ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій, цифровізації суспільства та зростання вимог до безпеки об’єктів різного призначення особливої актуальності набуває створення інтелектуальних систем контролю та керування доступом, здатних забезпечити надійну ідентифікацію користувачів, оперативне прийняття рішень та ефективне адміністрування [1, 2]. Зростання кількості об’єктів, що потребують контролю доступу, зокрема житлових будівель, офісних приміщень, промислових підприємств і критичної інфраструктури, обумовлює необхідність впровадження сучасних автоматизованих рішень, які поєднують високий рівень захисту, гнучкість конфігурації та можливість інтеграції з іншими інформаційними системами [3].

Традиційні системи доступу, що базуються на використанні механічних ключів, магнітних карток або кодових панелей, мають низку суттєвих недоліків, серед яких варто відзначити ризик втрати або копіювання ідентифікаторів, обмежені можливості централізованого керування, відсутність гнучких механізмів аутентифікації та недостатній рівень журналювання подій [2]. Крім того, такі системи часто не забезпечують можливості віддаленого доступу до керування, що значно знижує ефективність їх використання в умовах сучасних вимог до мобільності та оперативності прийняття рішень [4].

Використання мобільних пристроїв як засобів ідентифікації користувачів відкриває нові можливості для побудови систем контролю доступу, оскільки смартфон є персональним багатофункціональним пристроєм, який поєднує в собі засоби зв’язку, обчислювальні ресурси та можливості захищеного зберігання даних [4, 5]. Застосування мобільного ідентифікатора дозволяє реалізувати більш гнучкі та захищені механізми автентифікації, зокрема із використанням криптографічних методів та багатофакторної перевірки користувача, а також забезпечує зручність експлуатації та зниження витрат на обслуговування системи [1].

Важливим напрямом розвитку сучасних систем доступу є їх інтеграція з технологіями бездротового зв’язку та вбудованих систем керування, що забезпечує можливість віддаленого керування, моніторингу та адміністрування [3, 5]. Реалізація таких функцій потребує використання високопродуктивних мікроконтролерних платформ, здатних обробляти дані в режимі реального часу та підтримувати різноманітні інтерфейси зв’язку [5].

У цьому контексті доцільним є використання мікроконтролера STM32F407VET6-Mini, який характеризується високою продуктивністю, наявністю широкого набору периферійних модулів та підтримкою сучасних комунікаційних інтерфейсів, що дозволяє реалізувати ефективну систему керування доступом [5]. Застосування даного мікроконтролера забезпечує створення компактної, надійної та масштабованої системи, що відповідає сучасним вимогам до безпеки [3].

Таким чином, розробка системи віддаленого керування доступом із використанням мобільного ідентифікатора на базі мікроконтролера STM32F407VET6-Mini є актуальним науково-практичним завданням, спрямованим на підвищення рівня безпеки об’єктів, удосконалення процесів ідентифікації користувачів та впровадження сучасних мікропроцесорних технологій [1–5].

Мета бакалаврської роботи – розробити мікропроцесорну систему віддаленого керування доступом із використанням мобільного ідентифікатора на базі контролера STM32F407VET6-Mini, яка забезпечує ідентифікацію користувача, прийняття рішення щодо надання доступу, керування виконавчим механізмом замикання та ведення журналу подій.

Об’єкт дослідження. Процес функціонування системи контролю та віддаленого керування доступом до об’єкта.

Предметом дослідження. Методи, апаратні та програмні засоби реалізації системи віддаленого керування доступом із використанням мобільного ідентифікатора на базі мікроконтролера STM32F407VET6-Mini.

Практичне значення отриманих результатів підтверджується розробкою апаратно-програмного комплексу, що включає контролер доступу та інструменти взаємодії з ним. Запропоноване рішення забезпечує дистанційне керування правами користувачів через веб-інтерфейс із підтримкою автономного (офлайн) режиму функціонування.

1 АНАЛІЗ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ

1.1 Призначення та сфери застосування систем контролю доступу

Системи контролю та керування доступом є важливою складовою сучасних комплексів безпеки, що призначені для обмеження, регулювання та реєстрації доступу осіб до визначених об’єктів або зон [1, 2]. Основним призначенням таких систем є забезпечення ідентифікації користувачів, перевірки їх прав доступу та прийняття рішення щодо дозволу або заборони проходу, що дозволяє підвищити рівень захищеності об’єктів різного функціонального призначення [2].

Функціонування систем контролю доступу базується на реалізації процесів автентифікації, авторизації та обліку подій, що забезпечує не лише фізичний захист об’єкта, але й можливість аналізу дій користувачів та контролю за їх переміщенням [1]. У сучасних умовах такі системи інтегруються з іншими підсистемами безпеки, зокрема відеоспостереженням, охоронною сигналізацією та інформаційними системами управління, що дозволяє створювати комплексні рішення для забезпечення безпеки [3].

Системи контролю доступу широко застосовуються у різних сферах діяльності, що зумовлено необхідністю обмеження доступу до матеріальних, інформаційних та технологічних ресурсів [3]. У житловому секторі такі системи використовуються для організації доступу до під’їздів, квартир, приватних будинків та прибудинкових територій, забезпечуючи підвищення рівня безпеки мешканців та зниження ризику несанкціонованого проникнення [3]. В офісних та адміністративних будівлях системи контролю доступу застосовуються для розмежування доступу до службових приміщень, серверних кімнат, архівів та інших зон з обмеженим доступом, що дозволяє підвищити рівень інформаційної безпеки та контролю за персоналом [2].

На промислових підприємствах системи контролю доступу виконують функції обмеження доступу до виробничих зон, небезпечних ділянок та технологічного обладнання, що сприяє підвищенню рівня техніки безпеки та запобіганню аварійним ситуаціям [3]. У сфері критичної інфраструктури, зокрема на об’єктах енергетики, транспорту та зв’язку, такі системи є невід’ємною частиною комплексних систем безпеки, що забезпечують захист від несанкціонованого доступу та потенційних загроз [1].

Окремим напрямом застосування систем контролю доступу є використання їх у навчальних закладах, медичних установах та торговельних центрах, де вони забезпечують контроль відвідування, облік часу перебування та підвищення загального рівня безпеки [2]. У сучасних умовах розвитку інформаційних технологій особливого значення набуває впровадження систем доступу з можливістю віддаленого керування та моніторингу, що дозволяє здійснювати адміністрування системи в режимі реального часу незалежно від місцезнаходження оператора [4].

Сучасні системи контролю доступу також активно використовують мобільні технології та бездротові інтерфейси зв’язку, що дозволяє застосовувати смартфони як універсальні ідентифікатори користувачів та забезпечує підвищення зручності експлуатації системи [4, 5]. Це особливо актуально в умовах розвитку концепції Інтернету речей, де системи доступу інтегруються в єдині інформаційно-керуючі середовища та забезпечують автоматизовану взаємодію між різними пристроями [5].

Системи контролю та керування доступом виконують ключову роль у забезпеченні безпеки об’єктів, дозволяють ефективно управляти доступом користувачів, забезпечують облік подій та створюють основу для побудови інтегрованих систем безпеки, що відповідають сучасним вимогам до автоматизації та цифровізації [1–5].

1.2 Класифікація систем контролю та керування доступом

Класифікація систем контролю та керування доступом здійснюється за різними ознаками, що дозволяє систематизувати існуючі рішення, визначити їх функціональні можливості та обрати оптимальну конфігурацію для конкретних умов застосування [1, 3]. Основними критеріями класифікації є спосіб ідентифікації користувача, архітектура системи, тип носія ідентифікаційної інформації, рівень централізації та спосіб керування доступом [2].

За способом ідентифікації користувача системи доступу поділяються на карткові, кодові, біометричні та комбіновані. Карткові системи використовують RFID-картки або електронні ключі, що містять унікальний ідентифікатор користувача, який зчитується спеціальними пристроями [3]. Кодові системи базуються на введенні цифрового або символьного пароля, що дозволяє здійснювати доступ без використання фізичних носіїв, проте мають нижчий рівень захисту через можливість підбору або розголошення коду [2]. Біометричні системи застосовують фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, розпізнавання обличчя або райдужної оболонки ока, що забезпечує високий рівень достовірності ідентифікації [1]. Комбіновані системи поєднують декілька методів ідентифікації, що дозволяє реалізувати багатофакторну автентифікацію та значно підвищити рівень безпеки [1, 2].

За архітектурою системи контролю доступу поділяються на автономні та мережеві. Автономні системи функціонують як незалежні пристрої, що не потребують підключення до центрального сервера та виконують всі функції локально [3]. Мережеві системи передбачають наявність центрального контролера або серверного вузла, що забезпечує централізоване керування, облік подій та можливість інтеграції з іншими інформаційними системами [3].

За типом носія ідентифікаційної інформації системи поділяються на контактні, безконтактні та мобільні. Контактні системи передбачають фізичний контакт користувача з пристроєм, наприклад, використання смарт-карт або

ключів із контактними інтерфейсами [2]. Безконтактні системи базуються на технологіях RFID або NFC, що забезпечують швидку та зручну ідентифікацію без необхідності прямого контакту [3]. Мобільні системи використовують смартфони як засіб ідентифікації, що дозволяє реалізувати віддалене керування доступом та інтеграцію з сучасними інформаційними сервісами [4, 5].

За рівнем централізації системи доступу поділяються на централізовані, децентралізовані та розподілені. Централізовані системи передбачають управління всіма точками доступу з одного центру, що забезпечує високий рівень контролю та адміністрування [3]. Децентралізовані системи працюють незалежно на кожному об’єкті, що підвищує їх автономність та надійність [2]. Розподілені системи поєднують переваги обох підходів, забезпечуючи гнучкість та масштабованість [3].

Узагальнення класифікаційних ознак систем контролю доступу наведено у таблиці 1.1.

Таблиця 1.1 – Класифікація систем контролю доступу

Ознака класифікації	**Тип системи**	**Характеристика**
Спосіб ідентифікації	Карткова	RFID-картки, електронні ключі
	Кодова	Введення пароля
	Біометрична	Відбиток пальця, обличчя
	Комбінована	Декілька факторів
Архітектура	Автономна	Локальна робота
	Мережева	Централізоване керування
Тип носія	Контактна	Смарт-картки
	Безконтактна	RFID, NFC
	Мобільна	Смартфон
Рівень централізації	Централізована	Єдиний центр
	Децентралізована	Локальне керування
	Розподілена	Комбінована

Для наочного представлення структури класифікації систем контролю доступу наведено узагальнену структурну схему (рис. 1.1).

Рисунок 1.1 – Структурна схема класифікації систем контролю доступу

Наведена схема відображає основні напрямки класифікації систем контролю доступу, включаючи способи ідентифікації користувачів, архітектурні особливості, типи носіїв інформації та рівні централізації керування. Використання такої класифікації дозволяє системно підходити до вибору та проєктування систем доступу залежно від вимог конкретного об’єкта та умов його експлуатації [1–5].

1.3 Мобільний ідентифікатор як засіб авторизації користувача

Мобільний ідентифікатор у сучасних системах контролю та керування доступом розглядається як один із найбільш перспективних засобів авторизації користувача, оскільки поєднує високий рівень зручності, функціональності та гнучкості налаштування [1, 4]. На відміну від традиційних носіїв ідентифікаційної інформації, таких як механічні ключі, магнітні картки або брелоки, мобільний пристрій є персоналізованим технічним засобом, що

постійно перебуває у користувача та може виконувати функції цифрового ключа, засобу автентифікації й каналу взаємодії з інформаційною системою [2, 4].

Сутність використання мобільного ідентифікатора полягає у тому, що смартфон або інший мобільний пристрій застосовується для підтвердження прав доступу до певного об’єкта, приміщення або ресурсу шляхом передавання унікальних ідентифікаційних даних через відповідний канал зв’язку [3, 4]. Для цього можуть використовуватися технології NFC, Bluetooth Low Energy, Wi-Fi або мобільний Інтернет, що забезпечують можливість локальної чи віддаленої взаємодії з контролером системи доступу [4]. Такий підхід дозволяє реалізувати не лише процедуру розпізнавання користувача, але й функції централізованого адміністрування, дистанційного надання або скасування прав доступу, а також журналювання всіх подій авторизації [2, 3].

Важливою перевагою мобільного ідентифікатора є можливість використання додаткових механізмів захисту, реалізація яких є складною або неможливою у традиційних системах доступу [1]. Сучасні смартфони підтримують багатофакторну автентифікацію, яка може поєднувати знання користувача, наприклад пароль або PIN-код, володіння пристроєм як фізичним носієм ідентифікації, а також біометричні ознаки, зокрема відбиток пальця або розпізнавання обличчя [1, 2]. У результаті рівень достовірності авторизації значно зростає, а ризик несанкціонованого доступу зменшується [2, 4].

Ще однією важливою перевагою мобільного ідентифікатора є можливість оперативного оновлення параметрів доступу без необхідності фізичної заміни носія [3]. У разі втрати або компрометації смартфона адміністратор системи може швидко заблокувати відповідний цифровий ідентифікатор, змінити права доступу користувача або повторно видати електронний ключ у програмному вигляді [4]. Це суттєво спрощує експлуатацію системи, знижує витрати на обслуговування та підвищує рівень керованості всією інфраструктурою доступу [3].

Використання мобільного ідентифікатора також сприяє інтеграції систем

контролю доступу з іншими цифровими сервісами, зокрема системами відеоспостереження, охоронною сигналізацією, хмарними платформами адміністрування та базами даних користувачів [2, 3]. Завдяки цьому можлива реалізація єдиного інформаційного середовища, у межах якого здійснюється централізований контроль точок доступу, моніторинг стану об’єкта, формування звітів та аналіз подій безпеки [3]. Для сучасних об’єктів це має особливе значення, оскільки дозволяє поєднати функції фізичного захисту, обліку доступу та автоматизованого керування в межах однієї інтегрованої системи [1].

Попри значні переваги, використання мобільного ідентифікатора має і певні обмеження, які необхідно враховувати під час проєктування системи [4]. До таких обмежень належать залежність від стану акумулятора мобільного пристрою, потреба у стабільному функціонуванні бездротових каналів зв’язку, необхідність захисту даних від перехоплення, а також ризики, пов’язані з компрометацією програмного забезпечення смартфона [1, 4]. Саме тому при побудові сучасних систем доступу особлива увага приділяється впровадженню криптографічних алгоритмів, захищених протоколів обміну даними та механізмів резервної автентифікації [1].

Для реалізації мобільної авторизації у мікропроцесорній системі доступу важливе значення має вибір апаратної платформи, яка повинна забезпечувати обробку ідентифікаційних даних, підтримку периферійних інтерфейсів та взаємодію з виконавчими пристроями [5]. У цьому аспекті мікроконтролер STM32F407VET6-Mini є доцільним рішенням, оскільки характеризується достатньою продуктивністю, розвиненою периферією та можливістю інтеграції з модулями бездротового зв’язку, засобами індикації, виконавчими механізмами й сервісними підсистемами [5]. Це дозволяє реалізувати функції приймання ідентифікаційних даних зі смартфона, перевірки прав доступу, формування керуючих сигналів для замикального механізму та передавання інформації до верхнього рівня системи [5].

1.4 Принципи та технології віддаленого керування доступом

Сучасні системи віддаленого керування доступом активно використовують мобільні технології ідентифікації, серед яких найбільш поширеними є технології NFC (Near Field Communication) та BLE (Bluetooth Low Energy) [4].

Технологія NFC забезпечує безконтактну передачу даних на малих відстанях, як правило до 10 см, що робить її зручною для реалізації систем доступу з високим рівнем безпеки [4]. Основною перевагою NFC є коротка дистанція взаємодії, що знижує ризик несанкціонованого перехоплення даних. Крім того, NFC широко використовується у платіжних системах, що підтверджує її надійність та безпечність.

Технологія BLE дозволяє здійснювати бездротовий зв’язок на значно більших відстанях порівняно з NFC та характеризується низьким енергоспоживанням [4, 5]. Це дозволяє використовувати її для реалізації систем доступу з автоматичним розпізнаванням користувача при наближенні до точки доступу. BLE забезпечує гнучкість налаштування, можливість роботи у фоновому режимі та інтеграцію з мобільними додатками.

Порівняльний аналіз показує, що NFC доцільно використовувати у випадках, коли пріоритетом є безпека та контрольований доступ на короткій відстані, тоді як BLE є більш ефективним для реалізації систем із розширеною функціональністю та автоматизацією процесів доступу [4]. У сучасних системах часто застосовується комбіноване використання цих технологій, що дозволяє поєднати їх переваги.

Сучасні системи віддаленого керування доступом активно використовують мобільні технології ідентифікації, серед яких найбільш поширеними є технології NFC (Near Field Communication) та BLE (Bluetooth Low Energy) [4].

Технологія NFC забезпечує безконтактну передачу даних на малих відстанях, як правило до 10 см, що робить її зручною для реалізації систем

доступу з високим рівнем безпеки [4]. Основною перевагою NFC є коротка дистанція взаємодії, що знижує ризик несанкціонованого перехоплення даних. Крім того, NFC широко використовується у платіжних системах, що підтверджує її надійність та безпечність.

Технологія BLE дозволяє здійснювати бездротовий зв’язок на значно більших відстанях порівняно з NFC та характеризується низьким енергоспоживанням [4,5]. Це дозволяє використовувати її для реалізації систем доступу з автоматичним розпізнаванням користувача при наближенні до точки доступу. BLE забезпечує гнучкість налаштування, можливість роботи у фоновому режимі та інтеграцію з мобільними додатками.

Порівняльний аналіз показує, що NFC доцільно використовувати у випадках, коли пріоритетом є безпека та контрольований доступ на короткій відстані, тоді як BLE є більш ефективним для реалізації систем із розширеною функціональністю та автоматизацією процесів доступу [4]. У сучасних системах часто застосовується комбіноване використання цих технологій, що дозволяє поєднати їх переваги.

У системах віддаленого керування доступом важливу роль відіграють методи та протоколи аутентифікації, що забезпечують перевірку достовірності користувача та захист інформаційних ресурсів [1]. Веб-додатки, які використовуються для адміністрування систем доступу, повинні відповідати сучасним вимогам кібербезпеки та забезпечувати надійний захист даних.

До основних методів аутентифікації належать однофакторна, двофакторна та багатофакторна автентифікація [1, 2].

Однофакторна автентифікація базується на використанні пароля або PIN-коду, проте має обмежений рівень безпеки. Двофакторна автентифікація передбачає використання двох незалежних факторів, наприклад пароля та одноразового коду. Багатофакторна автентифікація поєднує декілька факторів, що забезпечує найвищий рівень захисту.

Серед сучасних протоколів аутентифікації у веб-додатках широко використовуються протоколи OAuth 2.0, OpenID Connect та JSON Web Token

(JWT) [1]. Ці протоколи забезпечують безпечну передачу даних, можливість делегування доступу та захист від несанкціонованого використання облікових даних. Використання таких протоколів дозволяє реалізувати гнучку систему авторизації з підтримкою мобільних пристроїв та хмарних сервісів.

Особливе значення має забезпечення захищеного каналу зв'язку між клієнтом і сервером, що реалізується за допомогою протоколу HTTPS та криптографічних алгоритмів [1]. Це дозволяє запобігти перехопленню або модифікації даних під час передавання.

1.5 Переваги та недоліки існуючих рішень

Сучасні системи контролю та керування доступом характеризуються значною різноманітністю технічних рішень, що відрізняються за способом ідентифікації, архітектурою побудови, рівнем захищеності та функціональними можливостями [1, 3]. Аналіз існуючих систем дозволяє визначити їх основні переваги та недоліки, що є необхідним етапом для обґрунтування вибору оптимального підходу до розробки нової системи доступу [2].

До основних переваг сучасних систем контролю доступу належить можливість автоматизованого керування доступом користувачів, що дозволяє значно підвищити рівень безпеки об'єкта та зменшити вплив людського фактору [3]. Використання електронних ідентифікаторів забезпечує швидку та зручну процедуру авторизації, а також можливість ведення журналу подій, що дозволяє здійснювати контроль за переміщенням користувачів і аналізувати їх дії [1]. Крім того, сучасні системи підтримують інтеграцію з іншими підсистемами безпеки, такими як відеоспостереження, сигналізація та системи управління будівлями, що дозволяє створювати комплексні рішення [3].

Важливою перевагою є також можливість централізованого керування доступом, що забезпечує оперативну зміну прав користувачів, дистанційне адміністрування та гнучке налаштування параметрів системи [2]. У випадку використання мобільних ідентифікаторів значно підвищується зручність

експлуатації системи, оскільки користувачеві не потрібно мати окремий фізичний носій доступу [4]. Крім того, впровадження сучасних криптографічних методів дозволяє забезпечити високий рівень захисту переданих даних і зменшити ризик несанкціонованого доступу [1].

Разом із тим існуючі системи контролю доступу мають низку недоліків, які обмежують їх ефективність та сферу застосування [2]. Одним із основних недоліків є залежність від технічних засобів та інфраструктури, зокрема електроживлення та каналів зв’язку, що може призводити до відмови системи у разі аварійних ситуацій [3]. Також існує ризик компрометації ідентифікаційних даних, особливо у випадку використання простих методів автентифікації, таких як паролі або RFID-картки без додаткового захисту [1].

Іншим суттєвим недоліком є складність впровадження та обслуговування мережевих систем доступу, що потребують налаштування серверного обладнання, програмного забезпечення та забезпечення кібербезпеки [2]. У випадку мобільних систем додатковими обмеженнями є залежність від стану мобільного пристрою, рівня заряду акумулятора та стабільності бездротового з’єднання [4]. Крім того, впровадження складних систем доступу може супроводжуватися значними фінансовими витратами, що обмежує їх застосування у невеликих об’єктах [3].

Для узагальнення основних характеристик існуючих систем контролю доступу доцільно представити їх переваги та недоліки у вигляді таблиці 1.2.

Таблиця 1.2 – Переваги та недоліки існуючих систем контролю доступу

Тип системи	Переваги	Недоліки
Карткові (RFID)	Простота використання, низька вартість, швидка ідентифікація	Можливість копіювання картки, втрата носія
Кодові	Відсутність фізичного носія, простота реалізації	Низький рівень безпеки, можливість підбору коду

Кінець таблиці 1.2

Біометричні	Високий рівень захисту, унікальність даних	Висока вартість, складність обробки
Мобільні	Зручність, дистанційне керування, багатофакторна автентифікація	Залежність від смартфона та мережі
Автономні	Надійність, незалежність від мережі	Обмежена функціональність
Мережеві	Централізоване керування, журналювання, масштабованість	Складність налаштування, залежність від серверу

Аналіз наведених переваг і недоліків показує, що жоден із існуючих підходів не є універсальним і кожен із них має свої обмеження, які необхідно враховувати при проєктуванні системи доступу [1–3]. Найбільш перспективним напрямом є використання комбінованих рішень, що поєднують переваги різних методів ідентифікації та забезпечують високий рівень безпеки при збереженні зручності експлуатації [1, 4].

Аналіз існуючих систем контролю доступу дозволяє зробити висновок про доцільність розробки нових підходів, що базуються на використанні мобільних ідентифікаторів, мікропроцесорних технологій та сучасних засобів захисту інформації, що дозволяє підвищити ефективність, надійність та функціональність систем доступу [3–5].

1.6 Постановка задачі

Проведений аналіз сучасних систем контролю та керування доступом показав, що, незважаючи на значний рівень розвитку технічних засобів ідентифікації та автоматизації, існуючі рішення мають низку обмежень, які знижують їх ефективність, гнучкість та рівень безпеки [1–3]. Зокрема, традиційні системи доступу, що базуються на використанні фізичних ідентифікаторів, таких як ключі або RFID-картки, характеризуються ризиком втрати, копіювання або несанкціонованого використання, що може призводити

до порушення режиму безпеки об’єкта [2]. Крім того, значна частина існуючих систем не забезпечує достатнього рівня інтеграції з сучасними інформаційними технологіями, що обмежує можливості віддаленого керування та моніторингу [3].

У зв’язку з цим виникає необхідність розробки мікропроцесорної системи віддаленого керування доступом, яка поєднує використання мобільного ідентифікатора, сучасних засобів зв’язку та ефективних алгоритмів обробки даних. Така система повинна забезпечувати надійну ідентифікацію користувача, прийняття рішення щодо надання доступу, керування виконавчими пристроями та передавання інформації до верхнього рівня системи [3, 5].

Основною задачею даної роботи є розробка структури та принципів функціонування системи віддаленого керування доступом на базі мікроконтролера STM32F407VET6-Mini із використанням мобільного ідентифікатора як засобу авторизації користувача. Система повинна забезпечувати взаємодію між мобільним пристроєм користувача та мікроконтролером, обробку ідентифікаційних даних, перевірку прав доступу та формування керуючих сигналів для виконавчого механізму доступу.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– проаналізувати існуючі методи і засоби реалізації систем контролю доступу;

– обґрунтувати вибір апаратної платформи та елементної бази системи;

– розробити загальну структурну схему системи керування доступом;

– визначити спосіб взаємодії мобільного ідентифікатора з контролером системи;

– розробити алгоритм ідентифікації та авторизації користувача;

– реалізувати програмне забезпечення мікроконтролера для обробки даних і керування доступом.

Результатом виконання даної роботи має стати створення прототипу або

моделі системи віддаленого керування доступом, що забезпечує підвищення рівня безпеки об’єкта, зручність використання та можливість інтеграції з сучасними інформаційними системами [1–5].

Висновок до розділу

У першому розділі дипломної роботи проведено комплексний аналіз сучасних систем контролю та керування доступом, що дозволило визначити їх основні функціональні можливості, принципи побудови та сфери застосування. Розглянуто призначення систем доступу, які забезпечують ідентифікацію користувачів, контроль їх переміщення та підвищення рівня безпеки об’єктів різного призначення.

Виконано класифікацію систем контролю доступу за основними ознаками, зокрема за способом ідентифікації, архітектурою побудови, типом носія інформації та рівнем централізації. Встановлено, що кожен із підходів має свої переваги та обмеження, що визначають доцільність його використання залежно від умов експлуатації та вимог до системи безпеки.

Особливу увагу приділено використанню мобільного ідентифікатора як сучасного засобу авторизації користувача. Визначено, що застосування смартфонів дозволяє підвищити зручність користування системою, забезпечити гнучке адміністрування та реалізувати багатофакторну автентифікацію, що значно підвищує рівень захисту.

Проведений аналіз переваг і недоліків існуючих рішень показав, що традиційні системи доступу мають обмеження, пов’язані з безпекою, гнучкістю та можливістю інтеграції з сучасними інформаційними технологіями. Встановлено, що перспективним напрямом розвитку є впровадження мобільних ідентифікаторів та використання мікропроцесорних систем керування з можливістю віддаленого доступу.

У результаті сформульовано постановку задачі, яка полягає у розробці системи віддаленого керування доступом із використанням мобільного

ідентифікатора на базі мікроконтролера, що забезпечує ідентифікацію користувача, керування виконавчими пристроями, журналювання подій та можливість роботи в офлайн-режимі.

2 РОЗРОБКА АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ СИСТЕМИ ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ

2.1 Загальна структура системи та принципи побудови контролера керування доступом

З результатів попереднього розділу встановлено, що одним із ключових елементів системи віддаленого керування доступом є контролер, який безпосередньо забезпечує прийняття рішення щодо надання або блокування доступу [5, 6]. Саме контролер виконує функції обробки ідентифікаційних даних, перевірки прав користувача та формування керуючих сигналів для виконавчих пристроїв. У зв’язку з цим наступним етапом є розробка структурної схеми контролера керування доступом.

Відповідно до наведених міркувань формується загальна структурна схема контролера віддаленого керування доступом, основними блоками якої є мікроконтролер, Bluetooth-модуль, Ethernet-модуль, Wi-Fi-модуль, блок комутації та блок індикації [5, 6]. Така структура (рис. 2.1) забезпечує поєднання локальної бездротової ідентифікації користувача, віддаленого обміну даними з сервером та фізичного керування виконавчим механізмом доступу.

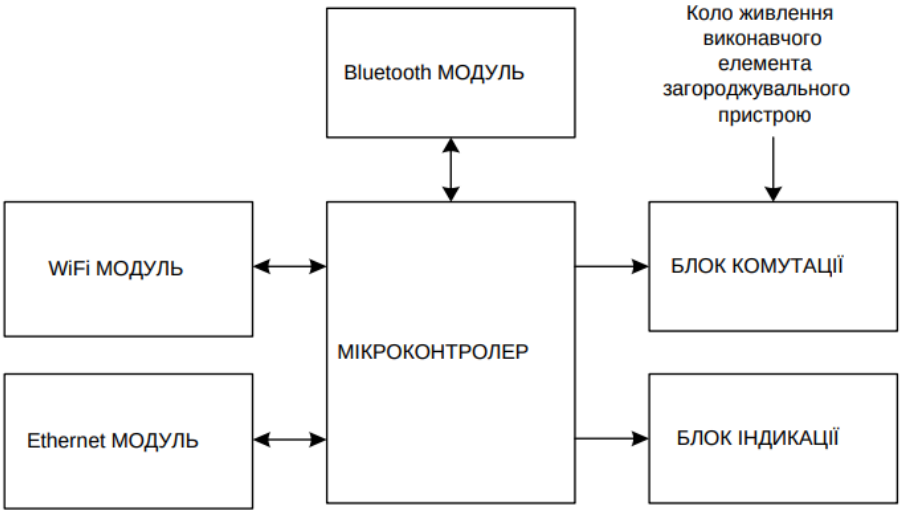


Рисунок 2.1 – Структурна схема контролера віддаленого керування доступом

Головним функціональним блоком пристрою є мікроконтролер, який координує роботу всіх інших вузлів системи [5, 6]. Саме він забезпечує функціонування контролера віддаленого керування доступом, а саме приймання ідентифікатора, що надсилається мобільним пристроєм через Bluetooth-з'єднання, перевірку його коректності та прийняття рішення щодо надання або заборони доступу [7, 15]. Для виконання цього завдання мікроконтролер також підтримує взаємодію з віддаленим сервером за мережевими протоколами стека TCP/IP у режимі клієнта з метою отримання ідентифікаторів, яким надано права доступу, а також службових параметрів конфігурації системи [8, 9]. За допомогою веб-додатка на сервері виконується реєстрація нового користувача або зміна його ідентифікатора, після чого відповідні дані передаються через мережу до контролера та зберігаються в його енергонезалежній пам'яті [8, 16].

Підключення контролера до мережі Інтернет може здійснюватися як за дротовим з'єднанням на основі витої пари, так і за бездротовим з'єднанням через Wi-Fi [10–12]. Дротове і бездротове підключення реалізуються відповідно модулями Ethernet та Wi-Fi, основним призначенням яких є забезпечення взаємодії із середовищем передачі даних [10, 12]. Зазначені модулі реалізують функції фізичного рівня та підрівня MAC канального рівня моделі OSI, тоді як функції мережевого, транспортного та прикладного рівнів реалізуються програмним забезпеченням мікроконтролера, зокрема за рахунок використання стека протоколів TCP/IP [9, 10].

Право доступу надається мікроконтролером за результатами порівняння ідентифікатора, що надсилається зі смартфона, з ідентифікаторами, які були попередньо отримані через мережу Інтернет та збережені в енергонезалежній пам'яті пристрою [7, 8]. Приймання ідентифікатора зі смартфона здійснюється через Bluetooth-канал, який використовується в режимі симетричного з'єднання типу «точка-точка» [7, 15]. Обмін даними між смартфоном і мікроконтролером забезпечується Bluetooth-модулем, основним елементом якого є радіочастотний блок, що виконує перетворення цифрових даних у радіосигнал у режимі

передавання та зворотне перетворення у режимі приймання [7]. Таким чином, Bluetooth-модуль забезпечує фізичний рівень зв’язку між смартфоном і контролером, тоді як створення логічного каналу та організація обміну даними через нього покладаються на програмне забезпечення мобільного пристрою та мікроконтролера [7, 15].

Фізичне надання доступу до об’єкта здійснюється за допомогою пристроїв загородження, до яких належать двері, ворота, шлагбауми або інші засоби обмеження проходу [17]. Підтримання їх закритого або відкритого стану реалізується виконавчим пристроєм, який за принципом дії може бути електромеханічним або електромагнітним [17, 18].

Електромеханічний принцип дії ґрунтується на переміщенні механічних елементів замикання, наприклад ригелів або засувок, під дією електродвигуна чи електромагніту. В електромагнітних виконавчих механізмах блокування здійснюється за рахунок магнітного притягання без необхідності складного механічного переміщення елементів замикання [17].

Оскільки керування як електромеханічними, так і електромагнітними виконавчими пристроями здійснюється шляхом подавання на них електричної напруги, до складу контролера введено блок комутації [6, 18]. За сигналом, сформованим мікроконтролером, блок комутації забезпечує подачу на виконавчий пристрій напруги, необхідної для його спрацювання. Основним елементом такого блоку є комутаційний прилад, який може перебувати у двох станах, а саме у стані електричного розмикання або замикання силового кола [18].

Як комутаційні елементи можуть використовуватися як напівпровідникові, так і електромеханічні пристрої [18, 19]. До напівпровідникових елементів належать транзистори, тиристори, симістори та твердотільні реле, які забезпечують високу швидкодію та відсутність механічного зношування [18]. Водночас електромагнітні реле залишаються поширеним рішенням у системах керування доступом завдяки простоті реалізації, електричній ізоляції між колом керування та силовим колом,

здатності комутувати значні потужності та відносно невисокій вартості [17, 19].

Електромагнітне реле є електромеханічним елементом, принцип роботи якого базується на створенні магнітного поля в котушці при протіканні електричного струму, що призводить до замикання або розмикання механічних контактів [19]. За принципом роботи реле поділяються на нейтральні, поляризовані та імпульсні. Нейтральні реле реагують лише на наявність струму в котушці, поляризовані враховують полярність сигналу керування, а імпульсні або бістабільні реле змінюють свій стан під дією короткого імпульсу та зберігають його після зняття сигналу керування [19].

Порівняно з електромагнітними реле напівпровідникові комутаційні елементи характеризуються меншим часом спрацювання та більшим ресурсом роботи, оскільки не містять рухомих контактів [18]. Однак електромагнітні реле мають низку важливих переваг, серед яких слід виділити можливість комутації відносно великих струмів і напруг, добру стійкість до імпульсних перенапруг, електричну розв’язку між силовими та керуючими колами, а також малу вартість при достатній функціональності [17, 19]. З урахуванням цих особливостей у розроблюваному контролері керування виконавчим пристроєм доцільно реалізувати за допомогою електромагнітного реле [17]. При цьому перспективним є використання імпульсного реле, оскільки воно споживає електричну енергію лише у момент перемикання та не змінює свій стан при короткочасному зникненні напруги живлення [19].

Для отримання інформації про фактичний стан пристрою загородження доцільно передбачити підключення відповідних датчиків положення або кінцевих вимикачів [6, 17]. Сигнали з виходів таких датчиків надходять на входи мікроконтролера, а визначення стану виконується програмно на основі логічного рівня сигналу. Це дозволяє не лише керувати виконавчим механізмом, але й контролювати реальний стан точки доступу, що підвищує надійність функціонування всієї системи [6].

Останнім блоком контролера є блок індикації, основним завданням якого є надання користувачеві візуальної інформації про поточний стан системи та

результат ідентифікації [6, 20]. Найпростішим і водночас достатньо інформативним рішенням є використання двох світлодіодів, зокрема червоного та зеленого кольору світіння. При зачиненому виконавчому механізмі активним є червоний світлодіод, а при відкритому — зелений [20]. Ці ж світлодіоди можуть бути використані для індикації результату ідентифікації користувача. Позитивний результат ідентифікації доцільно відображати вимиканням червоного світлодіода та вмиканням зеленого. Негативний результат, за якого виконавчий пристрій залишається у зачиненому стані, доцільно сигналізувати короткочасною зміною режиму світіння червоного світлодіода, що дозволяє користувачу зрозуміти факт обробки пред'явленого ідентифікатора [20].

Запропонована структура контролера віддаленого керування доступом поєднує мікроконтролерне ядро, модулі локальної та мережевої комунікації, блок комутації, підсистему контролю стану та блок індикації [5, 6]. Така побудова забезпечує можливість локальної авторизації користувача за допомогою смартфона, синхронізації даних із віддаленим сервером, керування виконавчими механізмами доступу та індикації поточного стану системи, що створює необхідну технічну основу для подальшої розробки принципової схеми та програмного забезпечення.

2.2 Обґрунтування вибору елементної бази системи

2.2.1 Мікроконтролер STM32F407VET6-Mini. Найбільш популярним сімейством ARM мікроконтролерів на ядрі Cortex-M є сімейство STM32 від компанії STMicroelectronics, що набуло широкого застосування у вбудованих системах завдяки високій продуктивності, гнучкості та розвиненій периферії [5, 22]. Однією з ключових причин популярності даного сімейства є орієнтація на максимальний комфорт розробника, що досягається за рахунок уніфікованої архітектури, широкого вибору програмних засобів та наявності великої кількості бібліотек і прикладів застосування [6, 21].

Важливою особливістю мікроконтролерів STM32 є так звана pin-to-pin сумісність у межах одного сімейства, що дозволяє змінювати варіанти мікроконтролерів із різними обсягами пам’яті або набором периферії без необхідності зміни друкованої плати [22]. Це суттєво спрощує модернізацію пристроїв та адаптацію системи до нових вимог.

Мікроконтролер STM32F407VET6 побудований на базі ядра ARM Cortex-M4 та забезпечує високу продуктивність обчислень при тактовій частоті до 168 МГц [5]. Він містить розвинену систему периферійних модулів, що дозволяє реалізувати складні алгоритми керування та обробки даних у реальному часі. Зовнішній вигляд наведено (рис. 2.2).

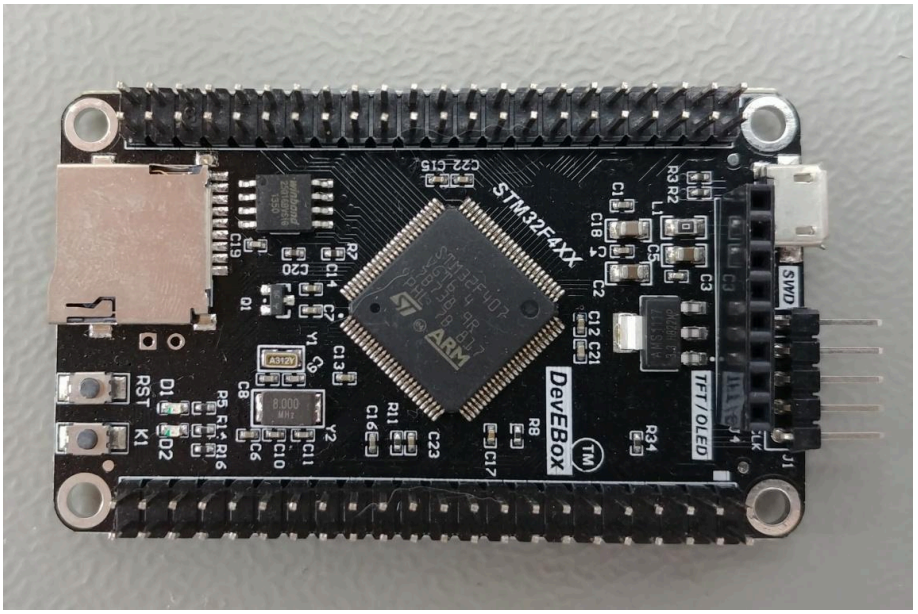


Рисунок 2.2 – Модуль STM32F407VET6-Mini

До складу периферії мікроконтролера входять багатоканальні 12-бітні аналого-цифрові перетворювачі, що дозволяють здійснювати вимірювання аналогових сигналів із високою точністю [22]. Наявність двоканального цифро-аналогового перетворювача з підтримкою 8- та 12-бітних режимів забезпечує можливість формування аналогових сигналів.

Контролер прямого доступу до пам’яті (DMA) підтримує до 12 каналів із різними рівнями пріоритету та дозволяє здійснювати обмін даними між

пам’яттю та периферією без участі центрального процесора, що підвищує ефективність системи [21]. Таймери загального призначення забезпечують гнучке керування часовими процесами, генерацію ШІМ-сигналів та реалізацію часових затримок.

Мікроконтролер також містить модуль годинника реального часу (RTC), що дозволяє вести облік часу та реалізовувати функції планування подій [5]. Для підвищення надійності роботи передбачено використання watchdog-таймерів, які забезпечують автоматичне перезавантаження системи у випадку виникнення збоїв.

Додатково реалізовано контролери зовнішньої пам’яті FSMC, інтерфейс SDIO для роботи з картами пам’яті, USB-контролер із підтримкою стандарту USB 2.0, а також Ethernet-контролер із підтримкою швидкостей до 100 Мбіт/с [5, 22]. Наявність інтерфейсів UART, SPI, I2C, CAN та I2S забезпечує широкі можливості інтеграції з іншими пристроями системи.

З урахуванням зазначених характеристик для реалізації контролера керування доступом обрано модуль STM32F407VET6-Mini, який є компактним та функціонально завершеним рішенням [6]. Використання готового модуля дозволяє зменшити складність розробки апаратної частини та скоротити час проєктування. Основні характеристики модуля STM32F407VET6-Mini наведені у таблиці 2.1.

Функціональне призначення виводів мікроконтролера визначається їх роллю у забезпеченні взаємодії з периферійними компонентами системи, при цьому лінії GPIO використовуються для керування релейними елементами та засобами індикації, інтерфейс UART забезпечує обмін даними з Bluetooth та Wi-Fi модулями, інтерфейс SPI застосовується для підключення Ethernet-модуля або дисплея, інтерфейс I2C призначений для взаємодії з датчиками, інтерфейс SDIO використовується для роботи з картами пам’яті SD, а інтерфейс FSMC забезпечує підключення зовнішньої пам’яті.

Таблиця 2.1 – Основні характеристики модуля STM32F407VET6-Mini

Параметр	Значення
Мікроконтролер	STM32F407VET6
Ядро	ARM Cortex-M4
Тактова частота	168 МГц
Flash пам’ять	512 КБ
SRAM	192 КБ
Додаткова Flash	16 Мбіт
Живлення	3.3 В
Інтерфейси	UART, SPI, I2C, CAN, USB
Ethernet	10/100 Мбіт/с

Мікроконтролер STM32F407VET6-Mini взаємодіє з іншими модулями системи наступним чином:

– через UART здійснюється обмін даними з Bluetooth та Wi-Fi модулями;

– через GPIO реалізується керування релейним модулем та світло-діодною індикацією;

– через SPI або інші інтерфейси здійснюється підключення додаткових модулів;

– через Ethernet або Wi-Fi забезпечується зв’язок із сервером.

Для підключення до фізичного середовища передачі даних мікроконтролер STM32F407 потребує використання зовнішнього фізичного рівня – трансивера PHY (Physical Layer Transceiver) [10]. Трансивер забезпечує перетворення цифрових сигналів MAC-рівня у сигнали, придатні для передавання по кабельному середовищу, виконує кодування та декодування даних, а також синхронізацію сигналів приймання і передавання [25].

Взаємодія між мікроконтролером і PHY-трансивером здійснюється через інтерфейси керування та передачі даних. Для доступу до регістрів керування трансивера використовується послідовний інтерфейс SMII (Serial Management Interface), який складається з двох сигналів [5]:

– MDIO (Management Data Input/Output) – двонаправлений канал даних для доступу до регістрів трансивера;

– MDC (Management Data Clock) – тактовий сигнал для синхронізації обміну даними по MDIO.

Основна передача даних між MAC-контролером і PHY-трансивером здійснюється через інтерфейс MII або RMII [10].

Інтерфейс MII забезпечує повнофункціональний обмін даними між MAC і PHY на швидкостях 10 Мбіт/с і 100 Мбіт/с у синхронному режимі [10]. Він використовує окремі паралельні шини для передачі та прийому даних, а також набір службових сигналів.

До основних сигналів інтерфейсу MII належать:

–MII_TXD[3:0] – паралельна шина передачі даних від MAC до PHY;

– MII_TX_CLK – тактовий сигнал передачі, що формується трансивером;

– MII_TX_EN – сигнал дозволу передачі даних;

– MII_CRS – сигнал виявлення несучої;

– MII_COL – сигнал виявлення колізій;

– MII_RXD[3:0] – паралельна шина прийому даних від PHY до MAC;

– MII_RX_CLK – тактовий сигнал прийому даних;

– MII_RX_DV – сигнал достовірності прийнятих даних;

– MII_RX_ER – сигнал помилки прийому.

Наявність окремих сигналів для передачі та прийому забезпечує високу надійність обміну даними, однак збільшує кількість необхідних виводів мікроконтролера [10].

Інтерфейс RMII є спрощеним варіантом MII та використовується для зменшення кількості сигнальних ліній [5]. У даному режимі ширина шини даних зменшується з 4 до 2 біт, а частота синхронізації відповідно збільшується. Це дозволяє зменшити кількість використовуваних виводів мікроконтролера без суттєвого зниження продуктивності системи [22]. Вибір режиму роботи інтерфейсу (MII або RMII) здійснюється програмно шляхом

встановлення відповідного біта MII_RMII_SEL у регістрі SYSCFG_PMC мікроконтролера [5].

Саме STM32F407VET6-Mini обумовлений поєднанням високої продуктивності, наявності необхідних інтерфейсів та широких можливостей розширення функціональності [5–7]. Крім того, наявність готових модулів значно спрощує реалізацію системи та знижує витрати на розробку.

2.2.2 Wi-Fi модуль ESP-07. Для підтримання підключення до бездротової мережі Wi-Fi у розроблюваній системі доцільно використовувати готові модулі, що мають вбудовану підтримку сімейства протоколів TCP/IP, оскільки це дозволяє суттєво спростити процес розроблення програмного забезпечення та зменшити навантаження на основний мікроконтролер [12, 24]. На сьогодні найбільш поширеними рішеннями є Wi-Fi модулі сімейства ESP, побудовані на мікросхемі ESP8266, які характеризуються низькою вартістю при достатньо широких функціональних можливостях та активно використовуються у вбудованих та IoT-системах [24, 36].

Модулі ESP8266 випускаються компанією Espressif Systems та представлені у декількох модифікаціях, що відрізняються обсягом флеш-пам’яті, конструктивним виконанням, типами роз’ємів та наявністю зовнішніх антен [36]. Конструктивно модуль об’єднує мікросхему ESP8266EX, зовнішню SPI Flash-пам’ять ємністю до 2 Мбайт та інтегровану або зовнішню антену для прийому та передачі радіосигналів [36]. Зовнішній вигляд модуля ESP-07 наведено (рис. 2.3).

Рисунок 2.3 – Wi-Fi модуль ESP-07 на базі ESP8266

Мікросхема ESP8266EX містить 32-бітний мікроконтролер Tensilica L106, який працює з тактовою частотою 80МГц із можливістю підвищення до 160МГц у режимі максимальної продуктивності [36]. Крім обчислювального ядра, мікросхема інтегрує радіочастотний тракт, що забезпечує підтримку стандартів Wi-Fi IEEE 802.11 b/g/n, а також апаратну реалізацію мережевих протоколів IPv4, TCP, UDP, HTTP та FTP [24, 36].

Модуль підтримує різні режими роботи, зокрема режим клієнта (Station), режим точки доступу (Access Point), а також комбінований режим, що дозволяє одночасно виконувати функції клієнта та точки доступу [24]. Для забезпечення безпеки передавання даних підтримуються сучасні алгоритми шифрування, такі як WPA/WPA2, WEP, TKIP та AES, що дозволяє використовувати модуль у захищених мережах [36, 37].

Важливою особливістю ESP8266 є те, що обробка мережевих протоколів виконується безпосередньо на модулі, при цьому, за даними виробника, підтримка Wi-Fi з’єднання займає лише близько 20% обчислювальних ресурсів, а решта може бути використана для виконання користувацьких задач [36]. Модуль функціонує під керуванням операційної системи реального часу (RTOS), що значно спрощує інтеграцію прикладного програмного забезпечення [36].

Серед різних модифікацій ESP-модулів у даній роботі доцільно обрати модель ESP-07, оскільки вона оснащена як вбудованою керамічною антеною, так і роз’ємом для підключення зовнішньої антени, що дозволяє підвищити дальність та якість бездротового зв’язку [36]. Це є важливим фактором для систем керування доступом, які можуть експлуатуватися в умовах значних електромагнітних завад або на відстані від точки доступу. Його основні технічні характеристики подано у таблиці 2.2.

Таблиця 2.2 – Основні технічні характеристики ESP-07

Параметр	**Значення**

Мікросхема	ESP8266EX
Ядро	Tensilica L106

Кінець таблиці 2.2

Тактова частота	80–160 МГц
Flash пам’ять	до 2 МБ
Стандарт Wi-Fi	IEEE 802.11 b/g/n
Частота	2.4 ГГц
Режими роботи	Station, AP, STA+AP
Шифрування	WPA/WPA2, WEP, AES
Інтерфейс	UART
Напруга живлення	3.3 В

Підключення модуля ESP-07 до мікроконтролера STM32 здійснюється через інтерфейс UART, при цьому лінія TX модуля підключається до входу RX мікроконтролера, а лінія RX модуля підключається до виходу TX мікроконтролера через подільник напруги або логічний перетворювач рівнів для забезпечення допустимого рівня сигналу 3.3 В [18, 24]. Живлення модуля здійснюється від стабілізованого джерела 3.3 В із достатнім струмовим запасом, оскільки під час передавання даних споживання струму може досягати 300 мА [24]. Для активації модуля сигнал CH_PD (EN) підтягується до логічної одиниці, а вивід GPIO0 використовується для вибору режиму завантаження або нормальної роботи [24].

Використання модуля ESP-07 на базі ESP8266 дозволяє реалізувати повноцінний бездротовий мережевий інтерфейс із підтримкою сучасних протоколів передачі даних, забезпечує простоту інтеграції з мікроконтролером STM32 та відповідає вимогам до надійності, швидкодії та функціональності системи віддаленого керування доступом [12, 24, 36].

2.2.3 Bluetooth модуль HC-05. Bluetooth модуль HC-05 використовується у складі системи віддаленого керування доступом для реалізації локальної бездротової ідентифікації користувача за допомогою смартфона, при цьому

модуль працює у діапазоні частот 2.4ГГц та підтримує стандарт Bluetooth 2.0, що забезпечує стабільний обмін даними на відстанях до 10 метрів у режимі «точка-точка» [7, 23].

Зовнішній вигляд модуля наведено на рисунку 2.4, а його основні технічні характеристики подано у таблиці 2.3.

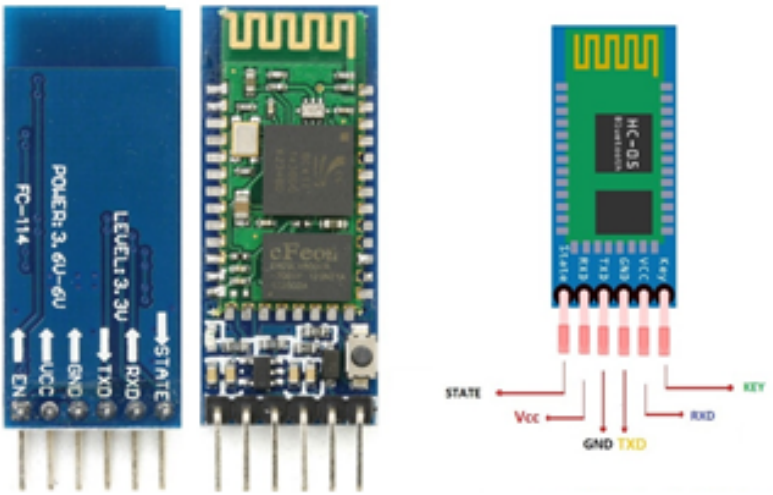


Рисунок 2.4 – Bluetooth модуль HC-05

Основним призначенням модуля є приймання ідентифікаційних даних від мобільного пристрою та передача їх до мікроконтролера для подальшої обробки, що дозволяє реалізувати механізм авторизації користувача без використання фізичних носіїв [7].

Таблиця 2.3 – Основні технічні характеристики HC-05

Параметр	Значення
Стандарт	Bluetooth 2.0 + EDR
Частота	2.4 ГГц
Дальність	до 10 м
Інтерфейс	UART
Напруга живлення	3.3–5 В
Швидкість UART	9600–115200 бод

Обмін даними між модулем HC-05 та мікроконтролером STM32 здійснюється через послідовний інтерфейс UART, що забезпечує простоту інтеграції та сумісність із більшістю вбудованих систем [6]. Модуль підтримує два основні режими роботи, а саме режим AT-команд для налаштування параметрів та робочий режим передачі даних, у якому здійснюється безпосередній обмін інформацією між пристроями [23]. У режимі налаштування можна задати ім’я пристрою, швидкість передачі даних, PIN-код для підключення та інші параметри, що забезпечують гнучкість конфігурації системи [23]. Важливою особливістю є те, що модуль працює з рівнями логіки 3.3В, хоча допускає живлення від 5В завдяки вбудованому стабілізатору, однак для лінії RX рекомендується використовувати узгодження рівнів сигналів при підключенні до мікроконтролера [18]. Передача даних здійснюється у вигляді послідовного потоку байтів, що дозволяє реалізувати прості протоколи обміну між смартфоном та контролером, наприклад передачу унікального ідентифікатора користувача у текстовому або бінарному форматі [7].

Функціональне призначення виводів модуля визначається їх роллю у забезпеченні живлення, обміну даними та керування режимами роботи, при цьому вивід VCC використовується для підключення живлення, GND – як загальний провід, TXD забезпечує передачу даних, RXD – прийом даних, вивід EN/KEY використовується для переведення модуля у режим AT-команд, а STATE призначений для індикації стану підключення.

Підключення Bluetooth модуля HC-05 до мікроконтролера STM32 здійснюється через інтерфейс UART, при цьому вихід TX модуля підключається до входу RX мікроконтролера, а вхід RX модуля підключається до виходу TX мікроконтролера через подільник напруги для забезпечення допустимого рівня сигналу, живлення модуля здійснюється від джерела 5В або 3.3В залежно від реалізації, а загальний провід об’єднується із загальним проводом системи, що забезпечує коректний обмін даними [18, 23] (рис 2.5).

У процесі роботи смартфон встановлює з’єднання з модулем, після чого передає ідентифікаційні дані, які приймаються мікроконтролером та

використовуються для прийняття рішення щодо надання доступу, що забезпечує реалізацію локального каналу автентифікації у системі віддаленого керування доступом [7].

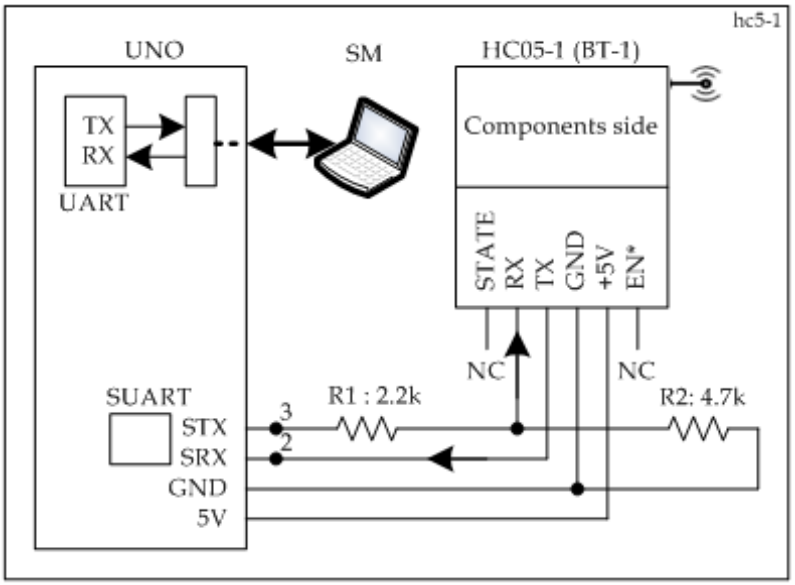


Рисунок 2.5 – Схема підключення HC-05 до мікроконтролера STM32

2.2.4 Ethernet-трансивер DP83848 Ethernet Boar. У якості трансивера фізичного рівня для реалізації дротового підключення до мережі Ethernet у розроблюваній системі обрано модуль DP83848 Ethernet Board, який конструктивно об’єднує Ethernet-трансивер фізичного рівня DP83848, роз’єм RJ-45 із вбудованими узгоджувальними елементами (магнітними трансформаторами), а також роз’єм керуючого інтерфейсу для підключення до мікроконтролерів із вбудованим Ethernet-модулем [10, 25].

Використання готового модуля дозволяє значно спростити апаратну реалізацію системи, оскільки усі необхідні компоненти для узгодження сигналів та підключення до мережі вже інтегровані в одному пристрої.

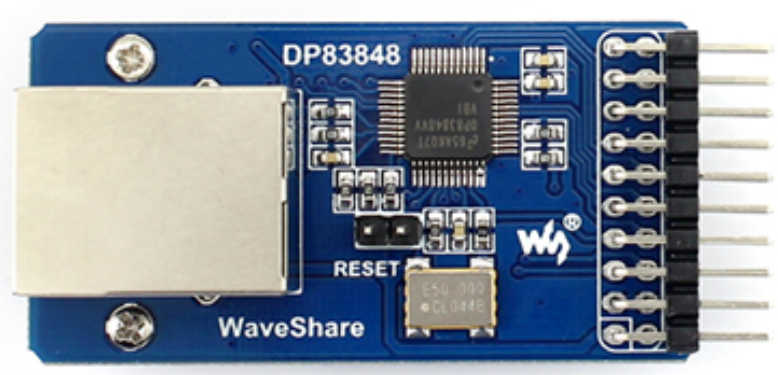


Рисунок 2.6 – Модуль DP83848 Ethernet Board

На рисунку 2.6 наведено зовнішній вигляд модуля, а його основні технічні характеристики подано у таблиці 2.4.

Таблиця 2.4 – Основні технічні характеристики DP83848 Ethernet Board

Параметр	Значення
Мікросхема	DP83848
Стандарт	IEEE 802.3
Швидкість	10/100 Мбіт/с
Інтерфейс	MII / RMII
Керування	MDIO / MDC
Живлення	3.3 В
Автоналаштування	Підтримується
Дуплекс	Half / Full duplex

Роз’єм	RJ-45 з трансформатором

Мікросхема DP83848 є високопродуктивним PHY-трансивером, який забезпечує фізичний рівень передачі даних відповідно до стандарту IEEE 802.3 та підтримує швидкості 10 Мбіт/с і 100 Мбіт/с [25]. Трансивер виконує функції кодування та декодування сигналів, узгодження рівнів напруги, формування та прийому диференційних сигналів, а також автоматичного визначення параметрів з’єднання, таких як швидкість передачі та режим дуплексу [10].

Взаємодія трансивера з мікроконтролером STM32F407VET6 здійснюється через інтерфейс MII або RMII, що дозволяє передавати дані між MAC-рівнем мікроконтролера та фізичним середовищем передачі [5, 22].

Для керування трансивером та доступу до його внутрішніх регістрів використовується інтерфейс MDIO/MDC, який забезпечує конфігурацію параметрів роботи та моніторинг стану з’єднання [10].

Модуль DP83848 Ethernet Board також містить роз’єм RJ-45, що забезпечує підключення до кабельної мережі на основі витої пари, а також вбудовані трансформатори, які виконують функції гальванічної розв’язки та захисту від електромагнітних завад [25]. Це дозволяє забезпечити надійність передачі даних та відповідність вимогам стандартів електробезпеки.

Підключення модуля DP83848 до мікроконтролера STM32 здійснюється через інтерфейс RMII або MII, при цьому основними сигнальними лініями є TXD0, TXD1, RXD0, RXD1, TX_EN, CRS_DV, REF_CLK, а також сигнали керування MDIO та MDC [5, 10].

Живлення модуля здійснюється від джерела 3.3 В, а роз’єм RJ-45 забезпечує фізичне підключення до мережі Ethernet через виту пару. Узгодження сигналів і гальванічна розв’язка забезпечуються вбудованими трансформаторами модуля, що дозволяє уникнути використання додаткових компонентів у схемі (рис 2.7) [25].

Вибір модуля DP83848 Ethernet Board обумовлений його повною сумісністю з мікроконтролерами STM32, підтримкою стандартних інтерфейсів

MII/RMII, високою надійністю та наявністю інтегрованих елементів для підключення до мережі [5, 25].

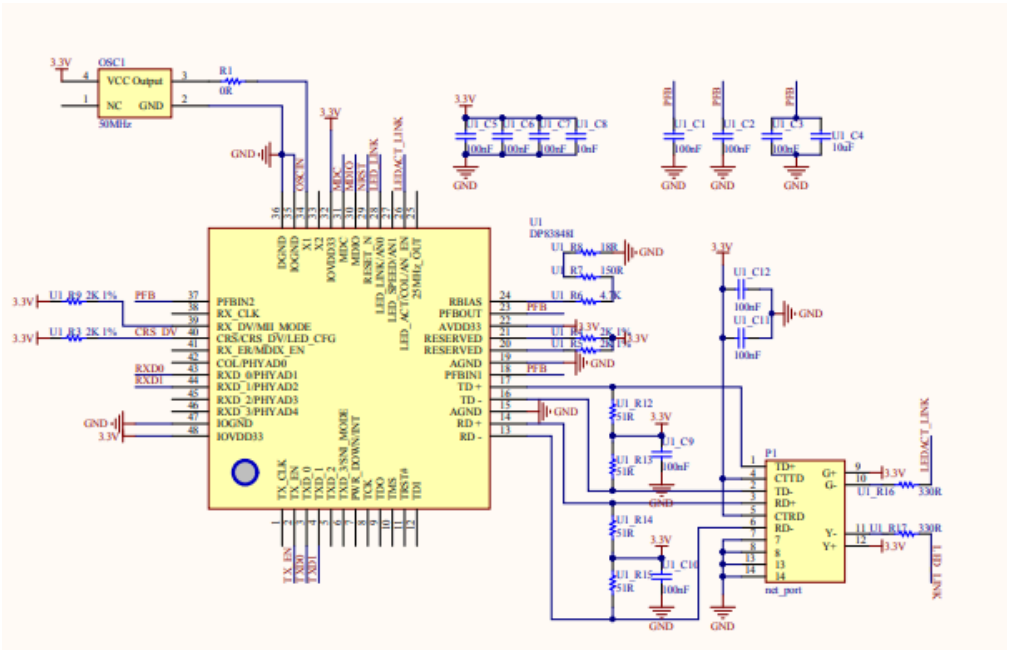


Рисунок 2.7 – Схема підключення DP83848

Використання готового модуля дозволяє зменшити складність розробки друкованої плати, підвищити якість сигналів та забезпечити стабільну роботу системи у реальних умовах експлуатації.

Застосування трансивера DP83848 забезпечує ефективну реалізацію фізичного рівня Ethernet у системі віддаленого керування доступом та є оптимальним рішенням з точки зору функціональності, надійності та вартості [10, 25].

2.2.5 Релейний блок керування виконавчим пристроєм. Релейний блок у складі системи віддаленого керування доступом призначений для комутації електричного кола виконавчого пристрою, зокрема електромеханічного замка, електромагнітної засувки або іншого засобу блокування проходу [17–20].

Необхідність використання окремого релейного блоку обумовлена тим, що мікроконтролер STM32F407VET6-Mini не може безпосередньо керувати

силовим навантаженням через обмеження за струмом та напругою на виводах портів введення-виведення [5, 20]. Тому для узгодження параметрів керуючого сигналу з параметрами виконавчого механізму використовується проміжний комутаційний каскад, побудований на основі транзисторного ключа та електромагнітного реле (рис. 2.8) [18, 19].

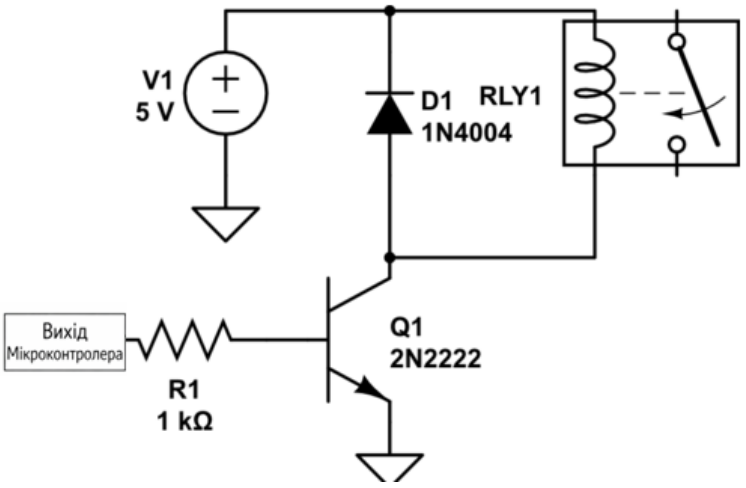


Рисунок 2.8 – Релейний блок керування виконавчим пристроєм

Принцип роботи релейного блоку полягає в тому, що мікроконтролер формує керуючий логічний сигнал, який через резистор надходить на базу транзистора [18]. У разі подавання логічної одиниці транзистор переходить у стан насичення та забезпечує протікання струму через котушку реле, внаслідок чого відбувається перемикання його контактів [19]. Це дозволяє замкнути або розімкнути силове коло виконавчого пристрою та, відповідно, забезпечити надання або блокування фізичного доступу до об’єкта [17].

У якості ключового елемента релейного блоку доцільно використовувати біполярний NPN-транзистор, наприклад типу BC547, 2N2222 або аналогічний, який забезпечує достатній коефіцієнт підсилення струму та просту реалізацію схеми керування [18, 20]. База транзистора підключається до виходу мікроконтролера через обмежувальний резистор, що запобігає перевищенню допустимого струму бази та забезпечує стабільний режим перемикання [18].

Емітер транзистора з’єднується із загальним проводом схеми, а колектор – з одним із виводів котушки реле.

Другий вивід котушки реле підключається до джерела живлення, як правило +5В або +12В, залежно від типу реле та параметрів виконавчого пристрою [19]. При подачі керуючого сигналу транзистор відкривається, через котушку починає протікати струм, і реле спрацьовує, перемикаючи свої контакти. У відсутності керуючого сигналу транзистор закритий, струм через котушку не протікає, а контакти реле перебувають у початковому стані [18].

Оскільки котушка реле є індуктивним навантаженням, при її вимиканні виникає імпульс самоіндукції, який може призвести до пошкодження транзистора або створення електромагнітних завад у схемі [18]. Для усунення цього негативного явища паралельно котушці реле в зворотному напрямку підключається захисний діод, який часто називають демпфуючим або flyback-діодом [18, 20]. У нормальному режимі діод не проводить струм, однак у момент вимикання реле він шунтує імпульс самоіндукції та забезпечує безпечне розсіювання накопиченої енергії. У якості такого діода доцільно використовувати 1N4148, 1N4007 або аналогічний напівпровідниковий елемент залежно від параметрів котушки [18].

Контактна частина реле зазвичай містить три основні виводи, а саме загальний контакт COM, нормально розімкнений контакт NO та нормально замкнений контакт NC [19]. Якщо необхідно, щоб виконавчий пристрій активувався лише у момент спрацювання реле, використовується пара контактів COM–NO. Якщо ж потрібно, щоб у нормальному стані коло було замкнутим, а при спрацюванні розмикалося, використовується пара COM–NC. Для системи керування доступом найчастіше застосовується варіант COM–NO, оскільки він дозволяє подавати живлення на замок лише в момент підтвердження доступу [17, 19].

Для підвищення надійності та безпеки роботи системи у релейному блоці також можуть бути передбачені світлодіодна індикація стану, запобіжні елементи та клемні роз’єми для підключення зовнішнього навантаження [20].

Світлодіодна індикація дозволяє візуально контролювати факт спрацювання реле, що є зручним під час налагодження та експлуатації. Клемні роз'єми спрощують монтаж виконавчих пристроїв і підвищують ремонтопридатність системи.

Застосування саме електромагнітного реле у даній системі є доцільним з огляду на простоту реалізації, наявність гальванічної розв'язки між низьковольтною частиною керування та силовим колом, можливість комутації відносно великих струмів і напруг, а також невисоку вартість таких компонентів [17, 19]. Хоча твердотільні ключі мають вищу швидкодію та більший ресурс роботи, у системах керування доступом швидкість перемикання реле є цілком достатньою, а його конструктивна простота та універсальність роблять це рішення практично обґрунтованим [18, 19].

Таким чином, релейний блок на основі електромагнітного реле, транзисторного ключа, базового резистора та захисного діода забезпечує надійне узгодження мікроконтролера з виконавчим пристроєм, захист схеми від перенапруги та можливість безпечного керування електричним навантаженням у складі системи віддаленого керування доступом [17–20].

2.2.6 Блок індикації системи керування доступом. Блок індикації у складі системи віддаленого керування доступом призначений для відображення поточного стану виконавчого пристрою та результатів ідентифікації користувача, що забезпечує зручність експлуатації та підвищує інформативність системи для користувача [20]. Реалізація блоку індикації здійснюється за допомогою світлодіодів, які є простими, надійними та енергоефективними елементами відображення інформації, що широко застосовуються у вбудованих системах [20].

У розроблюваній системі доцільно використовувати два світлодіоди різного кольору світіння, зокрема червоний та зелений, що дозволяє однозначно інтерпретувати стан системи [20]. Червоний світлодіод використовується для індикації зачиненого стану виконавчого пристрою, тобто відсутності доступу,

тоді як зелений світлодіод сигналізує про відкритий стан та надання доступу користувачу. Такий підхід відповідає загальноприйнятим принципам візуальної індикації та є інтуїтивно зрозумілим для користувача.

Світлодіоди підключаються до виходів мікроконтролера STM32 через обмежувальні резистори, що забезпечують обмеження струму до допустимого рівня та запобігають пошкодженню елементів [18, 20]. Керування світлодіодами здійснюється шляхом подавання логічних сигналів на відповідні GPIO-виводи мікроконтролера, що дозволяє програмно змінювати їх стан залежно від режиму роботи системи.

Принцип роботи блоку індикації полягає в тому, що при подачі логічної одиниці на відповідний вивід мікроконтролера через резистор протікає струм, який викликає світіння світлодіода, тоді як при подачі логічного нуля струм не протікає і світлодіод залишається вимкненим [20]. Таким чином, керування індикацією здійснюється програмно та може бути легко інтегроване у загальний алгоритм роботи системи.

У нормальному режимі роботи, коли доступ до об’єкта заблокований, активним є червоний світлодіод, що сигналізує про закритий стан системи. При успішній ідентифікації користувача та наданні доступу червоний світлодіод вимикається, а зелений вмикається, що відображає зміну стану виконавчого механізму. У випадку невдалої ідентифікації можливе короткочасне вимикання або блимання червоного світлодіода, що дозволяє користувачу зрозуміти факт обробки запиту системою.

Підключення світлодіодів до мікроконтролера STM32 здійснюється через послідовно увімкнені резистори, при цьому аноди світлодіодів підключаються до виходів GPIO через резистори, а катоди – до загального проводу, що забезпечує протікання струму при подачі логічної одиниці на відповідний вивід мікроконтролера [18, 20]. Альтернативно може використовуватися схема з підключенням катодів до GPIO та анодів до джерела живлення, у такому випадку керування здійснюється інверсною логікою.

Використання світлодіодної індикації у системі керування доступом є доцільним завдяки простоті реалізації, низькому енергоспоживанню, високій надійності та достатній інформативності [20]. Такий підхід не потребує складних схемотехнічних рішень та дозволяє ефективно відображати стан системи у реальному часі.

2.3 Розробка електричної функціональної схеми контролера керування доступом

Розробка електричної функціональної схеми контролера керування доступом здійснюється на основі вибраної елементної бази та прийнятих схемотехнічних рішень, що дозволяє забезпечити реалізацію всіх необхідних функцій системи, зокрема мережевої взаємодії, локальної ідентифікації користувача та керування виконавчими пристроями [5, 6]. З використанням зазначених компонентів сформовано функціональну схему контролера, що наведена в ДОДАТКУ А, яка відображає взаємозв’язки між основними структурними блоками системи.

Контролер побудований на основі мікроконтролерного модуля STM32F407VET6-Mini (DD2), який є завершеним функціональним блоком та містить у своєму складі 32-бітний високопродуктивний мікроконтролер STM32F407VET6, а також усі необхідні допоміжні елементи для забезпечення його стабільної роботи, зокрема тактові генератори, стабілізатори напруги та інтерфейсні лінії [5, 22]. Використання готового модуля дозволяє значно спростити розробку апаратної частини системи та підвищити її надійність.

Мікроконтролерний модуль DD2 забезпечує виконання основних функцій системи, серед яких обмін повідомленнями з хмарним сервером через мережу Інтернет із використанням Ethernet або Wi-Fi підключення, взаємодія зі смартфоном користувача через Bluetooth-з’єднання з метою визначення прав доступу, а також керування виконавчими елементами засобів загородження для фізичного надання доступу [6, 8].

Підключення до мережі Ethernet реалізується за допомогою вбудованого у мікроконтролер STM32F407VET6 Ethernet-контролера та зовнішнього модуля трансивера фізичного рівня DD1, побудованого на базі мікросхеми DP83848 [10, 25]. Ethernet-контролер мікроконтролера забезпечує підтримку функцій підрівня MAC канального рівня моделі OSI відповідно до стандарту IEEE 802.3, тоді як трансивер DD1 виконує функції фізичного рівня, зокрема кодування, декодування, передачу та прийом даних по витій парі [10].

Підключення трансивера DD1 до модуля DD2 здійснюється через інтерфейс RMII, сигнали якого виведені на відповідні роз'єми мікроконтролерного модуля. Фізичне підключення до мережі Ethernet забезпечується через стандартний 8-контактний роз'єм RJ-45, розташований на платі трансивера. Обмін даними з хмарним сервером через Ethernet здійснюється із використанням стеку протоколів TCP/IP, реалізованого програмними засобами мікроконтролера [9].

Підключення до бездротової мережі Wi-Fi здійснюється за допомогою модуля DA1, який забезпечує передачу даних по радіоканалу відповідно до стандартів IEEE 802.11 [12, 24]. Модуль DA1 має вбудовану підтримку стеку протоколів TCP/IP, що дозволяє реалізувати функції не лише фізичного та канального рівнів, але й мережевого, транспортного та прикладного рівнів. Завдяки цьому взаємодія мікроконтролера з модулем здійснюється за допомогою AT-команд, які передаються через послідовний асинхронний інтерфейс UART1 по лініях RxD та TxD [24]. Активація модуля здійснюється подачею логічного рівня на вхід CH_PD, який підключений до відповідного виводу мікроконтролера, тоді як сигнал скидання RST використовується для перезапуску модуля у разі необхідності.

Реалізація локальної ідентифікації користувача здійснюється за допомогою Bluetooth-модуля DA2, який забезпечує встановлення бездротового з'єднання зі смартфоном та передачу ідентифікаційних даних [7, 23]. Підключення модуля DA2 до мікроконтролера STM32F407VET6 здійснюється через послідовний асинхронний інтерфейс UART2, що дозволяє організувати

обмін даними через лінії Tx та Rx. У процесі роботи смартфон передає ідентифікатор користувача, який приймається мікроконтролером та використовується для визначення прав доступу.

Керування виконавчими пристроями засобів загородження реалізується за допомогою електромагнітних реле К1 та К2, які забезпечують комутацію силових кіл [17, 19]. У розроблюваній системі передбачено два незалежні канали керування виконавчими елементами, що дозволяє здійснювати керування декількома пристроями доступу. Особливістю використаних реле є їх імпульсний характер, при якому для перемикання стану контактів використовуються короткочасні сигнали керування, після чого реле зберігає свій стан без подальшого споживання енергії.

Керування реле здійснюється через вихідні лінії мікроконтролера PD0–PD3, які підключені до транзисторних ключових каскадів, побудованих на транзисторах VT1–VT4 [18]. Сигнали на лініях PD0 та PD1 використовуються для керування реле К1, тоді як сигнали на лініях PD2 та PD3 – для керування реле К2. При подачі логічної одиниці на відповідний вихід мікроконтролера транзистор переходить у відкритий стан, що забезпечує протікання струму через обмотку реле, підключену до його колекторного кола. У статичному режимі, коли керуючий сигнал відсутній, транзистор закритий, а реле зберігає свій попередній стан.

Розроблена електрична функціональна схема контролера керування доступом забезпечує інтеграцію всіх необхідних підсистем, включаючи мережеві інтерфейси, засоби ідентифікації користувача та виконавчі механізми, що дозволяє реалізувати повноцінну систему віддаленого керування доступом із використанням сучасних мікроконтролерних та комунікаційних технологій [5–25].

2.4 Програмна реалізація системи керування доступом

Програмна реалізація системи віддаленого керування доступом базується на використанні мікроконтролера STM32F407VET6 та передбачає виконання

комплексу функцій, пов’язаних із ініціалізацією апаратних ресурсів, обробкою ідентифікаційних даних, взаємодією з мережевими модулями, прийняттям рішень щодо надання доступу та керування виконавчими пристроями [31–33]. Логіка функціонування програмного забезпечення узгоджується з розробленою блок-схемою алгоритму роботи контролера доступу, яка наведена ДОДАТКУ Б, та реалізує подієво-циклічний принцип обробки інформації.

На початковому етапі роботи системи виконується процедура ініціалізації, яка включає налаштування тактової частоти мікроконтролера, конфігурацію портів введення-виведення, ініціалізацію інтерфейсів UART для взаємодії з Wi-Fi та Bluetooth модулями, запуск Ethernet-контролера, а також ініціалізацію внутрішніх структур даних, зокрема буферів обміну та таблиці дозволених ідентифікаторів [31]. Після завершення ініціалізації виконується початкова синхронізація даних із віддаленим сервером, що дозволяє сформувати актуальну локальну базу ідентифікаторів користувачів.

Подальша робота системи організована у вигляді нескінченного циклу, у межах якого реалізується два взаємопов’язані процеси, а саме обробка запитів користувачів та періодична синхронізація даних із сервером. У процесі виконання основного циклу система переходить у режим очікування, у якому здійснюється моніторинг стану каналів зв’язку та перевірка наявності запитів від користувачів через Bluetooth-з’єднання [32].

У разі надходження запиту система виконує зчитування ідентифікатора користувача та перевірку його коректності. Після цього здійснюється пошук відповідного запису у локальній базі даних. Якщо ідентифікатор знайдено, формується команда на надання доступу, яка реалізується шляхом керування виконавчим пристроєм через релейний блок, а також виконується передавання інформації про подію на сервер. У разі відсутності ідентифікатора у локальній базі система ініціює процедуру повторної синхронізації даних із сервером, після чого перевірка виконується повторно. Якщо після оновлення даних ідентифікатор залишається відсутнім, формується відмова у доступі та відповідний запис у журналі подій.

Керування виконавчими пристроями реалізується шляхом формування керуючих сигналів на виходах мікроконтролера, які подаються на транзисторні ключі релейного блоку. У випадку дозволу доступу формується імпульс на вмикання реле, що призводить до відкривання загороджувального механізму. Після завершення заданого інтервалу часу формується імпульс на повернення реле у вихідний стан, що забезпечує закривання доступу. Одночасно з цим здійснюється керування світлодіодною індикацією, яка відображає поточний стан системи та результат ідентифікації користувача.

Важливою складовою програмної реалізації є механізм періодичної синхронізації даних, який також відображено на блок-схемі. Для цього використовується таймер, що визначає інтервал між оновленнями локальної бази ідентифікаторів. Після завершення заданого інтервалу система автоматично ініціює процедуру синхронізації з сервером, що дозволяє підтримувати актуальність даних навіть за відсутності запитів від користувачів [32].

Програмне забезпечення контролера керування доступом реалізоване мовою програмування C із використанням середовища STM32CubeIDE та бібліотек HAL для мікроконтролерів сімейства STM32. Такий підхід забезпечує спрощення процесу розробки, уніфікацію доступу до периферійних модулів мікроконтролера та підвищення надійності програмного забезпечення [31, 32].

Програмний код побудований за модульним принципом, відповідно до якого окремі функціональні вузли системи реалізуються у вигляді незалежних програмних модулів (див. додаток Е). Основними модулями програмного забезпечення є:

– модуль ініціалізації апаратних ресурсів;

– модуль Bluetooth-зв’язку;

– модуль Wi-Fi або Ethernet-з’єднання;

– модуль обробки UUID користувачів;

– модуль керування релейним блоком;

– модуль індикації;

– модуль синхронізації із сервером.

Після запуску програми виконується ініціалізація системного тактування, портів введення-виведення, UART-інтерфейсів, таймерів та мережевих модулів. Далі контролер переходить у режим очікування запитів від мобільних пристроїв.

Приймання даних від Bluetooth-модуля HC-05 здійснюється через інтерфейс UART із використанням переривань. Після отримання UUID мобільного пристрою виконується його порівняння зі списком дозволених ідентифікаторів, які зберігаються у пам’яті контролера.

Фрагмент програмного коду перевірки UUID наведено нижче:

```
if(strcmp(received_uuid, saved_uuid[i]) == 0)
{
    access_granted = 1;
}
```

У разі успішної перевірки формується сигнал керування виконавчим пристроєм. Для цього активується відповідний GPIO-вивід мікроконтролера, який через транзисторний ключ керує реле.

```
HAL_GPIO_WritePin(RELAY_GPIO_Port, RELAY_Pin, GPIO_PIN_SET);
HAL_Delay(3000);
HAL_GPIO_WritePin(RELAY_GPIO_Port, RELAY_Pin, GPIO_PIN_RESET);
```

Для індикації стану системи використовуються світлодіоди, підключені до портів введення-виведення мікроконтролера. Зелений світлодіод сигналізує про успішне надання доступу, а червоний – про відмову або режим блокування.

Синхронізація даних із сервером виконується через Wi-Fi або Ethernet-з’єднання. Передача даних здійснюється з використанням TCP/IP-протоколу та HTTP-запитів. Під час синхронізації оновлюється список дозволених UUID та передається журнал подій.

Основний цикл програми працює у безперервному режимі та забезпечує:
– очікування запитів від користувачів;

– перевірку прав доступу;

– керування виконавчими пристроями;

– обробку мережевих запитів;

– періодичну синхронізацію із сервером.

Розроблене програмне забезпечення забезпечує стабільну роботу контролера керування доступом, реалізацію алгоритмів ідентифікації користувачів, взаємодію з серверною частиною системи та керування виконавчими пристроями у режимі реального часу [31–33].

Висновок до розділу

У другому розділі дипломної роботи виконано розробку апаратно-програмних засобів системи віддаленого керування доступом на базі мікроконтролера STM32F407VET6-Mini, що дозволило сформувати цілісну архітектуру контролера та обґрунтувати вибір основних компонентів системи. Проведений аналіз елементної бази показав доцільність використання сучасних мікроконтролерів із розвиненою периферією та підтримкою мережевих інтерфейсів, що забезпечує необхідний рівень продуктивності та функціональності системи.

У ході роботи обґрунтовано використання комбінованого підходу до організації зв’язку, який передбачає застосування дротового Ethernet-інтерфейсу для забезпечення стабільного підключення до мережі та бездротового Wi-Fi інтерфейсу для підвищення гнучкості системи. Для реалізації локальної ідентифікації користувача використано Bluetooth-модуль, що забезпечує взаємодію зі смартфоном та дозволяє використовувати мобільний пристрій як ідентифікатор доступу.

Розроблено та детально описано основні функціональні вузли системи, зокрема релейний блок керування виконавчими пристроями, який забезпечує надійну комутацію силових кіл, а також блок індикації, що відображає стан системи та результати ідентифікації користувача. На основі вибраних

компонентів сформовано електричну функціональну схему контролера, яка забезпечує узгоджену взаємодію між усіма елементами системи.

Окрему увагу приділено розробці алгоритму роботи системи та програмної реалізації, що базується на подієво-циклічному принципі. Запропонований алгоритм забезпечує обробку запитів користувачів у реальному часі, перевірку прав доступу на основі локальної бази даних, можливість її оновлення через віддалений сервер, а також підтримання працездатності системи в автономному режимі у разі відсутності мережевого з’єднання.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ

3.1 Розробка алгоритму роботи системи віддаленого керування доступом

Перед розглядом алгоритму функціонування мобільного додатку доцільно визначити логіку роботи адміністративної частини системи та її функціональне призначення. Основною функцією додатку адміністратора є формування та ведення переліку користувачів, яким надається доступ до об’єктів, шляхом запису у пам’ять контролера відповідних ідентифікаторів пристроїв. Початковим етапом роботи є активація контролера, яка полягає у встановленні зв’язку між контролером та панеллю адміністратора за унікальним ідентифікатором пристрою. Після виконання цієї операції адміністратор отримує можливість керування списком користувачів, зокрема додавання, редагування та видалення записів, що формують так званий «білий список» доступу [21–23].

Доступ до адміністративної панелі обмежується процедурою аутентифікації, що реалізується шляхом перевірки облікових даних користувача. У процесі додавання нового користувача формується відповідний запис у базі даних, розміщеній на сервері. Для цього через інтерфейс додатку вводяться необхідні параметри, після чого ініціюється запит на сервер для створення нового запису. У разі успішного виконання операції генерується унікальний код доступу, який передається користувачеві та використовується ним під час реєстрації [24, 25].

Реєстрація користувача передбачає збереження у базі даних унікального ідентифікатора Bluetooth-модуля мобільного пристрою. Це забезпечує можливість подальшої ідентифікації користувача при взаємодії з контролером доступу. Алгоритм роботи адміністративного додатку включає послідовність

дій, пов’язаних із керуванням обліковими записами та синхронізацією даних, що представлено у відповідній блок-схемі ДОДАТОКУ В.

Алгоритм функціонування мобільного додатку користувача орієнтований на реалізацію процесу отримання доступу до об’єктів. Після встановлення додатку користувач проходить процедуру реєстрації або автентифікації, після чого отримує доступ до переліку об’єктів, з якими пов’язаний його обліковий запис. Кожен об’єкт у системі відповідає конкретному контролеру доступу, ідентифікованому за унікальним ID, у пам’яті якого збережено відповідний UUID мобільного пристрою [26].

Розширення переліку доступних об’єктів здійснюється шляхом введення спеціального коду доступу, отриманого від адміністратора. У разі відповідності коду система додає новий об’єкт до списку доступних, що забезпечує гнучкість у керуванні правами доступу [27].

Процес безпосереднього отримання доступу реалізується через взаємодію мобільного додатку з контролером. Після вибору об’єкта активується інтерфейс керування, у якому автоматично ініціюється робота Bluetooth-модуля. У випадку виявлення контролера у зоні дії система сигналізує про готовність до взаємодії. При формуванні запиту на доступ додаток передає ідентифікаційні дані до контролера, використовуючи Bluetooth-з’єднання [28].

Контролер виконує обробку отриманого запиту шляхом вилучення унікального ідентифікатора пристрою та його порівняння з наявними записами у базі даних. У разі збігу ідентифікатора з дозволеним записом формується сигнал на відкриття доступу. У протилежному випадку доступ не надається. Особливістю реалізації є використання Bluetooth-з’єднання виключно як каналу передачі ідентифікаційної інформації без встановлення повноцінного сеансу зв’язку, що підвищує швидкодію та знижує енергоспоживання системи [29]. Алгоритм роботи клієнтського додатку представлено у ДОДАТКУ Д.

Забезпечення узгодженої роботи всіх компонентів системи покладається на веб-сервер, який виконує функції центрального координуючого елемента.

Веб-сервер відповідає за обробку запитів, збереження даних користувачів, керування правами доступу та взаємодію з контролерами. Через сервер здійснюється передавання ідентифікаторів користувачів до пам’яті контролерів, а також їх оновлення у разі зміни прав доступу [30].

Архітектурно серверна частина та адміністративний додаток реалізуються як окремі програмні сервіси, що функціонують у хмарному середовищі. Такий підхід забезпечує централізоване керування системою, підвищує її доступність та дозволяє масштабувати функціональні можливості відповідно до потреб користувачів. Алгоритм роботи серверної частини системи наведено у ДОДАТКУ Г і відображає послідовність обробки запитів та взаємодії з іншими компонентами системи [21–30].

3.2 Обґрунтування вибору технологій для реалізації програмних компонентів системи

Сучасні мови програмування забезпечують можливість реалізації широкого спектра прикладних задач, однак ефективність їх використання визначається відповідністю конкретній предметній області та вимогам до програмного забезпечення [31]. Незважаючи на універсальність більшості мов, вибір інструментів розробки повинен здійснюватися з урахуванням специфіки задачі, зручності реалізації, продуктивності та подальшої підтримки.

Для розробки системи віддаленого керування доступом визначено ключові критерії вибору технологій, до яких належать кросплатформеність, доступність, простота використання, можливість роботи з апаратними ресурсами та ефективність розробки [32]. Відповідно до цих вимог додаток адміністратора доцільно реалізувати у вигляді веб-додатку, що функціонує у браузері та не потребує встановлення додаткового програмного забезпечення. Такий підхід забезпечує універсальність доступу та спрощує використання системи.

Для реалізації веб-додатку обґрунтовано використання мови

програмування JavaScript, яка є стандартом для створення клієнтських веб-застосунків. З метою підвищення ефективності розробки проведено аналіз сучасних бібліотек і фреймворків, у результаті чого обрано бібліотеку React, яка забезпечує високу продуктивність, компонентний підхід та зручність супроводу програмного коду [33].

Вимоги до клієнтського додатку передбачають портативність, автономність роботи та доступ до апаратних можливостей мобільного пристрою, зокрема Bluetooth. У зв’язку з цим використання веб-додатків є обмеженим, тому доцільним є створення мобільного додатку. Для забезпечення кросплатформеності обрано підхід із використанням фреймворку React Native, що дозволяє реалізувати додатки для різних операційних систем на основі єдиної кодової бази [34].

Для реалізації серверної частини системи обрано середовище Node.js, яке забезпечує виконання JavaScript-коду на стороні сервера та підтримує асинхронну модель обробки запитів. Це дозволяє ефективно обробляти значну кількість одночасних з’єднань при відносно невеликих витратах ресурсів. Додатковою перевагою є використання єдиної мови програмування для всіх компонентів системи, що спрощує процес розробки та супроводу [35].

Обраний технологічний стек, що базується на використанні JavaScript, бібліотеки React, фреймворку React Native та середовища Node.js, забезпечує узгодженість, кросплатформеність та ефективність функціонування системи віддаленого керування доступом без ускладнення процесу розробки [31–35].

3.3 Розробка серверної частини системи віддаленого керування доступом

Розробка серверної частини системи віддаленого керування доступом передбачає побудову структурованої архітектури, яка забезпечує обробку запитів, керування доступом та взаємодію з базою даних. Веб-сервер доцільно розглядати як багаторівневу систему, що складається з чотирьох основних

функціональних блоків, а саме REST-інтерфейсу, контролерів запитів, обробників бізнес-логіки та сховища даних [31–33]. Загальна структура веб-сервера наведена на рисунку 3.1.

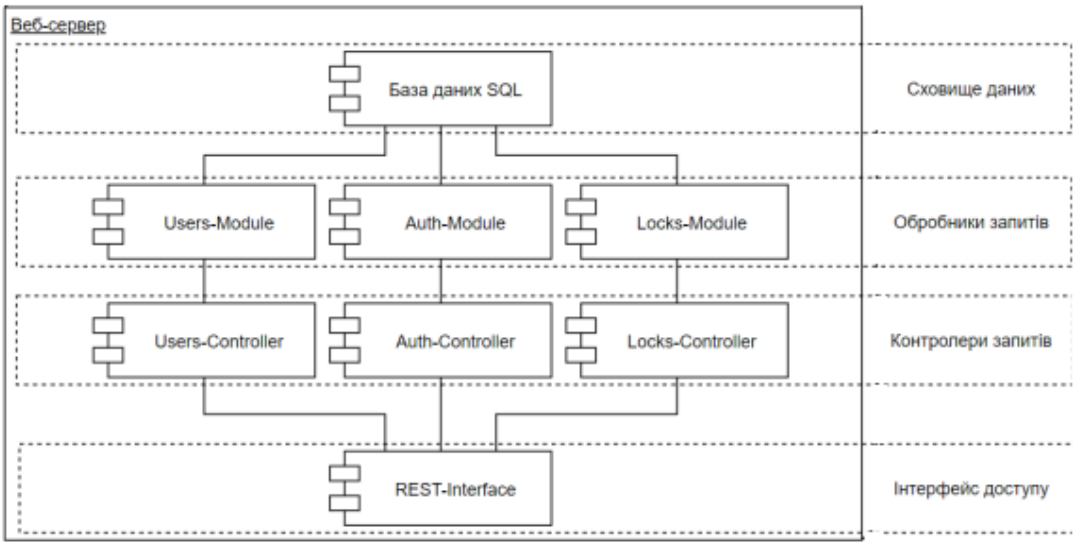


Рисунок 3.1 – Загальна структура веб-сервера

REST-інтерфейс виконує функцію точки входу до системи та забезпечує приймання усіх зовнішніх запитів. На цьому рівні здійснюється первинна обробка запиту, зокрема перевірка автентичності користувача за допомогою токена доступу. У разі успішної аутентифікації запит передається на наступний рівень системи для подальшої обробки [34].

Рівень контролерів запитів відповідає за маршрутизацію запитів та визначення необхідної операції. На цьому етапі аналізується структура запиту, визначається тип об’єкта та необхідна дія, після чого запит передається відповідному модулю. Такий підхід дозволяє реалізувати чітке розмежування функціональних областей системи та підвищити її масштабованість.

Рівень обробників запитів реалізує бізнес-логіку системи. Саме на цьому рівні виконуються основні операції, пов’язані зі створенням користувачів, керуванням пристроями та формуванням прав доступу. Обробники взаємодіють зі сховищем даних, виконуючи операції читання, запису та оновлення

інформації.

Сховище даних забезпечує довготривале збереження інформації про користувачів, пристрої та їхній стан. У якості сховища може використовуватися база даних або файлова система, що забезпечує доступ до даних та їх цілісність [35].

Усі зазначені рівні функціонують послідовно відповідно до визначеного алгоритму обробки запитів. Наприклад, при надходженні запиту на активацію пристрою REST-інтерфейс виконує перевірку токена доступу. У разі успішної перевірки запит передається до відповідного контролера, який визначає необхідний модуль обробки. Далі обробник виконує перевірку коректності параметрів запиту, зокрема серійного номера пристрою, та у разі відповідності здійснює оновлення даних у сховищі.

Основні функціональні можливості серверної частини реалізуються у вигляді окремих програмних процедур. Для реєстрації нового користувача використовується функція createUser, яка виконує перевірку введених даних та створює відповідний запис у базі даних. Ініціалізація адміністратора здійснюється функцією initAdmin, яка перевіряє унікальний код активації та створює обліковий запис із заданими параметрами.

Аутентифікація користувача реалізується функцією login, яка перевіряє облікові дані та у разі їх відповідності ініціює створення токена доступу за допомогою функції generateToken. Сформований токен містить зашифровану інформацію про користувача та використовується для подальшої ідентифікації. Перевірка токена виконується функцією checkToken, яка декодує його та визначає рівень доступу користувача.

Керування пристроями реалізується за допомогою функцій initLock, enableLock та disableLock, які забезпечують активацію пристроїв та зміну їхнього стану. Формування прав доступу здійснюється функцією assignUser, яка створює запис про надання доступу на визначений період часу. Видалення користувача зі списку доступу виконується функцією disableUser.

Обробка кодів доступу реалізується функцією activateCode, яка перевіряє

коректність коду та, у разі його відповідності, додає користувача до списку дозволених для конкретного пристрою. Отримання списку доступних пристроїв здійснюється функцією myLocks, яка формує відповідну вибірку з бази даних.

Синхронізація даних між контролером та сервером реалізується функцією syncData, яка передає актуальну інформацію про стан пристрою та перелік дозволених ідентифікаторів. Для ведення журналу подій використовується функція newAction, яка зберігає інформацію про виконані дії, включаючи час та користувача, що ініціював доступ.

Таким чином, розроблена серверна частина забезпечує централізоване керування системою, обробку запитів користувачів, формування прав доступу та ведення історії подій. Запропонована архітектура дозволяє забезпечити масштабованість, надійність та ефективність функціонування системи віддаленого керування доступом [31–35].

3.4 Розробка веб-додатку адміністратора системи

Наступним етапом після реалізації серверної частини є розробка додатку адміністратора, який забезпечує керування користувачами та налаштування параметрів системи віддаленого керування доступом. Проєктування додатку доцільно розпочинати з визначення його архітектури, що дозволяє забезпечити чітке розмежування функціональних складових та підвищити ефективність подальшої розробки [31, 32].

Архітектура додатку адміністратора побудована за принципом поділу на два основні рівні, а саме рівень бізнес-логіки та представницький рівень (Presentation Layer), що наведено на рисунку 3.2. Рівень бізнес-логіки виконує функції отримання, зберігання та обробки даних, а також забезпечує взаємодію з веб-сервером. Представницький рівень відповідає за відображення інформації користувачеві та організацію взаємодії з інтерфейсом додатку. Такий підхід дозволяє відокремити логіку обробки даних від інтерфейсу користувача, що

спрощує модифікацію та супровід програмного забезпечення [33].

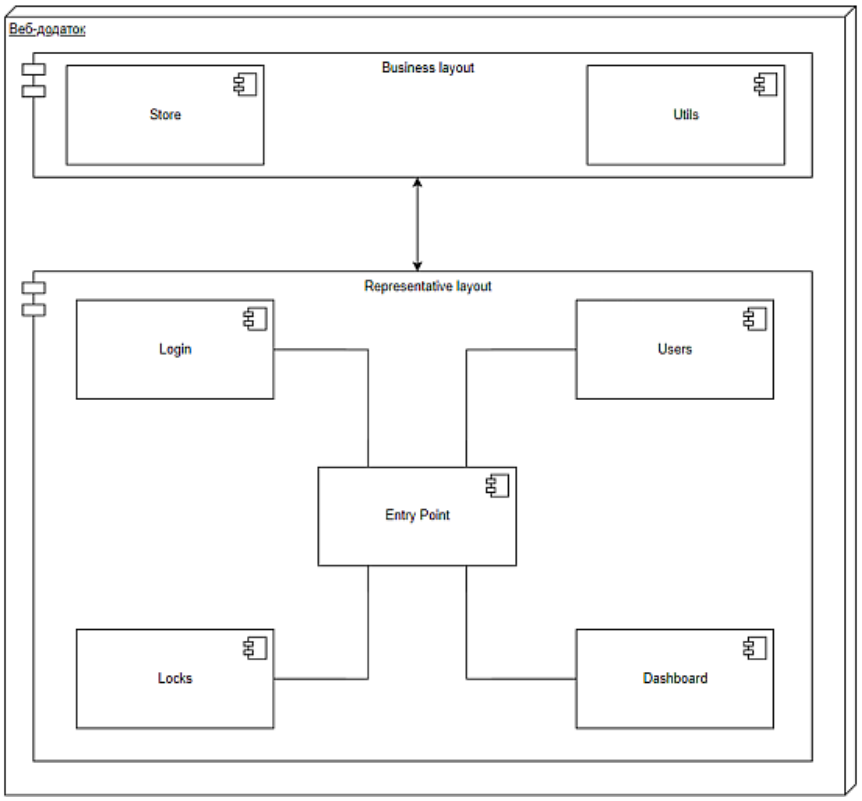


Рисунок 3.2 – Структурна схема веб-додатку адміністратора системи

Взаємодія між рівнями здійснюється за допомогою відповідних функціональних компонентів. Прикладом є процес авторизації користувача, який реалізується через формування запиту до веб-сервера. На представницькому рівні користувач вводить облікові дані та ініціює відповідну дію. Після цього запит передається до рівня бізнес-логіки, де формується HTTP-запит до сервера. Отримана відповідь обробляється та передається назад до представницького рівня для відображення результату у вигляді відповідного інтерфейсу.

Початковим етапом реалізації додатку є розробка сторінки авторизації, яка представлена на рисунку 3.3. Дана сторінка забезпечує доступ користувача до системи та містить основні функціональні елементи керування. Логіка її роботи реалізується за допомогою функцій login(), switchMode() та registration(), які забезпечують відповідно авторизацію користувача,

перемикання режимів роботи та реєстрацію нового облікового запису.

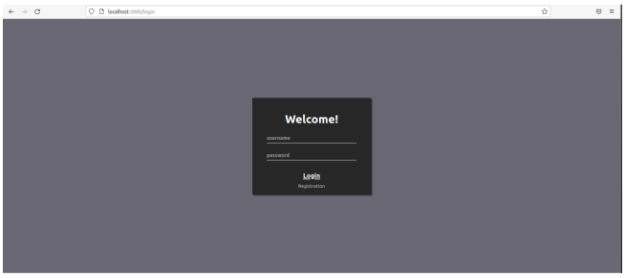


Рисунок 3.3 – Інтерфейс сторінки авторизації адміністратора

Особливістю реалізації є те, що зазначені функції не приймають вхідних параметрів безпосередньо, оскільки необхідні дані зберігаються на рівні бізнес-логіки. Такий підхід дозволяє централізувати управління даними та зменшити залежність між компонентами системи. Функція login() формує POST-запит до серверного інтерфейсу авторизації, у якому передаються ідентифікаційні дані користувача, зокрема ім’я користувача та пароль. Отримана відповідь обробляється на рівні бізнес-логіки, після чого результат передається до представницького рівня для відображення відповідного стану системи.

Розроблена архітектура додатку адміністратора забезпечує чіткий розподіл функцій між рівнями, ефективну взаємодію з серверною частиною та зручність використання інтерфейсу, що є важливими умовами для реалізації надійної та масштабованої системи керування доступом [31–33].

Для ініціалізації адміністратора використовується функція switchMode(), яка забезпечує перемикання режиму роботи додатку з авторизації на реєстрацію. У результаті виконання цієї функції відбувається динамічна зміна представницького компонента, і сторінка авторизації замінюється сторінкою ініціалізації адміністратора, що наведена на рисунку 3.4. Такий підхід дозволяє реалізувати єдину точку входу до системи з підтримкою декількох режимів роботи без перевантаження сторінки.

Після введення необхідних даних користувач ініціює процес реєстрації

шляхом натискання кнопки підтвердження, що викликає функцію registration().

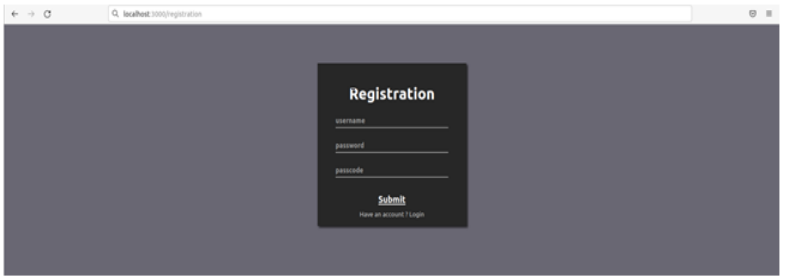


Рисунок 3.4 – Інтерфейс сторінки ініціалізації адміністратора

Дана функція формує запит типу PUT до серверного інтерфейсу авторизації. У запиті передаються параметри, необхідні для створення облікового запису адміністратора. Подальша обробка запиту виконується на стороні сервера відповідно до визначеного алгоритму ініціалізації.

Після успішного проходження процедури авторизації або реєстрації адміністратор перенаправляється на головну сторінку системи, що реалізована у вигляді інформаційної панелі Dashboard (рис. 3.5). Дана сторінка забезпечує узагальнене відображення стану системи та містить інформацію про всі доступні адміністратору пристрої і користувачів.

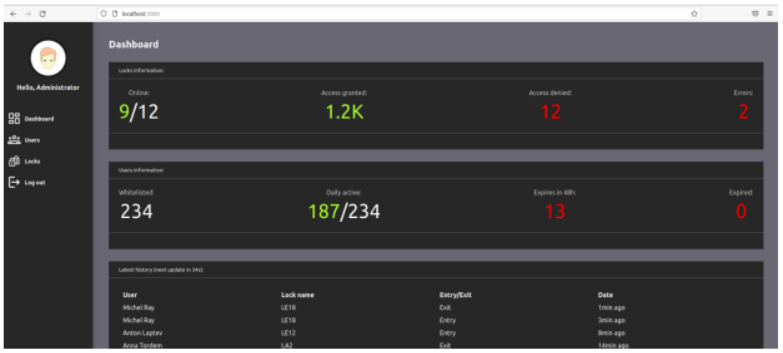


Рисунок 3.5 – Інтерфейс інформаційної панелі адміністратора (Dashboard)

Оскільки функціональне призначення цієї сторінки полягає у візуалізації даних, складні операції обробки інформації на ній не виконуються.

Сторінка Users (рис. 3.6) призначена для керування користувачами, які мають права доступу до пристроїв. На даній сторінці відображається перелік користувачів, асоційованих із конкретним адміністратором, а також реалізовано

можливість надання або обмеження доступу до окремих пристроїв. Таким чином забезпечується централізоване керування правами доступу.

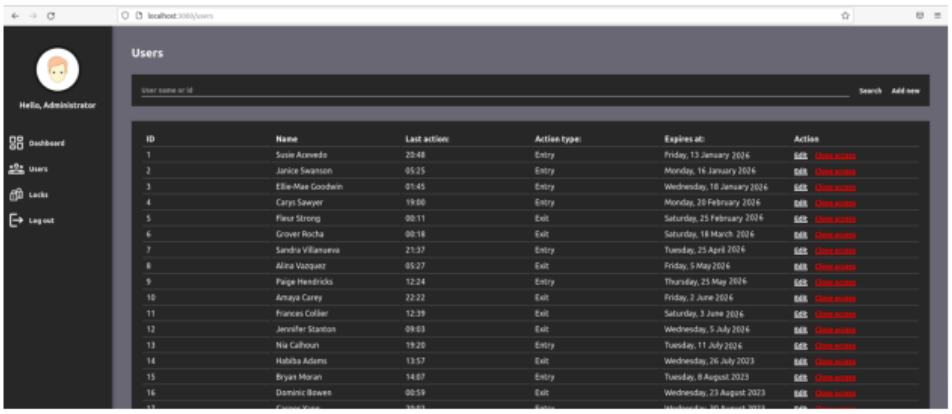


Рисунок 3.6 – Інтерфейс сторінки керування користувачами системи

Додавання нового користувача здійснюється за допомогою діалогового вікна, яке відкривається при активації відповідної функції. У цьому вікні адміністратор вводить параметри доступу, зокрема ім’я користувача, термін дії доступу та обирає пристрій, до якого надається доступ (рис. 3.7).

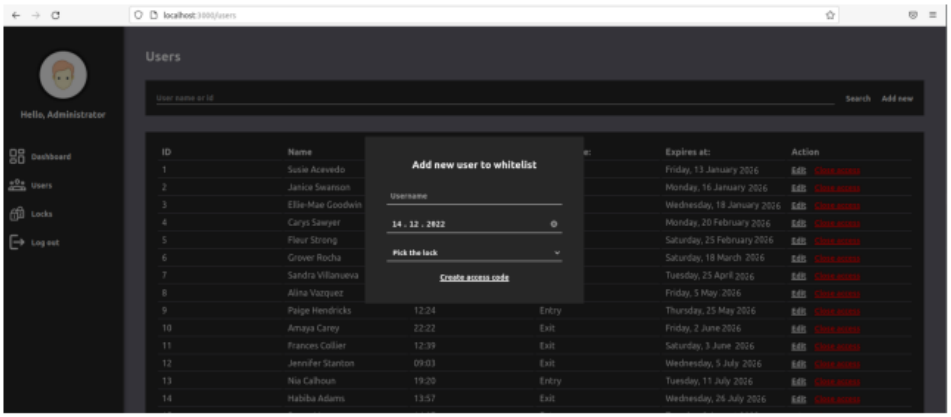


Рисунок 3.7 – Діалогове вікно додавання користувача до системи

Після підтвердження введених даних формується запит до серверної частини системи.

Генерація коду доступу реалізується через виклик відповідної функції, яка ініціює запит типу PUT до серверного ресурсу керування пристроями. У разі успішного виконання запиту сервер формує унікальний код доступу, який передається адміністратору та відображається у діалоговому вікні (рис. 3.8).

Даний код використовується користувачем для отримання прав доступу до відповідного пристрою.

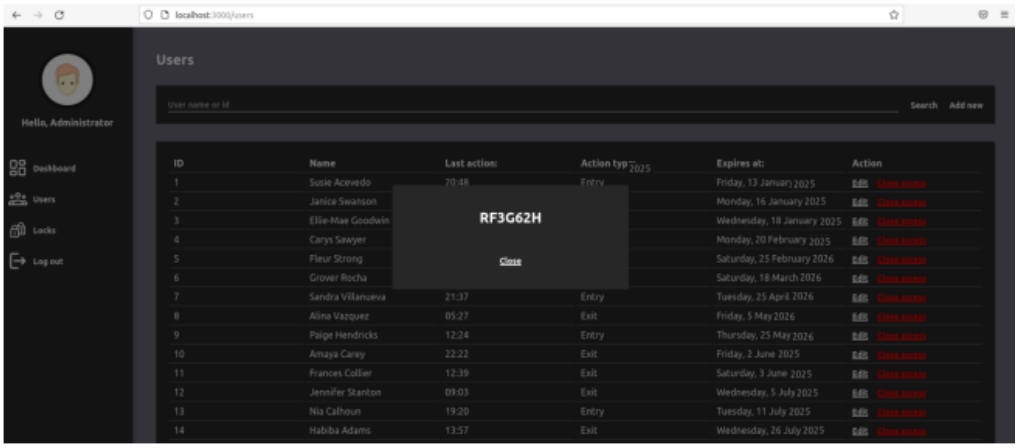
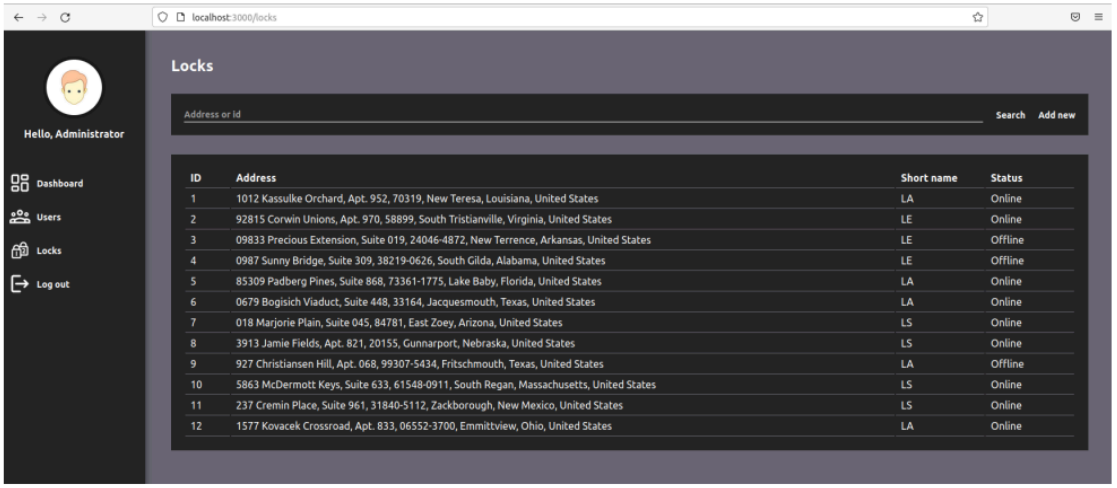


Рисунок 3.8 – Відображення згенерованого коду доступу користувача

Сторінка Locks (рис. 3.9) призначена для керування пристроями, які закріплені за адміністратором. Вона містить перелік усіх доступних пристроїв та забезпечує можливість додавання нових елементів системи. Таким чином реалізується централізоване управління апаратною частиною системи доступу.



ID	Address	Short name	Status
1	1012 Kassulke Orchard, Apt. 952, 70319, New Teresa, Louisiana, United States	LA	Online
2	92815 Corwin Unions, Apt. 970, 58899, South Tristianville, Virginia, United States	LE	Online
3	09833 Precious Extension, Suite 019, 24046-4872, New Terrence, Arkansas, United States	LE	Offline
4	0987 Sunny Bridge, Suite 309, 38219-0626, South Gilda, Alabama, United States	LE	Offline
5	85309 Padberg Pines, Suite 868, 73361-1775, Lake Baby, Florida, United States	LA	Online
6	0679 Bogisich Viaduct, Suite 448, 33164, Jacquesmouth, Texas, United States	LA	Online
7	018 Marjorie Plain, Suite 045, 84781, East Zoey, Arizona, United States	LS	Online
8	3913 Jamie Fields, Apt. 821, 20155, Gunnarport, Nebraska, United States	LS	Online
9	927 Christiansen Hill, Apt. 068, 99307-5434, Fritschmouth, Texas, United States	LA	Offline
10	5863 McDermott Keys, Suite 633, 61548-0911, South Regan, Massachusetts, United States	LS	Online
11	237 Cremin Place, Suite 961, 31840-5112, Zackborough, New Mexico, United States	LS	Online
12	1577 Kovacek Crossroad, Apt. 833, 06552-3700, Emmittview, Ohio, United States	LA	Online

Рисунок 3.9 – Інтерфейс сторінки керування пристроями доступу

Додавання нового пристрою здійснюється через спеціальне діалогове вікно (рис. 3.10), у якому адміністратор вводить необхідні параметри, зокрема адресу розташування об’єкта, умовну назву пристрою та його серійний номер.

Серійний номер використовується як унікальний ідентифікатор для активації пристрою в системі. Після підтвердження введених даних формується запит типу POST до серверного інтерфейсу активації пристрою.

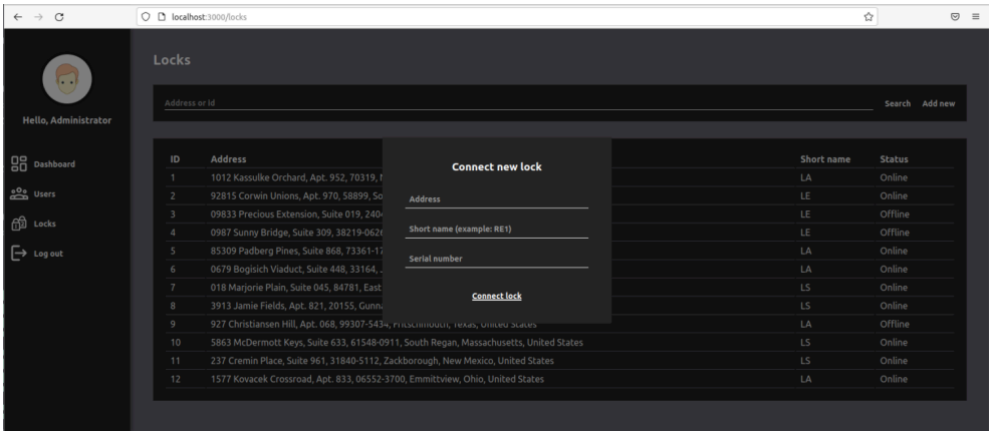


Рисунок 3.10 – Діалогове вікно активації нового пристрою доступу

У разі успішного виконання запиту новий пристрій додається до списку доступних, що відображається у відповідному інтерфейсі користувача. Такий підхід забезпечує зручність керування системою та дозволяє швидко масштабувати її шляхом додавання нових точок доступу.

Таким чином, розроблений додаток адміністратора забезпечує повний цикл керування системою доступу, включаючи реєстрацію користувачів, формування прав доступу, генерацію кодів та керування пристроями, що підтверджує його функціональну завершеність та відповідність поставленим вимогам [31–35].

3.5 Розробка клієнтського мобільного додатку користувача

Заключним етапом розробки програмної частини системи є створення клієнтського додатку для мобільних пристроїв, зокрема смартфонів та планшетів. Проєктування додатку доцільно розпочати з аналізу його структурної організації, що наведена на рисунку 3.11.

Архітектура додатку, аналогічно до веб-додатку адміністратора, базується на поділі на два функціональні рівні, а саме рівень бізнес-логіки та

представницький рівень. Такий підхід забезпечує розмежування обробки даних та їх візуалізації, що підвищує гнучкість і масштабованість програмного забезпечення [31–33].

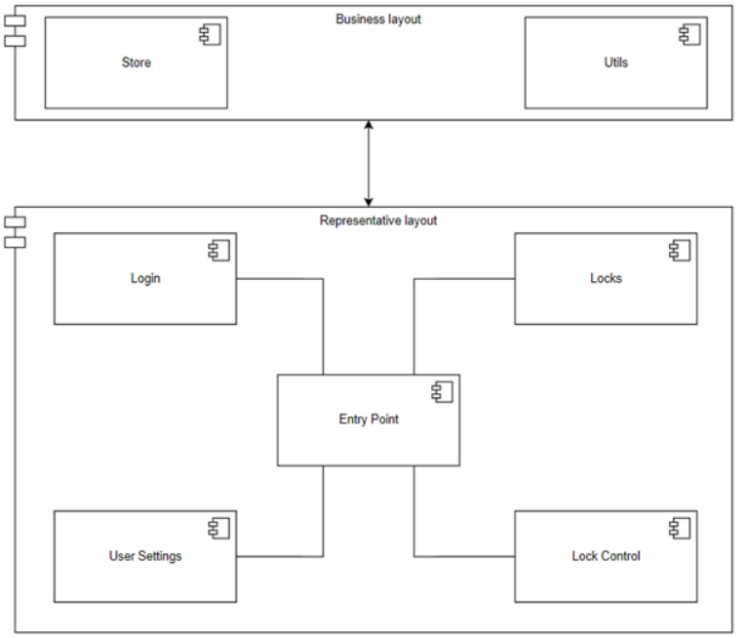


Рисунок 3.11 – Структурна схема додатку для смартфону/планшету

Рівень бізнес-логіки відповідає за обробку даних, взаємодію з серверною частиною та реалізацію основних алгоритмів функціонування системи. Оскільки принципи його роботи є аналогічними до відповідного рівня у додатку адміністратора, основна увага зосереджується на особливостях представницького рівня, який адаптований до мобільних пристроїв та їх інтерфейсних можливостей.

Сторінка авторизації Login (рис. 3.12) реалізує стандартну процедуру входу користувача до системи.

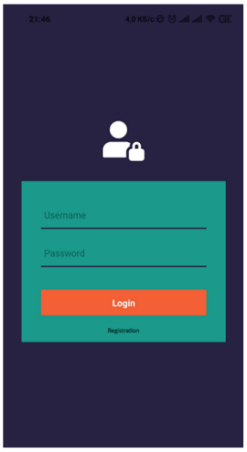


Рисунок 3.12 – Сторінка Login

Вона функціонує за аналогічними принципами до веб-інтерфейсу, забезпечуючи введення облікових даних та формування відповідного запиту до серверної частини. Сторінка реєстрації (рис. 3.13) забезпечує створення нового облікового запису користувача та передачу необхідних даних для їх подальшої обробки.

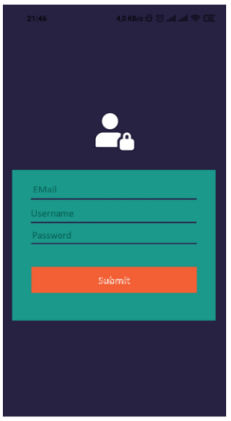


Рисунок 3.13 – Сторінка реєстрації

Основним елементом інтерфейсу є сторінка Locks, яка забезпечує взаємодію користувача з пристроями доступу. На цій сторінці реалізовано два функціональні блоки, а саме перелік доступних пристроїв та історію дій користувача. Перелік пристроїв представлений у вигляді інтерактивного списку, що дозволяє зручно перемикатися між доступними об’єктами. Історія дій містить інформацію про попередні спроби доступу та виконані операції.

Для підвищення зручності користування передбачено можливість

перемикання режимів відображення історії. У режимі «Selected» відображається інформація лише для вибраного пристрою, що дозволяє аналізувати події, пов’язані з конкретним об’єктом (рис. 3.14).

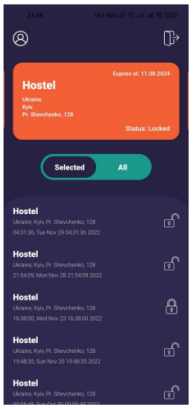


Рисунок 3.14 – Сторінка історії для пристрою

У режимі «All» відображається загальна історія дій користувача, що забезпечує комплексний огляд взаємодії з системою (рис. 3.15).

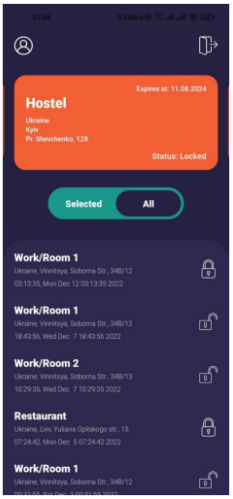


Рисунок 3.15 – Сторінка загальної історії

Керування пристроєм здійснюється шляхом вибору відповідного елемента зі списку. Після цього користувач переходить на екран керування (рис. 3.16), де реалізовано інтерфейс для ініціації доступу. При активації відповідної функції формується запит до контролера керування доступом, що передається через бездротовий канал зв’язку. Обробка запиту виконується відповідно до алгоритму, описаного у попередніх підрозділах [34].

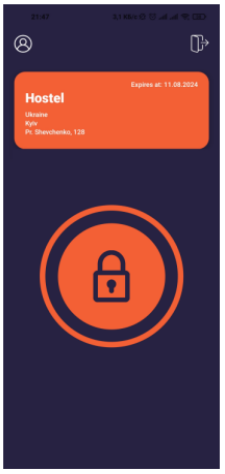


Рисунок 3.16 – Сторінка керування контролером доступу

Додавання нового пристрою до переліку доступних здійснюється через розділ налаштувань додатку. Для цього користувач обирає відповідний пункт меню, після чого відкривається інтерфейс введення коду доступу (рис. 3.17). Введений код перевіряється на сервері, і у разі його коректності відповідний пристрій додається до списку доступних. Такий механізм забезпечує контрольований процес надання доступу та підвищує безпеку системи.

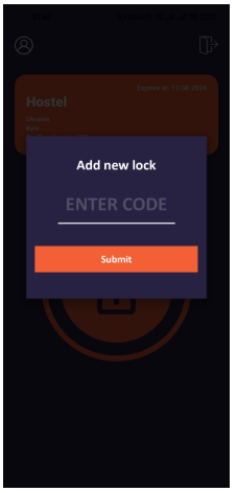


Рисунок 3.17 – Меню додавання нового пристрою

Розроблений клієнтський додаток забезпечує зручну взаємодію користувача з системою керування доступом, реалізує функції авторизації,

керування пристроями та перегляду історії подій. Використання уніфікованого підходу до побудови архітектури додатку дозволяє забезпечити узгодженість роботи всіх компонентів системи та ефективну взаємодію з серверною частиною [31–35].

Висновок до розділу

У розділі виконано розробку програмного забезпечення системи віддаленого керування доступом, що забезпечує взаємодію між користувачем, серверною частиною та контролером доступу. На початковому етапі сформовано алгоритм функціонування системи, який визначає послідовність обробки запитів, механізми ідентифікації користувачів та логіку прийняття рішень щодо надання доступу.

Обґрунтовано вибір технологічного стеку, який базується на використанні мови програмування JavaScript та відповідних інструментів розробки. Такий підхід дозволив забезпечити уніфікацію програмних компонентів, спростити процес розробки та підвищити ефективність подальшого супроводу системи.

Розроблено серверну частину системи, яка реалізує обробку запитів, керування правами доступу, взаємодію з базою даних та ведення журналу подій. Запропонована багаторівнева архітектура веб-сервера забезпечує масштабованість, надійність та ефективну обробку інформації.

Створено веб-додаток адміністратора, який забезпечує керування користувачами, пристроями та правами доступу. Реалізовано зручний інтерфейс для виконання основних операцій, що дозволяє ефективно адмініструвати систему без додаткових технічних знань.

Розроблено клієнтський мобільний додаток користувача, який забезпечує отримання доступу до об’єктів, взаємодію з контролером через бездротові технології та перегляд історії дій. Архітектура додатку побудована з урахуванням сучасних вимог до мобільних застосунків, що забезпечує його зручність та функціональність.

У результаті виконано комплексну розробку програмної частини системи віддаленого керування доступом, яка відповідає поставленим задачам, забезпечує надійну роботу та може бути використана як основа для подальшого розширення функціональних можливостей системи.

ВИСНОВКИ

У ході виконання дипломної роботи розроблено комплексну систему віддаленого керування доступом із використанням мобільного ідентифікатора на базі мікроконтролера STM32F407VET6. У роботі проведено аналіз сучасних підходів до організації систем контролю доступу, технологій ідентифікації користувачів та засобів побудови розподілених інформаційно-керуючих систем, що дозволило сформулювати обґрунтовані вимоги до розроблюваної системи.

У межах дослідження визначено архітектуру системи, яка включає мікроконтролерний пристрій керування доступом, серверну частину та програмні додатки користувача і адміністратора. Розроблено структурні та функціональні схеми, що відображають взаємодію апаратних і програмних компонентів, а також забезпечують реалізацію процесів ідентифікації, авторизації та керування доступом.

Виконано обґрунтування вибору елементної бази, зокрема мікроконтролера STM32F407VET6, модулів бездротового зв’язку та допоміжних компонентів, що забезпечують надійність, функціональність і масштабованість системи. Розроблено електричну функціональну схему контролера доступу, яка забезпечує інтеграцію всіх апаратних елементів та реалізацію взаємодії з виконавчими пристроями.

Розроблено алгоритмічне забезпечення системи, яке визначає послідовність обробки даних, взаємодію між компонентами та прийняття рішень щодо надання доступу. На основі алгоритмів реалізовано програмне забезпечення мікроконтролера, серверної частини, веб-додатку адміністратора та мобільного додатку користувача. Запропонована програмна архітектура забезпечує ефективну обробку запитів, зручність використання та можливість подальшого розширення функціональних можливостей системи.

Результатом виконаної роботи є створення функціонально завершеної системи віддаленого керування доступом, яка забезпечує надійну ідентифікацію користувачів, гнучке керування правами доступу та інтеграцію з

сучасними інформаційними технологіями. Розроблена система може бути використана у практичних застосуваннях для організації контролю доступу до об’єктів різного призначення, а також є основою для подальших досліджень і вдосконалення у напрямку підвищення безпеки та розширення функціональності.

Таким чином, поставлена мета роботи досягнута, а сформульовані завдання повністю виконані, що підтверджує ефективність запропонованих рішень та їх відповідність сучасним вимогам до систем віддаленого керування доступом

ПЕРЕЛІК ПОСИЛАНЬ НА ДЖЕРЕЛА

1 Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2017.

2 Bishop M. Computer Security: Art and Science. – Addison-Wesley, 2018.

3 Garcia M. The Design and Evaluation of Physical Protection Systems. – Elsevier, 2016.

4 Frankel S. Mobile Device Security. – NIST, 2016.

5 STMicroelectronics. STM32F407 Reference Manual. – 2020.

6 Wilmshurst T. Designing Embedded Systems with STM32. – Newnes, 2010.

7 Bluetooth SIG. Bluetooth Core Specification. – 2021.

8 OWASP Foundation. Web Security Testing Guide. – 2023.

9 Tanenbaum A., Wetherall D. Computer Networks. – 5th ed. – Pearson, 2011

10 IEEE Standard 802.3: Ethernet. – IEEE, 2018.

11 Gast M. 802.11 Wireless Networks: The Definitive Guide. – O'Reilly, 2013.

12 IEEE Standard 802.11: Wireless LAN Medium Access Control and Physical Layer Specifications. – IEEE, 2020.

13 Kurose J., Ross K. Computer Networking: A Top-Down Approach. – Pearson, 2017.

14 IEEE Standard 802.15.4: Low-Rate Wireless Personal Area Networks. – IEEE, 2020.

15 Frankel S., Eydt B., Owens L., Scarfone K. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. – NIST, 2008.

16 Fielding R., Reschke J. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. – IETF RFC 7231, 2014.

17 Garcia M. The Design and Evaluation of Physical Protection Systems. – Elsevier, 2016.

18 Rashid M. Power Electronics Handbook. – Butterworth-Heinemann, 2017.

19 Bolton W. Mechatronics: Electronic Control Systems in Mechanical and

Electrical Engineering. – Pearson, 2015.

20 Horowitz P., Hill W. The Art of Electronics. – 3rd ed. – Cambridge University Press, 2015.

21 ISO. ISO/IEC 7498-1: Information Technology – Open Systems Interconnection – Basic Reference Model. – Geneva, 2018.

22 IEEE. IEEE 802.3 Ethernet Standard. – New York: IEEE, 2018.

23 Bluetooth SIG. Bluetooth Core Specification. – 2020.

24 Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2017.

25 Kurose J., Ross K. Computer Networking: A Top-Down Approach. – Pearson, 2017.

26 Tanenbaum A. S. Computer Networks. – Pearson, 2018.

27 Google. Android Developers Documentation. – 2021.

28 IEEE. IEEE 802.11 Wireless LAN Standard. – 2020.

29 Espressif Systems. ESP8266 Technical Reference. – 2021.

30 OpenJS Foundation. Node.js Documentation. – 2021.

31 Tanenbaum A. S. Computer Networks. – Pearson, 2018.

32 Pressman R. Software Engineering. – McGraw-Hill, 2014.

33 React. React Documentation. – Meta, 2021.

34 React Native. React Native Documentation. – Meta, 2021.

35 Node.js. Node.js Documentation. – OpenJS Foundation, 2021.