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'ютерна система моніторингу середовища і контролю доступу до серверного приміщення*

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

	(підпис)	Дуніковський С. Б. (прізвище та ініціали)
Керівник	(підпис)	Жаровський Р.О. (прізвище та ініціали)
Нормоконтроль	(підпис)	Тиш Є.В. (прізвище та ініціали)
Завідувач кафедри	(підпис)	Осухівська Г.М. (прізвище та ініціали)
Рецензент	(підпис)	Млинко Б.Б. (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)
«25» 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)

студента *Дуніковського Стефана Богдановича*
(прізвище, ім'я, по батькові)

1. Тема роботи *Комп'ютерна система моніторингу середовища і контролю доступу до серверного приміщення*

Керівник роботи *кандидат технічних наук, доцент кафедри КС Жаровський Руслан Олегович*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від *« 24 » квітня 2026 року № 4/9-189*

2. Термін подання студентом завершеної роботи *15.06.2026*

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 охорони праці.
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. *Структурна схема*
2. *Функціональна схема*
3. *Блок схема роботи*
4. *Схема електрична принципова*
5. *Результати роботи*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці			

7. Дата видачі завдання *25.04.2026 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Розробка технічного завдання*	*26.01 – 02.02*	
2.	*Робота над першим розділом «Аналіз технічного завдання»*	*03.02 – 15.02*	
3.	*Робота над другим розділом «Проєктна частинв»*	*20.04 – 25.04*	
4.	*Робота над третім розділом «Практична частина»*	*26.04 – 05.05*	
5.	*Робота над четвертим розділом «Безпека життєдіяльності, основи охорони праці»*	*07.05 – 25.05*	
6.	*Оформлення пояснювальної записки і графічного матеріалу*	*26.05 – 7.06*	
7.	*Перевірка на академічний плагіат, перевірка керівником та консультантами*	*8.06 – 14.06*	
8.	*Попередній захист кваліфікаційної роботи бакалавра*	*15.06 – 21.06*	
9.	*Захист кваліфікаційної роботи бакалавра*	*22.06*	

Студент _____ *Дуніковський Стефан Богданович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Жаровський Руслан Олегович*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дуніковський С. Б. Комп’ютерна система моніторингу середовища і контролю доступу до серверного приміщення: робота на здобуття кваліфікаційного ступеня бакалавра: спец. 123 – комп’ютерна інженерія. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2026.

Ключові слова: серверне приміщення, моніторинг середовища, контроль доступу, RFID, Arduino Mega, вебінтерфейс, Blynk, система безпеки.

У кваліфікаційній роботі розроблено комп'ютерну систему моніторингу середовища та контролю доступу до серверного приміщення.

У роботі виконано аналіз існуючих рішень моніторингу серверних приміщень, обґрунтовано вибір апаратного та програмного забезпечення, розроблено структурну, функціональну та електричну принципову схеми системи. Як апаратну платформу використано мікроконтролер Arduino Mega 2560, датчики DHT22, MQ-2 та YL-83, RFID-зчитувач RC522, Ethernet-модуль W5500 та модуль реєстрації даних на карту пам'яті microSD.

Розроблене програмне забезпечення забезпечує моніторинг температури, вологості, задимлення та протікання води, керування системою кондиціонування, контроль доступу за RFID-мітками, ведення журналу подій, відображення інформації на LCD-дисплеї та віддалений моніторинг через вебінтерфейс і мобільний застосунок Blynk.

Проведене тестування підтвердило працездатність усіх функціональних підсистем та відповідність розробленої системи поставленим вимогам.

ANNOTATION

Dunikovskyi S. Computer System for Environmental Monitoring and Access Control of a Server Room: Bachelor's Graduation Thesis: speciality 123 – computer engineering. Ternopil: Ternopil Ivan Puluj National Technical University, 2026.

Keywords: server room, environmental monitoring, access control, RFID, Arduino Mega, web interface, Blynk, security system.

In the qualification work, a computer system for environmental monitoring and access control to the server room was developed.

The work analyzed existing solutions for monitoring server rooms, justified the choice of hardware and software, and developed a structural, functional and electrical schematic diagram of the system. The hardware platform used was the Arduino Mega 2560 microcontroller, DHT22, MQ-2 and YL-83 sensors, RC522 RFID reader, W5500 Ethernet module and a data logging module to a microSD memory card.

The developed software provides monitoring of temperature, humidity, smoke and water leakage, air conditioning system control, access control using RFID tags, event logging, displaying information on an LCD display and remote monitoring via a web interface and the Blynk mobile application.

The testing confirmed the operability of all functional subsystems and the compliance of the developed system with the requirements.

ЗМІСТ

ВСТУП

Сучасні інформаційні системи підприємств, установ та організацій значною мірою залежать від надійного функціонування серверного обладнання. Порушення умов експлуатації серверних приміщень може призвести до виходу з ладу дороговартісного обладнання, втрати даних, простою інформаційних сервісів та суттєвих фінансових збитків. Тому забезпечення безперервного контролю параметрів середовища та захисту серверних приміщень є важливим завданням сучасних інформаційно-комунікаційних систем.

Особливу небезпеку для серверного обладнання становлять підвищення температури та вологості, пожежі, витоки води, а також несанкціонований доступ сторонніх осіб. Традиційні засоби контролю часто виконують лише окремі функції моніторингу або безпеки, що потребує використання декількох незалежних систем та ускладнює їх експлуатацію.

Актуальність роботи полягає у необхідності створення інтегрованої комп'ютерної системи, яка поєднує функції моніторингу параметрів середовища, контролю доступу, реєстрації подій та віддаленого інформування користувачів про стан серверного приміщення.

Метою кваліфікаційної роботи є розробка комп'ютерної системи моніторингу середовища та контролю доступу до серверного приміщення, яка забезпечує автоматичний контроль температури, вологості, задимлення та протікання води, а також реалізує механізм санкціонованого доступу.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз сучасних систем моніторингу серверних приміщень та контролю доступу;

– визначити функціональні вимоги до розроблюваної системи;

– обґрунтувати вибір апаратних та програмних засобів;

– розробити структурну, функціональну та електричну принципову схеми системи;

– розробити програмне забезпечення для реалізації функцій моніторингу та контролю доступу;

– реалізувати засоби локального та віддаленого моніторингу;

– провести тестування розробленої системи.

Практичне значення роботи полягає у створенні працездатної комп'ютерної системи, яка може використовуватися для підвищення рівня безпеки серверних приміщень, забезпечення контролю параметрів експлуатації обладнання та оперативного реагування на аварійні ситуації.

РОЗДІЛ 1 АНАЛІЗ ТЕХІЧНОГО ЗАВДАННН

1.1 Аналіз серверних приміщень як об'єктів моніторингу та контролю доступу

Стрімкий розвиток інформаційних технологій та цифровізація діяльності підприємств призвели до значного зростання ролі серверного обладнання у забезпеченні функціонування інформаційних систем. Для забезпечення стабільної роботи такого обладнання на підприємствах обладнуються спеціалізовані серверні приміщення, в яких створюються необхідні умови експлуатації та забезпечується обмежений доступ персоналу.

Серверне приміщення являє собою спеціально обладнану кімнату, доскладу якої входять серверні шафи, комутатори, маршрутизатори, джерела безперебійного живлення, системи кондиціювання, кабельні траси та засоби фізичного захисту обладнання. Всі перелічені елементи утворюють єдиний комплекс, від працездатності якого залежить безперервність роботи інформаційної інфраструктури підприємства (рис. 1.1).

Навіть короткочасне порушення умов експлуатації може спричинити зниження продуктивності обладнання або його аварійне відключення. Саме тому підтримання належних умов навколишнього середовища є одним із ключових завдань під час експлуатації серверних приміщень.

Ефективне функціонування серверної залежить від великої кількості зовнішніх і внутрішніх факторів. До основних факторів належать температура повітря, відносна вологість, пожежна безпека (наявність диму), можливі витоки води та рівень захищеності приміщення від несанкціонованого доступу. Контроль зазначених параметрів дозволяє своєчасно виявляти

потенційно небезпечні ситуації та мінімізувати ризики виходу обладнання з ладу (рис.1.2).

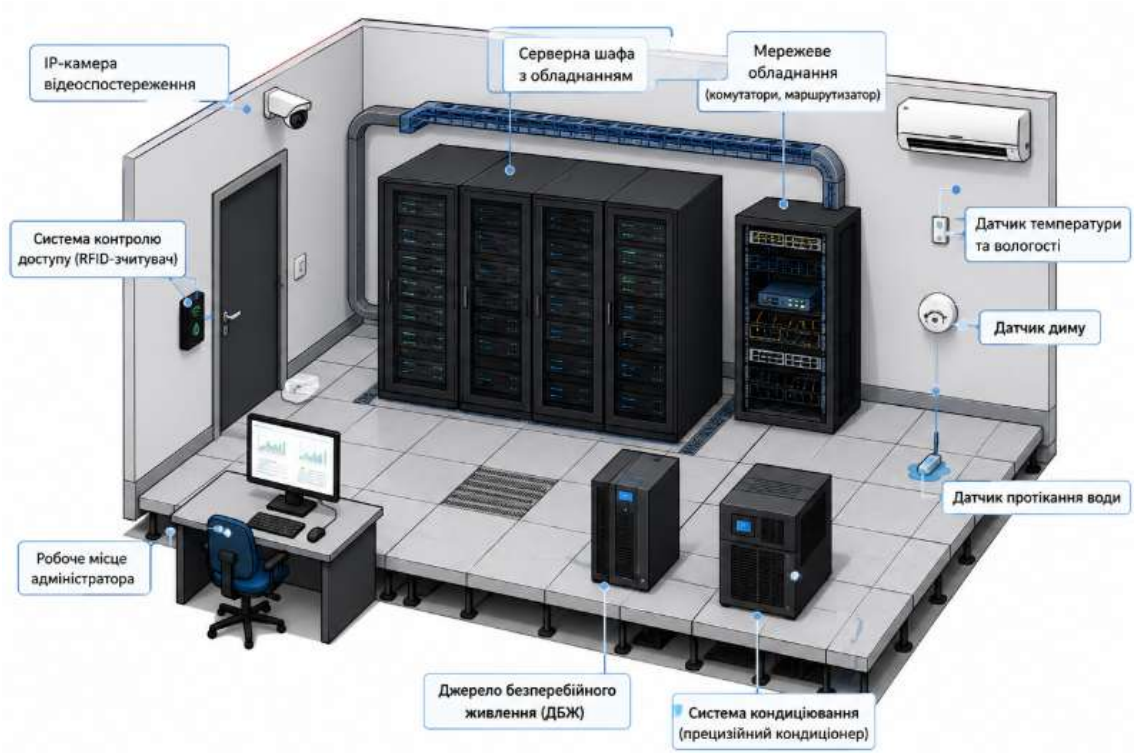

Рисунок 1.1 – Типова структура серверного приміщення

Окрім забезпечення належних параметрів навколишнього середовища важливим завданням є організація фізичного захисту серверного приміщення. Серверне обладнання містить інформаційні ресурси підприємства, доступ до яких повинен бути обмежений. Навіть за наявності сучасних засобів кібербезпеки несанкціонований фізичний доступ до серверів може призвести до викрадення інформації, пошкодження обладнання або порушення роботи інформаційної системи.

Для запобігання таким загрозам застосовуються системи контролю та керування доступом, які забезпечують ідентифікацію користувачів, ведення журналу подій та керування виконавчими пристроями замикання дверей [2].

Рисунок 1.2 – Основні фактори ризику для серверного приміщення

Зважаючи на необхідність постійного контролю параметрів середовища та обмеження доступу до обладнання, серверні приміщення доцільно оснащувати автоматизованими системами моніторингу. Такі системи забезпечують безперервний збір інформації від датчиків, реєстрацію подій, формування попереджень про аварійні ситуації та надання користувачу засобів дистанційного контролю. Використання автоматизованого моніторингу дозволяє підвищити надійність функціонування серверної інфраструктури та зменшити ймовірність виникнення аварійних ситуацій [2].

1.2 Аналіз факторів, що впливають на надійність функціонування серверного обладнання

1.2.1 Вплив факторів навколишнього середовища та аварійних ситуацій

Температурний режим є одним із найважливіших факторів, що визначають надійність та довговічність серверного обладнання. Більшість сучасних серверів оснащуються вбудованими системами охолодження, проте їх ефективність значною мірою залежить від температури навколишнього

середовища. Якщо температура повітря у приміщенні перевищує допустимі значення, система охолодження працює з підвищеним навантаженням, що призводить до збільшення енергоспоживання та прискореного зношування вентиляторів.

Найбільш чутливими до перегріву є центральні процесори, модулі оперативної пам’яті, накопичувачі інформації та блоки живлення. Підвищення температури призводить до зростання електричного опору провідників, збільшення струмів витоку в напівпровідникових елементах та прискорення процесів старіння електронних компонентів.

За таких умов можуть виникати помилки обробки даних, автоматичне зниження продуктивності процесорів, аварійне відключення окремих вузлів або повний вихід обладнання з ладу (рис. 1.3).

Крім безпосереднього впливу на електронні компоненти, підвищена температура може негативно впливати на роботу накопичувачів інформації. Жорсткі диски та твердотільні накопичувачі мають визначені виробниками температурні режими експлуатації, перевищення яких може призвести до скорочення терміну служби носіїв інформації та підвищення ризику втрати даних.

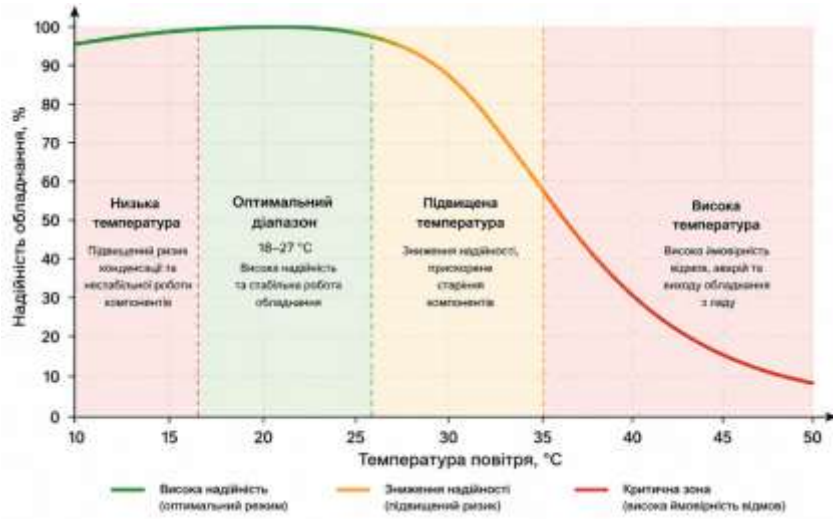

Рисунок 1.3 – Вплив температури на надійність серверного обладнання

Тому, контроль температурного режиму є обов’язковою складовою системи моніторингу серверного приміщення. Безперервне вимірювання температури дозволяє забезпечити стабільні умови експлуатації серверного обладнання, підвищити його надійність та зменшити ймовірність виникнення аварійних ситуацій.

Одним із важливих параметрів мікроклімату серверного приміщення є відносна вологість повітря. Незважаючи на те, що вплив вологості на роботу обладнання менш помітний порівняно з температурою, її відхилення від нормативних значень може негативно позначитися на надійності функціонування електронних систем та скоротити термін їх експлуатації.

Відносна вологість характеризує ступінь насичення повітря водяною парою і виражається у відсотках. Для більшості серверних приміщень рекомендованим є діапазон відносної вологості від 40 % до 60 %. Підтримання цього діапазону дозволяє забезпечити оптимальні умови роботи електронного обладнання та мінімізувати ризик виникнення пошкоджень (рис.1.4).

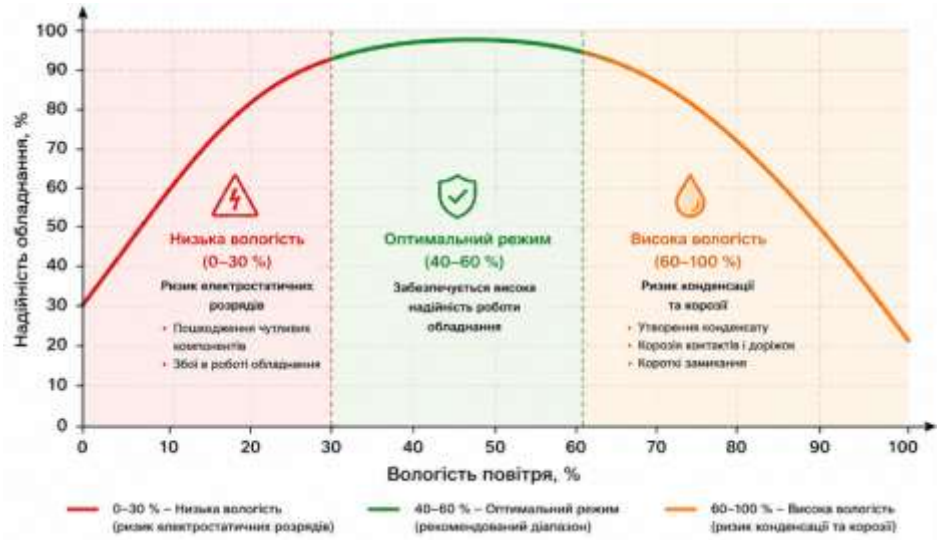

Рисунок 1.4 – Вплив вологості повітря на працездатність електронного обладнання

Підвищена вологість є небезпечною через можливість утворення конденсату на поверхні електронних компонентів. Конденсація вологи може виникати під час різких змін температури або внаслідок несправностей систем кондиціювання. Потрапляння вологи на друковані плати, роз'єми та контакти здатне викликати короткі замикання, корозію струмопровідних доріжок та деградацію електронних компонентів.

Особливо чутливими до підвищеної вологості є контактні з'єднання, мережеві інтерфейси та елементи систем живлення. Тривалий вплив вологи призводить до окиснення контактів, збільшення перехідного опору та погіршення електричних характеристик з'єднань. У результаті можуть виникати помилки передавання даних, нестабільна робота обладнання або його повна відмова.

Не менш небезпечним є надмірне зниження вологості повітря. При відносній вологості нижче 30 % суттєво підвищується ймовірність накопичення статичної електрики. Електростатичні розряди можуть виникати під час обслуговування обладнання персоналом або внаслідок руху повітряних потоків усередині серверних шаф. Навіть короткочасний електростатичний розряд здатний пошкодити чутливі електронні компоненти, мікросхеми пам'яті та мережеві інтерфейси. Тому контроль вологості повинен здійснюватися безперервно та автоматично.

Однією з менш очевидних, але надзвичайно небезпечних загроз для серверних приміщень є потрапляння води до місць розміщення електронного обладнання. Джерелами потрапляння води можуть бути несправності систем кондиціювання, аварії водопровідних або опалювальних мереж, пошкодження покрівлі будівлі, а також людський фактор під час проведення технічного обслуговування. Особливу небезпеку становлять системи кондиціювання повітря, які використовуються практично в кожній серверній кімнаті та містять конденсатовідвідні магістралі.

Потрапляння навіть незначної кількості води на електронне обладнання може призвести до виникнення коротких замикань, пошкодження друкованих плат, виходу з ладу блоків живлення та втрати працездатності серверів. Якщо вода потрапляє до силових ланцюгів, наслідком можуть бути аварійні відключення обладнання та пошкодження окремих електронних компонентів.

Типові джерела виникнення протікань у серверному приміщенні наведено на рис. 1.5.

Рисунок 1.5 – Основні джерела потрапляння води до серверного приміщення

Своєчасне отримання повідомлення про появу води дозволяє персоналу вжити необхідних заходів ще до того, як буде завдано значної шкоди обладнанню та інформаційній інфраструктурі.

Наступною загрозою є пожежі, які здатні за короткий проміжок часу призвести не лише до виходу з ладу окремих пристроїв, але й до повного знищення серверного обладнання, кабельної інфраструктури та інформаційних ресурсів підприємства.

Основними причинами виникнення пожеж у серверних є короткі замикання електричних мереж, перевантаження силових ліній, несправність блоків живлення, перегрів електронних компонентів, пошкодження ізоляції кабелів та порушення правил експлуатації електрообладнання. Додатковим фактором ризику є значна концентрація кабельних комунікацій, які можуть сприяти швидкому поширенню вогню.

У більшості випадків виникненню відкритого полум'я передує поява диму, який є результатом перегріву або займання ізоляційних матеріалів, пластикових корпусів та електронних компонентів. Саме тому своєчасне виявлення задимлення дозволяє виявити небезпечну ситуацію на ранній стадії та запобігти розвитку пожежі. Послідовність розвитку аварійної ситуації під час виникнення пожежі наведена на рис. 1.6.

Рисунок 1.6 – Етапи розвитку пожежонебезпечної ситуації в серверному приміщенні

І хоча серверні приміщення обладнуються системами автоматичного виявлення задимлення, пожежною сигналізацією та засобами пожежогасіння, доцільним є використання комп'ютерних систем моніторингу, які забезпечують оперативне інформування обслуговуючого персоналу про виникнення потенційно небезпечних ситуацій.

1.2.2 Наслідки несанкціонованого доступу до серверних приміщень

Фізична безпека серверного приміщення є невід'ємною складовою загальної системи захисту інформаційних ресурсів підприємства. Отримавши доступ до серверного приміщення, стороння особа може безпосередньо впливати на роботу обладнання, що значно підвищує ризик виникнення аварійних ситуацій та втрати інформації [5].

Однією з найсерйозніших загроз є викрадення або навмисне пошкодження обладнання. Крім того, зловмисник може отримати доступ до носіїв інформації та здійснити копіювання або викрадення конфіденційних даних, підключити несанкціоновані пристрої до локальної мережі.

Небезпечними є також випадкові дії персоналу, який не має відповідних повноважень або достатньої кваліфікації. Помилкове відключення кабельних з'єднань, зміна конфігурації мережевого обладнання або некоректне вимкнення серверів можуть призвести до порушення роботи інформаційної системи та втрати даних (рис. 1.7).

Рисунок 1.7 – Основні наслідки несанкціонованого доступу до серверного приміщення

Для зменшення ризику несанкціонованого доступу використовуються системи контролю та керування доступом, які забезпечують ідентифікацію користувачів, ведення журналу подій та керування виконавчими механізмами замикання дверей. Такі системи дозволяють обмежити доступ до серверного приміщення лише для авторизованих осіб та забезпечують контроль усіх подій, пов'язаних із входом і виходом персоналу [6].

У сучасних системах контролю доступу широко застосовуються RFID-технології, які забезпечують швидку ідентифікацію користувачів за допомогою електронних карток або брелоків. Інформація про кожне спрацювання системи може зберігатися у журналі подій та передаватися до системи моніторингу для подальшого аналізу.

1.3 Аналіз сучасних систем моніторингу серверних приміщень

Для визначення функціональних можливостей та особливостей побудови сучасних систем моніторингу серверних приміщень доцільно

розглянути найбільш поширені комерційні рішення, які застосовуються в центрах обробки даних, серверних кімнатах та телекомунікаційних вузлах [4].

1.3.1 Система моніторингу AKCP SensorProbe+

AKCP SensorProbe+ є однією з найбільш відомих професійних систем моніторингу параметрів навколишнього середовища для серверних приміщень та центрів обробки даних. Система побудована за модульним принципом і складається з центрального контролера та набору підключених датчиків (рис.1.8). До контролера можуть підключатися датчики температури, вологості, протікання води, задимлення, відкриття дверей, контролю електроживлення та інші типи сенсорів. Передача інформації здійснюється через локальну мережу Ethernet, що забезпечує можливість централізованого моніторингу параметрів у режимі реального часу [7].

Однією з основних переваг системи є висока масштабованість. Залежно від модифікації контролера до нього може бути підключено різну кількість датчиків, що дозволяє використовувати систему як у невеликих серверних кімнатах, так і у великих дата-центрах.

Система підтримує протокол SNMP, що дозволяє інтегрувати її з іншими мережевими засобами моніторингу та адміністрування. При перевищенні встановлених порогових значень система автоматично формує повідомлення для відповідального персоналу.

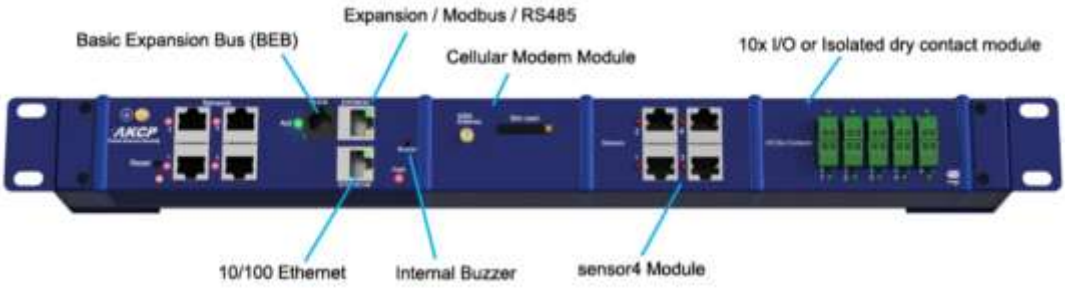

Рисунок 1.8 – Система моніторингу AKCP SensorProbe+

Основними перевагами системи є широкий набір підтримуваних датчиків, висока надійність та можливість інтеграції з корпоративними мережами моніторингу. До недоліків можна віднести високу вартість обладнання та необхідність використання спеціалізованого програмного забезпечення [8].

1.3.2 Система моніторингу NetBotz

Система NetBotz, що розробляється компанією Schneider Electric, призначена для комплексного контролю стану серверних приміщень та центрів обробки даних. На відміну від багатьох аналогічних рішень, NetBotz поєднує функції моніторингу параметрів середовища та фізичної безпеки об'єкта (рис. 1.9).

До складу системи входять контролери моніторингу, датчики температури та вологості, датчики протікання води, датчики відкриття дверей, а також мережеві камери відеоспостереження. Наявність відеоконтролю дозволяє отримувати додаткову інформацію про стан серверного приміщення та дії персоналу.

Важливою особливістю системи є підтримка централізованого адміністрування через мережу та можливість інтеграції з іншими системами управління інженерною інфраструктурою підприємства. У разі виникнення аварійної ситуації користувач отримує відповідні повідомлення через мережу або електронну пошту.

Рисунок 1.9 – Система моніторингу NetBotz

Перевагами системи є широкий функціонал, висока якість реалізації та можливість відеомоніторингу. Основними недоліками є значна вартість обладнання та складність впровадження на невеликих об'єктах [9].

1.3.3 Система моніторингу HW Group Poseidon

Система HW Group Poseidon призначена для дистанційного контролю параметрів навколишнього середовища та стану інженерних систем. Вона широко застосовується для моніторингу серверних кімнат, телекомунікаційних вузлів та технічних приміщень.

Основою системи є мережевий контролер Poseidon, до якого можуть підключатися датчики температури, вологості, протікання води, відкриття дверей та інші типи сенсорів. Контролер підтримує передачу даних через Ethernet-мережу та забезпечує віддалений доступ до інформації за допомогою вебінтерфейсу (рис.1.10). Система дозволяє формувати повідомлення про аварійні ситуації через електронну пошту, SNMP або інші мережеві сервіси. Завдяки цьому персонал може оперативно реагувати на відхилення контрольованих параметрів від встановлених значень.

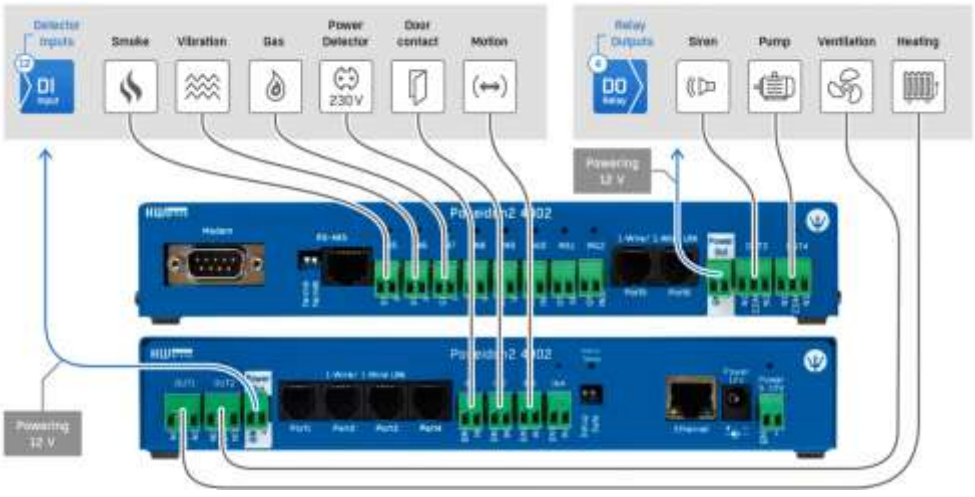

Рисунок 1.10 – Загальна структура системи моніторингу HW Group Poseidon

До переваг системи належать відносно невисока вартість, простота налаштування та широкий вибір сумісних датчиків. Недоліком є менша кількість функцій порівняно з комплексними рішеннями для великих центрів обробки даних [10].

1.3.4 Порівняльний аналіз існуючих рішень

Розглянуті системи мають схожий принцип побудови та забезпечують контроль основних параметрів навколишнього середовища. Проте вони відрізняються функціональними можливостями, складністю впровадження та вартістю (табл. 1.1).

Таблиця 1.1 – Порівняння сучасних систем моніторингу серверних приміщень

Характеристика	AKCP SensorProbe+	NetBotz	HW Group Poseidon
Контроль температури	+	+	+
Контроль вологості	+	+	+
Контроль задимлення	+	+	+
Контроль протікання води	+	+	+
Контроль відкриття дверей	+	+	+
Вебінтерфейс	+	+	+
Відеоспостереження	–	+	–
Підтримка SNMP	+	+	+
Масштабованість	висока	висока	середня
Вартість	висока	висока	середня

Аналіз показує, що всі розглянуті системи забезпечують контроль основних параметрів середовища серверного приміщення. Водночас їх використання пов'язане зі значними фінансовими витратами, що може бути недоцільним для невеликих підприємств, навчальних закладів або локальних серверних кімнат.

Крім того, більшість комерційних систем орієнтована на масштабні об'єкти та містить функції, які не є критично необхідними для невеликих серверних приміщень. Це обумовлює доцільність розробки власної комп'ютерної системи моніторингу середовища і контролю доступу, яка забезпечуватиме контроль температури, вологості, задимлення, протікання води та доступу до приміщення при значно нижчій вартості реалізації [11].

1.4 Постановка задачі кваліфікаційної роботи

Проведений аналіз серверних приміщень як об'єктів моніторингу показав, що надійність функціонування інформаційної інфраструктури значною мірою залежить від умов експлуатації серверного обладнання та рівня фізичної безпеки приміщення.

Аналіз сучасних комерційних систем моніторингу серверних приміщень показав, що існуючі рішення забезпечують широкий набір функцій контролю параметрів середовища та реєстрації подій, проте характеризуються високою вартістю та надлишковим функціоналом для невеликих серверних приміщень. Тому актуальним є розроблення спеціалізованої комп'ютерної системи, орієнтованої на контроль найбільш важливих параметрів середовища та забезпечення контролю доступу при мінімальних витратах на реалізацію.

Метою розробки є створення комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення, яка забезпечуватиме безперервний контроль параметрів навколишнього середовища, виявлення аварійних ситуацій, ведення журналу подій та обмеження доступу сторонніх осіб до обладнання.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– виконати моніторинг температури повітря в серверному приміщенні;

– забезпечити контроль відносної вологості повітря;

– реалізувати виявлення задимлення та пожежонебезпечних ситуацій;

– забезпечити контроль появи води в місцях розміщення серверного обладнання;

– реалізувати контроль відкриття дверей серверного приміщення;

– забезпечити ідентифікацію користувачів за допомогою RFID-карток або брелоків;

– реалізувати керування електромагнітним замком дверей;

– забезпечити відображення поточних параметрів середовища через мережевий інтерфейс;

– реалізувати ведення журналу подій системи;

– забезпечити формування повідомлень про виникнення аварійних ситуацій.

Для реалізації поставлених задач доцільно використати мікроконтролерну платформу з можливістю підключення мережевих інтерфейсів, датчиків контролю параметрів середовища та засобів контролю доступу. Система повинна забезпечувати збір та обробку інформації від датчиків, відображення поточних параметрів у режимі реального часу, формування попереджувальних повідомлень та керування виконавчими пристроями контролю доступу.

Результати проведеного аналізу є основою для розробки структури системи та обґрунтування вибору її апаратного і програмного забезпечення, що буде виконано у наступному розділі.

РОЗДІЛ 2 ПРОЄКТНА ЧАСТИНА

2.1 Розробка узагальненої структури комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення

На основі результатів аналізу предметної області та сформульованих вимог до розроблюваної системи було виконано розробку узагальненої структури комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення. Основною метою створення системи є забезпечення безперервного контролю параметрів середовища, виявлення аварійних ситуацій, реєстрація подій та обмеження доступу сторонніх осіб до серверного обладнання. Узагальнена структура системи наведена на рис. 2.1.

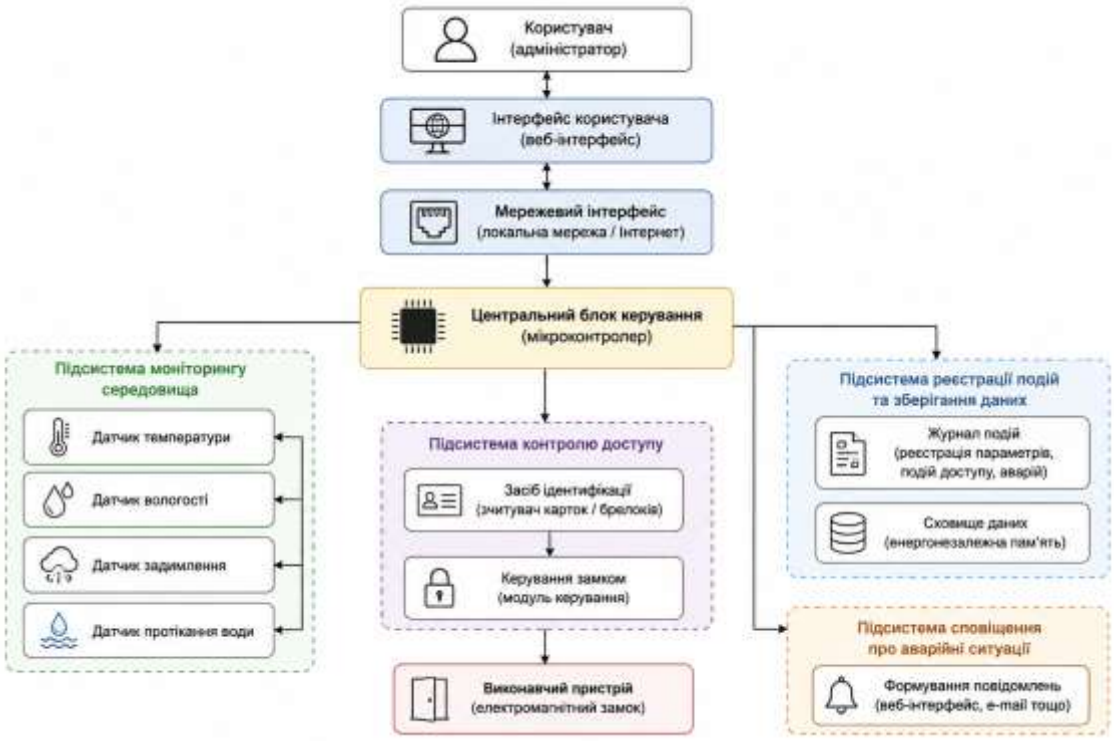

Рисунок 2.1 - Узагальнена структура системи

					КС КРБ 123.264.00.00 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Дуніковський			Проєктна частина	Літ.	Арк. 26 / Аркушів 20
Перевірив		Жаровський Р.					
Реценз.		Млинко Б.Б.				ТНТУ, каф. КС, гр. СІс-41	
Н. Контр.		Тиш Є.В.					
Затверд.		Осухівська Г.М.					

В основу побудови системи покладено принцип централізованого збору та обробки інформації від усіх функціональних підсистем за допомогою центрального блоку керування [12].

Центральний блок керування здійснює опитування датчиків, обробку отриманих даних, формування повідомлень про аварійні ситуації, керування виконавчими пристроями та взаємодію з користувачем через мережевий інтерфейс. Саме цей блок забезпечує координацію роботи всіх елементів системи та реалізацію її основних функцій.

Для контролю параметрів навколишнього середовища передбачено підсистему моніторингу середовища, до складу якої входять датчики температури, вологості, задимлення та протікання води. Дані, отримані від цих датчиків, використовуються для оцінки поточного стану серверного приміщення та своєчасного виявлення небезпечних відхилень від нормальних умов експлуатації.

Контроль доступу до серверного приміщення забезпечується підсистемою контролю доступу. До її складу входять засіб ідентифікації користувачів та модуль керування замком. Після успішної ідентифікації користувача центральний блок керування формує команду на відкриття виконавчого пристрою замикання дверей. Це дозволяє обмежити доступ до серверного обладнання лише для авторизованих осіб [13].

Для зберігання інформації про роботу системи використовується підсистема реєстрації подій та зберігання даних. Наявність журналу подій дозволяє здійснювати подальший аналіз роботи системи та виявляти можливі порушення режимів експлуатації серверного приміщення.

Окремою складовою є підсистема сповіщення про аварійні ситуації, яка призначена для оперативного інформування відповідального персоналу про перевищення допустимих значень контрольованих параметрів або виникнення інших небезпечних подій. Передача повідомлень може здійснюватися через вебінтерфейс або інші засоби мережевої взаємодії.

Взаємодія користувача із системою здійснюється через інтерфейс користувача, який надає можливість перегляду поточних параметрів середовища, контролю стану системи та аналізу зареєстрованих подій. Обмін інформацією між користувачем та системою забезпечується за допомогою мережевого інтерфейсу, що дозволяє здійснювати дистанційний моніторинг серверного приміщення.

2.2 Обґрунтування вибору апаратного забезпечення

Під час вибору апаратного забезпечення для комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення необхідно враховувати вимоги щодо можливості підключення декількох датчиків, засобів контролю доступу, мережевого інтерфейсу, пристроїв відображення інформації та реєстрації подій. Обране обладнання повинно забезпечувати надійну роботу системи, простоту інтеграції окремих модулів та можливість подальшого розширення функціональних можливостей.

2.2.1 Вибір мікроконтролерної платформи

Центральний контролер системи повинен забезпечувати опитування датчиків температури, вологості, задимлення та протікання води, взаємодію із засобами контролю доступу, роботу мережевого інтерфейсу, відображення інформації та реєстрацію подій на зовнішньому носії. Для вибору мікроконтролерної платформи було розглянуто плати Arduino Uno, Arduino Mega 2560, ESP32 та STM32F103C8T6 (табл.2.1).

За результатами порівняння для реалізації системи обрано плату Arduino Mega 2560 (рис. 2.2), яка має достатню кількість входів та виходів для підключення всіх необхідних модулів, підтримує одночасну роботу декількох інтерфейсів обміну даними та забезпечує просту інтеграцію з периферійними пристроями.

Таблиця 2.1 – Порівняння мікроконтролерних платформ

Характеристика	Arduino Uno	Arduino Mega 2560	ESP32	STM32F103 C8T6
Тактова частота, МГц	16	16	240	72
Flash-пам'ять, КБ	32	256	520 SRAM	64
Цифрові входи/виходи	14	54	34	37
Аналогові входи	6	16	18	10
Кількість UART	1	4	3	3
Напруга живлення, В	5	5	3,3	3,3
Простота підключення модулів	Висока	Висока	Середня	Середня

Рисунок 2.2 – Плата Arduino Mega 2560

Таблиця 2.2 – Основні характеристики Arduino Mega 2560

Параметр	Значення
Мікроконтролер	ATmega2560
Тактова частота	16 МГц
Flash-пам'ять	256 КБ
SRAM	8 КБ
EEPROM	4 КБ
Цифрові входи/виходи	54
Аналогові входи	16
UART	4
Робоча напруга	5 В
Рекомендована напруга живлення	7–12 В

2.2.2 Вибір засобів мережевої взаємодії

Засіб мережевої взаємодії повинен забезпечувати стабільний обмін даними, простоту інтеграції з мікроконтролерною платформою та можливість реалізації вебінтерфейсу. Для вибору мережевого інтерфейсу було розглянуто Ethernet Shield W5500, Ethernet Shield W5100 та модуль ESP8266 (табл.2.3).

Таблиця 2.3 – Порівняння засобів мережевої взаємодії

Характеристика	W5100	W5500	ESP8266
Тип підключення	Ethernet	Ethernet	Wi-Fi
Швидкість передачі	до 100 Мбіт/с	до 100 Мбіт/с	до 150 Мбіт/с
Кількість сокетів	4	8	5
Інтерфейс підключення	SPI	SPI	UART
Стабільність з'єднання	висока	висока	середня
Простота інтеграції з Arduino	висока	висока	середня

Для реалізації системи обрано модуль Ethernet Shield W5500 (рис. 2.3). Його використання забезпечує стабільну роботу в локальній мережі серверного приміщення, підтримку вебінтерфейсу та достатню продуктивність для передавання інформації від датчиків і системи контролю доступу (табл. 2.4).

Рисунок 2.3 – Модуль Ethernet Shield W5500

Таблиця 2.4 – Основні характеристики Ethernet Shield W5500

Параметр	Значення
Контролер	W5500
Інтерфейс	SPI
Кількість сокетів	8
Швидкість Ethernet	10/100 Мбіт/с
Напруга живлення	5 В
Підтримка TCP/IP	Так
Підтримка UDP	Так
Підтримка DHCP	Так

2.2.3 Вибір датчиків контролю параметрів середовища

Для контролю стану серверного приміщення необхідно забезпечити вимірювання температури та вологості повітря, виявлення задимлення та контроль появи води.

Для контролю температури та вологості було розглянуто датчики DHT11, DHT22 та SHT31 (табл. 2.5).

Таблиця 2.5 – Порівняння датчиків температури та вологості

Характеристика	DHT11	DHT22	SHT31
Діапазон температур, °C	0...50	-40...80	-40...125
Точність температури, °C	±2	±0,5	±0,3
Діапазон вологості, %	20...90	0...100	0...100
Точність вологості, %	±5	±2	±2
Вартість	низька	середня	висока

Для системи обрано DHT22 (рис. 2.4), який забезпечує достатню точність вимірювання при невисокій вартості.

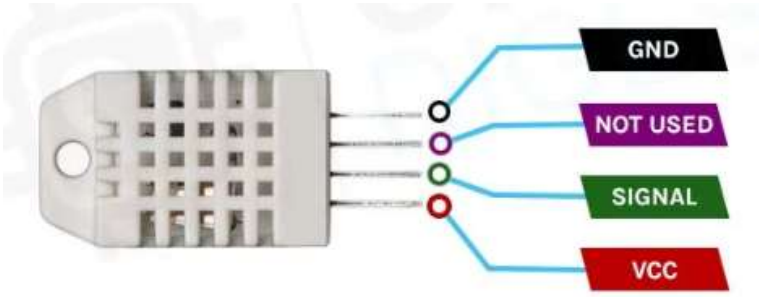

Рисунок 2.4 – Датчик температури та вологості DHT22

Для виявлення задимлення було розглянуто датчики MQ-2, MQ-135 та MQ-7 (табл.2.6).

Таблиця 2.6 – Порівняння датчиків задимлення

Характеристика	MQ-2	MQ-135	MQ-7
Виявлення диму	Так	Так	Ні
Простота підключення	висока	середня	середня
Аналоговий вихід	Так	Так	Так
Вартість	низька	середня	середня

Для реалізації системи обрано MQ-2 (рис. 2.5), який забезпечує виявлення диму та продуктів горіння на ранніх стадіях виникнення пожежонебезпечної ситуації (табл. 2.7).

Рисунок 2.5 – Датчик задимлення MQ-2

Таблиця 2.7 – Основні характеристики MQ-2

Параметр	Значення
Напруга живлення	5 В
Струм споживання	до 150 мА
Тип виходу	аналоговий, цифровий
Час прогріву	до 20 с

Для контролю протікання води було розглянуто модулі YL-83 та MH-RD (табл.2.8).

Таблиця 2.8 – Порівняння датчиків протікання води

Характеристика	YL-83	MH-RD
Аналоговий вихід	Так	Так
Цифровий вихід	Так	Так
Простота інтеграції	висока	висока
Вартість	нижча	вища

Для реалізації системи обрано YL-83 (рис. 2.6), харктеристики наведені в табл. 2.9.

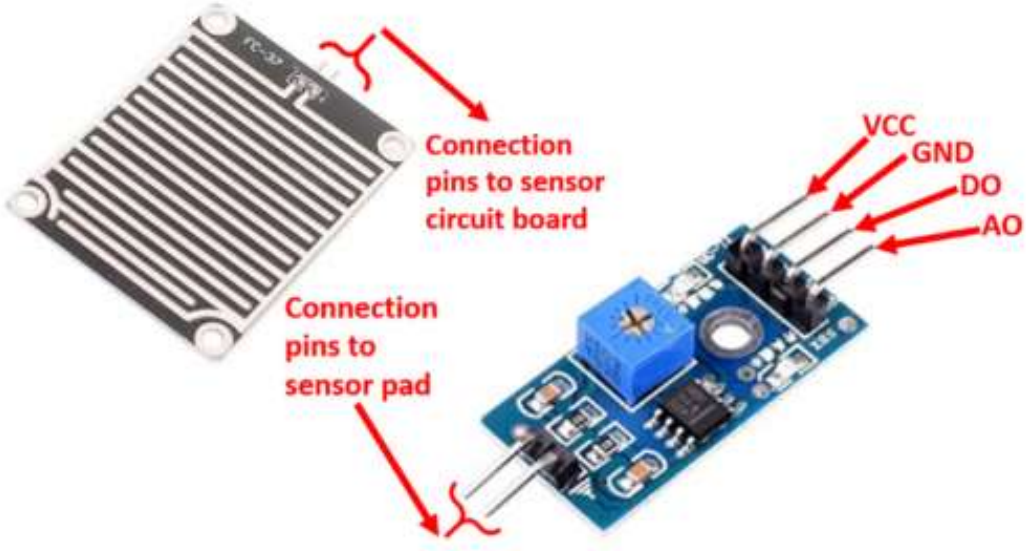

Рисунок 2.6 – Датчик протікання води YL-83

Таблиця 2.9 – Основні характеристики YL-83

Параметр	Значення
Напруга живлення	3,3–5 В
Тип виходу	аналоговий, цифровий
Робоча температура	-10...60 °C
Інтерфейс підключення	цифровий

2.2.4 Вибір засобів контролю доступу

Засіб контролю доступу повинен забезпечувати просту інтеграцію з мікроконтролерною платформою, достатній рівень надійності та невисоку вартість реалізації. Для реалізації системи контролю доступу було розглянуто клавіатурні кодові панелі, RFID-системи та біометричні зчитувачі (табл. 2.10).

Таблиця 2.10 – Порівняння засобів контролю доступу

Характеристика	Кодова панель	RFID	Біометричний доступ
Простота реалізації	висока	висока	середня
Вартість	низька	низька	висока
Швидкість доступу	середня	висока	висока
Ідентифікація користувача	обмежена	індивідуальна	індивідуальна

За результатами аналізу для реалізації системи обрано RFID-технологію, яка забезпечує просту ідентифікацію користувачів, високу швидкість спрацювання та можливість ведення журналу доступу. Як пристрій ідентифікації обрано модуль RFID RC522 (рис. 2.7).

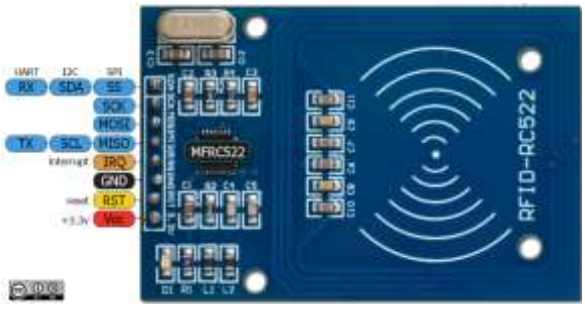

Рисунок 2.7 – RFID-зчитувач RC522

Таблиця 2.11 – Основні характеристики RFID RC522

Параметр	Значення
Робоча частота	13,56 МГц
Інтерфейс	SPI
Напруга живлення	3,3 В
Дальність зчитування	до 50 мм
Підтримка карт	MIFARE
Швидкість обміну	до 10 Мбіт/с

Для блокування дверей серверного приміщення необхідний виконавчий механізм замикання. Для цього було розглянуто електромеханічний замок та електромагнітний замок (табл. 2.12).

Таблиця 2.12 – Порівняння виконавчих механізмів замикання

Характеристика	Електромеханічний замок	Електромагнітний замок
Швидкість спрацювання	середня	висока
Знос механічних елементів	наявний	відсутній
Надійність	висока	висока
Інтеграція з контролером	середня	висока

Для реалізації системи обрано електромагнітний замок YM-280N (табл.2.13) на 12 В, який забезпечує керування з використанням реле.

Таблиця 2.13 – Основні характеристики електромагнітного замка

Параметр	Значення
Напруга живлення	12 В DC
Струм споживання	450–500 мА
Утримуюче зусилля	280 кг
Матеріал корпусу	Анодований алюміній
Робоча температура	-10...+55 °C
Маса	близько 2 кг

Рисунок 2.8 – Електромагнітний замок

Замок забезпечує надійне блокування дверей серверного приміщення та може безпосередньо керуватися за допомогою релейного модуля, підключеного до мікроконтролера.

Для комутації зовнішніх виконавчих пристроїв використовується двоканальний релейний модуль на базі електромагнітних реле SRD-05VDC-SL-C (табл. 2.14).

Перший канал забезпечує комутацію живлення електромагнітного замка YM-280N напругою 12 В. Другий канал використовується для формування сигналу керування системою кондиціонування через зовнішній інтерфейс типу Dry Contact. Такий підхід дозволяє здійснювати керування кондиціонером без комутації силових кіл мережі 220 В та підвищує електробезпеку системи.

Таблиця 2.14 – Технічні характеристики двоканального релейного модуля SRD-05VDC-SL-C

Параметр	Значення
Кількість каналів	2
Напруга живлення	5 В
Керуюча напруга	5 В
Максимальна комутована напруга AC	250 В
Максимальна комутована напруга DC	30 В
Максимальний комутований струм	10 А
Тип контактів	NO, NC, COM
Оптоізоляція	наявна

2.2.5 Вибір засобів відображення та реєстрації інформації

Для відображення поточного стану системи та параметрів середовища необхідний локальний пристрій індикації. Основними вимогами є простота підключення, достатня інформативність та можливість одночасного відображення декількох параметрів.

Для вибору пристрою відображення були розглянуті LCD 16×2, LCD 20×4 та OLED-дисплеї (табл.2.15).

Таблиця 2.15 – Порівняння пристроїв відображення інформації

Характеристика	LCD 16×2	LCD 20×4	OLED 128×64
Кількість символів	32	80	графічний
Простота програмування	висока	висока	середня
Вартість	низька	середня	вища
Інтерфейс I2C	так	так	так

Для реалізації системи обрано LCD-дисплей 20×4 (табл.2.16) з інтерфейсом I2C, який забезпечує одночасне відображення декількох параметрів моніторингу (рис.2.9).

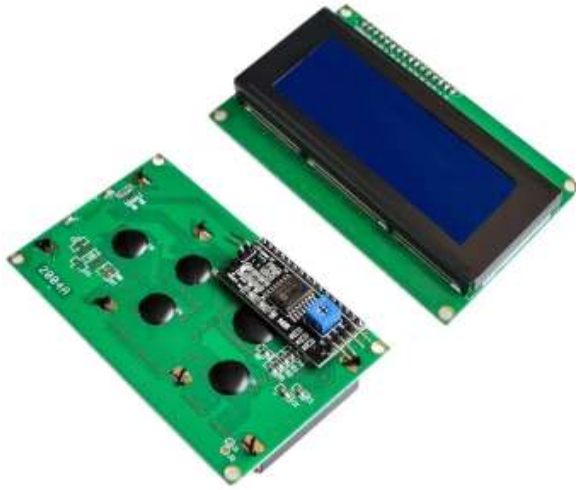

Рисунок 2.9 – LCD-дисплей 20×4 з інтерфейсом I2C

Таблиця 2.16 – Основні характеристики LCD 20×4

Параметр	Значення
Тип дисплея	символьний LCD
Розмір	20×4 символи
Інтерфейс	I2C
Напруга живлення	5 В
Підсвічування	LED

Для зберігання журналу подій необхідно забезпечити реєстрацію даних про параметри середовища та події доступу. Для цього було розглянуто використання EEPROM мікроконтролера та зовнішнього накопичувача на основі карти пам'яті microSD (табл.2.17).

Таблиця 2.17 – Порівняння засобів реєстрації інформації

Характеристика	EEPROM	microSD
Обсяг пам'яті	4 КБ	до десятків ГБ
Кількість записів	обмежена	практично необмежена
Простота обробки журналу	низька	висока
Можливість вилучення даних	відсутня	наявна

Для реалізації журналу подій обрано модуль MicroSD Card Module (рис. 2.10).

Таблиця 2.18 – Основні характеристики модуля microSD

Параметр	Значення
Тип носія	microSD
Інтерфейс	SPI
Напруга живлення	5 В
Максимальний обсяг карти	32 ГБ

Рисунок 2.10 – Модуль microSD Card Module

Для локального керування системою передбачено кнопку Exit для відкриття дверей та кнопку Reset Alarm для скидання аварійних повідомлень. Для звукової індикації стану системи та оповіщення про аварійні ситуації використовується активний бузер.

2.3 Розробка функціональної схеми системи

Функціональна схема комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення наведена на рис. 2.12.

Центральним елементом системи є мікроконтролер Arduino Mega 2560, який здійснює збір інформації від датчиків, обробку отриманих даних, формування керуючих сигналів та взаємодію з периферійними модулями.

Контроль параметрів середовища реалізується за допомогою датчика температури та вологості DHT22, датчика задимлення MQ-2 та датчика протікання води YL-83. Датчик DHT22 передає до контролера значення температури та відносної вологості через цифровий інтерфейс. Датчик MQ-2 забезпечує виявлення диму та продуктів горіння і передає сигнал до мікроконтролера через аналоговий або цифровий вихід. Датчик протікання

води YL-83 контролює появу води в місцях розташування обладнання та формує сигнал про виникнення аварійної ситуації.

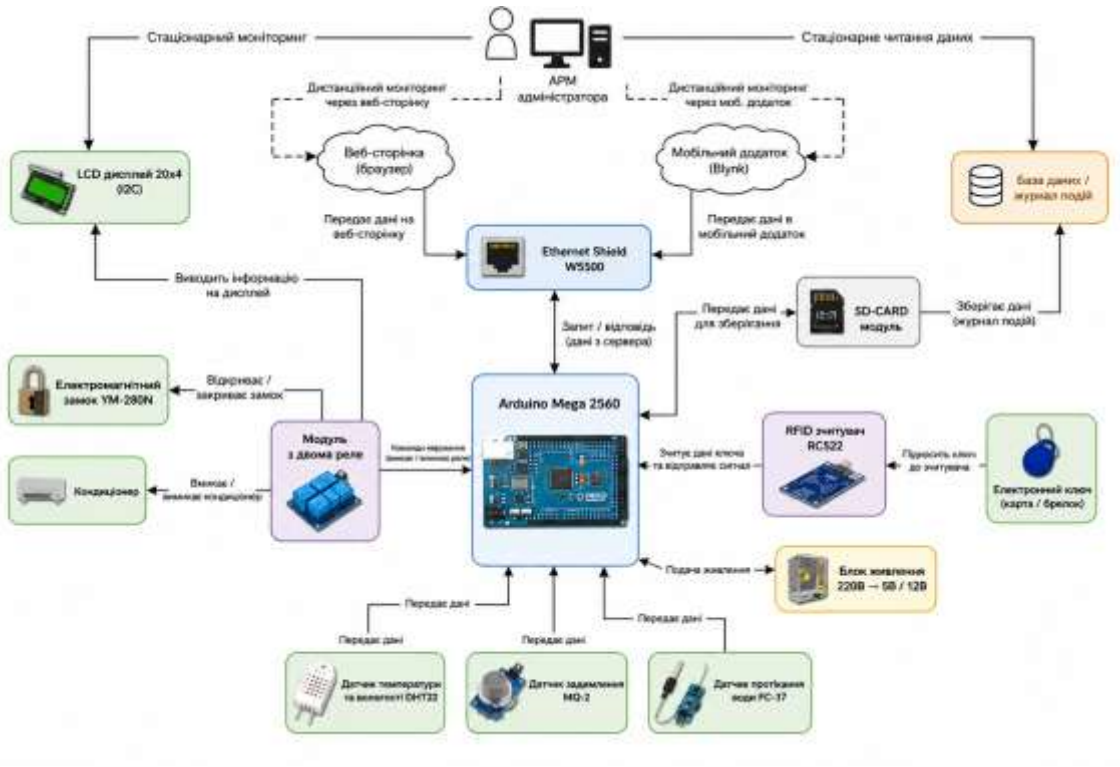

Рисунок 2.12 – Функціональна схема комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення

Підсистема контролю доступу реалізована на базі RFID-зчитувача RC522. Після піднесення RFID-картки або брелока до зчитувача формується ідентифікаційний код користувача, який передається до Arduino Mega через інтерфейс SPI. Після перевірки отриманого коду контролер формує сигнал керування для релейного модуля, який комутує коло живлення електромагнітного замка YM-280N та забезпечує відкриття або блокування дверей серверного приміщення.

Для локального відображення інформації використовується LCD-дисплей 20×4. Передача даних між дисплеєм та контролером здійснюється через інтерфейс I²C, що дозволяє зменшити кількість задіяних виводів мікроконтролера. На дисплеї відображаються поточні значення

контрольованих параметрів, результати авторизації користувачів та повідомлення про аварійні події.

Віддалений моніторинг системи забезпечується за допомогою Ethernet Shield W5500. Взаємодія між контролером та мережевим модулем здійснюється через інтерфейс SPI. На базі Ethernet Shield реалізовано вебсервер, який надає користувачу доступ до інформації про стан серверного приміщення через вебінтерфейс. Отримані від датчиків дані передаються на вебсторінку та відображаються на автоматизованому робочому місці адміністратора.

Для накопичення та збереження інформації використовується модуль microSD. Запис даних на карту пам'яті здійснюється через інтерфейс SPI. У журналі подій зберігаються результати вимірювань датчиків, події доступу користувачів, повідомлення про аварійні ситуації та службова інформація про роботу системи.

Живлення електронних модулів системи здійснюється від стабілізованого джерела напруги 5 В. Електромагнітний замок живиться від окремого джерела напруги 12 В, а його керування реалізується через релейний модуль, підключений до цифрового виходу мікроконтролера.

Таким чином, функціональна схема відображає взаємодію підсистем моніторингу середовища, контролю доступу, відображення інформації, мережевої взаємодії та реєстрації подій. Використання інтерфейсів SPI, I^2C та цифрових входів/виходів забезпечує сумісність усіх функціональних вузлів системи та ефективний обмін даними між ними.

2.4 Розробка електричної принципової схеми

Електрична принципова схема комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення наведена в графічній частині роботи. Мікроконтролер Arduino Mega 2560, забезпечує

опитування датчиків, обробку отриманих даних та формування керуючих сигналів (табл. 2.19).

Таблиця 2.19 – Призначення виводів Arduino Mega 2560

Пристрій	Контакт пристрою	Контакт Arduino Mega
DHT22	DATA	D6
MQ-2	AOUT	A0
YL-83	D0	D3
RFID RC522	NSS	D53
RFID RC522	SCK	D52
RFID RC522	MOSI	D51
RFID RC522	MISO	D50
RFID RC522	RST	D5
Ethernet W5500	CS	D10
Ethernet W5500	SCK	D52
Ethernet W5500	MOSI	D51
Ethernet W5500	MISO	D50
MicroSD	CS	D4
MicroSD	SCK	D52
MicroSD	MOSI	D51
MicroSD	MISO	D50
LCD 20×4 I²C	SDA	D20
LCD 20×4 I²C	SCL	D21
Релейний модуль	IN1	D8
Релейний модуль	IN2	D9
Кнопка Exit	S1	D22
Кнопка Reset Alarm	S2	D23
Активний бузер	BZ1	D26

Контроль параметрів середовища здійснюється за допомогою датчика температури та вологості DHT22, датчика задимлення MQ-2 та датчика

виявлення протікання води YL-83. Для забезпечення коректної роботи DHT22 використано підтягувальний резистор опором 4,7 кОм.

Для контролю доступу використовується RFID-зчитувач RC522, підключений до контролера через інтерфейс SPI. Після успішної авторизації користувача контролер формує сигнал керування двоканальним релейним модулем. Перший канал реле забезпечує керування електромагнітним замком YM-280N, а другий використовується для керування системою кондиціонування повітря серверного приміщення.

Відображення інформації реалізується за допомогою LCD-дисплея 20×4 з інтерфейсом I²C. Для дистанційного моніторингу використовується Ethernet-модуль W5500, а для зберігання журналу подій — модуль карти пам'яті microSD. Для локального керування системою передбачено кнопку Exit, кнопку Reset Alarm та активний бузер для звукового оповіщення про аварійні ситуації.

Живлення електронних модулів здійснюється від джерела напруги 5 В. RFID-зчитувач RC522 використовує напругу 3,3 В. Електромагнітний замок та коло керування кондиціонером живляться від окремого джерела напруги 12 В.

Використання інтерфейсів SPI, I²C та цифрових входів/виходів забезпечує ефективний обмін даними між усіма функціональними вузлами системи та дозволяє реалізувати необхідні функції моніторингу середовища і контролю доступу до серверного приміщення.

2.5 Обґрунтування вибору програмного забезпечення

Функціонування розробленої системи забезпечується комплексом програмних засобів, що реалізують локальний моніторинг параметрів середовища, контроль доступу до серверного приміщення, реєстрацію подій, віддалений моніторинг та мережеву взаємодію.

Основним середовищем розробки програмного забезпечення обрано Arduino IDE. Дане середовище забезпечує підтримку мікроконтролерної платформи Arduino Mega 2560, дозволяє виконувати розробку, компіляцію та завантаження програмного коду до мікроконтролера, а також підтримує велику кількість бібліотек для роботи з периферійними пристроями.

Для організації локальної мережевої взаємодії використовується Ethernet-модуль W5500 та бібліотека Ethernet. У програмному забезпеченні реалізовано вбудований HTTP-сервер, який формує вебсторінку з поточними значеннями температури, вологості та станом контрольованих пристроїв. Це дозволяє здійснювати моніторинг серверного приміщення через звичайний веббраузер локальної мережі.

Для реалізації віддаленого моніторингу використовується платформа Blynk. Програмний код забезпечує передачу до мобільного додатка значень температури, вологості, часу, стану замка та журналу подій. Крім відображення інформації, платформа використовується для формування електронних повідомлень про виникнення аварійних ситуацій та реєстрації подій доступу.

Контроль доступу реалізовано за допомогою RFID-зчитувача RC522 та бібліотеки MFRC522. Програмне забезпечення здійснює зчитування унікальних ідентифікаторів RFID-карток, порівняння їх із базою дозволених користувачів та формування команд керування електромагнітним замком.

Для збереження журналу подій використовується карта пам’яті microSD та бібліотека SD. У процесі роботи системи на карту пам’яті записуються дані про параметри середовища, а також інформація про відкриття та закриття серверного приміщення.

Відображення локальної інформації реалізовано за допомогою LCD-дисплея з інтерфейсом I²C. Для цього використовуються бібліотеки Wire та LiquidCrystal_I2C.

Для роботи з годинником реального часу DS3231 використовується спеціалізована бібліотека DS3231. Отримані дата та час використовуються для формування журналів подій та повідомлень про аварійні ситуації.

Для організації циклічного виконання програмних функцій застосовується бібліотека BlynkTimer. За допомогою програмних таймерів реалізовано періодичне опитування датчиків, оновлення дисплея, запис даних на карту пам’яті, контроль RFID-зчитувача та обробку мережевих запитів.

Таким чином, обране програмне забезпечення забезпечує реалізацію локального та віддаленого моніторингу, контролю доступу, реєстрації подій, мережевої взаємодії та аварійного оповіщення користувачів.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Реалізація програмного забезпечення

Програмне забезпечення комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення розроблено з використанням модульного підходу, що забезпечує незалежну реалізацію окремих функціональних підсистем та спрощує подальшу модернізацію системи. Структура програмного забезпечення наведена на рис. 3.1, а алгоритм його роботи — на рис. 3.2.

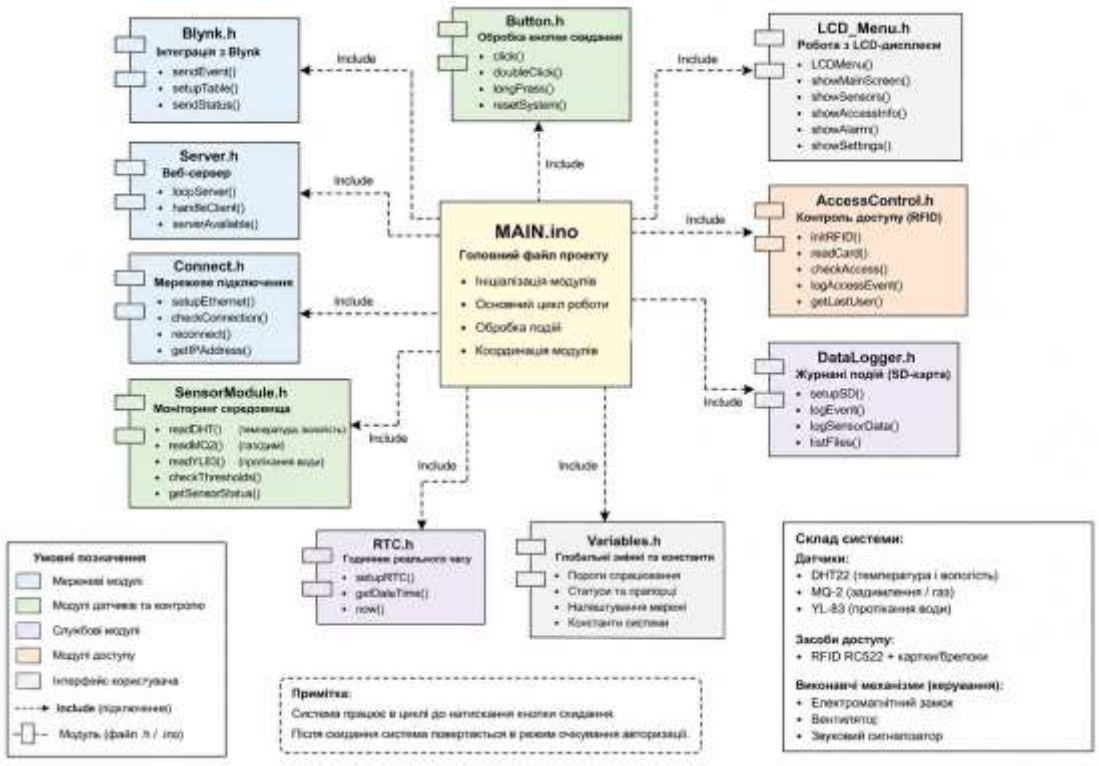

Рисунок 3.1 – Структура програмного забезпечення комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення

Центральним елементом програмного забезпечення є головний модуль MAIN.ino, який виконує ініціалізацію всіх програмних компонентів та координує їхню взаємодію. Після запуску системи здійснюється налаштування периферійних пристроїв, запуск мережевих сервісів, ініціалізація модулів контролю доступу, моніторингу середовища, журналювання подій та відображення інформації.

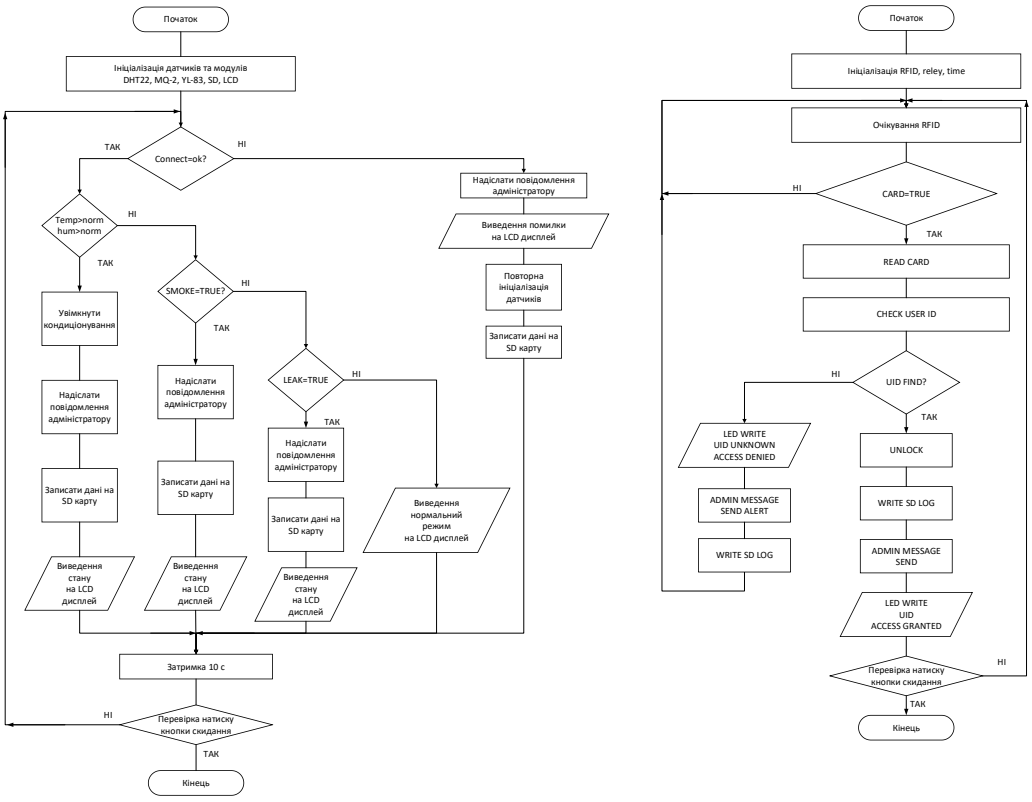

Рисунок 3.2 – Алгоритм роботи програмного забезпечення

Для підвищення структурованості програмного коду окремі функції реалізовані у вигляді незалежних програмних модулів. Модуль SensorModule.h забезпечує зчитування та обробку даних від датчика температури та вологості DHT22, датчика задимлення MQ-2 та датчика протікання води YL-83. Отримані значення аналізуються та порівнюються з установленими пороговими значеннями. У випадку виникнення аварійної ситуації формується відповідне повідомлення та активуються засоби сигналізації.

Модуль AccessControl.h реалізує функції контролю доступу до серверного приміщення. Його завданням є зчитування RFID-ідентифікаторів, перевірка прав доступу користувачів та формування подій авторизації. Після успішної перевірки ідентифікатора виконується керування електромагнітним замком, а інформація про подію передається до системи журналювання та віддаленого моніторингу.

Відображення інформації користувачу здійснюється за допомогою модуля LCD_Menu.h. Він забезпечує формування екранів інтерфейсу, відображення поточних параметрів середовища, стану системи контролю доступу, аварійних повідомлень та службової інформації.

Для забезпечення мережевої взаємодії використовується модуль Connect.h, який відповідає за встановлення та підтримку мережевого з'єднання. Робота локального вебінтерфейсу реалізована модулем Server.h, що формує вебсторінки з актуальними даними моніторингу. Передача інформації до мобільного застосунку реалізується за допомогою модуля Blynk.h.

Функції реєстрації подій реалізовані модулем DataLogger.h. Він забезпечує запис параметрів середовища, результатів авторизації користувачів та аварійних повідомлень на карту пам'яті microSD. Для фіксації часу виникнення подій використовується модуль RTC.h, який забезпечує отримання поточних значень дати та часу від годинника реального часу.

Обробка натискань кнопок реалізується модулем Button.h. Програмне забезпечення забезпечує контроль натискання кнопки виходу та кнопки скидання аварійних повідомлень. Після натискання кнопки скидання система завершує поточний цикл роботи та повертається до початкового режиму функціонування.

Алгоритм роботи програмного забезпечення базується на циклічному опитуванні функціональних модулів. Після завершення етапу ініціалізації система переходить до безперервного циклу виконання, у межах якого здійснюється моніторинг параметрів середовища, контроль доступу, оновлення інформації на дисплеї, журналювання подій та передача даних до

віддалених сервісів. У разі виявлення аварійних ситуацій або подій доступу відповідна інформація обробляється та передається користувачу через локальні та мережеві засоби індикації.

3.2 Реалізація експериментального зразка системи

Для перевірки працездатності розробленої системи було створено експериментальний макет, який містить усі основні функціональні компоненти системи моніторингу середовища та контролю доступу до серверного приміщення. Загальний вигляд макета наведено на рис. 3.3.

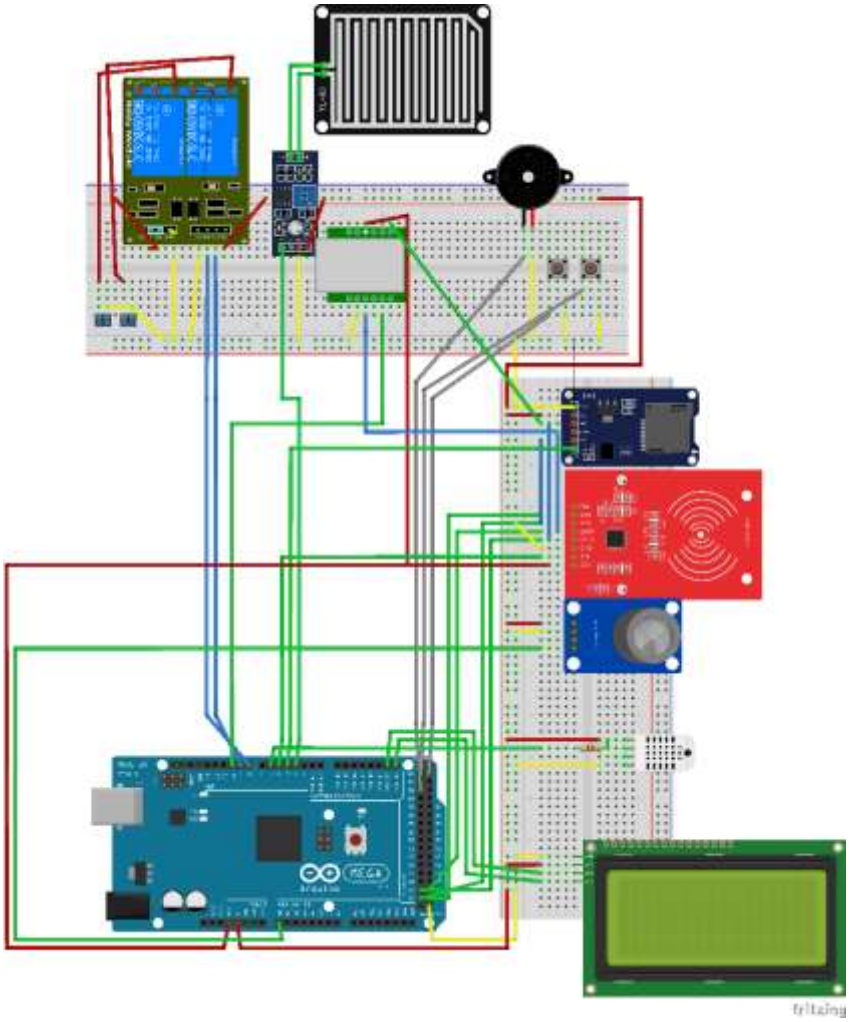

Рисунок 3.3 – Макет комп'ютерної системи моніторингу середовища і контролю доступу до серверного приміщення

Створений макет дозволив перевірити коректність роботи всіх функціональних вузлів системи, взаємодію між окремими програмними модулями та правильність реалізації алгоритмів моніторингу середовища і контролю доступу до серверного приміщення.

3.2.1 Реалізація інтерфейсу користувача та режимів роботи системи

Для відображення поточного стану системи використовується LCD-дисплей 20×4 з інтерфейсом I²C. Інтерфейс користувача забезпечує виведення інформації про параметри середовища серверного приміщення, стан виконавчих пристроїв, результати авторизації користувачів та повідомлення про аварійні ситуації.

У штатному режимі роботи на дисплей виводяться поточні значення температури та вологості повітря, концентрації диму, стан датчика протікання води, стан електромагнітного замка, а також поточна дата та час. Такий режим забезпечує оператору швидкий доступ до основних параметрів системи без необхідності використання додаткових засобів моніторингу.

Рисунок 3.4 – Головний екран системи у штатному режимі роботи.

У разі перевищення допустимого температурного порогу система автоматично переходить до режиму попередження про перегрів. На дисплеї відображається повідомлення про підвищену температуру та інформація про поточні параметри середовища.

Рисунок 3.5 – Повідомлення про перевищення допустимої температури.

Аналогічний механізм використовується при перевищенні допустимого рівня вологості. У цьому випадку система формує попередження про можливість утворення конденсату або порушення умов експлуатації серверного обладнання.

Рисунок 3.6 – Повідомлення про перевищення допустимого рівня вологості.

Для контролю пожежної безпеки реалізовано режим виявлення диму або газу. Після спрацювання датчика MQ-2 система формує аварійне повідомлення та відображає його на дисплеї. Одночасно активуються засоби звукового оповіщення та формується запис у журналі подій.

Рисунок 3.7 – Повідомлення про виявлення диму або підвищеної концентрації газу.

При виявленні води датчиком YL-83 програмне забезпечення переходить до режиму аварійного сповіщення про протікання. На дисплеї відображається відповідне повідомлення, що дозволяє оперативно виявити виникнення аварійної ситуації.

Рисунок 3.8 – Повідомлення про виявлення протікання води.

Для підтримання допустимого температурного режиму реалізовано керування системою кондиціонування. Користувач може контролювати стан кондиціонера та встановлене порогове значення температури.

Рисунок 3.9 – Відображення стану системи кондиціонування при перевищенні температурного порогу.

Після повернення температури до допустимого діапазону система автоматично відключає кондиціонер та відображає відповідне повідомлення.

Рисунок 3.10 – Відображення стану системи після відключення кондиціонера.

Окремий режим роботи інтерфейсу призначений для відображення результатів авторизації користувачів. Після зчитування RFID-картки система виводить її ідентифікатор та результат перевірки прав доступу.

Рисунок 3.11 – Повідомлення про успішну авторизацію користувача.

Якщо картка відсутня у списку дозволених користувачів, система формує повідомлення про заборону доступу та реєструє подію у журналі.

Рисунок 3.12 – Повідомлення про відмову у доступі.

Для підвищення надійності функціонування передбачено режим відображення помилок роботи датчиків. У разі втрати зв'язку з датчиком або отримання некоректних даних на дисплей виводиться повідомлення про несправність.

Рисунок 3.13 – Повідомлення про помилку роботи датчика.

Таким чином, реалізований інтерфейс користувача забезпечує наочне відображення поточного стану системи, оперативне інформування про

аварійні ситуації та результати контролю доступу, що підвищує ефективність експлуатації серверного приміщення.

3.2.2 Реалізація вебінтерфейсу та віддаленого моніторингу

Для забезпечення віддаленого доступу до інформації про стан серверного приміщення у складі програмного забезпечення реалізовано дві підсистеми мережевої взаємодії: локальний вебсервер на базі Ethernet-модуля W5500 та мобільний інтерфейс моніторингу на платформі Blynk.

Вебсервер забезпечує формування HTML-сторінки з поточними параметрами системи. Після підключення користувача через веббраузер сервер автоматично формує вебсторінку, яка містить значення температури та вологості повітря, інформацію про наявність аварійних ситуацій та стан серверного приміщення (рис.3.14).

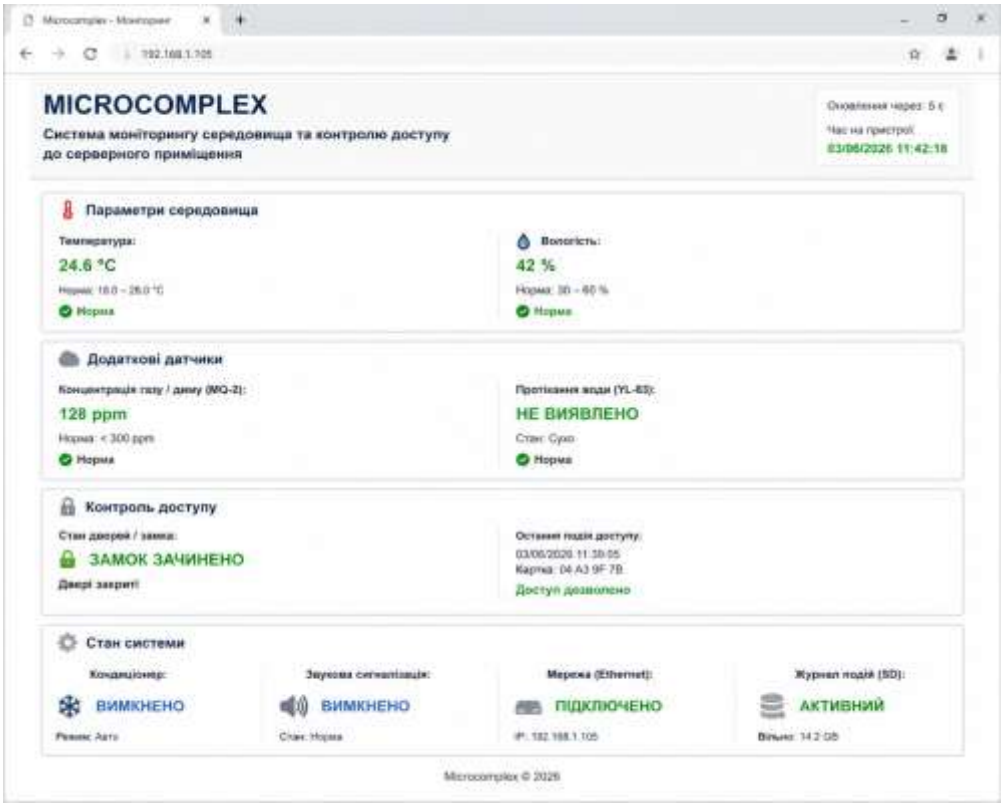

Рисунок 3.14 – Вебінтерфейс моніторингу параметрів серверного приміщення

У процесі формування вебсторінки виконується аналіз поточних значень контрольованих параметрів. У разі перевищення допустимих меж температури або вологості на сторінці додатково відображаються попереджувальні повідомлення. Це дозволяє користувачу оперативно оцінити стан серверного приміщення без необхідності підключення до локального дисплея системи.

Для віддаленого моніторингу через мобільні пристрої використовується хмарна платформа Blynk. Передавання інформації між мікроконтролером та сервером Blynk здійснюється через мережеве підключення Ethernet-модуля W5500. У мобільному застосунку відображаються поточні значення температури, вологості, стан системи контролю доступу та повідомлення про аварійні події.

Окремою функцією Blynk є ведення журналу подій доступу (рис.3.15). Після кожного зчитування RFID-картки програмне забезпечення формує запис, який містить дату, час, унікальний ідентифікатор RFID-мітки та результат авторизації. Сформований запис автоматично передається до табличного віджета мобільного застосунку, що забезпечує перегляд історії доступу до серверного приміщення в режимі реального часу.

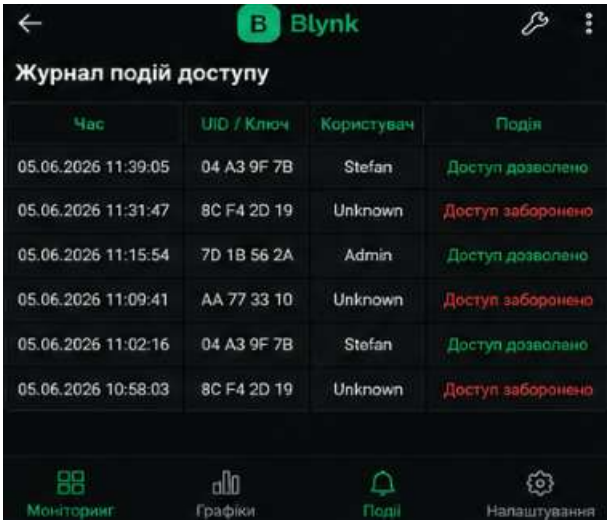

Рисунок 3.15 – Відображення журналу подій доступу у мобільному застосунку Blynk

Крім відображення поточних параметрів (рис. 3.16), система реалізує механізм автоматичного інформування користувачів про виникнення аварійних ситуацій (рис. 3.17). Повідомлення формуються автоматично при виникненні подій контролю доступу або перевищенні встановлених порогових значень контрольованих параметрів.

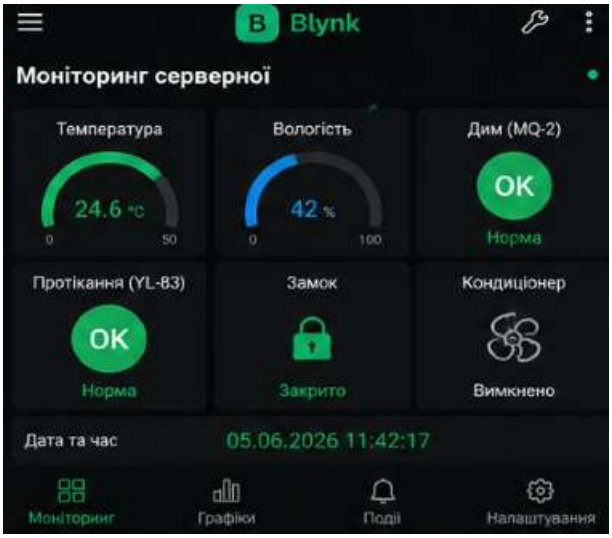

Рисунок 3.16 – Повідомлення про аварійні події в системі Blynk

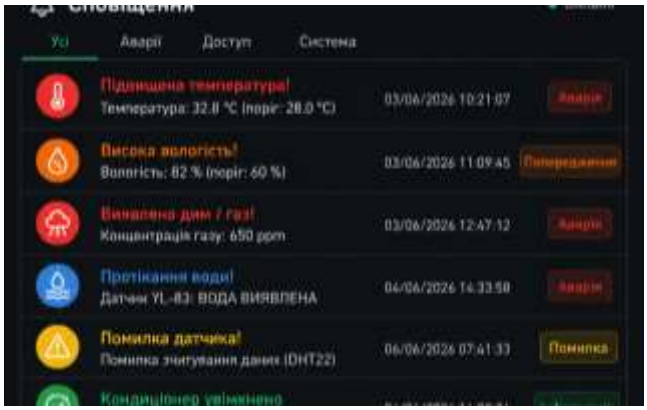

Рисунок 3.17 – Повідомлення про аварійні події в системі Blynk

Також зручно переглядати статистику (рис. 3.18) з датчиків серверної.

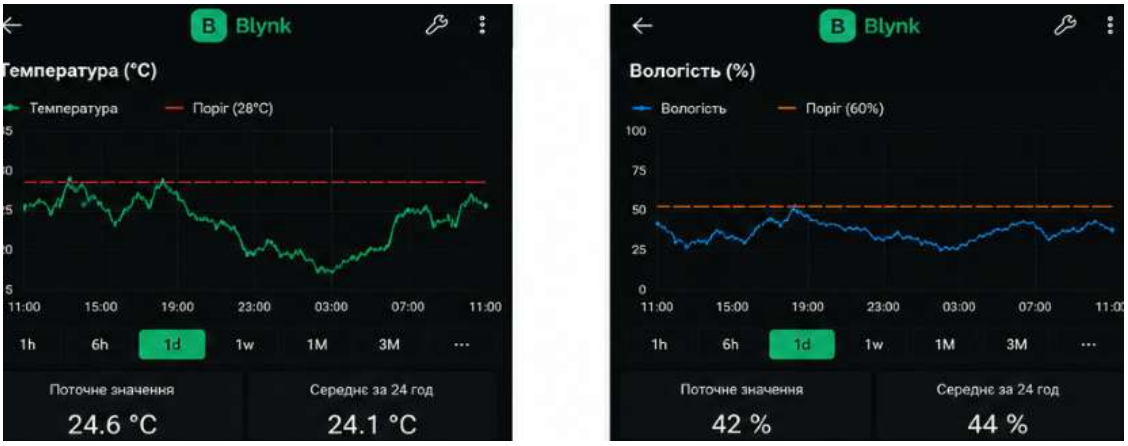

Рисунок 3.18 – Графіки зміни температури і вологості

Проведене тестування підтвердило працездатність усіх функціональних підсистем комп'ютерної системи моніторингу середовища та контролю доступу до серверного приміщення. У ході випробувань було перевірено роботу датчиків контролю параметрів середовища, підсистеми контролю доступу, механізмів оповіщення, вебінтерфейсу та мобільного застосунку Blynk. Отримані результати підтвердили правильність реалізації програмного забезпечення та відповідність системи поставленим вимогам.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вплив високої напруги на людину

Сучасна електрифікація всіх сфер людської діяльності ставить на перший план питання про захист персоналу, що обслуговує електроустаткування, а також інших осіб, які можуть підпадати під небезпеку ураження струмом. Практика свідчить про те, що майже у всіх галузях, де використовується електричний струм, безперечно бувають випадки ураження людей. Ураження електричним струмом є найрозповсюдженішим небезпечним і несподіваним для потерпілого видом виробничого травматизму. Вплив високої напруги на людину є надзвичайно важливим питанням, оскільки електричний струм може спричиняти серйозні травми та навіть смерть. Висока напруга значно збільшує ризик ураження електричним струмом через зменшення опору тіла та збільшення сили струму, що проходить через нього.

Організм людини не має здатності виявляти наявність електричного струму, і тому вплив електричного струму на організм часто стає непередбачуваним. Дія струму супроводжується зовнішнім ураженням тканин і органів, яке може включати механічні пошкодження, електричні знаки, електрометалізацію шкіри, опіки. Важливо зазначити, що електротравма може виникнути навіть без безпосереднього контакту з провідниками струму, наприклад, через електричну дугу або крокову напругу [14].

Проходячи через тіло людини, електричний струм не лише пошкоджує тканини на шляху проходження, але й впливає на центральну нервову систему, що може призвести до ураження внутрішніх органів, таких як серце або легені. У результаті цього можуть виникати такі наслідки, як термічні опіки, розлади

функцій внутрішніх органів, а також порушення м'язової і серцево–судинної діяльності.

Термічна дія електричного струму призводить до опіків окремих ділянок тіла, а також нагрівання кровоносних судин, нервів, серця та мозку, що спричиняє серйозні функціональні порушення в організмі. Електролітична дія струму виявляється в розкладі органічних речовин та крові, що веде до змін у їх фізико–хімічному складі, що ще більше ускладнює ситуацію для потерпілого.

Біологічна дія електричного струму полягає в подразненні збудливих тканин, що викликає мимовільне скорочення м'язів. Тривалість проходження струму через організм людини впливає на результат ураження: чим довше триває контакт, тим більша ймовірність тяжкого і смертельного результату.

Електричні травми умовно поділяються на місцеві та удари струмом. Місцеві травми включають електричні опіки, електричні знаки, електрометалізацію шкіри, електроофтальмію, а також механічні пошкодження, що виникають через мимовільні скорочення м'язів. Електричний удар є найбільш небезпечним видом ураження електричним струмом, оскільки він впливає на серцево–судинну та дихальну системи організму, що може призвести до порушень їх функціонування або навіть до клінічної смерті.

Небезпека ураження електричним струмом залежить від кількох факторів, серед яких основними є величина струму, тривалість його дії та шлях проходження через тіло людини. Величина струму в свою чергу залежить від опору тіла людини, який змінюється залежно від багатьох факторів: вологості шкіри, напруги, типу струму та інших.

Робота з електричним обладнанням повинна проводитись з урахуванням забезпечення належного заземлення, використання захисних засобів, а також навчання працівників правилам безпечної експлуатації електричних установок [15]. У разі ураження струмом важливим є швидке вимкнення

живлення аварійної ділянки і використання ізоляційних засобів для звільнення потерпілого.

Для забезпечення безпеки обслуговуючого персоналу важливі вимоги до розміщення електроустаткування і категорії приміщень, які встановлюють різні умови для застосування електричних установок, враховуючи вологість, температуру та можливі хімічні впливи на обладнання.

Підсумовуючи, високий рівень небезпеки, який супроводжує використання електричної енергії, необхідним є контроль, дотримання сучасних нормативних актів і регулярне навчання персоналу, що обслуговує електричні установки. Застосування надійних методів захисту від електричного струму, таких як заземлення, використання діелектричних засобів і правильне оснащення робочих місць, значно зменшує ймовірність виникнення нещасних випадків.

4.2 Вимоги безпеки праці під час експлуатації систем вентиляції, опалення чи кондиціонування повітря

Системи вентиляції, опалення та кондиціонування повітря є невід'ємною частиною серверних кімнат. Проте, під час експлуатації цих систем виникають певні ризики, пов'язані з безпекою праці. З метою забезпечення безпечного та здорового середовища існують вимоги, які необхідно враховувати під час проектування, монтажу та експлуатації цих систем.

Один з основних аспектів безпеки праці пов'язаний з відповідним проектуванням систем вентиляції, опалення та кондиціонування повітря. Проектування повинно враховувати тип приміщення, його розмір, кількість мешканців, а також їх потреби у повітрі та комфортних умовах.

Забезпечення належного обсягу повітря та правильного розподілу температури є важливими аспектами, що впливають на безпеку та здоров'я мешканців будинку.

Під час монтажу систем вентиляції, опалення та кондиціонування повітря важливо дотримуватись вимог безпеки. Роботи з монтажу повинні проводитись кваліфікованими спеціалістами з використанням відповідного обладнання та інструментів. Крім того, необхідно дотримуватись правил електробезпеки, особливо при підключенні електричних компонентів систем. При встановленні систем вентиляції слід також забезпечувати безпечний доступ до всіх елементів системи для обслуговування та ремонту.

Експлуатація систем вентиляції, опалення та кондиціонування повітря повинна здійснюватися відповідно до рекомендацій виробника та нормативних документів. Регулярна технічна перевірка та обслуговування систем допомагає попередити можливі аварійні ситуації та забезпечує безперебійну роботу.

Очищення фільтрів, перевірка роботи вентиляторів та контроль параметрів повітря (таких як вологість, температура, швидкість потоку повітря) є важливими аспектами регулярного обслуговування.

Додатковою мірою безпеки є навчання користувачів щодо правильного використання систем вентиляції, опалення та кондиціонування повітря.

Природна та штучна вентиляції повинні відповідати наступним санітарно-гігієнічним вимогам:

– створювати в робочій зоні приміщень нормовані метеорологічні умови праці (температуру, вологість і швидкість руху повітря);

– повністю усувати з приміщень шкідливі гази, пари, пил та аерозолі або розчиняти їх до гранично допустимих концентрацій;

– не вносити в приміщення забруднене повітря ззовні або шляхом засмоктування забрудненого повітря з суміжних приміщень;

– не створювати протягів чи різкого охолодження;

– бути доступними для управління та ремонту під час експлуатації;

– не створювати під час експлуатації додаткових незручностей (наприклад, шуму, вібрацій, попадання дощу, снігу).

Користувачі повинні бути ознайомлені з принципами роботи систем, процедурами заміни фільтрів, а також правилами експлуатації в разі аварійних ситуацій, наприклад, виникнення задимлення або пожежі. Знання про запобіжні заходи та процедури евакуації можуть врятувати життя і здоров'я працівників у випадку надзвичайних ситуацій.

Одним з основних аспектів безпеки праці є контроль якості повітря, яке постачається системами вентиляції. Регулярний аналіз якості повітря на наявність шкідливих речовин, таких як гази, пил, бактерії чи алергени, допомагає виявити можливі проблеми з системою та вжити відповідних заходів для їх вирішення.

Крім того, важливо враховувати нормативні вимоги щодо розміщення систем вентиляції, опалення та кондиціонування повітря. Наприклад, деякі компоненти систем можуть вимагати певної відстані від робочих місць або повинні бути відокремлені від інших приміщень з метою запобігання поширенню шкідливих речовин.

Усі користувачі, які мають прямий контакт з системами вентиляції, опалення та кондиціонування повітря, повинні мати необхідні засоби індивідуального захисту. Це можуть бути респіратори, захисні окуляри, відповідний одяг тощо. Застосування відповідних засобів індивідуального захисту допомагає зменшити ризик впливу шкідливих речовин на здоров'я працівників [16].

Забезпечення належного проектування, монтажу, обслуговування і користування цими системами допомагає забезпечити безпеку та здоров'я мешканців будівель, знизити ризик виникнення аварій та забезпечити комфортні умови проживання.

ВИСНОВКИ

У кваліфікаційній роботі розроблено комп'ютерну систему моніторингу середовища та контролю доступу до серверного приміщення, яка забезпечує комплексний контроль умов експлуатації серверного обладнання та захист приміщення від несанкціонованого доступу.

У процесі виконання роботи проведено аналіз сучасних засобів моніторингу серверних приміщень та систем контролю доступу, визначено функціональні вимоги до розроблюваної системи та обґрунтовано вибір апаратного і програмного забезпечення. Для реалізації проєкту обрано мікроконтролерну платформу Arduino Mega 2560, датчики температури і вологості DHT22, задимлення MQ-2, протікання води YL-83, RFID-зчитувач RC522, Ethernet-модуль W5500, модуль microSD та LCD-дисплей.

У роботі розроблено узагальнену структуру системи, функціональну схему, електричну принципову схему та алгоритми функціонування програмного забезпечення. Створене програмне забезпечення забезпечує моніторинг температури, вологості, задимлення та протікання води, автоматичне керування системою кондиціонування, контроль доступу за RFID-ідентифікаторами, ведення журналу подій та відображення інформації на локальному дисплеї.

Реалізовано засоби віддаленого моніторингу на основі вбудованого вебсервера та мобільного застосунку Blynk, що дозволяють контролювати стан серверного приміщення в режимі реального часу та отримувати повідомлення про аварійні ситуації.

Для перевірки працездатності системи створено експериментальний макет та проведено тестування всіх функціональних підсистем. Результати випробувань підтвердили коректність роботи засобів моніторингу середовища, механізмів контролю доступу, системи оповіщення, вебінтерфейсу та мобільного застосунку.

Отримані результати свідчать про досягнення поставленої мети та можливість практичного використання розробленої комп'ютерної системи для забезпечення безпеки та надійної експлуатації серверних приміщень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.

2. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп'ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ, 2019. 150 с.

3. Yatsyshyn V., Pastukh O., Palamar A., Zharovskyy R. Technology of relational database management systems performance evaluation during computer systems design. Scientific Journal of TNTU. 2023. Vol. 109, No. 1. P. 54–65.

4. Yatsyshyn V., Pastukh O., Zharovskyi R., Shabliy N. Software tool for productivity metrics measure of relational database management system. Mathematical Modeling. 2023. No. 1(48). P. 7–17.

5. Рожик А.М., Жаровський Р.О. Аналіз ефективності роботи адаптивної системи контролю доступу на основі нечіткої логіки. Матеріали наукової конференції ТНТУ. Тернопіль: ТНТУ, 2025. С. 12–13.

6. Рожик А.М., Жаровський Р.О. Методи та програмно-апаратні засоби ідентифікації працівників з метою визначення робочого часу та доступу до приміщення. Збірник тез доповідей науково-технічної конференції. Тернопіль: ТНТУ, 2025. С. 45.

7. Дячук О.А., Жаровський Р.О. Використання SDN для оптимізації передачі даних в комп'ютерних мережах. Матеріали XI науково-технічної конференції ТНТУ імені Івана Пулюя «Інформаційні моделі системи та технології». Тернопіль: ТНТУ, 2023. С. 149–150.

8. Дячук О.А., Жаровський Р.О. Управління потоком за критеріями доступності. Матеріали XI науково-технічної конференції ТНТУ імені Івана

Пулюя «Інформаційні моделі системи та технології». Тернопіль: ТНТУ, 2023. С. 151.

9. Ковтун Н., Жаровський Р. Алгоритмічне забезпечення систем виявлення вторгнень. Матеріали XI науково-технічної конференції ТНТУ імені Івана Пулюя «Інформаційні моделі системи та технології». Тернопіль: ТНТУ, 2023. С. 156.

10. Ковтун Н., Жаровський Р. Аналіз засобів протидії вторгненням і атакам на комп'ютерні системи. Матеріали XII Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». Тернопіль: ТНТУ, 2023. С. 453–454.

11. Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі. Тернопіль: ТНТУ імені Івана Пулюя, 2017. 384 с.

12. Palamar A., Karpinski M., Palamar M., Osukhivska H., Mytnyk M. Remote Air Pollution Monitoring System Based on Internet of Things. CEUR Workshop Proceedings. 2022. Vol. 3309. P. 194–204.

13. Palamar A., Palamar M., Osukhivska H. Real-time Health Monitoring Computer System Based on Internet of Medical Things. CEUR Workshop Proceedings. 2023. Vol. 3628. P. 106–115.

14. ДСТУ 12.2.047:2018. Охорона праці в електричних установках. Загальні вимоги. Київ : Мінекономрозвитку України, 2018. 32 с.

15. Гарасевич В. І., Шевчук В. М. Електрична безпека та захист від електричних травм. Київ : Техніка, 2020. 360 с.

16. Жидецький В.Ц. Охорона праці користувачів комп'ютерів: підручник. Львів: Афіша, 2020. 176 с.

Додаток А

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра комп'ютерних систем та мереж

"Затверджую"

Завідувач кафедри КС

_____ Осухівська Г.М.

" 2 " лютого 2026 р.

КОМП'ЮТЕРНА СИСТЕМА МОНІТОРИНГУ СЕРЕДОВИЩА І КОНТРОЛЮ ДОСТУПУ ДО СЕРВЕРНОГО ПРИМІЩЕННЯ

ТЕХНІЧНЕ ЗАВДАННЯ

на _9_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп'ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІс-41
_____ к.т.н., доц. Жаровський Р.О.	_____ Дуніковський С. Б.
" 2 " лютого 2026 р.	" 2 " лютого 2026 р.

Тернопіль 2026

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Комп’ютерна система моніторингу середовища і контролю доступу до серверного приміщення».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.264.00.00

1.2 Виконавець

Студент групи СІс-41, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Дуніковський С. Б.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету № 4/9-189 від 24.04.2026 р.

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 26.01.2026 р.

Плановий термін завершення виконання кваліфікаційної роботи – 21.06.2026 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ISO, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи. Попередній захист кваліфікаційної роботи відбувається при готовності роботи – наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Проєктована комп’ютерна система призначена для автоматизованого моніторингу параметрів середовища та контролю доступу до серверного приміщення.

Система повинна забезпечувати безперервний контроль температури, вологості повітря, рівня задимлення, появи води у приміщенні, а також здійснювати контроль доступу користувачів за допомогою RFID-ідентифікаторів.

Система повинна виконувати реєстрацію подій, формування аварійних повідомлень, керування електромагнітним замком та системою кондиціонування, а також забезпечувати локальний і віддалений моніторинг стану серверного приміщення.

2.2 Мета створення системи

Метою створення комп’ютерної системи є підвищення рівня безпеки серверного приміщення шляхом автоматизації процесів моніторингу

параметрів навколишнього середовища, виявлення аварійних ситуацій та контролю доступу до обладнання.

2.3 Характеристика об'єкту

Об’єктом автоматизації є серверне приміщення, у якому розміщене серверне та мережеве обладнання, що потребує підтримання визначених умов експлуатації та обмеження фізичного доступу сторонніх осіб.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Система повинна забезпечувати цілодобовий моніторинг параметрів середовища та контроль доступу до серверного приміщення.

3.1.1 Вимоги до структури та функціонування системи

До складу системи повинні входити:

– мікроконтролер;

– Ethernet-модуль;

– RFID-зчитувач;

– датчик температури та вологості;

– датчик диму та газу;

– датчик протікання води;

– LCD-дисплей;

– модуль карти пам’яті microSD;

–релейний модуль;

–замок;

– кнопки;

– активний бузер;

– блок живлення.

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

Обмін інформацією між компонентами системи повинен здійснюватися через цифрові інтерфейси мікроконтролера. Для передачі даних повинні використовуватись:

– інтерфейс SPI;

– інтерфейс I^2C;

– цифрові входи та виходи для датчиків і виконавчих пристроїв;

– Ethernet-мережа для вебінтерфейсу.

3.1.3 Вимоги до режимів функціонування системи

Система повинна підтримувати такі режими:

– нормальний режим моніторингу;

– режим контролю доступу;

– режим аварійного сповіщення;

– режим ведення журналу подій;

– режим дистанційного моніторингу;

– режим налаштування.

У разі виникнення аварійної ситуації система повинна формувати повідомлення користувачу та активувати звукову сигналізацію.

3.1.4 Вимоги по діагностуванню системи

Для діагностування системи використовуються інструменти діагностування основних процесів системи, які вмонтовані в операційну систему і програмне забезпечення, а також засоби для діагностики апаратного забезпечення.

Система повинна контролювати:

– справність датчиків;

– роботу дисплея;

– роботу модулів;

– працездатність виконавчих пристроїв;

– коректність показників температури та вологості.

У разі виникнення несправності система повинна повідомляти користувача за допомогою дисплея та звукової сигналізації.

3.1.5 Перспективи розвитку, проектування системи

Передбачається можливість:

– інтеграції з хмарними сервісами моніторингу;

– підключення додаткових датчиків;

– реалізації резервного живлення;

– інтеграції із системами відеоспостереження;

– розширення функцій контролю доступу.

3.2 Показники призначення

Система повинна передбачати можливість масштабування. Можливості масштабування повинні забезпечуватися засобами використовуваного базового програмного і технічного забезпечення.

Система повинна забезпечувати:

– контроль температури в діапазоні від 0 до +50 °C;

– контроль вологості в діапазоні від 20 до 90 %;

– виявлення диму та продуктів горіння;

– виявлення протікання води;

– ідентифікацію користувачів за RFID-картками;

– реєстрацію подій на карту пам’яті;

– віддалений моніторинг через вебінтерфейс та Blynk;

– безперервний режим роботи.

3.2.1 Вимоги до надійності

Система повинна забезпечувати працездатність:

– при тривалій безперервній роботі;

– при короткочасних змінах напруги живлення;

– при зміні температури навколишнього середовища.

Для захисту елементів системи повинні використовуватись:

– запобіжники;

– захисні діоди;

– система аварійного вимкнення нагрівача.

Для захисту апаратури від стрибків напруги і комутаційних завад повинні застосовуватися мережні фільтри.

3.3 Вимоги до безпеки

Зовнішні елементи технічних засобів системи, що перебувають під напругою, повинні мати захист від випадкового дотику, а самі технічні засоби мати занулення або захисне заземлення .

Система електроживлення повинна забезпечувати захисне вимикання при перевантаженнях і коротких замиканнях в колах навантаження, а також аварійне ручне вимикання.

Загальні вимоги пожежної безпеки повинні відповідати нормам на побутове електрообладнання. У разі пожежі не мають виділятися отруйні гази і дим. Після зняття електроживлення має бути доступне застосування будь-яких засобів пожежогасіння.

3.3.1 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи

Мікроклімат повинен відповідати нормам виробничого мікроклімату по ДСН 3.3.6.042-99:

– температура повітря в межах від +10ºС до +35ºС;

– відносна вологість повітря при 25°С в межах від 30% до 80%;

– атмосферний тиск 760±25 мм рт. ст.

Періодичне технічне обслуговування використовуваних технічних засобів має проводитися відповідно до вимог технічної документації, але не рідше ніж один раз на рік.

Періодичне технічне обслуговування і тестування технічних засобів повинні включати обслуговування і тестування всіх використовуваних засобів, датчики, контроллери, системи передачі даних, пристрої безперебійного живлення.

На підставі результатів тестування технічних засобів повинні проводитися аналіз причин виникнення виявлених дефектів і прийматися заходи по їх ліквідації.

3.4 Вимоги до захисту інформації від несанкціонованого доступу

Система повинна забезпечувати контроль доступу до серверного приміщення на основі RFID-ідентифікації користувачів.

Усі події доступу повинні реєструватися у журналі подій

3.4.1 Вимоги по стандартизації і уніфікації

Система повинна відповідати вимогам ергономіки і зручності користування за умови комплектування високоякісним обладнанням (ЕОМ, монітор і інше обладнання), що має необхідні сертифікати відповідності і безпеки.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальну записку;

– структурну схему системи;

– функціональну схему системи;

– блок-схеми алгоритмів роботи;

– схему електричну принципову;

– макет реалізованої системи;

– результати тестування.

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

5 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання КРБ

№ етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1	Розробка технічного завдання	26.01 – 02.02
2	Робота над першим розділом «Аналіз технічного завдання»	03.02 – 15.02
3	Робота над другим розділом «Проєктна частинв»	20.04 – 25.04
4	Робота над третім розділом «Практична частина»	26.04 – 05.05
5	Робота над четвертим розділом «Безпека життєдіяльності, основи охорони праці»	07.05 – 25.05
6	Оформлення пояснювальної записки і графічного матеріалу	26.05 – 7.06
7	Перевірка на академічний плагіат, перевірка керівником та консультантами	8.06 – 14.06
8	Попередній захист кваліфікаційної роботи бакалавра	15.06 – 21.06
9	Захист кваліфікаційної роботи бакалавра	22.06

6 Додаткові умови виконання кваліфікаційної роботи

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

Додаток Б

Перелік елементів

Позн.	Найменування	К-ть	Примітка
	Мікроконтролер		
A1	Arduino Mega 2560 Rev3	1	
	Модулі		
A2	Relay 2 Ch.5V	1	
A3	W5500 Ethernet Module	1	
U1	MFRC522 RFID Reader	1	
SD1	MicroSD Card Module SPI	1	
L1	LCD2004 I2C (20×4)	1	
	Датчики		
D5	MQ-2	1	
DHT2	DHT22 (AM2302)	1	
YL1	YL-83 Rain Sensor Plate	1	
YL2	YL-83 Detection Board	1	
	Кнопки, роз'єми		
S1	Tact Switch 6×6 mm	1	
S2	Tact Switch 6×6 mm	1	
J1, J2	Terminal Block 2 Pin	2	
J3	Active Buzzer 5V	1	
R1	МЛТ-0,125 4,7 кОм	1	(+/-5%)

Змн.	Арк.	№ докум.	Підпис	Дата	КС КРБ 123.264.00.00 ПЕ		
Розроб.		Дуніковський			Комп'ютерна система моніторингу середовища і контролю доступу до серверного приміщення	Літ.	Арк. 1 / Аркушів 1
Перевірив		Жаровський Р.					
Реценз.		Млинко Б.Б.				ТНТУ, каф. КС, гр. СІс-41	
Н. Контр.		Тиш Є.В.					
Затверд.		Осухівська Г.М.			Перелік елементів		