB. Для зв'язку з RFID–модулем RC522 використовується SPI інтерфейс: MOSI, MISO, SCK та SS підключені до відповідних пінів ESP32–CAM. Buzzer під’єднаний до U0T. Сервопривід SG90 керується за допомогою PWM сигналу з GPIO 12, при цьому живлення подається окремо від джерела 5 В, враховуючи обмеження по струму ESP32. Датчик руху HC–SR501 підключається до GPIO 4 для зчитування сигналу про присутність. Тактова кнопка з’єднується з U0R. Загальна схема представлена в таблиці 2.1:

Таблиця 2.1 – Таблиця з’єднань.

Компонент	Пін ESP32– CAM	Інтерфейс	Живлення
RC522 RFID	GPIO 15, 14, 2, 13,16	SPI	3,3 В
SG90 Серво	GPIO 12	PWM	5 В
HC–SR501 PIR	GPIO 4	Digital	5 В
Buzzer	U0T	Digital	5 В
Тактова кнопка	U0R	Digital	3,3 В
Камера (OV2640)	Вбудована	I2C	3,3 В

З'єднання реалізоване через макетну плату MB–102, що дозволяє легко розміщувати всі компоненти без пайки. Живлення подається через зовнішній блок живлення 5 В, 2 А, що забезпечує достатню

потужність для ESP32–CAM, сервоприводу та інших пристроїв.

2.3 Принцип роботи апаратної частини

Принцип роботи апаратної частини системи доступу до виробничого приміщення базується на взаємодії між різними електронними компонентами, які забезпечують розпізнавання користувача, обробку запиту на доступ, прийняття рішення щодо відкриття дверей, а також фіксацію подій у системі. Усі елементи з'єднані в єдину структуру з використанням мікроконтролера ESP32– CAM, який є "мозком" системи. Нижче детально описується, як працює кожен з компонентів у взаємозв'язку з іншими, і як формується повний цикл авторизації користувача.

Система активується, коли інфрачервоний датчик руху HC–SR501 фіксує наявність об’єкта у зоні дії. Датчик передає сигнал високого рівня на ESP32–CAM, що слугує тригером для запуску подальших перевірок. Це дозволяє зменшити енергоспоживання системи та уникнути зайвих сканувань у моменти без активності.

Отримавши сигнал активації, ESP32–CAM переходить у активний режим. У цей момент камера OV2640, вбудована у модуль, може виконати фото– або відеофіксацію відвідувача. У перспективі цей функціонал можна використати для реалізації розпізнавання облич на базі штучного інтелекту або для збереження архіву спроб входу. Якщо розпізнавання облич не використовується, система переходить до RFID–ідентифікації.

Користувач прикладає RFID–картку або брелок до модуля RC522, який зчитує унікальний ідентифікатор та передає його до ESP32 по інтерфейсу SPI. Контролер перевіряє ID в базі дозволених користувачів, яка може бути збережена локально (у flash–пам’яті) або передаватися з сервера через Wi–Fi (за наявності підключення до локальної мережі чи хмари).

У разі успішної ідентифікації контролер генерує імпульс керування на

сервопривід SG90, який змінює своє положення, фізично відкриваючи замок або привід засувки. Користувач отримує доступ у приміщення. Якщо ідентифікація не вдалася – система активує п’єзодинамік (buzzer), який подає звуковий сигнал помилки.

Крім RFID і камери, модульна кнопка 12 мм х 12 мм виконує допоміжну функцію ручного керування –наприклад, дозволяє відкривати двері зсередини, або активує повторну перевірку при помилці, або слугує аварійною кнопкою розблокування. Цей варіант забезпечує більшу зручність і безпеку експлуатації.

Живлення всієї апаратної частини відбувається через макетну плату MB– 102, яка дозволяє зручно розподіляти напругу до 5 В та підключати всі модулі за допомогою перемичок. Адаптер ESP32 дозволяє прошивати мікроконтролер і підтримує живлення пристрою через USB.

Усі компоненти працюють у синхронному режимі за допомогою прошивки, яка обробляє сигнали від вхідних пристроїв, керує логікою відкриття дверей, виводить повідомлення, контролює серво–привід і надає зворотній зв'язок користувачу через світлові або звукові сигнали. Потенційно в систему можна інтегрувати логування подій, зберігання історії входів та підключення до мобільного застосунку або Telegram–бота для віддаленого спостереження.

Таким чином, принцип роботи апаратної частини полягає в багаторівневій обробці подій: виявлення присутності, перевірка особи, прийняття рішення та виконання дії. Усі елементи працюють як частини одного логічного ланцюжка, що забезпечує ефективний та безпечний доступ до виробничих приміщень. Завдяки гнучкості платформи ESP32 та широкому набору датчиків, систему можна масштабувати –додавати нові рівні авторизації, підключати камери для зйомки відео, вводити біометричну перевірку або віддалене адміністрування.

3 РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ ТА ЛАГОРИТМУ РОБОТИ СИСТЕМИ ДОСТУПУ

3.1 Обґрунтування вибору архітектури системи на базі ESP32–CAM

На сучасному етапі розвитку промислових систем автоматизації особливого значення набуває побудова ефективних, економічно доступних і масштабованих рішень для контролю доступу. Вибір апаратної архітектури є ключовим етапом у проєктуванні таких систем, оскільки саме він визначає функціональні можливості, рівень інтеграції, енергоефективність та потенціал до розширення. У межах даної розробки було обґрунтовано використання модульної мікроконтролерної платформи ESP32–CAM як основи для створення інтелектуальної системи доступу до виробничого приміщення.

ESP32–CAM –це модуль, побудований на основі мікроконтролера ESP32 від компанії Espressif Systems, до якого додатково інтегровано камеру OV2640 та інтерфейс для карти пам’яті microSD. Основними перевагами цієї платформи є наявність бездротових інтерфейсів зв’язку (Wi–Fi та Bluetooth), достатній обсяг оперативної та флеш–пам’яті, а також підтримка периферійних пристроїв через цифрові входи/виходи, UART, SPI, I2C та PWM. Саме така конфігурація дозволяє використовувати ESP32–CAM як центральний елемент вбудованої системи, що забезпечує обробку сигналів від датчиків, керування виконавчими механізмами та передачу даних до зовнішніх сервісів.

Крім того, архітектура ESP32–CAM дає змогу поєднувати кілька функцій одночасно: розпізнавання або фіксація облич за допомогою камери, авторизація користувачів через RFID–модуль RC522, реагування на рух за допомогою датчика HC–SR501, подача звукових сигналів через п’єзодинамік, а також керування електромеханічним замком на основі

сервоприводу SG90.

Усі ці компоненти можуть бути підключені до ESP32–CAM без використання додаткових контролерів або комунікаційних модулів, що суттєво спрощує конструкцію, зменшує вартість і підвищує надійність системи.

Одним із ключових аргументів на користь вибору саме ESP32–CAM стала його здатність до роботи в складі інфраструктури Інтернету речей (IIoT). Завдяки підтримці Wi–Fi контролер може передавати дані на сервер, в хмарне сховище або напряму у месенджер через HTTP API, що реалізує віддалений моніторинг та керування доступом. Це відкриває можливості інтеграції системи з платформами типу SCADA, MES або внутрішніми корпоративними системами безпеки.

Крім технічних характеристик, ESP32–CAM вирізняється широкою спільнотою розробників, відкритим програмним забезпеченням і великою кількістю бібліотек, які дозволяють швидко реалізувати складну логіку без глибоких знань у сфері програмування мікроконтролерів. Це особливо важливо для швидкого прототипування та адаптації системи до специфічних умов конкретного підприємства.

Отже, на основі аналізу функціональних вимог, технічних характеристик і перспектив масштабування було обґрунтовано вибір архітектури системи на основі ESP32–CAM як найбільш оптимального рішення для побудови багаторівневої, бездротової та економічно ефективної системи доступу у виробниче приміщення з використанням технологій IIoT.

3.2 Розробка структурної схеми взаємодії компонентів системи

Розробка структурної схеми взаємодії компонентів системи доступу є одним з ключових етапів, оскільки саме на цьому рівні визначаються фізичні та логічні зв’язки між основними елементами системи. Структурна схема

дозволяє візуалізувати архітектуру пристрою, окреслити напрямки обміну сигналами, розмежувати функціональні блоки за призначенням та забезпечити чітке розуміння їхньої взаємодії для подальшого програмного та апаратного реалізування.

На основі обраного апаратного ядра –контролера ESP32–CAM – система умовно розбивається на п’ять функціональних блоків: блок ідентифікації користувача, блок фіксації події, блок прийняття рішення, виконавчий блок і блок зворотного зв’язку. Кожен із них включає відповідні компоненти, які підключаються до ESP32–CAM через GPIO–піни, з урахуванням типу сигналу (цифровий, PWM, SPI тощо) та енергоспоживання.

Блок ідентифікації представлений RFID–модулем RC522, який підключається до ESP32–CAM через інтерфейс SPI. Цей модуль зчитує унікальні ідентифікатори карт або брелоків користувача і передає їх у контролер для подальшої перевірки у внутрішній або зовнішній базі дозволених ID. У разі розширення функціоналу можливо також додати модуль з пам’яттю або базу в хмарному середовищі.

Блок фіксації події реалізується за допомогою вбудованої камери OV2640, яка може знімати фото або відео при активації системи. Камера активується сигналом від ІЧ–датчика руху HC–SR501, який виконує роль тригера. Така логіка дозволяє уникнути зайвого енергоспоживання та зменшує обсяг непотрібної інформації, адже камера працює лише тоді, коли фіксується фізична присутність людини перед дверима.

Блок прийняття рішення реалізовано у вигляді програмної логіки на ESP32–CAM. У цьому блоці обробляються сигнали з датчика руху, зчитувача карт та камери, порівнюється ID з дозволеними значеннями, генеруються команди для виконавчих механізмів та формується відповідь (дозволити/заборонити доступ). За потреби ця логіка може бути доповнена комунікацією з хмарним сервером або ботом у месенджері.

Виконавчий блок представлений сервоприводом SG90, який фізично

керує замком або механізмом відкриття дверей. При отриманні команди "доступ дозволено" сервомотор змінює свій кут положення, відкриваючи замок на заданий період часу. Після цього він автоматично повертається у вихідне положення, блокуючи доступ.

Блок зворотного зв’язку реалізовано через активний бузер, який сигналізує про результат спроби доступу: короткий високий звук у разі дозволу, подвійний низький –при відмові. Додатково передбачена кнопка ручного відкриття, яка дозволяє зсередини ініціювати відкриття замка незалежно від авторизації. Це важливо для забезпечення евакуації або обслуговування.

Таким чином, структурна схема системи включає чітко визначені блоки, взаємодія яких забезпечує надійність, логічну завершеність та гнучкість системи. Усі елементи розміщуються на макетній платі МВ–102, що дозволяє легко протестувати та змінювати компонування під час налаштування або модернізації системи. Такий підхід дозволяє створити прототип з можливістю подальшої інтеграції в реальне виробниче середовище (рис. 3.1).

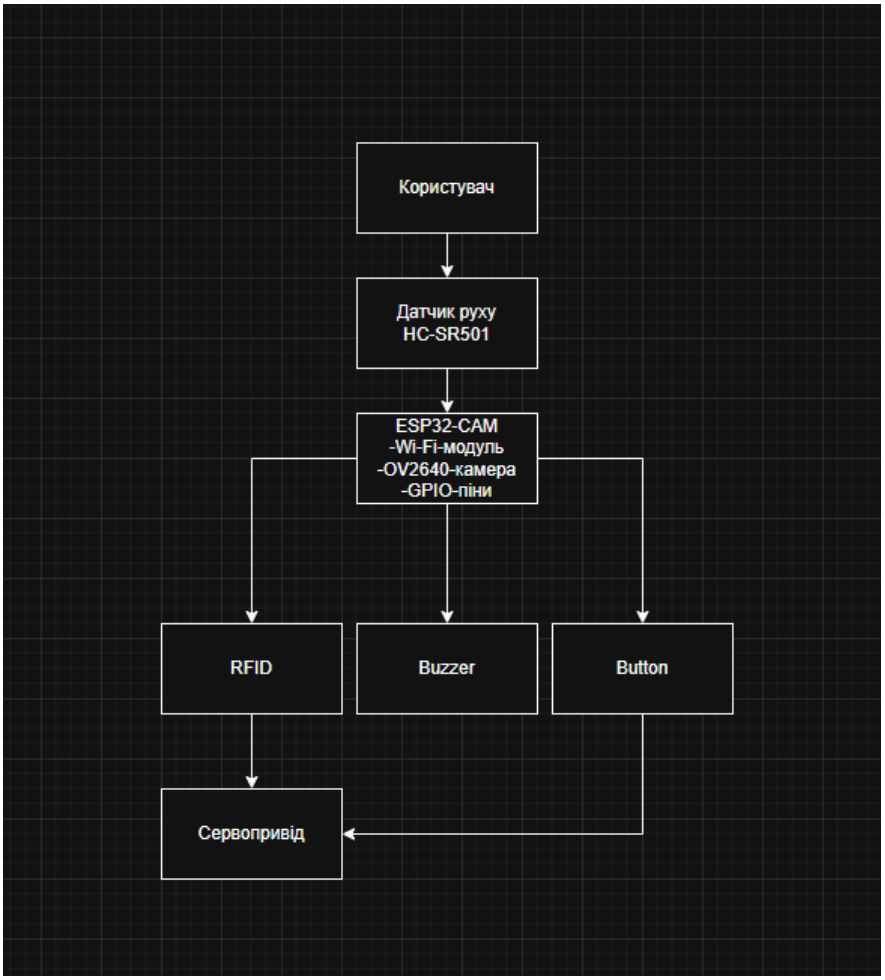

Рисунок 3.1 – Структурна схема системи доступу на базі ESP32–CAM

3.3 Побудова функціональної схеми системи доступу

Функціональна схема є логічним продовженням структурної і служить для детального опису принципу дії системи доступу у динаміці –від моменту виявлення об’єкта до фізичного відкриття або блокування дверей. Побудова функціональної схеми дозволяє розділити процес на етапи, визначити логіку реагування на вхідні сигнали, черговість виконання команд, а також забезпечити узгодженість роботи всіх модулів у реальному часі. Це особливо важливо для систем на базі мікроконтролерів, які працюють за принципом циклічного виконання програми.

У функціональній схемі системи доступу першою активною ланкою є

датчик руху HC–SR501, який постійно моніторить простір перед входом. При виявленні руху він генерує логічний сигнал високого рівня, що подається на контролер ESP32–CAM. Цей сигнал виконує роль тригера, який активує процес перевірки доступу. На цьому етапі камера може зробити знімок для збереження в архіві або передачі адміністратору через мережеве підключення, у разі реалізації розширеного функціоналу.

Після цього контролер переходить у режим очікування зчитування ідентифікатора користувача за допомогою модуля RC522. У випадку, якщо RFID–картка або брелок піднесені до зчитувача, відбувається зчитування UID (унікального ідентифікатора), який миттєво порівнюється з внутрішньою таблицею дозволених доступів. Якщо UID збігається з одним із дозволених, ESP32–CAM подає команду на відкриття замка –сигналізуючи про це звуковим сигналом на buzzer (одноразовий високочастотний звук) і подаючи сигнал на сервопривід SG90, який фізично повертає ричаг замка на певний кут, відкриваючи двері.

У разі невідповідності UID або його відсутності в базі контролер подає сигнал про відмову: buzzer генерує два короткі низькі сигнали, а замок залишається в закритому стані. У цей момент у систему також може надходити зворотна команда від адміністратора (через бота в месенджері) – наприклад, дистанційне відкриття дверей у виняткових ситуаціях.

Окремо передбачено кнопку ручного відкриття, розташовану з внутрішньої сторони приміщення. Натискання кнопки ініціює обхід авторизації –це дозволяє персоналу або охороні відкривати двері без використання RFID або команди ззовні. Такий підхід відповідає стандартам безпеки, зокрема, у ситуаціях евакуації.

Завершальний етап функціонального циклу –повернення сервоприводу у вихідне положення (замкнено) через запрограмовану затримку в кілька секунд. Це дозволяє людині пройти крізь двері, але не залишає їх відкритими довше, ніж це необхідно. Вся логіка працює в безперервному циклі, що забезпечує швидкий відгук і надійність системи.

Таким чином, функціональна схема охоплює основні стани системи: очікування, активація, перевірка, дозвіл/відмова, виконання дії, повернення у вихідний стан. Кожен компонент працює у чітко визначений момент часу, з урахуванням черговості та залежності від сигналів інших блоків. Це дозволяє забезпечити стабільну та логічну роботу системи без затримок, конфліктів або помилкових спрацювань (рис. 3.2).

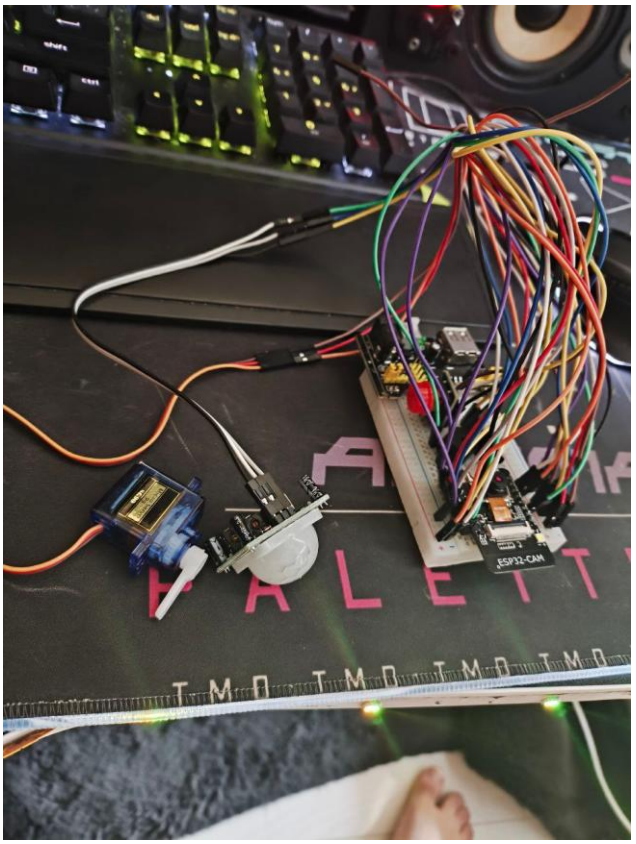

Рисунок 3.2 – Функціональна схема системи доступу

3.4 Алгоритм авторизації користувача та відкриття замка

Удосконалений алгоритм авторизації користувача побудований на принципах енергоефективності, розумного реагування на події та негайного інформування адміністратора у випадку несанкціонованого доступу. Він інтегрує механізми керування живленням, перевірки RFID–картки, фото, а також надсилання результатів взаємодії в месенджер. Алгоритм включає

наступні логічні етапи:

У звичайному стані система перебуває у режимі енергозбереження – активним залишається лише датчик руху HC–SR501, який періодично перевіряє навколишнє середовище. Як тільки датчик фіксує рух поблизу вхідної зони, система виходить із режиму сну. Увімкнення камери ESP32–CAM, ініціалізація RFID–зчитувача RC522 та активація бездротового модуля Wi–Fi відбуваються одночасно в межах одного запуску.

Одночасно система очікує прикладання RFID–картки до зчитувача. При зчитуванні картки модуль ESP32–CAM ідентифікує її UID та порівнює його з локальним переліком дозволених ідентифікаторів. У разі успішного збігу ідентифікаторів користувача з елементом дозволеного списку, система вважає авторизацію завершеною успішно.

Серводвигун SG90 подає команду на відкриття замка, і фізичний доступ до приміщення дозволяється. Чикає 10 секунд і після цього сервомеханізм автоматично повертає замок у закрите положення, і система фіксує завершення сеансу доступу.

У випадку, якщо UID не відповідає жодному дозволеному значенню, або картка взагалі не була прикладена, система реагує як на спробу несанкціонованого доступу. У такому разі камера негайно робить фотографію особи, яка перебуває перед дверима, та надсилає її адміністратору з відповідним текстовим коментарем. Замок залишається закритим, доступ до приміщення не надається.

Після будь–якої взаємодії система починає відлік часу бездіяльності. Якщо протягом 30 секунд не відбувається жодної активності (рух, зчитування картки, натискання кнопки), система автоматично вимикає непотрібні модулі – камеру, Wi–Fi, RFID–зчитувач – та повертається в режим енергозбереження. Це дозволяє значно зменшити споживання енергії та подовжити час автономної роботи системи у випадку живлення від акумулятора.

Алгоритм передбачає також ручний режим відкриття замка через

натискання кнопки. У разі натискання кнопки (наприклад, у надзвичайній ситуації або при обслуговуванні системи) замок відкривається на той самий проміжок часу. Ця подія також логгується і надсилається у вигляді повідомлення адміністратору.

Таким чином, розроблений алгоритм охоплює повний цикл роботи системи доступу – від виявлення активності до прийняття рішення, відкриття замка, фіксації дій та повернення у стан сну.

3.5 Взаємодія з периферійними пристроями (RFID, buzzer, сервомотор, датчик руху)

Периферійні пристрої у складі системи контролю доступу виконують роль засобів зчитування, сигналізації, виявлення подій та фізичного впливу на механізми. Їх взаємодія з центральним контролером –ESP32–CAM – забезпечується через стандартні цифрові інтерфейси: GPIO, SPI, PWM та аналогові входи. Кожен з цих пристроїв виконує окрему функцію, але всі вони синхронізовані єдиною логікою роботи системи, що забезпечує цілісність алгоритму.

Один із головних компонентів системи – це RFID–модуль RC522, який використовується для зчитування ідентифікаційних карток користувачів. RC522 підключається до ESP32–CAM через інтерфейс SPI, що забезпечує швидку і стабільну передачу даних. Модуль постійно опитується мікроконтролером у циклічному режимі, а при виявленні карти формує відповідь у вигляді 4–байтного UID. Далі цей UID порівнюється з внутрішнім списком дозволених ідентифікаторів. У разі збігу –дозволяється доступ. Якщо UID не знайдено, контролер блокує вхід. RC522 має вбудований антенний модуль і працює на частоті 13,56 МГц, що забезпечує стабільний зчитувальний діапазон до 3 см.

Для подання зворотного зв’язку в системі використовується активний п’єзосигналізатор (buzzer), який виконує роль індикатора результату

авторизації. Він підключається до цифрового виходу ESP32–CAM та керується через функцію tone() у мові Arduino C++. У разі успішної авторизації сигналізатор видає короткий високий тон, а у разі відмови –два короткі низькі сигнали. Це дозволяє користувачу миттєво отримати аудіоінформацію про статус спроби входу, навіть без візуального інтерфейсу.

Сервопривід SG90 є виконавчим елементом, який фізично відкриває або закриває дверний замок. Він підключається до PWM–виходу ESP32–CAM (наприклад, GPIO12), і керується зміною положення валу за допомогою команди servo.write(кут). У звичайному стані привід утримується в положенні "замкнено" (кут 0°). У разі дозволу на вхід він повертається в положення "відкрито" (наприклад, кут 90°) на 3–5 секунд, після чого автоматично повертається назад. Сервомеханізм SG90 споживає до 500 мА струму під навантаженням, тому бажано передбачити окреме джерело живлення або використати конденсатор для стабілізації.

Датчик руху HC–SR501 працює як ініціатор активації системи. Він виявляє теплове випромінювання тіла людини та генерує логічний сигнал HIGH (3,3–5 В) при фіксації руху. Цей сигнал подається на цифровий вхід ESP32–CAM (наприклад, GPIO16), що слугує початковою умовою для переходу системи у режим очікування RFID або спроби ідентифікації. HC–SR501 має вбудовані регулятори затримки та чутливості, що дозволяє налаштувати його під конкретні умови приміщення, зменшити кількість хибних спрацювань та підвищити енергоефективність.

Крім того, у системі передбачена кнопка ручного відкриття, підключена до цифрового входу з підтягувальним резистором (режим INPUT_PULLUP). Її натискання генерує сигнал, який дозволяє відкрити замок зсередини приміщення, навіть якщо не використовується RFID. Це рішення підвищує безпеку та дозволяє екстрене розблокування без доступу до бази ідентифікаторів.

Усі периферійні пристрої узгоджено взаємодіють з ESP32–CAM,

утворюючи єдиний механізм. Завдяки використанню стандартних протоколів і цифрових інтерфейсів, система легко розширюється – наприклад, можна підключити датчик температури, камеру з більш високою роздільною здатністю, модуль збереження даних на microSD або блок зв'язку з хмарним сервісом. Таким чином, реалізована взаємодія з периферійними пристроями дозволяє забезпечити повноцінну, автономну та безпечну роботу системи доступу в реальному середовищі.

3.6 Візуалізація роботи системи за допомогою блок–схем

Для повного розуміння логіки функціонування розробленої системи доступу доцільно використовувати блок–схемне подання алгоритмів. Візуалізація у вигляді блок–схеми дозволяє відобразити послідовність подій, логічні умови, гілки прийняття рішень та взаємодію між елементами системи в зручній для аналізу формі. Це особливо важливо на етапі моделювання й тестування поведінки системи, оскільки наочно демонструє, як саме відбувається обробка подій та які дії виконує контролер у відповідь на зовнішні стимули.

У розробленій системі основний алгоритм функціонування починається з моніторингу стану датчика руху HC–SR501. У початковому стані система перебуває в режимі очікування й не споживає додаткових ресурсів. У разі спрацювання датчика – тобто фіксації присутності людини в зоні дії – мікроконтролер переходить у активну фазу. На цьому етапі активується камера, а також ініціюється режим очікування надання ідентифікаційних даних користувача.

Далі система сканує зону на наявність RFID–картки. Якщо картка виявлена, здійснюється зчитування UID і його порівняння з базою дозволених ідентифікаторів. У разі відповідності UID системі –формуються команди на відкриття замка, генерацію сигналу підтвердження через buzzer та старт короткого таймера на повторне блокування. Якщо UID відсутній у

базі, активується гілка відмови в доступі з відповідним звуковим сигналом і поверненням у початковий стан.

Окремо у схемі відображається можливість ручного відкриття дверей за допомогою кнопки. Якщо кнопка натиснута –алгоритм миттєво переходить у режим відкриття, оминаючи фазу перевірки ідентифікатора. Ця функція є критичною для внутрішньої евакуації, технічного обслуговування або у разі збою в мережі.

Блок–схема також включає перевірку тайм–ауту на введення UID. Якщо користувач не підносить RFID–картку впродовж заданого часу, система повертається у початковий стан без спроб авторизації. Це мінімізує ризик зависання або зайвого споживання ресурсів.

На завершальному етапі, після будь–якої дії –дозволеної чи відхиленої – система переходить у стан готовності до нової ітерації, очікуючи повторного спрацювання датчика руху. Така циклічність забезпечує безперервний режим роботи з мінімальними затримками.

Таким чином, побудована блок–схема чітко відображає всі основні сценарії взаємодії користувача з системою, а також умови прийняття рішень у контролері. Це дозволяє не лише протестувати логіку роботи, а й у майбутньому –спростити модернізацію системи, додати нові функції (наприклад, розпізнавання обличчя, біометрію, спілкування з сервером або хмарою) (рис. 3.3).

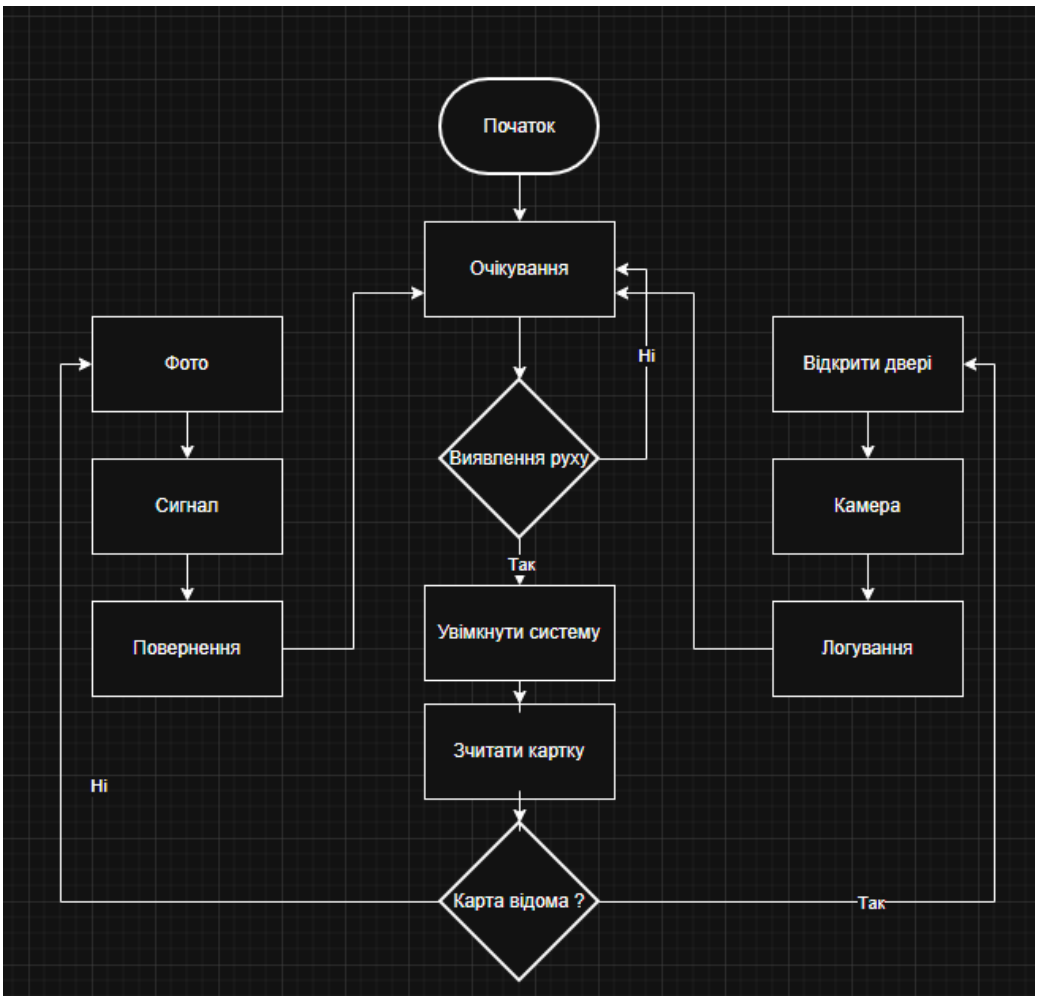

Рисунок 3.3 – Візуалізація роботи системи

3.7 Реалізація взаємодії з ботом у месенджері

Інтеграція системи доступу з ботом у месенджері є важливою складовою концепції IIoT, яка передбачає не лише локальну автоматизацію, але й віддалене управління та моніторинг. Взаємодія з ботом дозволяє забезпечити інформаційний зворотний зв’язок у режимі реального часу, а також надати адміністраторам або відповідальним особам можливість оперативного реагування на події, пов’язані з контролем доступу. Це особливо важливо для виробничих підприємств з підвищеними вимогами до безпеки та обліку.

У рамках розробленої системи бот у месенджері виконує кілька

функцій: приймання повідомлень від пристрою з деталями спроби доступу, передавання фото, знятого камерою в момент активації системи, а також отримання команд на керування. Система надсилає такі повідомлення при кожному спрацюванні –незалежно від результату авторизації. Повідомлення містить дату, час, статус доступу (дозволено/заборонено), ID картки та, за потреби, знімок з камери ESP32–CAM.

З технічної точки зору, взаємодія з ботом реалізується через HTTP–запити за допомогою стандартних бібліотек Wi–Fi–клієнта. Контролер після підключення до мережі виконує POST–запит до API месенджера з передачею параметрів повідомлення. У разі потреби також можлива передача медіафайлів (фото) на сервер за попередньо сформованим запитом. Усе це виконується в автоматичному режимі без втручання людини.

Окремою функціональністю бота є можливість приймання команд. Наприклад, адміністратор може надіслати команду “Відкрити” або “Заблокувати”, яка буде сприйнята мікроконтролером як команда на відповідну дію. Це дозволяє забезпечити дистанційне керування доступом у випадках, коли система не розпізнала UID або коли вхід потрібно дозволити за виняткових обставин. Також передбачена можливість отримання стану системи, останніх подій або оновлення переліку дозволених UID.

Важливо зазначити, що такий підхід не лише підвищує інформативність системи, але й значно розширює її функціональність. З одного боку, вона працює автономно, як класична система контролю доступу, а з іншого – взаємодіє з людиною на вищому логічному рівні, підтримуючи двосторонній обмін інформацією. Таким чином, взаємодія з ботом у месенджері підвищує рівень цифровізації, інтеграції та гнучкості системи, що відповідає сучасним вимогам до інтелектуальних виробничих рішень.

4 РОЗРАХУНКИ З ТЕОРІЇ АВТОМАТИЧНОГО УПРАВЛІННЯ

4.1 Визначення типу керуючої системи

У контексті розробки системи контролю доступу на базі технологій Інтернету речей (IIoT), важливо правильно визначити тип керуючої системи, що дозволить забезпечити ефективне функціонування всіх підсистем, своєчасну обробку даних, адаптивність та масштабованість рішення.

Керуюча система, що застосовується у проєкті, є мікропроцесорною, оскільки основою апаратної частини виступає модуль ESP32–CAM. Цей модуль поєднує в собі обчислювальні можливості, засоби введення/виведення, вбудовану камеру та бездротові інтерфейси [3]. Завдяки цьому він виконує функції локального контролера, що обробляє дані з сенсорів (датчик руху, зчитувач RFID), керує виконавчими механізмами (сервомотор, буззер) та забезпечує передачу інформації до віддаленого сервера чи месенджера [5].

Тип керуючої системи, який реалізовано, можна класифікувати як автономну цифрову систему реального часу з елементами розподіленого управління. Вона приймає рішення в залежності від вхідних сигналів у режимі реального часу –наприклад, розпізнає RFID–картку, фіксує рух або активує камеру. При цьому частина функцій, пов’язаних з аналізом і збереженням даних, винесена у хмарне середовище або на інтерфейс користувача (через бота в месенджері), що є характерним для розподілених систем [6].

Основними характеристиками цієї керуючої системи є:

– модульність;

– інтерактивність, оскільки система реагує не лише на фізичні події; але й на команди оператора [2];

– автономність;

– гнучкість, що полягає у можливості змінити логіку роботи програмним шляхом;

– масштабованість, тобто можливість розширення системи до кількох точок доступу, підключення до мережі підприємства або інтеграції з іншими IIoT–сервісами.

Таким чином, обрана керуюча система повністю відповідає концепції індустрії 4.0, в якій автономність, взаємодія пристроїв, обробка великих обсягів даних та гнучкість управління є ключовими елементами. Такий підхід дозволяє не лише реалізувати базовий функціонал контролю доступу, а й створити платформу для подальшого розвитку функціоналу в межах підприємства.

4.2 Розрахунок часу реакції системи

Час реакції системи контролю доступу є критично важливим параметром, що визначає її ефективність, безпечність і комфортність у користуванні. У контексті розроблюваної системи, яка включає модуль ESP32–CAM, RFID–зчитувач, датчик руху, сервомотор, камеру та бот в месенджері, необхідно врахувати час затримок на всіх етапах обробки сигналів –від надходження вхідного сигналу до спрацьовування виконавчого механізму [13].

Розглянемо основні етапи, які формують загальний час реакції системи:

1. Зчитування RFID–картки або сигналу з датчика руху.

2. RFID–зчитувач RC522 працює з частотою 13,56 МГц та забезпечує час зчитування даних з картки в межах 100–200 мс [14]. Датчик руху HC–SR501 має затримку спрацьовування близько 200–300 мс залежно від налаштувань[15].

3. Обробка сигналу контролером ESP32–CAM.

4. Процесор ESP32 працює на частоті до 240 МГц, тому обробка простих умовних операторів (перевірка UID, зчитування даних з GPIO) займає менше 10 мс. Проте, якщо відбувається передача зображення або обмін даними з мережею, час обробки може збільшитися до 200–500 мс.

5. Передача інформації до бота в месенджері (при потребі). Комунікація через Wi–Fi та API месенджера Telegram займає від 500 мс до 1,5 с, залежно від швидкості інтернет–з'єднання та навантаження на сервери.

6. Виконання дії (наприклад, відкриття дверей). Сервомотор SG90 реагує на подану команду за 50–100 мс, а повний поворот на 90 градусів триває до 500 мс.

7. Активація буззера або іншого звукового сигналу. Час реакції практично миттєвий (до 10 мс) після подачі логічного сигналу з ESP32.

Загальний час реакції системи можна представити як суму всіх вищевказаних компонентів:

При RFID–авторизації без участі камери та бота:

– очитування RFID: ~ 150 мс;

– обробка ESP32: ~ 10 мс;

– сервомотор: ~ 100 мс;

– загалом: ~ 260 мс;

При авторизації з повідомленням у месенджер:

– зчитування/виявлення руху: ~ 200 мс;

– обробка ESP32 + камера: ~ 500 мс;

– передача даних до бота: ~ 1 с;

– відповідь бота й реакція системи: ~ 1 с;

– сервомотор: ~ 100 мс;

– загалом: ~ 2,8 с.

Таким чином, у базовому режимі без інтернет–з'єднання система працює практично миттєво, з часом реакції менше 0,5 секунди. У розширеному режимі з хмарною інтеграцією реакція може затягуватися до 3 секунд, що є прийнятним для користувача.

Цей розрахунок дозволяє оптимізувати логіку системи, наприклад, використовувати лише локальне рішення у критичних зонах, а месенджер – для моніторингу або резервного підтвердження. Також є можливість використовувати буферні механізми або кешування для зменшення затримок.

4.3 Розрахунок надійності системи

Надійність системи контролю доступу –це здатність виконувати задані функції протягом встановленого часу без збоїв. Для обчислення показників надійності враховуються характеристики окремих компонентів системи, частота їхніх відмов і вплив зовнішніх факторів [21].

Найбільш поширеним показником надійності є середній напрацювання на відмову (MTBF –Mean Time Between Failures), що обчислюється як:

$$\text{MTBF} = \frac{1}{\lambda},$$

де $\boldsymbol{\lambda}$ –інтенсивність відмов (кількість відмов за одиницю часу).

Для спрощеного розрахунку приймемо умовно оцінені значення MTBF для основних компонентів системи (на основі даних виробників та відкритих джерел) (таблиця 4.1).

Таблиця 4.1 – Таблиця оцінки значення MTBF для основних компонентів

Компонент	MTBF, годин
ESP32–CAM	100 000
RFID–зчитувач RC522	50 000
Сервомотор SG90	25 000
Датчик руху HC–SR501	30 000

Продовження таблиці 4.1

Компонент	MTBF, годин
Камера OV2640	80 000
Буззер	100 000

Система в цілому складається з послідовно підключених елементів. У цьому випадку загальний MTBF системи визначається за формулою:

$$\frac{1}{\text{M}TBF\text{системи}} = \sum_{i=1}^{n} \frac{1}{MTBFi}.$$

Підставимо значення:

$$\frac{1}{\text{M}TBF\text{системи}} = \frac{1}{100000} + \frac{1}{50000} + \frac{1}{25000} + \frac{1}{30000} + \frac{1}{80000} + \frac{1}{100000} \approx$$

$$\approx 0{,}00001 + 0{,}00002 + 0{,}00004 + 0{,}0000333 + 0{,}0000125 + 0{,}00001 =$$

$$= 0{,}0001258 \approx 7950\text{годин}$$

Це означає, що в середньому система здатна працювати без збоїв приблизно 7 950 годин або понад 330 днів при безперервній роботі. Для умов використання в системі контролю доступу, яка працює періодично, це є прийнятним рівнем надійності.

Щоб підвищити надійність:

– можна реалізувати резервування ключових компонентів (наприклад, дублюючий зчитувач);

– використовувати захист від перенапруг, стабілізатори живлення, перевірку зв’язку з ботом;

– додати діагностичні функції, які дозволять попереджати користувача про потенційні збої (наприклад, через логування або

повідомлення у месенджер);

Таким чином, розроблена система має достатній запас надійності для невеликого офісного або виробничого приміщення з можливістю масштабування у разі необхідності.

4.4 Розрахунок енергоспоживання системи

Оцінка енергоспоживання є важливою складовою проєктування системи контролю доступу, особливо якщо передбачається автономна або енергоефективна робота пристрою. Розрахунок здійснюється на основі паспортних даних кожного з компонентів системи [22].

Склад системи:

– ESP32–CAM;

– RFID–зчитувач RC522;

– сервомотор SG90;

– датчик руху HC–SR50;

– буззер;

– камера OV2640 (інтегрована в ESP32–CAM).

Номінальні споживання струму компонентами (таблиця 4.2).

Таблиця 4.2 – Споживання струму компонентами.

Компонент	Напруга,В	Струм, мА	Потужність, мВт
ESP32–CAM	5	160	800
RFID RC522	3,3	13	43
Сервомотор SG90	5	250	1250
HC–SR501	5	50	250
Буззер (активний)	5	30	150

Сервомотор споживає піковий струм у момент активації (до 250 мА), у стані спокою – значно менше.

Максимальне споживання потужності системи в активному режимі:

$$P\text{заг} = P_{ESP32-CAM} + P_{RFID} + P_{\text{серво}} + P_{HC-SR501} + P_{\text{буззер}} =$$
$$= 800 + 43 + 1250 + 250 + 150 = 2493 \approx 2{,}5 \text{ Вт.}$$

Тобто система у момент пікового навантаження споживає приблизно 2,5 Вт. У реальному використанні середнє споживання буде меншим, оскільки більшість компонентів не активні постійно. Наприклад, сервомотор працює лише при відкритті дверей, а буззер –кілька секунд під час сигналу.

Оцінка середнього споживання.

Припустимо, що середній робочий цикл (відсканування карти, відкриття дверей, сигнал) триває 5 секунд.

Таких подій за день –до 100. Період активності за день:

$$5 \cdot 100 = 500 = 0{,}14 \text{ год.}$$

Решту часу (23,86 год.) система працює в режимі очікування, де ESP32–CAM може бути переведено в енергозберігаючий режим (до 20 мА), а інші компоненти споживають мінімум.

Денне споживання:

– активний режим: 2,5 Вт · 0,14 год. ≈ 0,35 Вт·год;

– очікування (0,2 Вт): 0,2 Вт · 23,86 год ≈ 4,77 Вт·год;

– разом за добу: ≈ 5,12 Вт·год.

Місячне споживання – 5,12 Вт\cdotpгод·30=153,6 Вт\cdotpгод =

= 0,1536 кВт.

Це менше 0.2 кВт·год на місяць, що робить систему дуже енергоефективною. Навіть за поточною ціною електроенергії, вартість

живлення системи залишається мізерною.

5 РЕАЛІЗАЦІЯ ПРОТОТИПУ ТА ТЕСТУВАННЯ СИСТЕМИ ДОСТУПУ

5.1 Збірка прототипу на макетній платі Розрахунок надійності системи

Після того, як ідея системи оформлювалась у голові та на схемах, настав момент перейти до реального збирання. Було вирішено почати з макетної версії – це дає змогу швидко тестувати підключення, змінювати розводку без пайки та бачити одразу результат. Основою став звичайний макетний стенд MB–102 і модуль живлення з перемикачами на 5 В та 3,3 В – без нього не обійтись, бо компоненти у схемі мають різні вимоги до напруги.

Спочатку розмістимо на платі ESP32–CAM, приєднав адаптер для живлення та прошивки. Потім підключив RFID–модуль RC522, який працює виключно на 3,3 В – для нього спеціально виділяємо одну сторону макетної плати з пониженим живленням. Далі – інфрачервоний датчик руху HC–SR501, який оріємо на передбачувану зону входу. Після нього – сервомотор SG90, підключений до PWM–виходу. На завершення – кнопка, яку можна натиснути в обхід RFID, для ручного запуску (перевірено – працює як треба) (рис. 5.1).

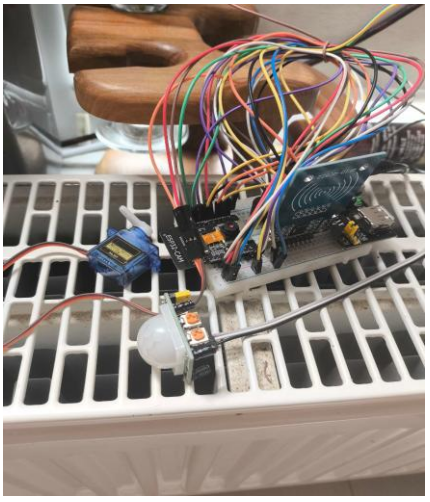

Рисунок 5.1 –Зібрана модель

Коли все зібрано, треба кілька разів перевірити підключення мультиметром, особливо перед тим, як подавати живлення. Подаючи через DC–адаптер 9 В на модуль живлення макетної плати – так отримаємо стабільні 5 В і 3,3 В одночасно на дві шини. Це була ключова частина: ESP32, RFID та серво – усі повинні отримувати правильну напругу, інакше або не працюють, або перезавантажуються.

Зовні система виглядає як невеличкий модульний щит з кількома компонентами, але всередині вона вже «живе»: камера дивиться, RFID чекає на картку, серво готове крутитися.

Цей етап збирання дав змогу буквально «відчути» систему – коли тримаєш в руках макет і бачиш, як усе пов’язано, значно краще розумієш, що і навіщо ти робиш.

5.2 Підключення компонентів та налагодження живлення

Після того як усі компоненти зайняли свої місця на макетній платі, настав найвідповідальніший момент – зробити правильне підключення й не спалити нічого з першої спроби. На цьому етапі треба діяти максимально уважно.

Починаючи із підключення модуля живлення MB–102 до макетної плати. На ліву сторону подаємо 5 В, а на праву – 3,3 В, тому що RC522 не терпить перенапруги й може вийти з ладу при 5 В. (рис. 5.2).

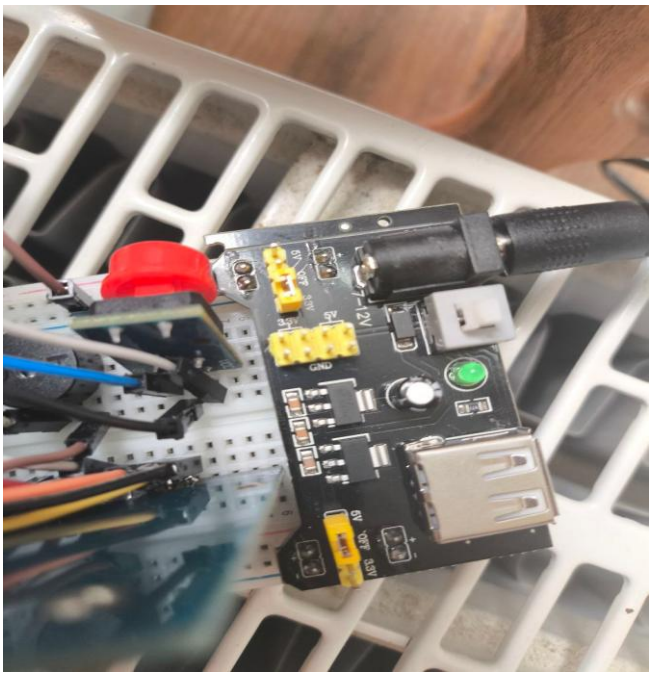

Рисунок 5.2 – Перемикачі живлення на MB - 102 – 5 В і 3,3 В.

Наступним кроком буде взятися за ESP32 - CAM. Підключивчи живлення на пін 5 В, GND – на спільну шину. Оскільки ESP32 треба стабільне живлення, особливо коли працює Wi-Fi або камера – треба переконатися, що адаптер видає не менше 1 А при 9 В (рис. 5.3).

Рисунок 5.3 – Подача живлення на ESP32–CAM через макетну плату

Далі – RC522. Підключення йшло за SPI–протоколом, тож з’єднуємо SDA з GPIO2, SCK з GPIO14, MOSI з GPIO15, MISO з GPIO12, а RST – з GPIO13. Живлення подав із шини 3.3 В, земля – на загальний GND. Усе акуратно розводимо по боках, щоб можна було прикладати картку, не чіпаючи дроти.

Сервомотор SG90 підключаємо до GPIO0, а живлення подаємо безпосередньо з 5 В – шини. Тут головне – не перевантажити, бо при старті серво бере короткий імпульс до 500 мА. На щастя, адаптер витримав. GND серво – на спільну землю (рис. 5.4).

Рисунок 5.4 – Підключення сервомотора SG90

Датчик руху HC–SR501 подав на GPIO4. Тут усе просто – він має три пина: VCC (5 В), GND і OUT. Налаштування чутливості та затримки здійснював на місці обертанням потенціометрів – щоб він реагував не на кожен рух, а саме на людину, що наближається до дверей (рис. 5.5).

Рисунок 5.5 – Розташування HC–SR501 на макетній платі

Наостанок підключивчи кнопку до GPIO16. Вона працює в режимі INPUT_PULLUP – тобто підтягування резистором не потрібно, просто один контакт на землю, інший – на GPIO.

Після підключення всіх модулів треба кілька разів перевірити правильність під’єднання та мультиметром пройшовся по лініях живлення. Це допомогло виявити, наприклад, що випадково підключен один з GND на вільний пін. Добре, що перевіряв перед подачею живлення.

Після подачі живлення система «ожила»: ESP32 засвітився, серво коротко смикнувся, а камера через серійний порт видала повідомлення про запуск.

5.3 Завантаження прошивки та конфігурація ESP32–CAM

Коли вся схема вже зібрана й перевірена – настає найбільш хвилюючий етап: завантаження прошивки. Це той момент, коли ти переходиш від «заліза» до «мозку» системи. В цьому випадку вся логіка, включно з перевіркою картки, обробкою сигналів, відкриттям замка й

відправкою повідомлень у бот, писалась у Arduino IDE.

Щоб завантажити скетч у ESP32 - CAM, спочатку потрібно підключити його до ПК через адаптер USB - UART. Для цього використовуємо звичайний FTDI - адаптер, але важливо, щоб він мав можливість перемикання між 3.3В і 5 В. У нашому випадку ESP32 живився окремо через макетну плату, тому з USB передаємо тільки RX, TX та GND.

Перед завантаженням потрібно активувати режим прошивки: з'єднавши пін IO0 із GND – це обов'язкова умова, щоб ESP32 - CAM увійшов у режим Bootloader

У Arduino IDE попередньо встановлюємо такі налаштування (рис.5.6).

Рисунок 5.6 – налаштування перед завантаженням скетчу

Після цього натискаємо «Upload», в консолі з'явився знайомий «Connecting...», а потім – успішна заливка (рис. 5.7).

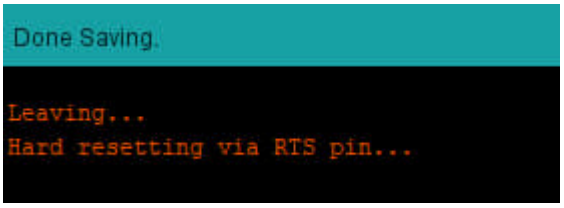

Рисунок 5.7 – Завантаження скетчу в Arduino IDE

Як тільки прошивка завершилась, трема розімкнути IO0 і натиснути кнопку Reset на ESP. У моніторі порту почали з’являтися системні повідомлення. Це означало, що ESP32 - CAM запустився у звичайному режимі. Після цього прикладаємо RFID–картку, та бачимо у консолі UID.

У скетчі також додємо логіку для надсилання фото в бот месенджера. Для цього попередньо створимо Telegram–бота через BotFather, отримавши токен і вставив його у код. Також був прописаний ID чату, щоб бот знав, куди надсилати сповіщення (рис.5.8).

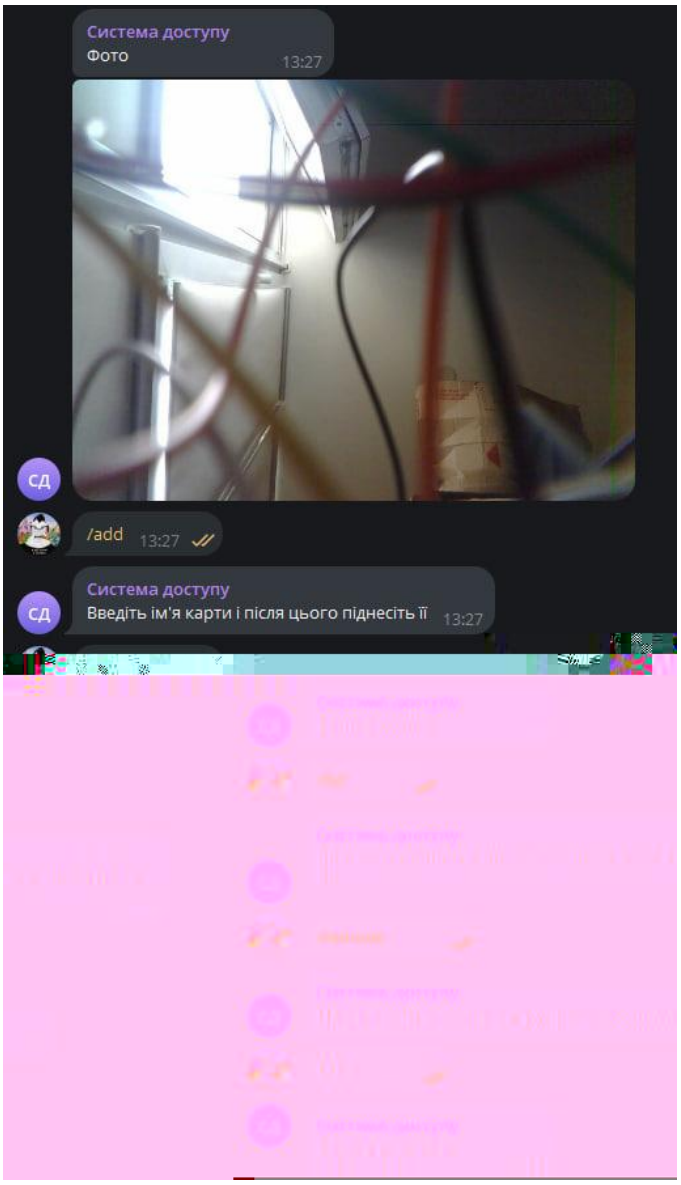

Рисунок 5.8 – Повідомлення в Telegram з фото

Після перевірки всіх функцій (реакція на рух, обробка картки, робота серво) треба протестувати таймер неактивності: через 30 секунд без подій система сама вимикає камеру та Wi–Fi й переходить у сплячий режим. Це важливо, особливо якщо живлення – від акумулятора.

Таким чином, на цьому етапі контролер отримав свою «свідомість». Із простого набору електроніки він перетворився на повноцінну систему, здатну ідентифікувати, реагувати та фіксувати події, як це робить будь–який «розумний» пристрій на сучасному виробництві.

5.4 Демонстрація авторизації RFID–картки та відкриття замка

Коли прошивка вже працює, а всі компоненти реагують – настає той момент, коли ти вперше прикладаєш картку й дивишся: відкриється замок чи ні? Саме з цієї сцени, мабуть, і починається справжній "екзамен" для системи доступу.

Після запуску скетчу ESP32 - CAM перейшла в активний режим. Підносимо руку до датчика руху HC - SR501, і одразу ліхтарик на платці засвітився, це означає що датчик спрацював. Система активна. У цей момент включилась камера, ініціалізувався RFID–зчитувач і з'явилось вікно очікування картки.

Прикладаємо попередньо додану RFID–картку і одразу відкрився замок (рис. 5.9).

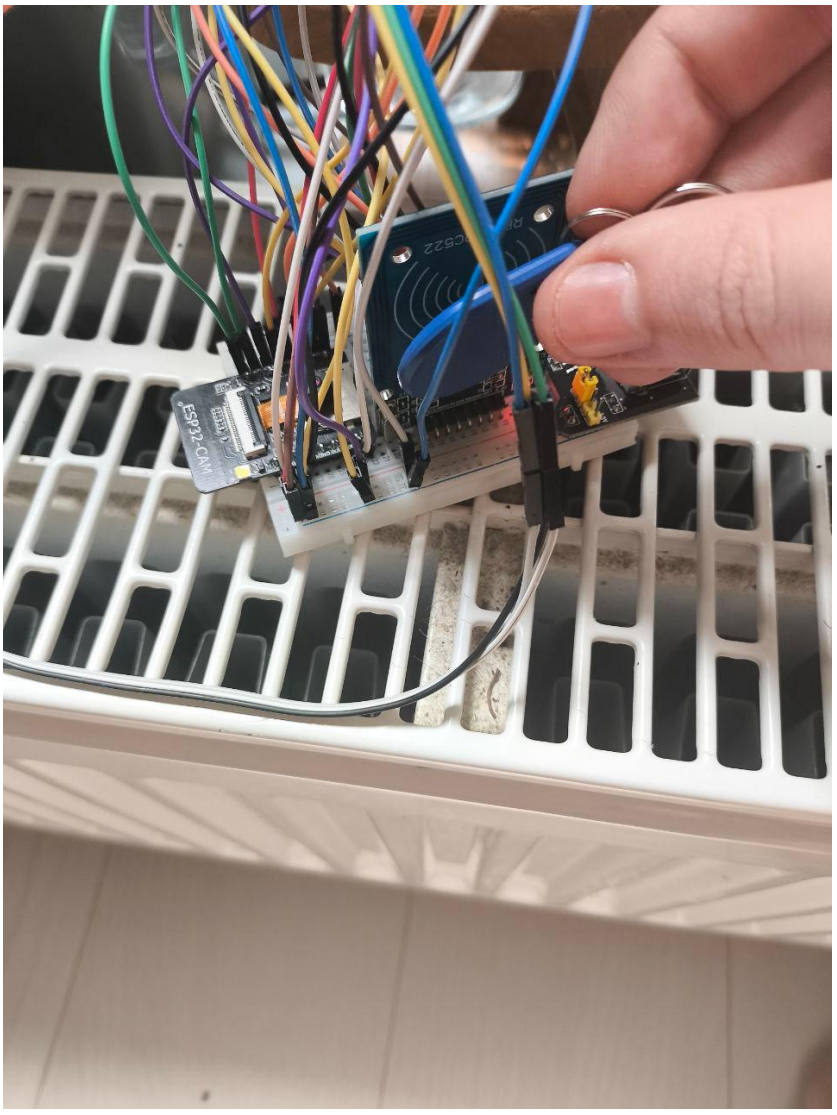

Рисунок 5.9 – Момент прикладання RFID–картки до модуля RC522

Одразу після цього серводвигун SG90 плавно повернувся на 90 градусів – імітуючи відкриття дверей, і через 10 секунд система автоматично закрила замок (серво повернулось у початкову позицію).

Для перевірки безпеки спробуємо прикласти іншу RFID–картку, яка не була в базі. У відповідь з’явилось фото і пропищав зумер.

Також був реалізований варіант ручного відкриття замка через кнопку. При натисканні – ті ж самі дії: серво відкриває, камера знімає, замок закривається. Це стало в нагоді при моделюванні ситуації, коли адміністратор або технічний персонал має відкрити вручну.

Ця демонстрація стала ключовим моментом –ми побачили, як із

набору окремих модулів утворилась цілісна система, здатна реагувати, приймати рішення, і навіть взаємодіяти з користувачем на відстані.

5.5 Тестування реакції на рух та фіксація подій камерою

Після перевірки базової функціональності системи доступу, наступним кроком стало тестування модуля виявлення руху та механізму фіксації подій камерою. Даний етап був необхідним для підтвердження здатності системи своєчасно реагувати на наближення користувача та забезпечувати фотофіксацію подій, залежно від сценарію доступу.

У режимі очікування система перебувала в енергозберігаючому стані, де активним залишався лише інфрачервоний датчик руху HC–SR501. Як тільки датчик фіксував рух у межах встановленого радіусу дії (приблизно 3–5 метрів), мікроконтролер ESP32–CAM виходив із режиму сну та активував усі необхідні модулі: камеру, RFID–зчитувач, сервомотор та Wi–Fi–з’єднання. стан після виявлення руху.

У ході випробувань перевірялося, наскільки швидко система реагує на появу людини в зоні дії датчика. Затримка між виявленням руху та повною активацією камери склала в середньому менше 2 секунд, що є прийнятним показником для систем безпеки початкового рівня.

Тестування показало, що рівень фіксації подій є достатньо високим: жоден сценарій не залишився непоміченим або невідредагованим. Також були змодельовані ситуації, коли декілька людей підходили до системи одна за одною. Система коректно обробляла кожну подію, перезапускаючи цикл фіксації після кожної активації.

Після завершення тестування було підтверджено, що всі ключові події – зокрема виявлення руху, авторизація картки, відкриття дверей та неуспішна спроба – супроводжуються збереженням відповідного фото – та його оперативною передачею до адміністратора.

Загалом результати тестування підтвердили працездатність та

надійність реалізованої функції фіксації подій. Це забезпечує не лише контроль доступу, а й створює доказову базу у випадку спірних ситуацій або інцидентів безпеки.

5.6 Виявлення помилок та коригування роботи системи

У процесі збирання, прошивки та тестування прототипу системи доступу були зафіксовані окремі технічні труднощі та логічні помилки, які впливали на стабільність або коректність роботи системи. Проведення повного циклу перевірок дозволило своєчасно виявити недоліки та внести необхідні коригування в апаратну схему та програмну логіку.

Першою проблемою, з якою довелось зіткнутися, було нестабільне живлення ESP32–CAM. У момент активного використання камери та увімкнення Wi–Fi модуль іноді перезавантажувався або «зависав». Причиною виявився недостатній струм від живлення, зокрема при використанні USB–порту ноутбука або слабкого адаптера. Було прийнято рішення використовувати зовнішній адаптер на 9 В (1 А) у поєднанні з модулем живлення MB–102. Це забезпечило стабільну подачу 5 В на ESP32–CAM, навіть у пікові моменти навантаження.

Другим недоліком став неправильний пін підключення сервомотора, який спочатку був налаштований на пін, зайнятий внутрішньою функцією ESP32. Це призводило до конфліктів, серво не працював або поводився хаотично. Проблему вирішено зміною піну керування на GPIO0, що є стабільним для PWM–виводу у режимі роботи модуля.

Ще однією проблемою стало занадто чутливе спрацьовування датчика руху, який реагував навіть на незначні тіні або коливання повітря. Було проведено ручне налаштування потенціометра на корпусі HC–SR501, щоб скоригувати зону виявлення та затримку спрацьовування. Після налаштування система почала реагувати лише на реальні наближення людини.

Загалом, усі виявлені недоліки були пов’язані із типовими для етапу прототипування помилками – апаратними конфліктами, енергоспоживанням, програмною оптимізацією. Їх своєчасне усунення дозволило забезпечити стабільну та передбачувану роботу системи навіть у складних умовах.

6 ОХОРОНА ПРАЦІ

У процесі розроблення системи автоматизованого контролю доступу з використанням мікроконтролера ESP32–CAM та RFID–модуля особливу увагу приділяється питанням охорони праці. Це забезпечує безпечні умови роботи для персоналу, що експлуатує та обслуговує систему, а також запобігає виникненню аварійних ситуацій на виробництві.

Під час розробки та впровадження електронних систем необхідно дотримуватись вимог законодавства України у сфері охорони праці, зокрема Закону України «Про охорону праці», а також правил безпечної експлуатації електроустановок споживачів. Всі роботи з електронними компонентами слід виконувати при відключеному живленні, використовуючи інструменти з ізольованими ручками та засоби індивідуального захисту (ЗІЗ).

Усі елементи системи, включаючи ESP32–CAM, RFID RC522, сервомотор SG90 та інші периферійні пристрої, живляться від низьковольтного джерела (3.3–5 В), що суттєво знижує ризик ураження електричним струмом. Однак при підключенні до комп’ютера через USB або живленні від мережевого адаптера необхідно дотримуватись правил електробезпеки – уникати коротких замикань, перевантаження по струму, використання пошкоджених кабелів чи контактів.

Компоненти, які використовуються в системі, не мають високої пожежної небезпеки. Проте під час експлуатації обладнання слід уникати перегріву, особливо при тривалому живленні сервоприводу або камери. Необхідно дотримуватись правил зберігання горючих матеріалів та передбачити наявність первинних засобів пожежогасіння (вогнегасник, пісок, азбестова ковдра тощо).

Робоче місце розробника повинно бути обладнане відповідно до ергономічних норм. Джерела живлення та електронні модулі мають бути надійно закріплені, мати захисні елементи (корпуси, кожухи), а всі з'єднання

повинні бути виконані за допомогою ізольованих проводів. Освітлення повинно бути достатнім, без мерехтіння, а температура в приміщенні – комфортною для тривалого перебування.

Оскільки робота пов’язана з тривалим перебуванням перед монітором, необхідно передбачити дотримання режиму праці та відпочинку. Рекомендується кожні 60 хвилин робити 5–10–хвилинні перерви, виконувати вправи для очей, а також підтримувати правильну позу під час роботи за комп’ютером.

Проект не передбачає шкідливих викидів чи використання токсичних речовин. Однак при утилізації електронних компонентів слід дотримуватись правил поводження з електронними відходами відповідно до чинного законодавства.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було реалізовано повнофункціональну прототипну систему контролю доступу до виробничого приміщення з використанням технологій Industrial Internet of Things (IIoT). Враховуючи сучасні потреби підприємств у безпеці, автономності та цифровізації, обрана тема є актуальною та має практичне значення.

На першому етапі було проаналізовано проблематику традиційних систем доступу, визначено ключові вимоги до новітньої IIoT–орієнтованої архітектури та обґрунтовано необхідність впровадження інтелектуального підходу з використанням безконтактної ідентифікації, сенсорного моніторингу, та віддаленої взаємодії з користувачем.

У рамках апаратної реалізації було здійснено добір і поелементне підключення всіх компонентів системи: мікроконтролера ESP32–CAM, RFID–зчитувача RC522, сервомотора SG90, інфрачервоного датчика руху HC–SR501, кнопки, модуля живлення MB–102 та логічного інтерфейсу для взаємодії з користувачем. Особливу увагу було приділено стабільності живлення та енергоефективному режиму роботи, що дозволило забезпечити надійність у автономному режимі.

Програмна частина передбачала створення логіки виявлення активності, перевірки авторизації, відкриття/закриття замка, фіксації подій за допомогою камери, а також передачі фото адміністраторам через бот у месенджері. Була реалізована гнучка логіка: при санкціонованому доступі надсилається фото, а при несанкціонованій спробі – фотографія особи. Також передбачено автоматичне повернення системи до режиму сну після 30 секунд бездіяльності.

У процесі тестування система показала стабільну роботу: швидке

реагування на рух, точну обробку UID RFID–карток, коректну роботу сервомеханізму та успішну передачу повідомлень. Завдяки налаштуванням камери та оптимізації тривалості записів було досягнуто балансу між якістю фіксації подій та обмеженими ресурсами мікроконтролера.

Результатом виконаної роботи стало створення реального функціонального прототипу інтелектуальної системи доступу, яку в подальшому можливо масштабувати, адаптувати під потреби конкретного підприємства або використовувати як базу для інтеграції з більш складними IIoT–рішеннями. Отримані знання та практичні навички з мікроконтролерного програмування, побудови схем, роботи з API месенджера та теорії автоматичного управління підтвердили професійну готовність здобувача до виконання інженерних задач у галузі автоматизації та комп’ютерно–інтегрованих технологій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ДСТУ 3008–15. Документація. Звіти у сфері науки та техніки. Структура та правила оформлення. Введ. 2015–06–22. К. Держстандарт України, 2017. – 29с

2. Методичні вказівки з підготовки кваліфікаційної роботи бакалавра для студентів усіх форм навчання спеціальності 151 «Автоматизація та комп'ютерно–інтегровані технології» освітньої програми «Автоматизація та комп'ютерно–інтегровані технології» / Упоряд.: І.Ш. Невлюдов, А.О. Андрусевич, О.В. Токарєва, С.П. Новоселов, О.В Сичова. Харків: ХНУРELee I., Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises // Business Horizons. – 2016. – № 58(4). – P. 431–440.

3. Невлюдов І.Ш., Євсєєв В.В., Максимова С.С. BEAM робототехніка: Навчальний посібник. – Oktan Print – Prague.: 2024.- 276 с.

4. Гнатюк С. О., Іванов В. С. Технології IIoT в системах безпеки підприємств // Технології та засоби автоматизації. – 2020. – № 3(67). – С. 55–62.

5. Комплекс навчально-методичного забезпечення навчальної дисципліни «Безпека праці в індустрії ІТ-технологій» підготовки освітнього рівня бакалавр усіх спеціальностей та усіх напрямів університету [http://catalogue.nure.ua/knmz] / ХНУРЕ; розроб.: Т. Є. Стиценко, Г. В. Пронюк, Н. М. Сердюк. – Харків, 2017. – 122 с.

6. Основи наукових досліджень : підручник / І. Ш. Невлюдов, Ю. М. Олександров, А. О. Андрусевич, О. О. Чала ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Prague : OKTAN PRINT, 2024. – 468 с.

7. Невлюдов І.Ш. Виробничі процеси та обладнання об'єктів автоматизації. Збірник задач: Навчальний посібник / І.Ш. Невлюдов, А.О. Андрусевич, Г.В. Пономарьова, А.О. Функендорф. Кривий Ріг: КК НАУ. 2018. – 332 с.

8. Шевченко А.І. Індустріальний Інтернет речей: виклики і перспективи впровадження в Україні // Науковий вісник ХПІ. Серія: Системи управління. Навігація та зв'язок. – 2019. – № 2(1327). – С. 11–17.

9. Мельник І. А. Інтернет речей як рушійна сила цифрової трансформації підприємств // Економіка та держава. – 2022. – № 2. – С. 47–52.

10. Коваленко С. Індустріальний Інтернет речей: прикладні аспекти впровадження на українських підприємствах // Науково–технічний вісник ІФНТУНГ. – 2020. – № 1(21). – С. 45–50.

11. Слободянюк А. П. Безпека інформаційних систем на основі IIoT: проблеми та підходи // Вісник НТУ «ХПІ». – 2021. – № 45(1417). – С. 96–102.

12. Коваленко В. Інтернет речей у промисловості: від концепції до

впровадження // Техніка та енергетика АПК. – 2020. – № 3. – С. 25–31.

13. Al–Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications // IEEE Communications Surveys & Tutorials. – 2017. – № 17(4). – P. 2347–2376.

14. Zhang Y., Wang K., Sun Y. Industrial Big Data Analytics: Challenges, Methodologies, and Applications // IEEE Transactions on Industrial Informatics. – 2017. – № 13(4). – P. 2053–2066.

15. He W., Xu L.D. Integration of Distributed Enterprise Applications: A Survey // IEEE Transactions on Industrial Informatics. – 2017. – № 13(6). – P. 2809– 2819.

16. Boyes H., Hallaq B., Cunningham J., Watson T. The Industrial Internet of Things (IIoT): An Analysis Framework // Computers in Industry. – 2018. – № 101. – P. 1–12.

17. Wan J., Tang S., Shu L., Wang S. Software–Defined Industrial Internet of Things in the Context of Industry 4.0 // IEEE Sensors Journal. – 2017.

– № 16(20). – P. 7373–7380.

18. Choi Y., Lee H. Industrial IoT security threats and real–time detection based on deep learning // Sensors. – 2020. – № 20(13). – P. 3787.

19. Lin J., Yu W., Zhang N., Yang X., Zhang H., Zhao W. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications // IEEE Internet of Things Journal. – 2017. – № 4(5). – P. 1125–1142.

20. Zhang C., Huang Y. An IIoT architecture for smart manufacturing based on 5G and edge computing // IEEE Access. – 2021. – № 9. – P. 42563–42575.

21. Кулик А. В. IIoT у машинобудуванні: сучасні тенденції та підходи //

Вісник машинобудування. – 2021. – № 5. – С. 13–20.

22. Mavromoustakis C.X., Mastorakis G., Batalla J.M. Internet of Things (IoT) in 5G Mobile Technologies. – Springer, 2016. – 374 p.

23. Papacharalampopoulos A., Mourtzis D. Design and planning of smart manufacturing systems // Procedia CIRP. – 2018. – № 78. – P. 153–158.

24. Jing Q., Vasilakos A.V., Wan J., Lu J., Qiu D. Security of the Internet of Things: perspectives and challenges // Wireless Networks. – 2016. – № 20(8). – P. 2481– 2501.

25. Zhou K., Liu T., Zhou L. Industry 4.0: Towards future industrial opportunities and challenges // Proceedings of the 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). – 2016. – P. 2147–2152.

26. Xu L.D., He W., Li S. Internet of Things in Industries: A Survey // IEEE Transactions on Industrial Informatics. – 2016. – № 10(4). – P. 2233–2243.

27. Kang H.S., Lee J.Y., Choi S., Kim H., Park J.H., Son J.Y., Kim B.H., Do Noh S. Smart manufacturing: Past research, present findings, and future directions // International Journal of Precision Engineering and Manufacturing–Green Technology. – 2016. – № 3(1). – P. 111–128.

28. Chang Y.C., Hung S.C. A framework for smart manufacturing

based on IIoT // Sustainability. – 2018. – № 10(2). – P. 482.

29. Oliveira R.A., Rodrigues J.J., Kumar N., de Albuquerque V.H.C. Industrial IoT security threats and vulnerabilities: A systematic review // IEEE Communications Surveys & Tutorials. – 2021. – № 23(1). – P. 586–630.