Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС КОНТРОЛЮ ДОСТУПУ З БАГАТОФАКТОРНОЮ АУТЕНТИФІКАЦІЄЮ

HARDWARE AND SOFTWARE ACCESS CONTROL COMPLEX WITH MULTIFACTOR AUTHENTICATION

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-42
Ковалюк Валерій Ігорович

(підпис)

Керівник:
к.т.н., доцент
Гринюк Сергій Васильович

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» червня 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
« 23 » 12 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Ковалюку Валерію Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Апаратно-програмний комплекс контролю доступу з багатофакторною аутентифікацією*

Керівник роботи *к.т.н., доцент Гринюк Сергій Васильович*

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026 р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Теоретичні основи побудови систем контролю доступу з багатофакторною аутентифікацією
Проєктування та розробка апаратно-програмного комплексу
Практична реалізація та тестування комплексу контролю доступу
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Загальний вигляд апаратного прототипу комплексу контролю доступу
Структура програмного забезпечення комплексу контролю доступу на основі Arduino
Реалізація алгоритму багатофакторної аутентифікації в комплексі контролю доступу
Режими роботи комплексу контролю доступу на основі Arduino

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Теоретичні основи побудови систем контролю доступу з багатофакторною аутентифікацією	*Гринюк С.В., доцент*		
Проєктування та розробка апаратно-програмного комплексу	*Гринюк С.В., доцент*		
Практична реалізація та тестування комплексу контролю доступу	*Гринюк С.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І., ст. викладач*		

7. Дата видачі завдання 23.12.2025 р.

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2026 р.	
2.	*Теоретичні основи побудови систем контролю доступу з багатофакторною аутентифікацією*	до 02.03.2026 р.	
3.	*Проєктування та розробка апаратно-програмного комплексу*	до 02.04.2026 р.	
4.	*Практична реалізація та тестування комплексу контролю доступу*	до 10.04.2026 р.	
5.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 10.05.2026 р.	
6.	*Нормоконтроль*	до 23.05.2026 р.	
7.	*Інструментальна перевірка на академічний плагіат*	до 25.05.2026 р.	
8.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 28.05.2026 р.	

КАЛЕНДАРНИЙ ПЛАН

Здобувач вищої освіти _____ Валерій КОВАЛЮК
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Сергій ГРИНЮК
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Ковалюк В. І. Апаратно-програмний комплекс контролю доступу з багатофакторною аутентифікацією. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, переліку використаних джерел, додатків.

В першому розділі проаналізовано сучасні методи аутентифікації користувачів, особливості багатофакторної аутентифікації в системах фізичного доступу та апаратно-програмні засоби, які можуть застосовуватися для побудови систем контролю доступу.

У другому розділі виконано вибір та обґрунтування компонентної бази комплексу, розроблено структурну і принципову схеми пристрою, визначено порядок підключення RFID-модуля, клавіатури, LCD-дисплея, релейного модуля, індикаторів та інших елементів до Arduino Uno. Також сформовано алгоритм функціонування системи, який передбачає послідовну перевірку RFID-картки та PIN-коду.

У третьому розділі описано практичну реалізацію комплексу контролю доступу, розробку програмного забезпечення для Arduino, реалізацію алгоритму багатофакторної аутентифікації, налаштування режимів роботи та тестування працездатності прототипу. У роботі передбачено режими очікування RFID-картки, введення PIN-коду, дозволеного доступу, відмови в доступі, тимчасового блокування, виходу з приміщення та сервісного моніторингу.

Ключові слова: контроль доступу, багатофакторна аутентифікація, Arduino Uno, RFID, RC522, PIN-код, клавіатура 4x4, LCD-дисплей, сервопривід, релейний модуль, апаратно-програмний комплекс.

ANNOTATION

Kovalyuk V. Hardware and software access control complex with multi-factor authentication. Manuscript.

Qualification work of the bachelor of the EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

The qualification work consists of an introduction, three sections, conclusions, a list of sources used, and appendices.

The first section analyzes modern methods of user authentication, features of multi-factor authentication in physical access systems and hardware and software tools that can be used to build access control systems.

The second section selects and justifies the component base of the complex, develops a structural and schematic diagram of the device, determines the procedure for connecting the RFID module, keyboard, LCD display, relay module, indicators and other elements to the Arduino Uno. An algorithm for the system's operation is also formed, which involves sequential verification of the RFID card and PIN code.

The third section describes the practical implementation of the access control complex, the development of software for Arduino, the implementation of the multi-factor authentication algorithm, the configuration of operating modes and testing the prototype's performance. The work provides for the modes of RFID card waiting, PIN code entry, permitted access, denied access, temporary blocking, exit from the premises and service monitoring.

Keywords: access control, multi-factor authentication, Arduino Uno, RFID, RC522, PIN code, 4x4 keyboard, LCD display, servo drive, relay module, hardware and software complex.

ЗМІСТ

ВСТУП

Сучасний розвиток інформаційних технологій супроводжується активним впровадженням електронних систем контролю доступу в освітніх установах, офісних приміщеннях, лабораторіях, виробничих об’єктах, серверних кімнатах та інших зонах з обмеженим доступом. Такі системи дають змогу автоматизувати процес ідентифікації користувачів, зменшити залежність від традиційних механічних ключів, підвищити рівень безпеки приміщень та забезпечити контроль за подіями входу і виходу. Особливої актуальності набувають апаратно-програмні комплекси, які поєднують електронні ідентифікатори, мікроконтролерні платформи, виконавчі пристрої, засоби індикації та програмні алгоритми прийняття рішень.

Одним із важливих напрямів удосконалення систем контролю доступу є використання багатофакторної аутентифікації. На відміну від простих систем, що базуються лише на одному способі підтвердження особи, багатофакторний підхід передбачає застосування двох або більше незалежних факторів перевірки. Наприклад, користувач може підтверджувати право доступу за допомогою RFID-картки та PIN-коду. Такий підхід істотно підвищує надійність системи, оскільки втрата або копіювання одного ідентифікатора не забезпечує автоматичного отримання доступу до захищеного об’єкта.

Актуальність теми кваліфікаційної роботи зумовлена необхідністю розробки доступних, гнучких і простих у реалізації рішень для контролю фізичного доступу з використанням мікроконтролерних платформ. Arduino є зручною апаратною основою для створення навчально-дослідних і експериментальних комплексів, оскільки підтримує роботу з великою кількістю периферійних модулів, має просте середовище програмування та дає змогу реалізувати основні функції системи доступу без застосування складного промислового обладнання. На базі Arduino можна створити прототип системи, що виконує зчитування RFID-картки, перевірку PIN-коду, керування

електрозамком, індикацію результату аутентифікації та обробку помилкових спроб доступу.

Метою кваліфікаційної роботи є розробка апаратно-програмного комплексу контролю доступу з багатофакторною аутентифікацією на базі Arduino, який забезпечує перевірку користувача за кількома факторами та керування виконавчим пристроєм доступу.

Об’єктом дослідження є процес організації електронного контролю доступу до приміщень або захищених зон.

Предметом дослідження є апаратні засоби, програмні алгоритми та методи багатофакторної аутентифікації в системі контролю доступу на базі Arduino.

Для досягнення поставленої мети необхідно виконати такі завдання:

1. Проаналізувати призначення, класифікацію та принципи побудови сучасних систем контролю доступу.

2. Розглянути особливості використання багатофакторної аутентифікації в системах фізичного доступу.

3. Обґрунтувати вибір апаратної платформи Arduino та периферійних компонентів для реалізації комплексу.

4. Розробити структурну та функціональну схему апаратно-програмного комплексу контролю доступу.

5. Сформувати алгоритм роботи системи з використанням RFID-картки та PIN-коду.

6. Реалізувати програмне забезпечення для мікроконтролера Arduino.

7. Виконати тестування працездатності комплексу та проаналізувати результати його роботи.

У роботі використано методи аналізу технічної літератури та наявних рішень у сфері контролю доступу, методи структурного та функціонального моделювання, методи алгоритмізації, програмування мікроконтролерів, а також експериментальне тестування розробленого прототипу.

Практичне значення роботи полягає у створенні працездатного прототипу апаратно-програмного комплексу контролю доступу, який може бути

використаний як навчальна модель для вивчення принципів роботи систем безпеки, мікроконтролерного керування, RFID-ідентифікації та багатофакторної аутентифікації. Запропоноване рішення може бути адаптоване для невеликих приміщень, лабораторій, навчальних стендів або подальших дослідницьких розробок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ КОНТРОЛЮ ДОСТУПУ З БАГАТОФАКТОРНОЮ АУТЕНТИФІКАЦІЄЮ

1.1 Аналіз сучасних методів аутентифікації користувачів

Аутентифікація користувачів є одним із ключових процесів у системах інформаційної та фізичної безпеки, оскільки саме вона забезпечує перевірку того, чи справді користувач є тією особою, за яку себе видає. У системах контролю доступу аутентифікація виконує роль проміжної ланки між ідентифікацією користувача та прийняттям рішення про надання або заборону доступу. Якщо ідентифікація відповідає на питання «хто звертається до системи?», то аутентифікація визначає, чи має ця особа достатні підтвердження для отримання доступу до захищеного об’єкта [1].

У сучасних системах безпеки методи аутентифікації зазвичай поділяють за типом фактора, який використовується для підтвердження особи. Найпоширенішими є три основні групи: фактор знання, фактор володіння та біометричний фактор. До фактора знання належать паролі, PIN-коди, контрольні фрази та інші секретні дані, які користувач повинен пам’ятати. До фактора володіння належать фізичні або електронні засоби, якими користувач володіє: RFID-картки, смарткартки, USB-токени, мобільні пристрої, OTP-генератори. Біометричний фактор ґрунтується на унікальних фізичних або поведінкових характеристиках користувача, зокрема відбитках пальців, рисах обличчя, сітківці ока або голосі [1].

Найпростішим і найпоширенішим методом є парольна аутентифікація. Вона передбачає введення користувачем секретної комбінації символів, яка порівнюється із записом, збереженим у системі. Перевагами цього методу є простота реалізації, низька вартість і відсутність потреби в додатковому обладнанні. Водночас парольна аутентифікація має суттєві недоліки: користувачі часто обирають слабкі паролі, повторно використовують їх у різних системах або зберігають у незахищеному вигляді. Саме тому сучасні

рекомендації з безпеки наголошують на необхідності використання додаткових механізмів захисту, зокрема багатофакторної аутентифікації [2].

Загальну класифікацію сучасних методів аутентифікації користувачів доцільно подати на рисунку 1.2.

Рисунок 1.2 – Класифікація сучасних методів аутентифікації користувачів [2]

PIN-код є різновидом аутентифікації за фактором знання. На відміну від повноцінного пароля, PIN-код зазвичай є коротшою числовою комбінацією, що спрощує його введення на клавіатурі або сенсорній панелі. У системах фізичного доступу PIN-код часто використовується як другий фактор після картки або електронного ідентифікатора. Його перевагою є простота застосування, однак недоліком є можливість підглядання, підбору або передачі іншій особі. Тому PIN-код доцільно використовувати не як єдиний засіб захисту, а в поєднанні з іншим фактором, наприклад RFID-карткою [2].

До методів аутентифікації за фактором володіння належать RFID-картки, NFC-мітки, смарткартки, апаратні токени та мобільні ідентифікатори. У

системах контролю доступу такі засоби є дуже поширеними, оскільки дають змогу швидко і зручно підтверджувати право входу до приміщення. Користувач підносить картку або мітку до зчитувача, після чого система отримує її унікальний ідентифікатор і порівнює його з базою дозволених значень. Такий підхід є зручним для офісів, навчальних аудиторій, лабораторій і технічних приміщень. Водночас картка може бути втрачена, передана іншій особі або скопійована у разі використання недостатньо захищених технологій [3].

Більш захищеним різновидом фактора володіння є апаратні криптографічні ключі та сучасні passkey-рішення. Passkeys базуються на криптографічних ключових парах і призначені для безпарольної та стійкої до фішингу аутентифікації. Приватний ключ залишається на пристрої користувача або в апаратному ключі, а сервіс зберігає лише відкритий ключ, що зменшує ризики, пов’язані з витоком паролів або їх повторним використанням [4].

Біометрична аутентифікація використовує індивідуальні характеристики користувача. До найбільш поширених біометричних методів належать розпізнавання відбитка пальця, обличчя, райдужної оболонки ока та голосу. Перевагою біометрії є те, що користувачеві не потрібно запам’ятовувати пароль або носити окремий ідентифікатор. Проте біометричні системи потребують точного налаштування, якісних сенсорів, захисту біометричних шаблонів і врахування можливих помилкових спрацювань. Крім того, біометричні дані є особливо чутливими, оскільки їх не можна легко змінити у випадку компрометації [1].

Окрему групу становлять одноразові паролі, або OTP. Вони можуть генеруватися мобільним застосунком, апаратним токеном або надсилатися через повідомлення. OTP-коди мають обмежений час дії, тому їх складніше використати повторно. Проте OTP через SMS або електронну пошту може бути менш надійним у разі перехоплення повідомлень, компрометації облікового запису або атак соціальної інженерії. Через це сучасні рекомендації дедалі більше орієнтуються на стійкі до фішингу методи багатофакторної аутентифікації, зокрема FIDO/WebAuthn та апаратні криптографічні ключі [5].

Порівняльну характеристику основних методів аутентифікації користувачів наведено в таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика сучасних методів аутентифікації користувачів

Метод аутентифікації	Тип фактора	Переваги	Недоліки	Доцільність використання
Пароль	Знання	Простота реалізації, не потребує додаткового обладнання	Може бути слабким, викраденим або повторно використаним	Інформаційні системи, бажано у поєднанні з MFA
PIN-код	Знання	Швидке введення, зручність для локальних систем	Можливість підглядання або підбору	Системи фізичного доступу як додатковий фактор
RFID-картка	Володіння	Швидкість використання, зручність, низька вартість	Можлива втрата, передача або копіювання	Контроль доступу до приміщень
Смарткартка	Володіння	Вищий рівень захисту порівняно зі звичайними картками	Потребує сумісної інфраструктури	Корпоративні та службові системи доступу
OTP-код	Володіння / знання	Обмежений час дії, підвищення захисту входу	Можливість перехоплення або фішингу	Двофакторна аутентифікація в облікових записах
Біометрія	Біометричний фактор	Зручність, складність передачі іншій особі	Потреба в якісному сенсорі, ризики обробки біометричних даних	Об’єкти з підвищеними вимогами до безпеки
Passkey / FIDO-ключ	Володіння + локальна перевірка	Стійкість до фішингу, відсутність паролів	Потребує сумісних пристроїв і сервісів	Сучасні системи захищеної аутентифікації

Найбільш ефективним підходом у сучасних умовах є багатофакторна аутентифікація, яка поєднує два або більше незалежних фактори. Наприклад, для системи контролю доступу на базі Arduino можна використати комбінацію RFID-картки та PIN-коду. У такому випадку RFID-картка підтверджує фактор володіння, а PIN-код - фактор знання. Навіть якщо картку буде втрачено,

стороння особа не зможе отримати доступ без правильного PIN-коду. Така модель є доцільною для навчально-дослідного прототипу, оскільки вона не потребує складного обладнання, але демонструє принцип підвищення рівня безпеки за рахунок поєднання кількох факторів [2, 3].

Для розроблюваного комплексу контролю доступу найбільш раціональним є використання саме двофакторної аутентифікації на основі RFID-картки та PIN-коду. Це рішення має кілька переваг. По-перше, воно є доступним за вартістю, оскільки RFID-модуль, матрична клавіатура та Arduino Uno є поширеними компонентами. По-друге, така система є достатньо простою для програмної реалізації та налагодження. По-третє, вона дозволяє наочно продемонструвати принцип роботи багатофакторної аутентифікації в системі фізичного доступу. По-четверте, запропонована архітектура може бути розширена за рахунок додавання LCD-дисплея, журналювання подій, датчика стану дверей або мережевого модуля [2; 5].

Отже, сучасні методи аутентифікації користувачів охоплюють широкий спектр технологій - від традиційних паролів і PIN-кодів до біометричних систем, апаратних токенів і безпарольних passkey-рішень. Для систем фізичного доступу особливе значення має поєднання зручності, вартості, надійності та простоти інтеграції з виконавчими пристроями. У контексті цієї роботи найбільш доцільним є використання багатофакторної моделі, у якій RFID-картка виконує роль фактора володіння, а PIN-код - фактора знання. Такий підхід забезпечує вищий рівень захисту порівняно з однофакторною аутентифікацією та є придатним для реалізації апаратно-програмного комплексу на базі Arduino [1, 3].

1.2 Особливості багатофакторної аутентифікації в системах фізичного доступу

Багатофакторна аутентифікація є одним із важливих підходів до підвищення надійності систем фізичного доступу, оскільки вона передбачає перевірку користувача не за одним, а за кількома незалежними факторами. У

традиційних системах контролю доступу часто використовується лише один ідентифікатор, наприклад RFID-картка, електронний ключ або PIN-код. Такий підхід є простим у реалізації, однак має низку недоліків: картку можна втратити, передати іншій особі або скопіювати, а PIN-код можна підглянути, підібрати або розголосити. Саме тому у сучасних системах безпеки дедалі частіше застосовується багатофакторна модель, яка поєднує кілька різних способів підтвердження особи користувача [1, 2].

У системах фізичного доступу багатофакторна аутентифікація має певні особливості порівняно з інформаційними системами. Якщо в комп'ютерних сервісах вона найчастіше застосовується для входу в обліковий запис, то у фізичному доступі її результатом є керування реальним виконавчим пристроєм - електрозамком, турнікетом, шлагбаумом або дверним контролером. Тому помилка аутентифікації може призвести не лише до несанкціонованого входу в систему, а й до фізичного проникнення в приміщення, лабораторію, серверну кімнату або іншу захищену зону. З цієї причини системи фізичного доступу повинні забезпечувати не лише перевірку користувача, а й надійне керування виконавчими механізмами, журналювання подій, контроль стану дверей і можливість аварійного реагування [1].

Загальну модель багатофакторної аутентифікації в системі фізичного доступу доцільно подати на рисунку 1.3.

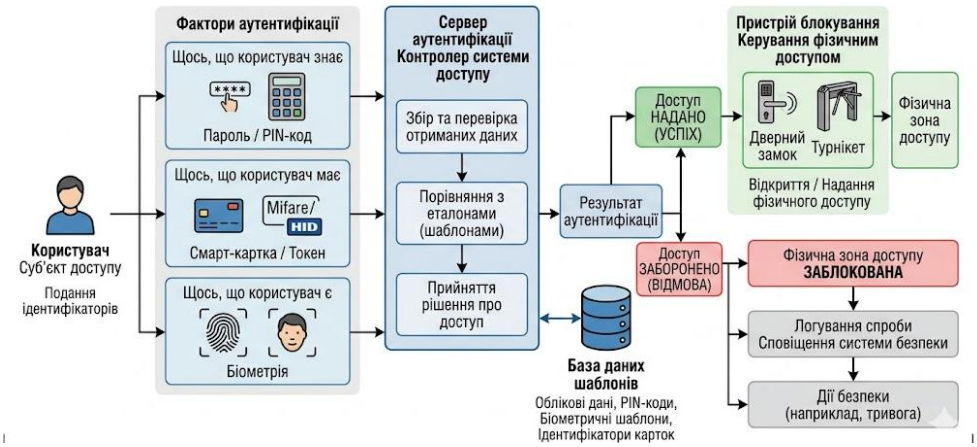

Рисунок 1.3 – Узагальнена модель багатофакторної аутентифікації в системі фізичного доступу [6]

Основна ідея багатофакторної аутентифікації полягає у використанні щонайменше двох незалежних факторів. До першого фактора належить те, що користувач знає, наприклад пароль або PIN-код. До другого - те, чим користувач володіє, наприклад RFID-картка, смарткартка, мобільний пристрій або апаратний токен. До третього - те, чим користувач є, тобто його біометричні характеристики: відбиток пальця, обличчя, голос або райдужна оболонка ока. Важливо, що використання двох однотипних факторів не вважається повноцінною багатофакторною аутентифікацією. Наприклад, пароль і PIN-код належать до фактора знання, тому їх поєднання не забезпечує такого рівня захисту, як комбінація RFID-картки та PIN-коду або картки та біометрії [2].

Для систем фізичного доступу найбільш поширеними є комбінації «картка + PIN-код», «картка + біометрія», «мобільний ідентифікатор + PIN-код», «смарткартка + біометричний шаблон». У навчально-дослідних і прототипних системах, зокрема на базі Arduino, найбільш раціональним є використання поєднання RFID-картки та PIN-коду. RFID-картка виконує роль фактора володіння, а PIN-код - фактора знання. Така модель є достатньо простою для реалізації, не потребує дорогого обладнання, добре демонструє принцип багатофакторної перевірки та дозволяє підвищити рівень захисту порівняно з однофакторним доступом [2].

Особливістю багатофакторної аутентифікації у фізичних системах є необхідність узгодження логіки перевірки з реальним сценарієм проходу користувача. Наприклад, система може спочатку зчитувати RFID-картку, перевіряти її наявність у списку дозволених ідентифікаторів, після чого запитувати PIN-код. Якщо обидва фактори підтверджено, мікроконтролер формує керуючий сигнал на релейний модуль і відкриває замок. Якщо хоча б один із факторів не підтверджено, доступ блокується, активується світлова або звукова індикація відмови, а подія може бути зафіксована в журналі. Такий підхід дозволяє уникнути ситуації, коли втрата картки автоматично надає сторонній особі можливість входу [1, 2].

У системах фізичного доступу важливе значення має швидкість проходження процедури аутентифікації. На відміну від інформаційних систем, де користувач може витратити більше часу на введення коду або підтвердження входу, у дверних системах надмірно складна процедура може створювати незручності, черги або затримки. Тому багатофакторна аутентифікація повинна поєднувати безпеку та ергономічність. Наприклад, використання RFID-картки забезпечує швидке зчитування ідентифікатора, а короткий PIN-код додає другий рівень перевірки без значного ускладнення роботи користувача [2].

Ще однією особливістю є необхідність захисту каналів зв’язку між периферійними пристроями та контролером. У сучасних системах контролю доступу для взаємодії між зчитувачами та контролерами застосовуються спеціалізовані протоколи. Зокрема, OSDP розроблений для покращення сумісності засобів контролю доступу та був затверджений як міжнародний стандарт IEC 60839-11-5 у 2020 році [6, 7]. Це важливо, оскільки навіть надійна багатофакторна аутентифікація може бути ослаблена, якщо зчитувач або канал передавання даних між зчитувачем і контролером не захищений від підміни або втручання.

З погляду безпеки важливим є також обмеження кількості невдалих спроб. Якщо користувач кілька разів поспіль вводить неправильний PIN-код після пред’явлення RFID-картки, система може тимчасово заблокувати подальші спроби, подати звуковий сигнал або сформувати запис про підозрілу активність. Це дозволяє зменшити ризик підбору PIN-коду. У складніших системах може також використовуватися часовий розклад доступу, розмежування прав за ролями, контроль повторного проходу, журналювання подій і повідомлення адміністратора про аномальні ситуації [1, 2].

Порівняльну характеристику варіантів багатофакторної аутентифікації в системах фізичного доступу наведено в таблиці 1.2.

Таблиця 1.2 – Варіанти багатофакторної аутентифікації в системах фізичного доступу

Варіант MFA	Фактори перевірки	Переваги	Недоліки	Доцільність використання
RFID-картка + PIN-код	Володіння + знання	Простота реалізації, низька вартість, зручність для Arduino-прототипу	Можливе підглядання PIN-коду, втрата картки	Навчальні, офісні та лабораторні системи
RFID-картка + біометрія	Володіння + біометрія	Вищий рівень захисту, складність передачі доступу іншій особі	Вища вартість, потреба в біометричному сенсорі	Об’єкти з підвищеними вимогами до безпеки
Смарткартка + PIN-код	Володіння + знання	Кращий захист ідентифікатора, підтримка корпоративних рішень	Потребує сумісної інфраструктури	Корпоративні системи доступу
Мобільний ідентифікатор + PIN-код	Володіння + знання	Зручність, можливість дистанційного адміністрування	Залежність від смартфона, живлення та зв’язку	Сучасні офісні системи
Картка + часовий розклад + роль користувача	Володіння + контекстні обмеження	Додаткове обмеження доступу за часом і правами	Не є повноцінною MFA без другого фактора	Допоміжний механізм контролю доступу

Для розроблюваного апаратно-програмного комплексу на базі Arduino найбільш доцільною є схема «RFID-картка + PIN-код». Її перевага полягає в тому, що обидва фактори легко реалізуються за допомогою доступних електронних компонентів: RFID-модуля RC522, матричної клавіатури, Arduino Uno, LCD-дисплея, релейного модуля та електрозамка. У такій системі логіка роботи може бути побудована за послідовним принципом: спочатку перевіряється RFID-ідентифікатор, після чого користувачеві пропонується ввести PIN-код. Лише у разі успішної перевірки обох факторів система надає доступ [2].

Важливою перевагою такої архітектури є її модульність. За потреби до системи можна додати додаткові засоби захисту: датчик стану дверей, журналювання подій у пам’ять, SD-карту або базу даних, мережевий модуль для передавання сповіщень, біометричний сканер або мобільний застосунок. Це

дозволяє розглядати Arduino-комплекс не лише як простий навчальний макет, а як основу для подальшого вдосконалення системи фізичного доступу.

Водночас необхідно враховувати обмеження обраного підходу. Arduino Uno має обмежений обсяг пам’яті та продуктивність, тому не призначений для зберігання великої бази користувачів або реалізації складних криптографічних протоколів. RFID-модуль RC522 у типовій навчальній реалізації також не забезпечує рівня захисту, характерного для промислових систем. Тому запропоноване рішення доцільно розглядати як прототип або навчально-дослідну модель, що демонструє принципи багатофакторної аутентифікації, але для критично важливих об’єктів потребує використання професійних контролерів, захищених ідентифікаторів і сертифікованих протоколів обміну [6, 7].

Окремо слід зазначити, що в сучасних рекомендаціях із кібербезпеки значна увага приділяється стійким до фішингу методам MFA, зокрема FIDO/WebAuthn та криптографічним аутентифікаторам [5]. Для систем фізичного доступу це означає загальну тенденцію до переходу від простих ідентифікаторів до більш захищених засобів перевірки користувача.

Отже, багатофакторна аутентифікація в системах фізичного доступу має низку специфічних особливостей: вона пов’язана з керуванням реальними виконавчими пристроями, потребує швидкої та зручної процедури проходу, повинна враховувати захист каналів зв’язку, журналювання подій, обмеження кількості помилкових спроб і можливість аварійного реагування. Для бакалаврської кваліфікаційної роботи доцільним є використання двофакторної моделі на основі RFID-картки та PIN-коду, оскільки вона поєднує доступність компонентів, простоту програмної реалізації та достатню наочність для демонстрації принципів підвищення безпеки систем контролю доступу [1, 2, 6].

1.3 Огляд апаратно-програмних засобів для реалізації систем контролю доступу

Системи контролю доступу належать до апаратно-програмних комплексів, у яких поєднуються електронні засоби ідентифікації користувача, пристрої обробки запиту, виконавчі механізми, програмна логіка прийняття рішень та засоби моніторингу подій. Відповідно до IEC 60839-11-1:2013, електронні системи контролю доступу застосовуються для керування фізичним доступом до будівель і захищених зон, а також охоплюють вимоги до ідентифікації, керування інформацією та журналювання подій [8].

Загальну структуру апаратно-програмних засобів системи контролю доступу доцільно подати на рисунку 1.4.

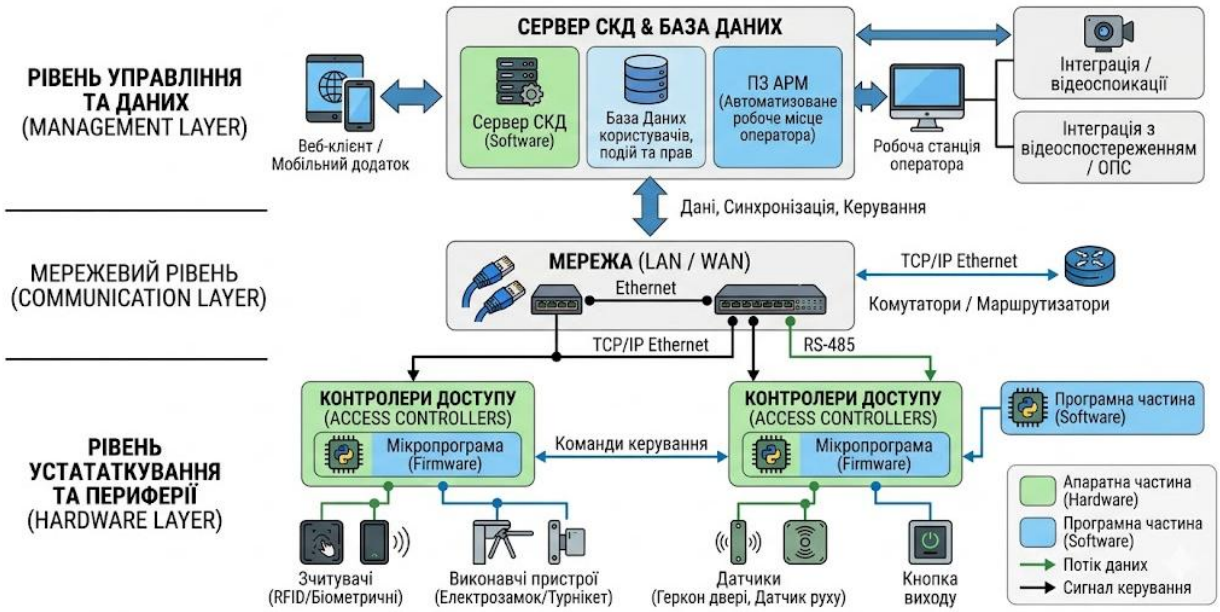

Рисунок 1.4 – Узагальнена структура апаратно-програмних засобів системи контролю доступу [8]

До апаратної частини систем контролю доступу належать зчитувачі ідентифікаторів, контролери, виконавчі пристрої, засоби індикації, датчики стану дверей, джерела живлення та комунікаційні модулі. Зчитувач виконує первинне приймання ідентифікаційних даних користувача. У сучасних системах

це можуть бути RFID- або NFC-зчитувачі, клавіатури для введення PIN-коду, біометричні сенсори, QR-сканери або мобільні ідентифікатори. Контролер доступу приймає дані від зчитувача, перевіряє їх відповідно до заданих правил і формує керуючий сигнал для виконавчого пристрою. У промислових системах такі контролери можуть бути окремими IP-пристроями, а в навчально-дослідних прототипах їхню функцію може виконувати мікроконтролерна плата.

У промислових рішеннях дедалі частіше використовуються мережеві дверні контролери, які працюють на основі IP-архітектури та дозволяють централізовано керувати точками доступу. Наприклад, Axis характеризує мережеві дверні контролери як основу сучасних IP-систем контролю доступу з відкритою архітектурою [9]. Такий підхід є ефективним для великих об’єктів, оскільки забезпечує масштабування, віддалене адміністрування, інтеграцію з відеоспостереженням і централізоване журналювання подій.

Для реалізації навчального або експериментального апаратно-програмного комплексу доцільно використовувати мікроконтролерну платформу Arduino. Arduino Uno є платою на основі ATmega328P, має 14 цифрових входів/виходів, 6 аналогових входів, USB-з’єднання, роз’єм живлення, ICSP-роз’єм і кнопку скидання [10]. Такі характеристики є достатніми для підключення RFID-зчитувача, клавіатури, дисплея, релейного модуля, світлодіодів, звукового сигналізатора та датчика стану дверей.

Одним із найпоширеніших модулів для реалізації RFID-ідентифікації в Arduino-проєктах є RC522, побудований на базі мікросхеми MFRC522. Цей модуль працює на частоті 13,56 МГц і підтримує роботу з безконтактними картками ISO/IEC 14443 A/MIFARE [11]. У системі контролю доступу RFID-модуль виконує роль засобу перевірки фактора володіння, тобто підтверджує наявність у користувача фізичного ідентифікатора - картки або брелока.

Для реалізації другого фактора аутентифікації доцільно використовувати матричну клавіатуру. Вона дає змогу користувачу вводити PIN-код, який порівнюється із заданим значенням у програмі або збереженим записом у пам’яті контролера. Arduino має окрему бібліотеку Keypad, призначену для роботи з

матричними клавіатурами [12]. Використання клавіатури дозволяє реалізувати просту двофакторну схему «RFID-картка + PIN-код», яка є придатною для навчального прототипу системи контролю доступу.

Виконавча частина системи контролю доступу зазвичай включає електромагнітний або електромеханічний замок, релейний модуль, турнікет, шлагбаум або інший пристрій блокування проходу. У прототипі на основі Arduino найпростішим рішенням є використання релейного модуля, який виконує роль проміжної ланки між низьковольтною логікою мікроконтролера та силовим колом замка. Це дозволяє безпечно керувати навантаженням, що має іншу напругу живлення, наприклад 12 В для електрозамка.

Для інформування користувача про стан системи можуть застосовуватися LCD-дисплей, світлодіоди та звуковий сигналізатор. LCD-дисплей дає змогу виводити повідомлення «очікування картки», «введіть PIN-код», «доступ дозволено», «доступ заборонено» або «помилка». Бібліотека LiquidCrystal дозволяє платам Arduino керувати LCD-дисплеями на основі чипсета Hitachi HD44780 або сумісних з ним контролерів [13]. Світлодіоди та бузер виконують допоміжну роль, забезпечуючи швидку візуальну та звукову індикацію результату аутентифікації.

Програмна частина системи контролю доступу складається з алгоритму зчитування ідентифікатора, перевірки PIN-коду, прийняття рішення щодо доступу, керування реле, індикації результату, обробки помилок і журналювання подій. У простій реалізації список дозволених RFID-ідентифікаторів і PIN-кодів може бути записаний безпосередньо в програмному коді. У складнішій версії дані можуть зберігатися в EEPROM-пам’яті мікроконтролера. Бібліотека EEPROM дає змогу читати та записувати байти у внутрішню енергонезалежну пам’ять підтримуваних мікроконтролерів Arduino [14].

Для розробки програмного забезпечення використовується Arduino IDE. Це середовище дозволяє створювати скетчі, підключати бібліотеки, компілювати програмний код, завантажувати прошивку на плату та виконувати налагодження через Serial Monitor. Arduino IDE 2 підтримує встановлення бібліотек, роботу з

платами, синхронізацію скетчів з Arduino Cloud і налагодження програм [15]. У межах розробки комплексу контролю доступу Arduino IDE є достатнім інструментом для написання та тестування програмної логіки.

Порівняльну характеристику основних апаратно-програмних засобів для реалізації системи контролю доступу наведено в таблиці 1.3.

Таблиця 1.3 – Основні апаратно-програмні засоби для реалізації систем контролю доступу

Засіб	Призначення	Приклад використання в роботі
Мікроконтролерна плата	Обробка даних, прийняття рішення, керування периферією	Arduino Uno
RFID-зчитувач	Зчитування фізичного ідентифікатора користувача	RC522 / MFRC522
Матрична клавіатура	Введення PIN-коду як другого фактора	Клавіатура 4x4 або 4x3
Релейний модуль	Комутація виконавчого пристрою	Керування електрозамком
Електрозамок	Фізичне блокування або розблокування дверей	Електромагнітний або електромеханічний замок
LCD-дисплей	Відображення повідомлень системи	LCD 16x2 з I2C-адаптером
Світлодіоди та бузер	Візуальна і звукова індикація	Дозвіл, відмова, помилка
Датчик стану дверей	Контроль відкриття або закриття дверей	Геркон або кінцевий вимикач
EEPROM-пам’ять	Збереження службових даних	Збереження UID або параметрів
Arduino IDE	Розробка та завантаження програми	Написання скетчу для Arduino

Апаратно-програмні засоби для реалізації систем контролю доступу охоплюють як промислові IP-контролери, серверні платформи та спеціалізоване програмне забезпечення, так і мікроконтролерні рішення для навчальних і прототипних систем. Для цієї роботи найбільш раціональним є використання Arduino Uno як центрального керуючого модуля, RFID RC522 як засобу ідентифікації, матричної клавіатури як другого фактора аутентифікації та релейного модуля для керування електрозамком. Такий набір апаратних і програмних засобів забезпечує достатню функціональність для створення прототипу системи контролю доступу з багатофакторною аутентифікацією.

РОЗДІЛ 2
ПРОЄКТУВАННЯ ТА РОЗРОБКА АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ

2.1 Вибір та обґрунтування компонентної бази

Вибір компонентної бази є важливим етапом розробки апаратно-програмного комплексу контролю доступу з багатофакторною аутентифікацією, оскільки саме від апаратних модулів залежать функціональні можливості системи, стабільність її роботи, простота програмування, вартість реалізації та можливість подальшого розширення. Для створення навчально-дослідного прототипу доцільно використовувати доступні мікроконтролерні компоненти, які мають достатню кількість інтерфейсів для підключення RFID-зчитувача, клавіатури, LCD-дисплея, релейного модуля, електрозамка та додаткових сенсорів.

Загальний склад апаратних компонентів, які можуть бути використані для побудови комплексу контролю доступу з багатофакторною аутентифікацією, подано на рисунку 2.1.

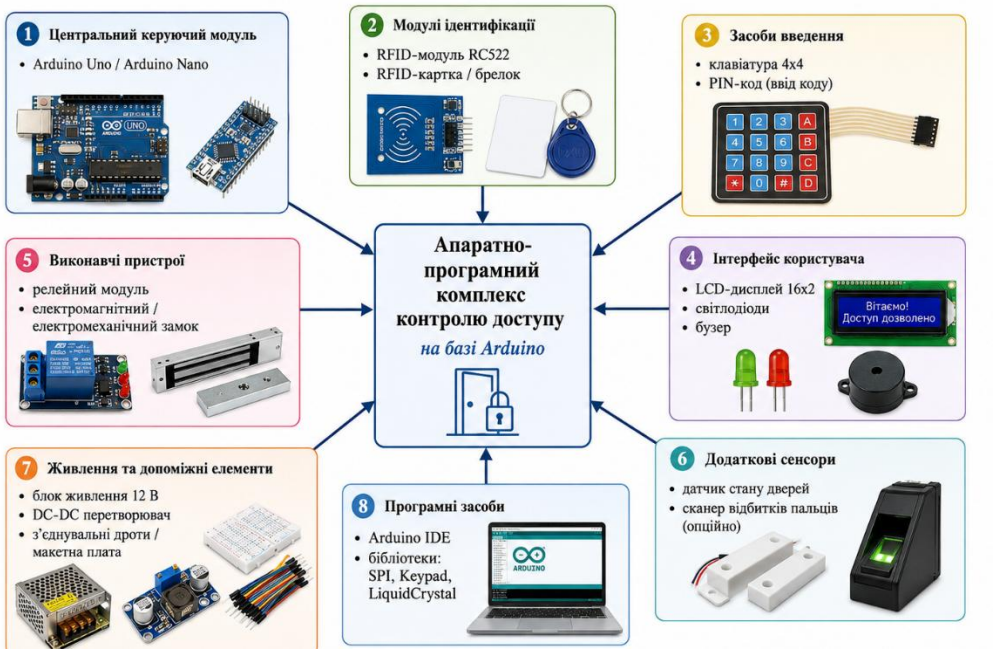

Рисунок 2.1 – Загальний склад компонентної бази апаратно-програмного комплексу контролю доступу [12]

У ролі центрального керуючого модуля доцільно обрати Arduino Uno. Ця плата побудована на базі мікроконтролера ATmega328P, має 14 цифрових входів/виходів, з яких 6 можуть використовуватися як PWM-виходи, 6 аналогових входів, USB-інтерфейс, роз'єм живлення, ICSP-роз'єм і кнопку скидання [10]. Такі характеристики є достатніми для реалізації системи контролю доступу, у якій Arduino виконує функції зчитування даних, перевірки ідентифікатора, обробки PIN-коду, керування релейним модулем та формування сигналів індикації.

Альтернативою Arduino Uno може бути Arduino Nano. Вона має компактніші габарити, тому може використовуватися у випадках, коли важливо зменшити розміри готового пристрою. Проте для навчального прототипу доцільніше застосувати саме Arduino Uno, оскільки вона зручніша для макетування, має стандартний USB-роз'єм, простіше підключається до макетної плати та краще підходить для демонстраційної реалізації комплексу [16].

Для реалізації першого фактора аутентифікації, тобто фактора володіння, обрано RFID-модуль RC522. Цей модуль побудований на базі мікросхеми MFRC522, яка є інтегрованим зчитувачем/записувачем для безконтактного зв'язку на частоті 13,56 МГц і підтримує ISO/IEC 14443 A/MIFARE та NTAG [11]. У межах розроблюваної системи RFID-картка або брелок використовується як фізичний ідентифікатор користувача. Після піднесення картки до зчитувача модуль передає її UID до Arduino через SPI-інтерфейс, після чого контролер виконує перевірку ідентифікатора.

Для реалізації другого фактора аутентифікації доцільно використати матричну клавіатуру 4x4. Вона дає змогу користувачу вводити PIN-код після успішного зчитування RFID-картки. Такий підхід дозволяє реалізувати двофакторну схему «RFID-картка + PIN-код», де RFID-картка підтверджує фактор володіння, а PIN-код - фактор знання. Для роботи з матричними клавіатурами в Arduino-проєктах може використовуватися бібліотека Keypad, яка призначена для обробки натискань у матричних клавіатурах [12].

Логіку взаємодії RFID-модуля RC522, клавіатури 4x4 та Arduino Uno у процесі двофакторної аутентифікації подано на рисунку 2.2.

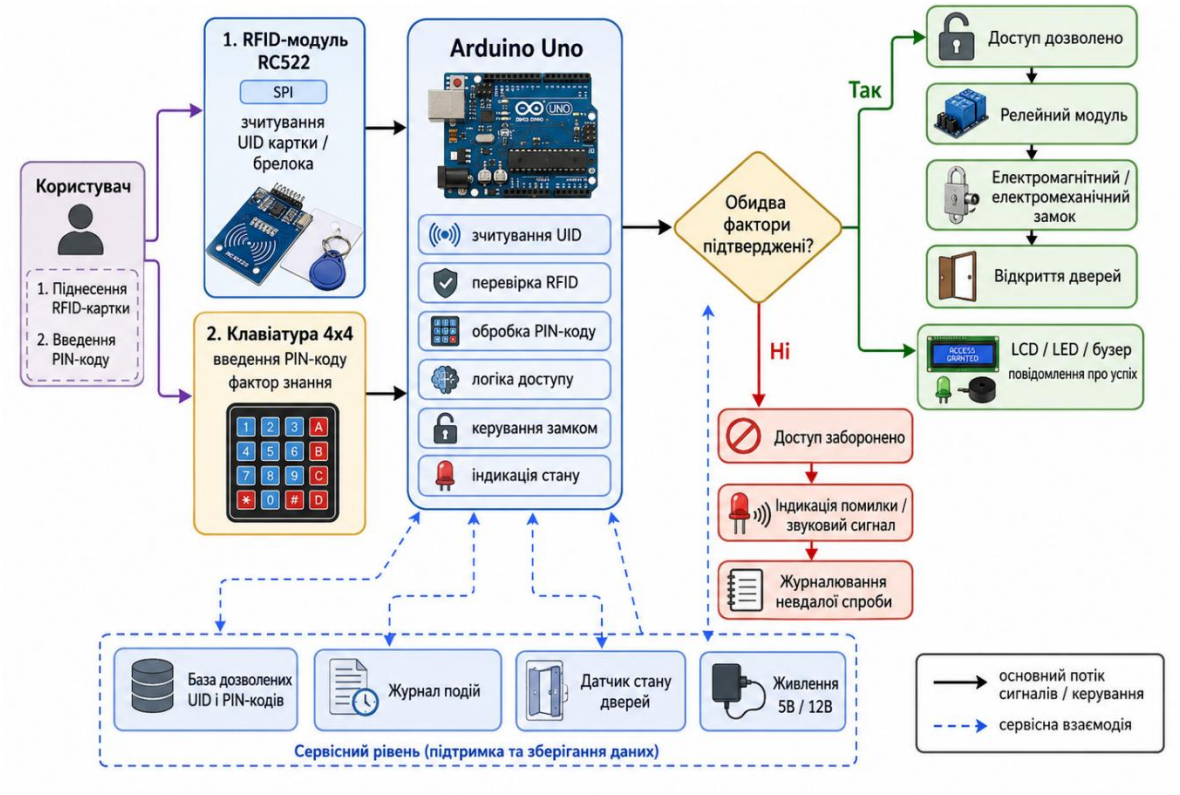

Рисунок 2.2 – Взаємодія RFID-модуля, клавіатури та Arduino Uno під час багатофакторної аутентифікації [13]

Для відображення повідомлень системи доцільно використати LCD-дисплей 16x2 з I2C-адаптером. Він дає змогу виводити службові повідомлення, наприклад «очікування картки», «введіть PIN-код», «доступ дозволено», «доступ заборонено» або «помилка». Використання I2C-адаптера зменшує кількість задіяних виводів Arduino, що є важливим у системі з кількома периферійними модулями. Бібліотека LiquidCrystal дозволяє Arduino керувати LCD-дисплеями на основі контролера Hitachi HD44780 або сумісного з ним чипсета [13].

Додатково до системи можна включити сканер відбитків пальців як третій фактор аутентифікації. Такий модуль доцільний для розширеної версії комплексу, коли потрібно підвищити рівень захисту за рахунок біометричної перевірки користувача. Проте у базовій реалізації бакалаврської роботи доцільно

обмежитися RFID-карткою та PIN-кодом, оскільки така схема є простішою, дешевшою, стабільнішою для налагодження та достатньою для демонстрації принципів багатофакторної аутентифікації [17].

Виконавчим елементом системи є електромагнітний або електромеханічний замок. Оскільки Arduino не може безпосередньо комутувати навантаження замка, між мікроконтролером і виконавчим пристроєм необхідно використати релейний модуль. Реле виконує роль електрично ізольованого комутаційного елемента: Arduino подає керуючий сигнал на реле, а реле замикає або розмикає коло живлення електрозамка. Це дозволяє безпечно поєднати низьковольтну логіку мікроконтролера з навантаженням, яке може працювати від окремого джерела живлення 12 В.

Для індикації стану системи доцільно використати світлодіоди та звуковий сигналізатор. Зелений світлодіод може повідомляти про дозвіл доступу, червоний – про відмову, а бузер – дублювати результат перевірки коротким звуковим сигналом. Такі елементи не є обов'язковими для логіки аутентифікації, однак вони суттєво підвищують зручність користування системою та полегшують процес тестування прототипу.

Узагальнену структурну схему апаратної взаємодії компонентів комплексу контролю доступу наведено на рисунку 2.3.

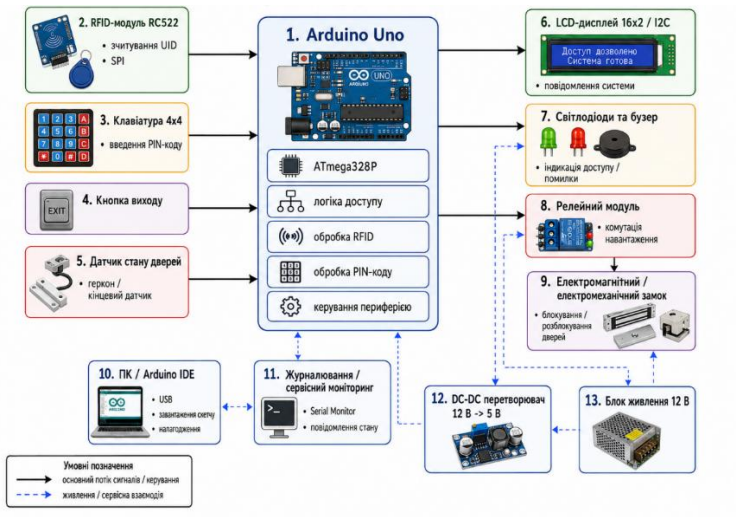

Рисунок 2.3 – Структурна схема взаємодії компонентів комплексу контролю доступу на базі Arduino

Основні компоненти обраної апаратної бази наведено в таблиці 2.1.

Таблиця 2.1 – Обґрунтування вибору компонентної бази системи контролю доступу

Компонент	Призначення	Обґрунтування вибору
Arduino Uno	Центральний керуючий модуль	Має достатню кількість цифрових і аналогових входів/виходів, підтримує USB-програмування, SPI, I2C та UART, зручна для навчального прототипування
Arduino Nano	Альтернативна компактна плата	Може застосовуватися у зменшеному корпусі, однак менш зручна для макетування порівняно з Arduino Uno
RFID RC522	Зчитування RFID-картки або брелока	Працює на частоті 13,56 МГц, підтримує картки MIFARE/ISO 14443 A, підключається до Arduino через SPI
Клавіатура 4x4	Введення PIN-коду	Дозволяє реалізувати другий фактор аутентифікації за принципом «те, що користувач знає»
LCD-дисплей 16x2 I2C	Відображення стану системи	Дає змогу виводити повідомлення для користувача та зменшує кількість задіяних виводів Arduino завдяки I2C
Релейний модуль	Керування електрозамком	Забезпечує комутацію навантаження та розділення логічної частини Arduino і силового кола замка
Електромагнітний або електромеханічний замок	Фізичне блокування дверей	Реалізує практичне надання або заборону доступу до приміщення
Світлодіоди та бузер	Візуальна і звукова індикація	Повідомляють про дозвіл, відмову або помилку аутентифікації
Датчик стану дверей	Контроль відкриття/закриття	Дає змогу контролювати фактичний стан точки проходу
Сканер відбитків пальців	Додатковий біометричний фактор	Може застосовуватися у розширеній версії системи для підвищення рівня захисту

Для реалізації апаратно-програмного комплексу контролю доступу з багатофакторною аутентифікацією обґрунтовано вибір Arduino Uno як центральної платформи, RFID-модуля RC522 як засобу ідентифікації користувача, клавіатури 4x4 як засобу введення PIN-коду, LCD-дисплея як інформаційного інтерфейсу та релейного модуля для керування електрозамком. У базовій реалізації доцільно застосувати двофакторну модель «RFID-картка + PIN-код», а сканер відбитків пальців розглядати як перспективний компонент для подальшого розширення системи.

2.2 Розробка структурної та принципової схеми пристрою

Розробка структурної та принципової схеми пристрою є одним із ключових етапів створення апаратно-програмного комплексу контролю доступу з багатофакторною аутентифікацією. На цьому етапі визначається склад основних функціональних вузлів, порядок їхньої взаємодії, типи електричних з'єднань, інтерфейси обміну даними та логіка керування виконавчими пристроями. Для проєктованого комплексу передбачено використання Arduino Uno як центрального керуючого модуля, RFID-модуля RC522 для зчитування ідентифікатора картки, клавіатури 4x4 для введення PIN-коду, LCD-дисплея для відображення повідомлень, релейного модуля для керування електрозамком, а також допоміжних засобів індикації та контролю стану дверей.

Структурна схема пристрою відображає загальну організацію апаратних компонентів і напрямки передавання сигналів між ними. Центральним елементом схеми є Arduino Uno, яка виконує функції приймання даних від RFID-зчитувача та клавіатури, перевірки двох факторів аутентифікації, формування керуючого сигналу для реле, керування індикацією та обробки подій. У цій системі RFID-картка виступає фактором володіння, а PIN-код - фактором знання. Лише після успішної перевірки обох факторів система активує релейний модуль і розблоковує електромагнітний або електромеханічний замок.

У структурній схемі можна виділити кілька основних функціональних блоків. Перший блок – модуль ідентифікації користувача, який складається з RFID-модуля RC522, RFID-картки або брелка. Його завданням є зчитування унікального UID-ідентифікатора та передавання його до Arduino через SPI-інтерфейс. Другий блок - модуль введення PIN-коду, реалізований на основі клавіатури 4x4. Він забезпечує введення другого фактора аутентифікації після успішного зчитування RFID-картки. Третій блок – центральний керуючий модуль Arduino Uno, який обробляє всі вхідні дані та приймає рішення щодо доступу. Четвертий блок – виконавча частина, до якої належать релейний модуль

і електрозамок. П’ятий блок – інтерфейс користувача, що включає LCD-дисплей, світлодіоди та звуковий сигналізатор.

Принципова схема пристрою деталізує електричні з’єднання між компонентами. Вона показує, до яких виводів Arduino підключаються окремі модулі, які напруги живлення використовуються, як організовано спільну «землю» та яким чином мікроконтролер керує виконавчим пристроєм. Оскільки RFID-модуль RC522 працює з логічним рівнем 3,3 В, його живлення необхідно підключати саме до виводу 3.3V Arduino, а не до 5V. Водночас LCD-дисплей, клавіатура, релейний модуль, бузер і світлодіоди можуть працювати від 5 В, якщо це передбачено їхніми технічними характеристиками.

Принципову схему підключення компонентів до Arduino Uno доцільно подати на рисунку 2.4.

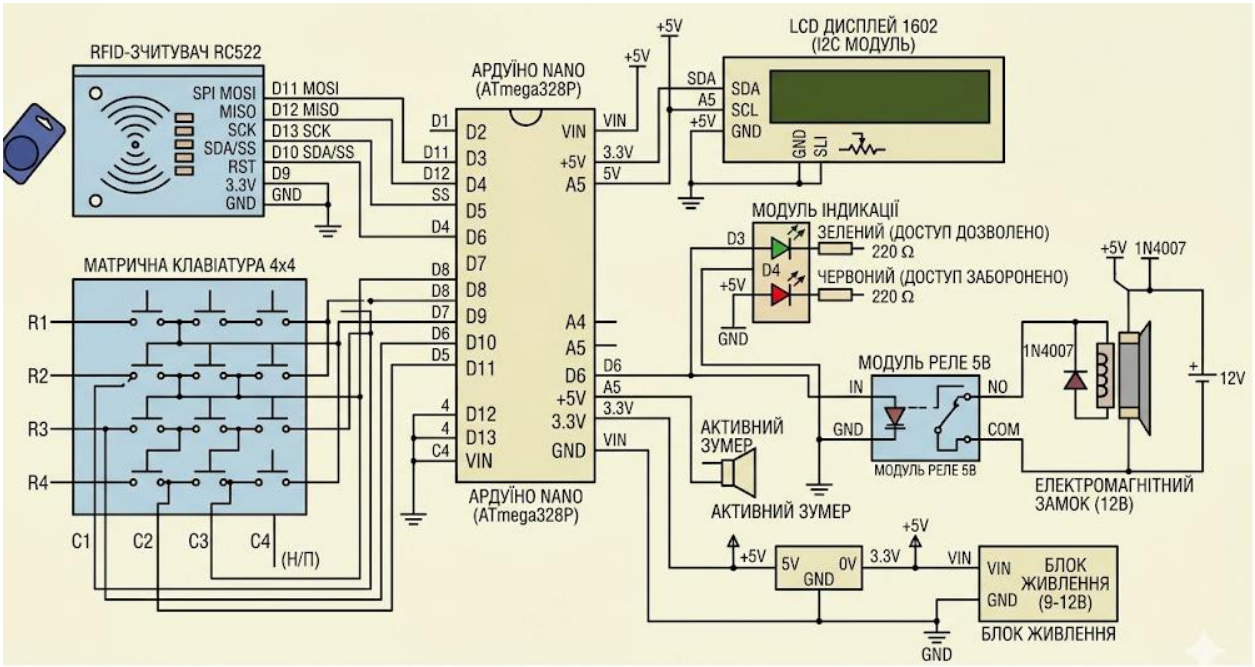

Рисунок 2.4 – Принципова схема підключення компонентів комплексу контролю доступу на базі Arduino

Для обміну даними між Arduino Uno та RFID-модулем RC522 використовується SPI-інтерфейс. Відповідно до типової схеми підключення, лінія SDA/SS модуля RC522 підключається до цифрового виводу D10 Arduino,

SCK - до D13, MOSI - до D11, MISO - до D12, RST - до D9, VCC - до 3.3V, а GND - до GND. Таке підключення відповідає особливостям роботи SPI на Arduino Uno та технічним характеристикам мікросхеми MFRC522 [10; 11].

Клавіатура 4x4 може бути підключена безпосередньо до цифрових виводів Arduino або через I2C-розширювач портів, наприклад на основі PCF8574. У цій роботі доцільно передбачити використання I2C-адаптера для клавіатури, оскільки пряме підключення клавіатури 4x4 потребує восьми виводів мікроконтролера. Використання I2C-шини дозволяє зменшити кількість зайнятих контактів і залишити більше виводів для реле, індикації, кнопки виходу та датчика стану дверей. LCD-дисплей 16x2 також може бути підключений через I2C-адаптер до ліній SDA та SCL, які на Arduino Uno відповідають аналоговим виводам A4 та A5 [13; 18].

Релейний модуль підключається до одного з цифрових виводів Arduino, наприклад D8. При успішній аутентифікації Arduino подає на цей вивід керуючий сигнал, унаслідок чого реле замикає коло живлення електрозамка. Електрозамок бажано живити від окремого джерела 12 В, оскільки Arduino не призначена для безпосереднього живлення силових виконавчих пристроїв. При цьому обов’язково потрібно забезпечити правильне з’єднання загального проводу логічної частини та модуля реле, якщо цього вимагає конкретна схема підключення.

Датчик стану дверей, наприклад геркон, може бути підключений до цифрового входу Arduino з використанням внутрішнього підтягувального резистора. Його завданням є фіксація фактичного відкриття або закриття дверей після надання доступу. Кнопка виходу підключається до окремого цифрового входу та дозволяє розблокувати двері з внутрішнього боку без використання RFID-картки та PIN-коду. Така функція є важливою для практичного використання системи, оскільки забезпечує зручний і безпечний вихід із приміщення.

Рекомендований розподіл виводів Arduino Uno для підключення компонентів комплексу наведено в таблиці 2.2.

Таблиця 2.2 – Розподіл виводів Arduino Uno для підключення компонентів пристрою

Компонент	Контакт компонента	Вивід Arduino Uno	Призначення
RFID RC522	SDA/SS	D10	Вибір пристрою SPI
RFID RC522	SCK	D13	Тактовий сигнал SPI
RFID RC522	MOSI	D11	Передавання даних від Arduino до RC522
RFID RC522	MISO	D12	Передавання даних від RC522 до Arduino
RFID RC522	RST	D9	Скидання RFID-модуля
RFID RC522	VCC	3.3V	Живлення RFID-модуля
RFID RC522	GND	GND	Загальний провід
Релейний модуль	IN	D8	Керування електрозамком
Бузер	S	D7	Звукова індикація
Зелений світлодіод	Анод через резистор	D6	Індикація дозволеного доступу
Червоний світлодіод	Анод через резистор	D5	Індикація відмови в доступі
Кнопка виходу	Signal	D4	Запит на відкриття дверей зсередини
Датчик стану дверей	Signal	D3	Контроль відкриття або закриття дверей
LCD 16x2 I2C	SDA	A4	Передавання даних по I2C
LCD 16x2 I2C	SCL	A5	Тактовий сигнал I2C
Клавіатура 4x4 через I2C	SDA	A4	Передавання даних по I2C
Клавіатура 4x4 через I2C	SCL	A5	Тактовий сигнал I2C

Як видно з таблиці 2.2, у схемі використано кілька різних типів інтерфейсів. SPI застосовується для RFID-модуля RC522, оскільки він забезпечує швидкий обмін даними між зчитувачем і мікроконтролером. I2C використовується для LCD-дисплея та клавіатури через розширювач портів, що дозволяє зменшити кількість зайнятих виводів Arduino. Цифрові виходи застосовуються для керування релейним модулем, світлодіодами та бузером, а цифрові входи - для кнопки виходу та датчика стану дверей.

Логіка роботи пристрою відповідно до структурної та принципової схеми передбачає кілька послідовних етапів. Спочатку система після ввімкнення живлення ініціалізує RFID-модуль, LCD-дисплей, клавіатуру, релейний модуль та інші периферійні пристрої. Після цього Arduino переходить у режим

очікування RFID-картки. Коли користувач підносить картку до зчитувача, система зчитує UID і порівнює його з дозволеними значеннями. Якщо UID знайдено в базі, користувачеві пропонується ввести PIN-код. Якщо PIN-код правильний, Arduino активує релейний модуль, електрозамок розблоковується на заданий час, а на LCD-дисплеї відображається повідомлення про дозвіл доступу. Якщо RFID-картка або PIN-код не підтверджені, система блокує доступ і вмикає відповідну індикацію.

Під час розробки принципової схеми важливо враховувати вимоги електробезпеки та стабільності роботи пристрою. Електрозамок повинен живитися від окремого джерела 12 В, а Arduino та логічні модулі – від стабілізованого джерела 5 В. Для захисту мікроконтролера від впливу комутаційних процесів у колі замка доцільно застосовувати релейний модуль з оптронною розв’язкою або додатковий захисний діод у колі індуктивного навантаження. Також необхідно уникати перевантаження виводів Arduino, оскільки вони призначені лише для керування логічними сигналами, а не для живлення потужних виконавчих пристроїв.

Отже, у межах розробки структурної та принципової схеми пристрою визначено основні апаратні вузли комплексу, їхнє функціональне призначення та порядок електричного підключення до Arduino Uno. Запропонована структура передбачає використання RFID-модуля RC522 як першого фактора аутентифікації, клавіатури 4x4 як другого фактора, LCD-дисплея для взаємодії з користувачем, релейного модуля для керування електрозамком, а також допоміжних елементів індикації та контролю стану дверей. Розроблена схема є придатною для подальшої програмної реалізації та експериментального тестування апаратно-програмного комплексу контролю доступу з багатофакторною аутентифікацією.

2.3 Алгоритм функціонування системи

Алгоритм функціонування апаратно-програмного комплексу контролю доступу визначає послідовність дій, які виконує система від моменту подачі живлення до прийняття рішення про надання або заборону доступу. У розроблюваному пристрої передбачено використання багатофакторної аутентифікації, де першим фактором є RFID-картка або брелок, а другим фактором - PIN-код, що вводиться користувачем за допомогою клавіатури 4x4. Такий підхід дозволяє підвищити рівень захисту порівняно з однофакторною системою, оскільки доступ надається лише за умови успішної перевірки обох факторів.

Основна логіка роботи системи полягає у послідовній перевірці факторів аутентифікації. Спочатку користувач підносить RFID-картку до зчитувача RC522. Модуль зчитує унікальний ідентифікатор картки та передає його до Arduino Uno через SPI-інтерфейс. Після цього мікроконтролер порівнює отриманий UID із переліком дозволених ідентифікаторів. Якщо картка не зареєстрована в системі, доступ одразу блокується, а користувач отримує повідомлення про відмову. Якщо RFID-картка розпізнана, система переходить до другого етапу - запиту PIN-коду.

Другий етап передбачає введення користувачем PIN-коду за допомогою матричної клавіатури 4x4. Отримана числова комбінація порівнюється з еталонним PIN-кодом, який відповідає конкретному RFID-ідентифікатору. Якщо PIN-код введено правильно, Arduino формує керуючий сигнал на релейний модуль, після чого електромагнітний або електромеханічний замок розблоковується на визначений проміжок часу. У разі неправильного PIN-коду система блокує доступ, активує червоний світлодіод, подає попереджувальний звуковий сигнал і повертається до режиму очікування.

Блок-схему взаємодії факторів аутентифікації в системі контролю доступу доцільно подати на рисунку 2.5.

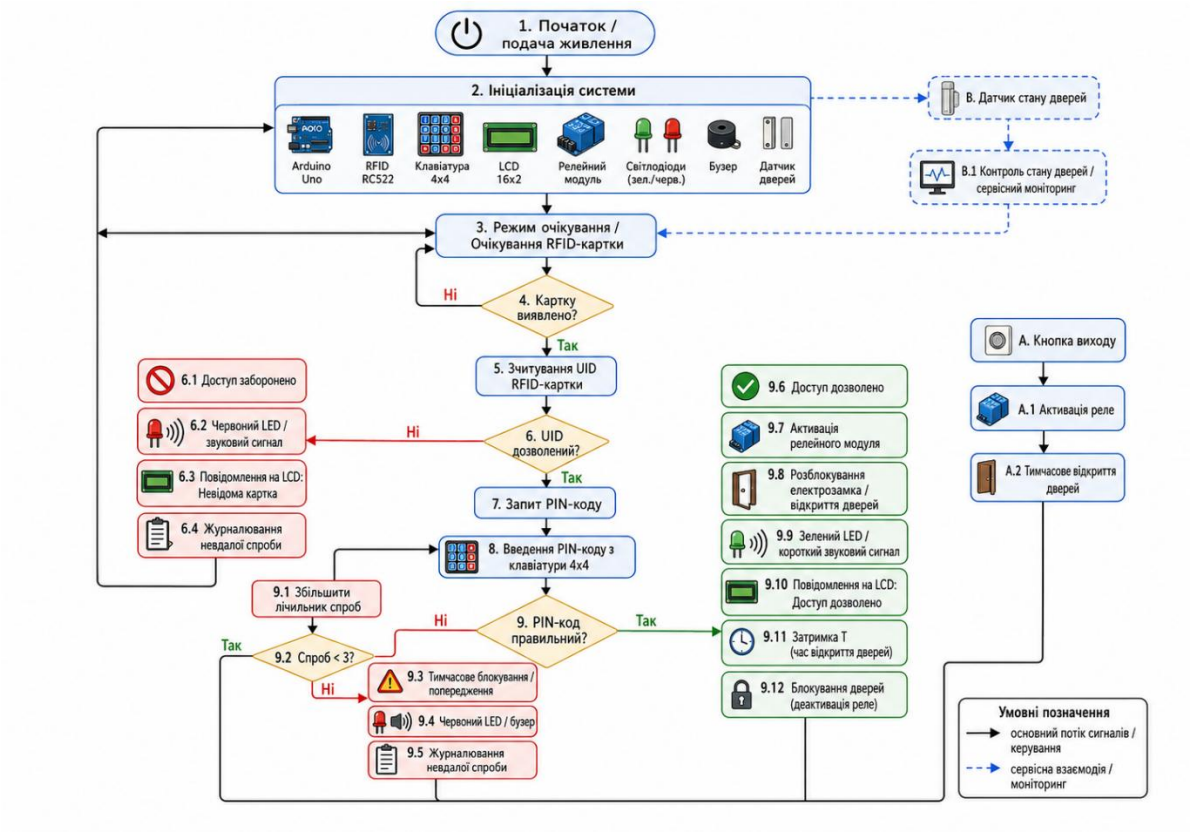

Рисунок 2.5 – Блок-схема алгоритму функціонування системи контролю доступу з багатофакторною аутентифікацією

Алгоритм роботи системи можна подати у вигляді таких основних етапів:

1. Ініціалізація системи після подачі живлення.
2. Налаштування RFID-модуля RC522, клавіатури 4x4, LCD-дисплея, релейного модуля, світлодіодів і бузера.
3. Перехід системи в режим очікування RFID-картки.
4. Зчитування UID-картки або брелока.
5. Перевірка UID у списку дозволених ідентифікаторів.
6. У разі невідповідності - відмова в доступі та індикація помилки.
7. У разі відповідності - запит PIN-коду.
8. Зчитування PIN-коду з клавіатури.
9. Порівняння введеного PIN-коду з еталонним значенням.
10. У разі правильного PIN-коду - активація реле та відкриття замка.
11. У разі неправильного PIN-коду - відмова в доступі та журналювання невдалої спроби.

12. Повернення системи до режиму очікування.

У процесі функціонування системи LCD-дисплей виконує роль інформаційного інтерфейсу користувача. На ньому можуть відображатися повідомлення «Піднесіть картку», «Введіть PIN», «Доступ дозволено», «Доступ заборонено», «Невідома картка» або «Помилка введення». Це спрощує взаємодію користувача з пристроєм і дозволяє краще контролювати поточний стан системи.

Важливим елементом алгоритму є обробка помилкових спроб. Якщо користувач вводить неправильний PIN-код, система не повинна відкривати замок навіть за умови правильного RFID-ідентифікатора. Для підвищення безпеки можна передбачити обмеження кількості невдалих спроб введення PIN-коду. Наприклад, після трьох неправильних спроб система може тимчасово заблокувати подальше введення, активувати звукову сигналізацію або записати подію у журнал. Такий механізм зменшує ризик підбору PIN-коду.

Логіку прийняття рішення у системі можна подати таким чином: доступ дозволяється лише тоді, коли перший фактор «RFID-картка» та другий фактор «PIN-код» підтверджені одночасно. Якщо хоча б один із факторів не підтверджений, доступ забороняється. Узагальнену логіку взаємодії факторів наведено в таблиці 2.3.

Таблиця 2.3 – Логіка прийняття рішення під час багатофакторної аутентифікації

RFID-картка	PIN-код	Рішення системи	Дія пристрою
Невідома	Не перевіряється	Доступ заборонено	Замок залишається заблокованим
Відома	Неправильний	Доступ заборонено	Вмикається індикація помилки
Відома	Правильний	Доступ дозволено	Активується реле та відкривається замок
Помилка зчитування	Не перевіряється	Доступ заборонено	Виводиться повідомлення про помилку

Окремо в алгоритмі може бути передбачено обробку кнопки виходу. Якщо користувач перебуває всередині приміщення, натискання кнопки виходу активує релейний модуль без проходження процедури RFID- та PIN-аутентифікації. Це

необхідно для зручного та безпечного виходу з приміщення. Також до алгоритму може бути включено перевірку датчика стану дверей. Після відкриття замка система може контролювати, чи були двері фактично відкриті та закриті після проходу користувача.

У спрощеному вигляді алгоритм функціонування системи можна описати так:

Після запуску Arduino ініціалізує всі підключені модулі та переходить у режим очікування. Коли RFID-модуль виявляє картку, система зчитує її UID і перевіряє наявність цього ідентифікатора у списку дозволених. Якщо UID не знайдено, доступ блокується. Якщо UID підтверджено, користувач вводить PIN-код. У разі правильного PIN-коду активується релейний модуль, замок розблоковується, а користувач отримує повідомлення про дозвіл доступу. Після завершення заданої затримки реле вимикається, замок знову блокується, а система повертається до режиму очікування.

Таким чином, розроблений алгоритм функціонування системи забезпечує послідовну взаємодію двох факторів аутентифікації – RFID-картки та PIN-коду. Така логіка дозволяє підвищити рівень захисту системи контролю доступу, оскільки рішення про відкриття замка приймається лише після підтвердження двох незалежних факторів. Побудована блок-схема алгоритму є основою для подальшої програмної реалізації системи на платформі Arduino Uno.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОМПЛЕКСУ КОНТРОЛЮ ДОСТУПУ

3.1 Складання апаратного прототипу комплексу контролю доступу

Практична реалізація апаратно-програмного комплексу контролю доступу передбачає поетапне складання фізичного прототипу пристрою, перевірку працездатності окремих модулів та їх об’єднання в єдину систему. На відміну від попереднього розділу, у якому було обґрунтовано вибір компонентів, розроблено структурну та принципову схему, у цьому підрозділі основна увага приділяється саме практичному монтажу, підключенню елементів, організації живлення та підготовці пристрою до програмування й тестування.

Апаратний прототип комплексу контролю доступу побудовано на основі Arduino Uno, RFID-модуля RC522, клавіатури 4x4, LCD-дисплея 16x2 з I2C-адаптером, релейного модуля, електромагнітного або електромеханічного замка, світлодіодів, звукового сигналізатора, кнопки виходу, датчика стану дверей та блока живлення. Такий склад компонентів дозволяє реалізувати повний цикл роботи системи: ідентифікацію користувача за RFID-карткою, введення PIN-коду, перевірку двох факторів аутентифікації, керування замком та індикацію результату доступу.

Перед початком складання було виконано попередню перевірку основних електронних компонентів. Зокрема, було оглянуто плату Arduino Uno, перевірено справність USB-підключення до комп’ютера, працездатність RFID-модуля RC522, клавіатури 4x4, LCD-дисплея, релейного модуля, світлодіодів і бузера. Така перевірка є необхідною, оскільки несправність навіть одного модуля може ускладнити подальше тестування всієї системи та призвести до помилкових висновків щодо роботи програмного забезпечення.

Першим етапом складання стало підключення центрального керуючого модуля – Arduino Uno. Плата була розміщена на макетній основі таким чином, щоб забезпечити зручний доступ до цифрових і аналогових виводів. Arduino Uno

виконує роль основного обчислювального вузла, який приймає сигнали від RFID-зчитувача, клавіатури, кнопки виходу та датчика стану дверей, а також керує релейним модулем, LCD-дисплеєм, світлодіодами й звуковим сигналізатором.

Наступним етапом було підключення RFID-модуля RC522. Цей модуль використовується для зчитування унікального ідентифікатора RFID-картки. Підключення здійснювалося через SPI-інтерфейс. Лінії SDA/SS, SCK, MOSI, MISO та RST були підключені до відповідних цифрових виводів Arduino Uno. Особливу увагу було приділено живленню RFID-модуля, оскільки RC522 працює від напруги 3,3 В. Підключення цього модуля до 5 В може призвести до його пошкодження, тому живлення було організовано через вивід 3.3V плати Arduino.

Після підключення RFID-модуля було встановлено клавіатуру 4x4, яка призначена для введення PIN-коду користувача. У розробленому комплексі клавіатура виконує функцію другого фактора аутентифікації. Після успішного зчитування RFID-картки користувач повинен ввести правильний PIN-код. Лише після підтвердження обох факторів система формує дозвіл на відкриття замка. Практичне підключення клавіатури виконувалося відповідно до обраної схеми – безпосередньо до цифрових входів Arduino або через I2C-розширювач портів. Використання I2C-рішення є зручним, оскільки дозволяє зменшити кількість зайнятих виводів мікроконтролера.

Важливим елементом прототипу є LCD-дисплей 16x2 з I2C-адаптером. Його встановлення дозволило реалізувати зручний інформаційний інтерфейс для користувача. На дисплеї можуть відображатися поточні стани системи: «Піднесіть картку», «Введіть PIN», «Доступ дозволено», «Доступ заборонено», «Невідома картка» або «Помилка». Підключення LCD-дисплея через I2C-шину виконувалося до ліній SDA та SCL Arduino Uno. Такий спосіб підключення є доцільним, оскільки потребує лише двох сигнальних ліній і не перевантажує цифрові виводи плати.

Загальний вигляд зібраного апаратного прототипу комплексу контролю доступу доцільно подати на рисунку 3.1.

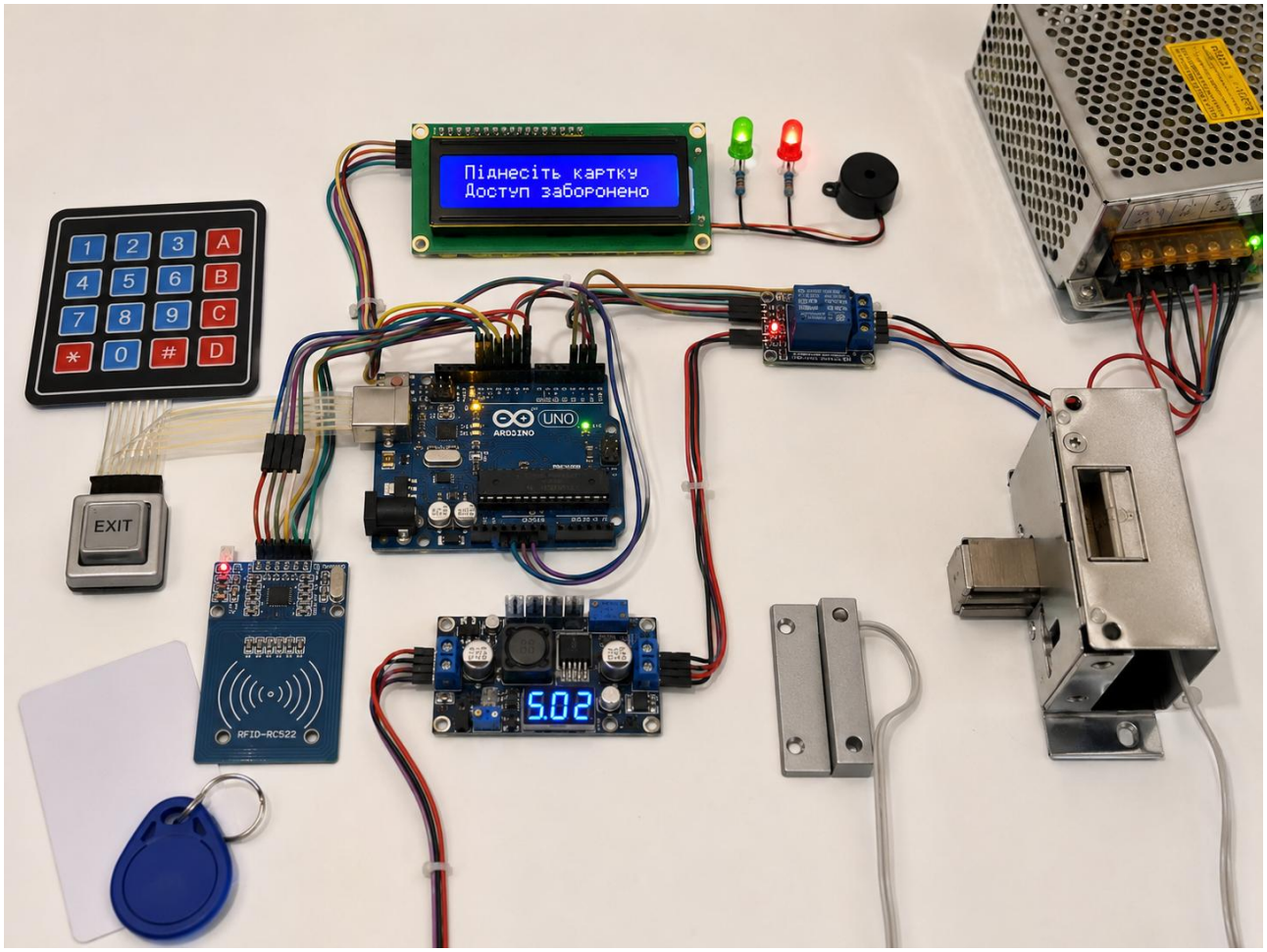

Рисунок 3.1 – Загальний вигляд апаратного прототипу комплексу контролю доступу

Окрему увагу було приділено виконавчій частині пристрою. Для керування електрозамком використано релейний модуль, який забезпечує комутацію силового кола. Arduino Uno не може безпосередньо живити або комутувати електромагнітний чи електромеханічний замок, оскільки такі пристрої зазвичай потребують вищої напруги та більшого струму. Тому релейний модуль виконує роль проміжного елемента між логічною частиною системи та виконавчим пристроєм. Керуючий вхід реле було підключено до одного з цифрових виводів Arduino, а контакти реле використано для замикання або розмикання кола живлення електрозамка.

Для інформування користувача про результат аутентифікації було підключено світлодіоди та звуковий сигналізатор. Зелений світлодіод використовується для позначення дозволеного доступу, червоний - для індикації відмови або помилки. Бузер застосовується для дублювання подій звуковим сигналом. Така індикація є важливою під час практичного тестування, оскільки дозволяє швидко визначити стан системи без обов'язкового аналізу повідомлень у Serial Monitor або на LCD-дисплеї.

До складу прототипу також включено кнопку виходу. Вона дає змогу розблокувати двері з внутрішнього боку без проходження процедури RFID- та PIN-аутентифікації. Такий елемент є типовим для реальних систем контролю доступу, оскільки забезпечує зручний і безпечний вихід із приміщення. Кнопка була підключена до цифрового входу Arduino з використанням підтягувального резистора або внутрішнього режиму INPUT_PULLUP.

Датчик стану дверей використовується для контролю фактичного відкриття та закриття точки проходу. У прототипі таким датчиком може бути геркон або кінцевий вимикач. Його сигнал дозволяє системі визначати, чи були двері відкриті після надання доступу, а також фіксувати можливі нестандартні ситуації, наприклад тривале перебування дверей у відкритому стані. У подальшому ці дані можуть використовуватися для журналювання подій або формування тривожного повідомлення.

Організація живлення апаратного прототипу є важливим етапом практичної реалізації. Логічна частина пристрою, до якої належать Arduino Uno, LCD-дисплей, клавіатура, світлодіоди та бузер, може працювати від 5 В. RFID-модуль RC522 повинен живитися від 3,3 В. Виконавча частина, зокрема електрозамок, зазвичай потребує окремого джерела живлення 12 В. Для узгодження цих напруг може застосовуватися DC-DC-перетворювач. Розділення живлення логічної та силової частин дозволяє підвищити стабільність роботи системи та зменшити ризик перезавантаження Arduino під час активації замка.

Під час складання прототипу було враховано необхідність спільного заземлення між модулями, які обмінюються логічними сигналами. Наявність

спільної лінії GND є обов’язковою умовою коректного передавання сигналів між Arduino, релейним модулем, дисплеєм, клавіатурою та іншими периферійними елементами. Водночас силове коло електрозамка повинно бути організоване таким чином, щоб не перевантажувати виводи мікроконтролера.

3.2 Розробка програмного забезпечення для Arduino

Розробка програмного забезпечення для Arduino є важливим етапом практичної реалізації апаратно-програмного комплексу контролю доступу, оскільки саме програмна частина забезпечує узгоджену роботу всіх підключених модулів, обробку даних від RFID-зчитувача, перевірку PIN-коду, керування виконавчим пристроєм та формування повідомлень для користувача. Якщо апаратна частина визначає фізичну структуру пристрою, то програмне забезпечення задає логіку його функціонування, послідовність переходів між режимами роботи та реакцію системи на правильні або помилкові дії користувача.

Програмне забезпечення розробляється в середовищі Arduino IDE, яке дає змогу створювати скетчі мовою C/C++, підключати необхідні бібліотеки, компілювати програмний код і завантажувати його на плату Arduino Uno через USB-інтерфейс. Для налагодження роботи системи використовується Serial Monitor, через який можна переглядати службові повідомлення, UID RFID-карток, результати перевірки PIN-коду та поточний стан системи. Такий підхід спрощує процес пошуку помилок і дає змогу поетапно перевіряти роботу кожного програмного модуля.

Програмна логіка комплексу контролю доступу побудована за модульним принципом. У коді можна виділити окремі функціональні блоки: ініціалізацію апаратних модулів, зчитування RFID-картки, введення PIN-коду, перевірку прав доступу, керування релейним модулем, відображення повідомлень на LCD-дисплеї, керування світлодіодами та бузером, обробку кнопки виходу і контроль стану дверей. Такий поділ полегшує подальше редагування програми, дає змогу

швидко змінювати окремі параметри та розширювати функціональність комплексу без повного переписування коду.

Загальну структуру програмного забезпечення комплексу контролю доступу доцільно подати на рисунку 3.2.

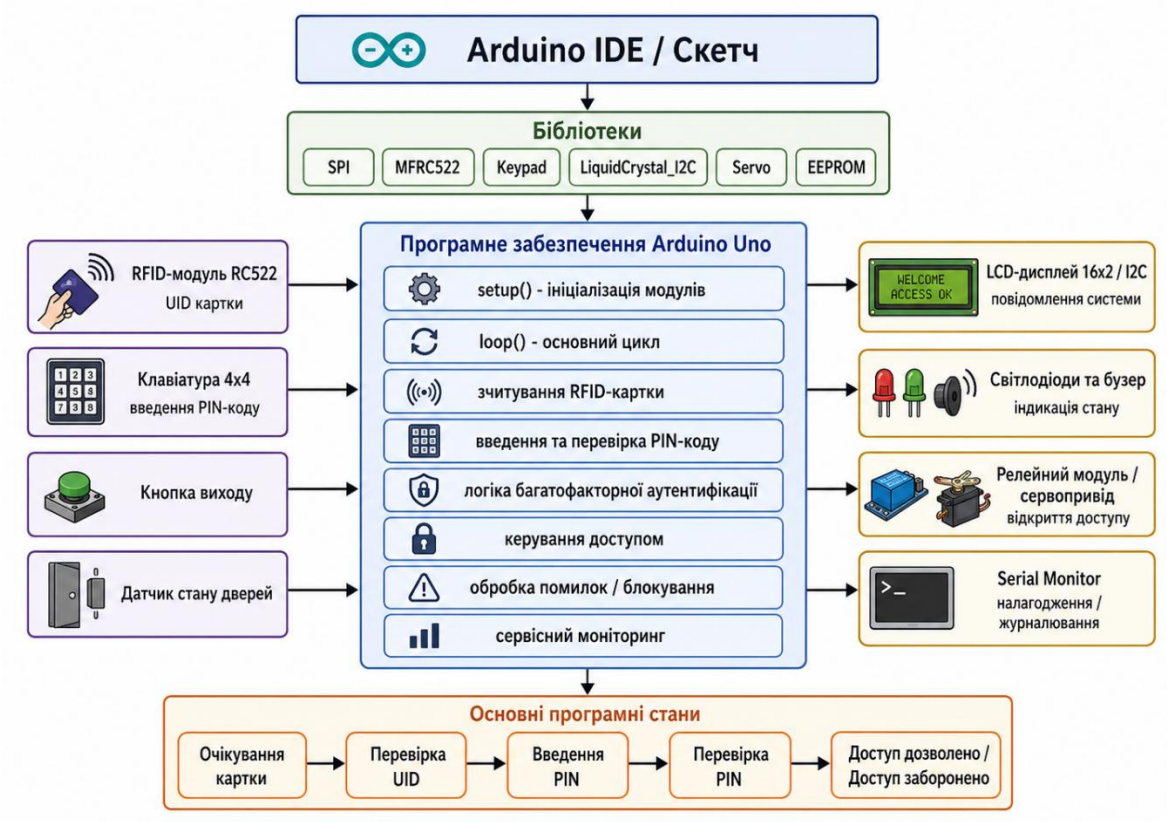

Рисунок 3.2 – Структура програмного забезпечення комплексу контролю доступу на основі Arduino

На етапі підготовки програмного коду підключаються необхідні бібліотеки. Для роботи RFID-модуля RC522 використовується бібліотека MFRC522 та SPI, оскільки обмін даними між зчитувачем і Arduino Uno здійснюється через SPI-інтерфейс. Для обробки натискань клавіатури 4x4 може застосовуватися бібліотека Keypad. Для керування LCD-дисплеєм 16x2 з I2C-адаптером використовується бібліотека LiquidCrystal_I2C або сумісна з нею бібліотека. У разі збереження UID-карток або параметрів доступу в енергонезалежній пам’яті може використовуватися бібліотека EEPROM [10-15].

Основні програмні бібліотеки, які доцільно застосувати в системі, наведено в таблиці 3.1.

Таблиця 3.1 – Програмні бібліотеки для реалізації комплексу контролю доступу

Бібліотека	Призначення	Використання в системі
SPI	Обмін даними через SPI-інтерфейс	Передавання даних між Arduino Uno та RFID-модулем RC522
MFRC522	Робота з RFID-модулем RC522	Зчитування UID RFID-картки або брелока
Keypad	Обробка матричної клавіатури	Введення PIN-коду користувача
LiquidCrystal_I2C	Керування LCD-дисплеєм	Виведення повідомлень про стан системи
EEPROM	Збереження даних у пам’яті	Збереження дозволених ідентифікаторів або параметрів
Servo	Керування сервоприводом	Використовується у випадку, якщо електрозамок моделюється сервоприводом

У програмному коді спочатку задаються константи та змінні, які відповідають за підключення апаратних компонентів. Наприклад, для RFID-модуля визначаються піни SDA/SS та RST, для релейного модуля - цифровий вихід керування, для світлодіодів - окремі виходи індикації, для бузера - пін звукового сигналу, для кнопки виходу та датчика стану дверей - цифрові входи. Також створюються змінні для зберігання UID зчитаної RFID-картки, введеного PIN-коду, кількості помилкових спроб і поточного стану системи.

Функція setup() використовується для початкової ініціалізації всіх апаратних модулів. У ній запускається послідовний порт для налагодження, ініціалізується SPI-шина, RFID-модуль RC522, LCD-дисплей, клавіатура, релейний модуль, світлодіоди та бузер. Також у цій функції задаються режими роботи цифрових виводів: для реле, світлодіодів і бузера - режим OUTPUT, для кнопки виходу та датчика стану дверей - режим INPUT або INPUT_PULLUP. Після завершення ініціалізації система виводить на дисплей повідомлення про готовність до роботи, наприклад «Піднесіть картку».

Функція loop() реалізує основний цикл роботи пристрою. У цьому циклі Arduino постійно перевіряє наявність RFID-картки, стан кнопки виходу та

сигнали від датчика стану дверей. Якщо користувач підносить RFID-картку, система зчитує її UID і порівнює з дозволеними ідентифікаторами. Якщо картка розпізнана, користувачеві пропонується ввести PIN-код. Якщо PIN-код правильний, система активує виконавчий механізм і надає доступ. Якщо хоча б один фактор не підтверджено, система відмовляє в доступі та вмикає відповідну індикацію.

Окрему увагу в програмному забезпеченні приділено реалізації перевірки RFID-картки. Після виявлення картки модуль RC522 зчитує її UID, який складається з послідовності байтів. Отриманий UID перетворюється у зручний для порівняння формат і зіставляється зі списком дозволених ідентифікаторів. Якщо значення UID збігається з одним із дозволених записів, система переходить до перевірки другого фактора. Якщо збігу немає, доступ забороняється без запиту PIN-коду.

Другий фактор аутентифікації реалізується через введення PIN-коду з клавіатури 4x4. Програма послідовно зчитує натиснуті клавіші та формує рядок введеного коду. Для завершення введення може використовуватися окрема клавіша, наприклад «#», а для очищення введених символів - клавіша «*». Після завершення введення PIN-код порівнюється з еталонним значенням, яке може бути задане в програмному коді або збережене в пам’яті мікроконтролера. Якщо код правильний, система дозволяє доступ, якщо ні - формує відмову.

Для підвищення безпеки програмно передбачено обробку помилкових спроб. Якщо користувач кілька разів вводить неправильний PIN-код, система може тимчасово заблокувати подальші спроби, подати звуковий сигнал або вивести попереджувальне повідомлення на LCD-дисплей. Такий механізм зменшує ймовірність підбору PIN-коду та підвищує надійність багатофакторної аутентифікації. У межах навчального прототипу достатньо реалізувати лічильник помилкових спроб і тимчасову затримку після досягнення встановленого порогу.

Керування виконавчим пристроєм здійснюється через релейний модуль або сервопривід залежно від практичної конфігурації прототипу. Якщо

використовується релейний модуль та електрозамок, Arduino подає логічний сигнал на вхід реле, після чого реле комутує коло живлення замка. Якщо замість електрозамка використовується сервопривід, то відкриття доступу моделюється поворотом вала сервоприводу на заданий кут, наприклад з положення 0° у положення 90°. Після завершення заданої затримки система повертає виконавчий пристрій у початковий стан.

LCD-дисплей у програмі використовується для відображення поточного стану системи. На ньому можуть з’являтися повідомлення «Піднесіть картку», «Введіть PIN», «Доступ дозволено», «Доступ заборонено», «Невідома картка», «Помилка PIN» або «Спробуйте ще раз». Такі повідомлення підвищують зручність користування пристроєм і спрощують процес тестування. Світлодіоди та бузер виконують роль додаткової індикації: зелений світлодіод сигналізує про дозвіл доступу, червоний - про помилку або відмову, а бузер дублює основні події короткими звуковими сигналами.

У програмному забезпеченні також може бути передбачено обробку кнопки виходу. Якщо така кнопка натиснута, система активує виконавчий механізм без перевірки RFID-картки та PIN-коду, оскільки ця дія виконується з внутрішнього боку приміщення. Такий режим є необхідним для практичного використання комплексу, оскільки забезпечує зручний вихід із контрольованої зони. Крім того, датчик стану дверей може використовуватися для перевірки фактичного відкриття або закриття дверей після надання доступу.

Основні програмні стани системи наведено в таблиці 3.2.

Таблиця 3.2 – Основні програмні стани комплексу контролю доступу

Стан системи	Умова переходу	Дія програми
Ініціалізація	Подача живлення або перезапуск Arduino	Налаштування модулів і виводів
Очікування RFID-картки	Завершення ініціалізації	Виведення повідомлення «Піднесіть картку»
Перевірка UID	Картку виявлено	Зчитування та порівняння UID
Введення PIN-коду	UID дозволений	Зчитування символів із клавіатури
Перевірка PIN-коду	Завершено введення PIN	Порівняння з еталонним значенням
Доступ дозволено	UID і PIN підтверджено	Активація реле або сервоприводу

Продовження таблиці 3.2

Стан системи	Умова переходу	Дія програми
Доступ заборонено	Помилка UID або PIN	Індикація відмови та повернення в режим очікування
Кнопка виходу	Натискання кнопки	Відкриття доступу з внутрішнього боку
Помилка або блокування	Перевищено кількість спроб	Тимчасова затримка або попередження

Після написання програмного коду виконується його компіляція та завантаження на плату Arduino Uno. Якщо компіляція проходить без помилок, програма передається на мікроконтролер через USB-кабель. Далі здійснюється поетапна перевірка роботи: спочатку перевіряється RFID-модуль, потім клавіатура, LCD-дисплей, індикація, реле або сервопривід, кнопка виходу та датчик стану дверей. Такий порядок дає змогу швидко виявити, чи пов’язана помилка з апаратним підключенням, чи з програмною логікою.

Під час розробки програмного забезпечення для Arduino було сформовано логіку роботи комплексу контролю доступу з багатофакторною аутентифікацією. Програма забезпечує ініціалізацію підключених модулів, зчитування RFID-картки, перевірку UID, введення та перевірку PIN-коду, керування виконавчим пристроєм, індикацію результату та обробку помилкових спроб. Розроблена програмна структура є основою для подальшого тестування комплексу, аналізу його працездатності та оцінювання ефективності реалізованої багатофакторної аутентифікації.

3.3 Реалізація алгоритму багатофакторної аутентифікації

Реалізація алгоритму багатофакторної аутентифікації є центральним етапом програмної частини комплексу контролю доступу, оскільки саме цей алгоритм визначає порядок перевірки користувача та умови надання або заборони доступу. У розробленому пристрої застосовано двофакторну модель аутентифікації, яка поєднує RFID-картку як фактор володіння та PIN-код як фактор знання. Такий підхід дає змогу підвищити рівень захисту порівняно з

однофакторною системою, оскільки для відкриття доступу користувач повинен не лише мати фізичний ідентифікатор, а й знати правильний код.

Узагальнену логіку реалізації алгоритму багатофакторної аутентифікації доцільно подати на рисунку 3.3.

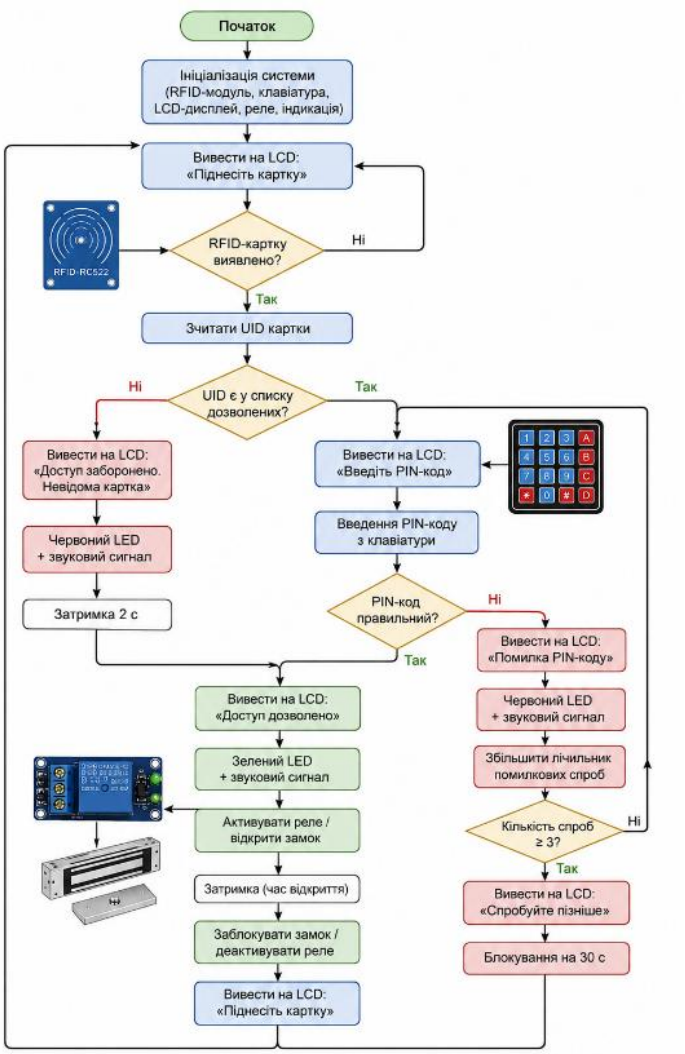

Рисунок 3.3 – Реалізація алгоритму багатофакторної аутентифікації в комплексі контролю доступу

Алгоритм реалізовано за послідовним принципом. Спочатку система очікує піднесення RFID-картки або брелока до модуля RC522. Після виявлення картки Arduino Uno зчитує її унікальний ідентифікатор UID і виконує його порівняння зі списком дозволених значень. Якщо UID не відповідає жодному запису, система одразу формує відмову в доступі, активує червоний світлодіод,

подає звуковий сигнал і виводить відповідне повідомлення на LCD-дисплей. Якщо RFID-картка є дозволеною, система переходить до другого етапу - введення PIN-коду.

На другому етапі користувач вводить PIN-код за допомогою клавіатури 4x4. Введені символи послідовно зберігаються у програмній змінній, після чого порівнюються з еталонним PIN-кодом. Для завершення введення може використовуватися клавіша «#», а для очищення помилково введених символів - клавіша «*». Така логіка є зручною для користувача та дає змогу уникнути випадкового підтвердження неповного або неправильного коду.

У програмній реалізації алгоритм працює за принципом станів. Після запуску пристрій переходить у стан очікування RFID-картки. Якщо картку виявлено, система переходить у стан перевірки UID. У разі успішної перевірки активується стан введення PIN-коду. Після введення PIN-коду виконується його перевірка. Якщо обидва фактори підтверджено, система переходить у стан дозволеного доступу. Якщо хоча б один із факторів не підтверджено, система переходить у стан відмови або помилки.

Основні стани алгоритму багатофакторної аутентифікації наведено в таблиці 3.3.

Таблиця 3.3 – Основні стани алгоритму багатофакторної аутентифікації

Стан алгоритму	Умова переходу	Дія системи
Очікування картки	Завершена ініціалізація пристрою	Виведення повідомлення «Піднесіть картку»
Зчитування UID	RFID-картку виявлено	Отримання унікального ідентифікатора картки
Перевірка RFID	UID зчитано	Порівняння UID зі списком дозволених карток
Запит PIN-коду	RFID-картка дозволена	Виведення повідомлення «Введіть PIN»
Введення PIN-коду	Натискання клавіш на клавіатурі	Формування введеного коду
Перевірка PIN-коду	Введення завершено	Порівняння PIN-коду з еталонним значенням
Доступ дозволено	UID і PIN-код правильні	Активація реле або сервоприводу, відкриття доступу
Доступ заборонено	UID або PIN-код неправильні	Індикація помилки, блокування доступу
Тимчасове блокування	Перевищено кількість помилкових спроб	Затримка роботи системи та попереджувальна індикація

Під час реалізації першого фактора аутентифікації RFID-модуль RC522 виконує зчитування UID картки. Отриманий UID може бути представлений у вигляді послідовності байтів, які в програмі перетворюються у рядковий формат для подальшого порівняння. У найпростішій реалізації дозволені UID зберігаються безпосередньо в програмному коді у вигляді масиву. У більш розширеній версії їх можна зберігати в EEPROM-пам’яті або передавати до зовнішньої бази даних, однак для навчального прототипу достатньо локального списку дозволених ідентифікаторів.

Другий фактор аутентифікації реалізовано за допомогою клавіатури 4x4. Після підтвердження RFID-картки програма очищує буфер введення та очікує послідовного натискання клавіш. Кожна натиснута клавіша додається до змінної, у якій формується PIN-код. Для підвищення зручності роботи на LCD-дисплеї може відображатися не сам код, а символи «*», що зменшує ризик візуального підглядання введеної комбінації. Після натискання клавіші підтвердження система порівнює введений код із допустимим значенням.

У разі успішної перевірки обох факторів Arduino формує сигнал керування виконавчим пристроєм. Якщо у прототипі використано релейний модуль та електрозамок, на цифровий вихід подається сигнал, який активує реле на заданий проміжок часу. Якщо в макетній реалізації замість електрозамка використано сервопривід, то доступ моделюється поворотом вала сервоприводу в положення відкриття. Після завершення затримки система повертає реле або сервопривід у початковий стан і знову переходить у режим очікування.

Окрему увагу приділено обробці помилкових спроб. Якщо RFID-картка не розпізнана, система не переходить до введення PIN-коду. Це зменшує кількість зайвих операцій і унеможливлює перевірку PIN-коду без наявності дозволеної картки. Якщо RFID-картка правильна, але PIN-код введено неправильно, система збільшує лічильник помилкових спроб. Після перевищення встановленої кількості спроб, наприклад трьох, може активуватися тимчасове блокування введення. Це зменшує ризик підбору PIN-коду та підвищує стійкість комплексу до несанкціонованого доступу.

У практичній реалізації важливо забезпечити коректне повернення системи до початкового стану після кожного сценарію. Після дозволеного доступу виконавчий пристрій повинен повернутися у заблоковане положення, індикатори мають вимкнутися або перейти до стандартного режиму, а LCD-дисплей знову повинен відобразити повідомлення «Піднесіть картку». Аналогічно після відмови в доступі система не повинна залишатися в стані помилки, а має автоматично повернутися до режиму очікування.

Для перевірки правильності реалізації алгоритму було передбачено кілька типових сценаріїв роботи: піднесення дозволеної RFID-картки та введення правильного PIN-коду; піднесення дозволеної картки та введення неправильного PIN-коду; використання невідомої RFID-картки; перевищення кількості помилкових спроб; натискання кнопки виходу. Такі сценарії дають змогу оцінити коректність роботи всіх основних гілок алгоритму та переконатися, що доступ надається лише після успішного підтвердження двох факторів.

Реалізація алгоритму багатофакторної аутентифікації в розробленому комплексі базується на послідовній перевірці RFID-картки та PIN-коду. Перший фактор підтверджує наявність у користувача фізичного ідентифікатора, а другий – знання персонального коду. Доступ надається лише за умови успішної перевірки обох факторів, що підвищує рівень захисту пристрою. Запропонований алгоритм є достатньо простим для реалізації на Arduino Uno, але водночас забезпечує базові механізми безпеки, необхідні для навчально-дослідного прототипу системи контролю доступу.

3.4 Налаштування режимів роботи системи

Налаштування режимів роботи комплексу контролю доступу є важливим етапом практичної реалізації пристрою, оскільки саме режими визначають послідовність реакцій системи на дії користувача, стан апаратних модулів та результати багатофакторної аутентифікації. У розробленому комплексі на базі Arduino передбачено кілька основних режимів: режим ініціалізації, режим

очікування RFID-картки, режим введення PIN-коду, режим дозволеного доступу, режим відмови в доступі, режим тимчасового блокування, режим виходу з приміщення та режим сервісного моніторингу.

Кожен режим має власні умови активації, набір дій і результат виконання. Такий підхід дозволяє зробити роботу системи більш передбачуваною, зручною для користувача та стійкою до помилкових або несанкціонованих дій. У програмній реалізації режими можуть задаватися за допомогою змінної стану, наприклад currentMode, яка визначає, на якому етапі роботи перебуває пристрій. Після виконання дій у певному режимі система переходить до наступного стану або повертається в режим очікування.

Загальну логіку переходів між режимами роботи комплексу подана на рисунку 3.4.

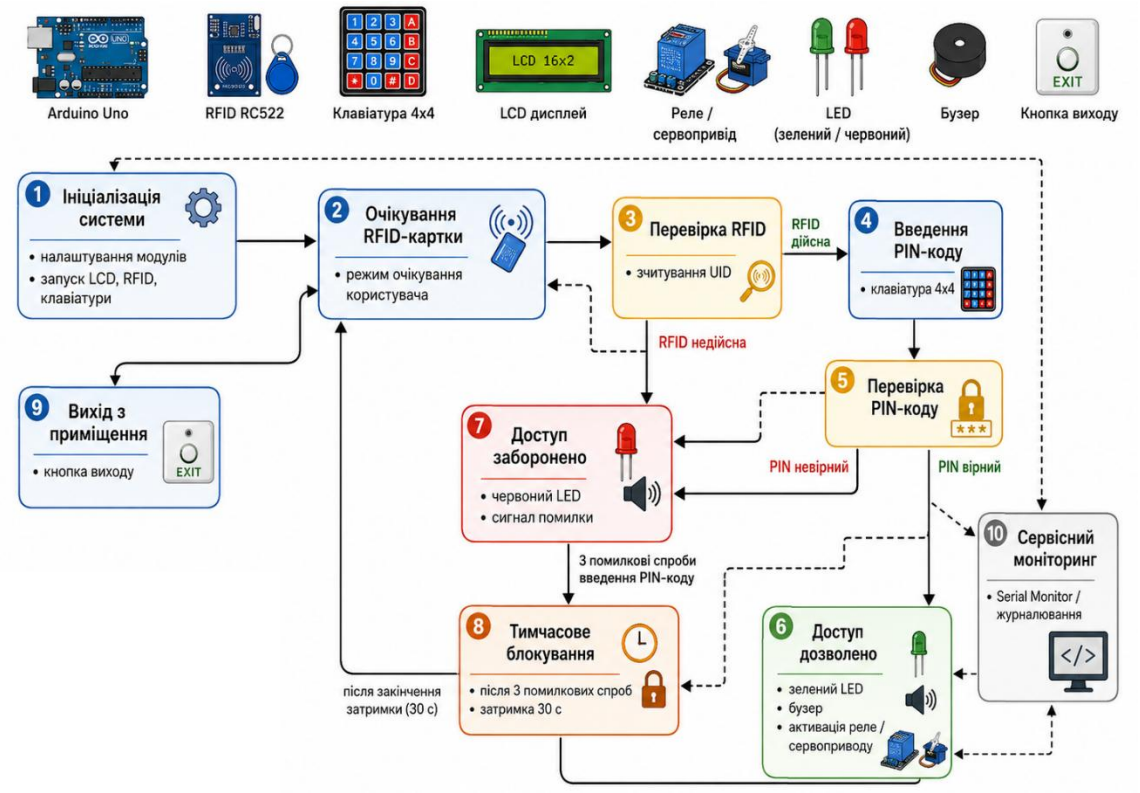

Рисунок 3.4 – Режими роботи комплексу контролю доступу на основі Arduino

Початковим режимом є режим ініціалізації. Він активується після подачі живлення на плату Arduino Uno або після перезапуску пристрою. У цьому

режимі програма виконує налаштування всіх апаратних модулів: RFID-зчитувача RC522, клавіатури 4x4, LCD-дисплея, релейного модуля, сервоприводу або електрозамка, світлодіодної індикації, бузера, кнопки виходу та датчика стану дверей. Також запускається Serial Monitor для сервісного налагодження. Після успішної ініціалізації на LCD-дисплеї відображається повідомлення «Піднесіть картку», а система переходить у режим очікування.

Режим очікування RFID-картки є основним робочим станом комплексу. У цьому режимі пристрій не виконує активних дій з відкриття доступу, а постійно перевіряє наявність RFID-картки в зоні зчитування. Arduino циклічно опитує модуль RC522 та одночасно контролює кнопку виходу і датчик стану дверей. На LCD-дисплеї відображається повідомлення, яке підказує користувачу необхідну дію. У цьому стані реле або сервопривід перебувають у положенні блокування, зелений і червоний світлодіоди вимкнені або працюють у режимі короткої службової індикації.

Після виявлення RFID-картки система переходить до режиму перевірки першого фактора. У цьому режимі зчитується UID-картки або брелока, після чого отримане значення порівнюється зі списком дозволених ідентифікаторів. Якщо UID відсутній у списку, система переходить у режим відмови в доступі. Якщо UID підтверджено, на дисплеї з’являється повідомлення «Введіть PIN», і пристрій переходить у режим введення другого фактора.

Режим введення PIN-коду призначений для перевірки фактора знання. Користувач вводить код за допомогою клавіатури 4x4, а програма послідовно зчитує натиснуті клавіші та формує введений рядок

Після завершення введення PIN-коду система переходить у режим перевірки другого фактора. У цьому режимі введений код порівнюється з еталонним значенням, яке може бути закріплене за конкретним RFID-ідентифікатором. Якщо PIN-код правильний, система переходить у режим дозволеного доступу. Якщо PIN-код неправильний, активується режим відмови або режим підрахунку помилкових спроб. Такий підхід забезпечує умову, за якої

відкриття доступу можливе лише після успішної перевірки двох незалежних факторів.

Режим дозволеного доступу активується лише у випадку, коли RFID-картка та PIN-код підтверджені. У цьому режимі Arduino подає керуючий сигнал на релейний модуль або сервопривід. Якщо використовується реле та електрозамок, відбувається розмикання або замикання відповідного кола живлення замка. Якщо у прототипі замість електрозамка використовується сервопривід, то вал сервоприводу повертається на заданий кут, імітуючи відкриття механізму доступу. Одночасно вмикається зелений світлодіод, подається короткий звуковий сигнал, а на LCD-дисплеї відображається повідомлення «Доступ дозволено».

Після завершення заданого часу відкриття система повертає виконавчий пристрій у початкове положення. Наприклад, реле вимикається, електрозамок блокується, а сервопривід повертається у закрите положення. Після цього LCD-дисплей знову відображає повідомлення «Піднесіть картку», і комплекс переходить у режим очікування. Така логіка забезпечує автоматичне повернення системи до початкового стану після кожної успішної спроби доступу.

Режим відмови в доступі активується у випадках, коли RFID-картка невідома, PIN-код введено неправильно або сталася помилка зчитування. У цьому режимі електрозамок або сервопривід не активуються, а доступ залишається заблокованим. Для інформування користувача вмикається червоний світлодіод, подається попереджувальний звуковий сигнал, а на LCD-дисплеї виводиться повідомлення «Доступ заборонено», «Невідома картка» або «Помилка PIN». Після короткої затримки система автоматично повертається в режим очікування.

Для підвищення безпеки у програмі доцільно передбачити режим тимчасового блокування. Він активується після перевищення допустимої кількості помилкових спроб введення PIN-коду. Наприклад, якщо користувач тричі поспіль вводить неправильний PIN-код після підтвердженої RFID-картки, система блокує подальші спроби на певний час, наприклад 30 секунд. У цей

період на дисплеї може відображатися повідомлення «Спробуйте пізніше», а червоний світлодіод або бузер можуть сигналізувати про блокування. Такий режим зменшує ризик підбору PIN-коду.

Окремим режимом є режим виходу з приміщення. Він активується при натисканні кнопки виходу, яка розташовується з внутрішнього боку контрольованої зони. У цьому випадку система не вимагає RFID-картки та PIN-коду, оскільки користувач уже перебуває всередині приміщення. Після натискання кнопки Arduino активує реле або сервопривід на заданий час, після чого знову блокує доступ. Такий режим є важливим для практичної експлуатації комплексу, оскільки забезпечує зручний і безпечний вихід.

Також у системі може бути передбачений режим сервісного моніторингу. У цьому режимі через Serial Monitor виводяться службові повідомлення: зчитаний UID-картки, результат перевірки PIN-коду, поточний режим роботи, кількість помилкових спроб, стан кнопки виходу та датчика дверей. Такий режим не є основним для користувача, однак він є важливим під час налагодження, тестування та перевірки стабільності роботи апаратно-програмного комплексу.

Основні режими роботи комплексу наведено в таблиці 3.4.

Таблиця 3.4 – Характеристика режимів роботи комплексу контролю доступу

Режим роботи	Умова активації	Основні дії системи	Результат
Ініціалізація	Подача живлення або перезапуск	Налаштування RFID-модуля, клавіатури, LCD-дисплея, індикації та виконавчого пристрою	Перехід у режим очікування
Очікування RFID-картки	Завершення ініціалізації	Опитування RC522, контроль кнопки виходу та датчика дверей	Очікування дії користувача
Перевірка RFID	Картку виявлено	Зчитування UID та порівняння зі списком дозволених	Перехід до PIN або відмова
Введення PIN-коду	UID дозволений	Зчитування символів із клавіатури 4x4	Формування введеного PIN-коду
Перевірка PIN-коду	PIN введено	Порівняння з еталонним кодом	Дозвіл або відмова
Доступ дозволено	UID і PIN правильні	Активація реле або сервоприводу, зелений LED, повідомлення на LCD	Відкриття доступу

Продовження таблиці 3.4

Режим роботи	Умова активації	Основні дії системи	Результат
Доступ заборонено	Невідомий UID або неправильний PIN	Червоний LED, бузер, повідомлення про помилку	Блокування доступу
Тимчасове блокування	Перевищено кількість помилкових спроб	Затримка, заборона введення, попереджувальна індикація	Захист від підбору PIN
Вихід з приміщення	Натиснуто кнопку виходу	Активація виконавчого пристрою без RFID і PIN	Відкриття зсередини
Сервісний моніторинг	Увімкнено Serial Monitor	Виведення службових повідомлень	Налагодження та тестування

Практичне налаштування режимів роботи передбачає вибір часових параметрів системи. До таких параметрів належать час відкриття доступу, тривалість звукового сигналу, час відображення повідомлення на LCD-дисплеї, кількість допустимих помилкових спроб та тривалість тимчасового блокування. Наприклад, для навчального прототипу час відкриття можна встановити на 3-5 секунд, час індикації помилки – на 1-2 секунди, а тимчасове блокування після трьох неправильних PIN-кодів – на 30 секунд.

Налаштування режимів роботи також передбачає коректне відображення повідомлень на LCD-дисплеї. Повідомлення мають бути короткими, зрозумілими та відповідати поточному стану системи. Наприклад, у режимі очікування доцільно виводити «Піднесіть картку», у режимі введення другого фактора – «Введіть PIN», у разі успішної перевірки – «Доступ дозволено», а у разі помилки – «Доступ заборонено». Це підвищує зручність використання комплексу та зменшує ймовірність неправильних дій користувача.

Налаштування режимів роботи комплексу забезпечує узгоджену взаємодію апаратної та програмної частини системи. Виділення окремих режимів дозволяє чітко описати поведінку пристрою у різних ситуаціях: під час запуску, очікування користувача, перевірки RFID-картки, введення PIN-коду, надання доступу, відмови, блокування та виходу з приміщення. Запропонована модель режимів є достатньо гнучкою для навчально-дослідного прототипу та може бути розширена шляхом додавання журналювання подій, біометричного модуля або мережевого сповіщення.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було розроблено апаратно-програмний комплекс контролю доступу з багатофакторною аутентифікацією на базі Arduino. У роботі обґрунтовано актуальність створення доступного та гнучкого рішення для автоматизації фізичного доступу до приміщень, лабораторій, навчальних стендів або інших зон з обмеженим доступом. Запропонований комплекс поєднує мікроконтролерну платформу, засоби ідентифікації користувача, виконавчий пристрій, індикацію стану та програмну логіку прийняття рішення.

Під час дослідження було проаналізовано призначення, класифікацію та основні принципи побудови сучасних систем контролю доступу. Встановлено, що такі системи є важливим елементом фізичної безпеки, оскільки забезпечують автоматизовану перевірку користувача, керування точкою проходу, зменшення залежності від механічних ключів та підвищення контрольованості подій входу і виходу. Особливу увагу приділено апаратно-програмним комплексам, у яких рішення про надання доступу приймається на основі обробки електронних ідентифікаторів і заданих правил.

У роботі розглянуто особливості використання багатофакторної аутентифікації в системах фізичного доступу. Показано, що застосування лише одного фактора, наприклад RFID-картки, не забезпечує достатнього рівня захисту, оскільки такий ідентифікатор може бути втрачений, переданий іншій особі або скопійований. Поєднання RFID-картки та PIN-коду дає змогу реалізувати двофакторну перевірку, у якій перший фактор підтверджує володіння фізичним ідентифікатором, а другий - знання персонального коду. Це підвищує надійність системи та ускладнює несанкціоноване отримання доступу.

Було обґрунтовано вибір апаратної платформи Arduino та периферійних компонентів для реалізації комплексу. Центральним керуючим модулем обрано Arduino Uno, оскільки ця плата має достатню кількість входів і виходів, підтримує роботу з поширеними інтерфейсами, легко програмується та є

зручною для створення навчально-дослідного прототипу. Для реалізації першого фактора аутентифікації використано RFID-модуль RC522, для введення другого фактора - клавіатуру 4x4, для інформування користувача - LCD-дисплей, світлодіоди та бузер, а для керування доступом - релейний модуль або сервопривід як макетний виконавчий механізм.

У процесі проєктування було розроблено структурну та функціональну схему апаратно-програмного комплексу контролю доступу. Структурна схема дала змогу визначити склад основних вузлів пристрою та зв'язки між ними, а функціональна схема - описати послідовність роботи системи від моменту зчитування RFID-картки до прийняття рішення про дозвіл або відмову в доступі. Також було сформовано принципову схему підключення компонентів до Arduino Uno, що стало основою для практичного складання апаратного прототипу.

Сформований алгоритм роботи системи передбачає послідовну перевірку двох факторів аутентифікації. Спочатку система зчитує UID RFID-картки та перевіряє його у списку дозволених ідентифікаторів. Якщо картка розпізнана, користувач вводить PIN-код з клавіатури. Доступ надається лише за умови правильного підтвердження обох факторів. Якщо RFID-картка невідома або PIN-код введено неправильно, система блокує доступ, активує індикацію помилки та повертається до режиму очікування.

У межах практичної реалізації було розроблено програмне забезпечення для мікроконтролера Arduino. Програма забезпечує ініціалізацію підключених модулів, зчитування RFID-картки, обробку введення PIN-коду, перевірку прав доступу, керування реле або сервоприводом, виведення повідомлень на LCD-дисплей, роботу світлодіодної та звукової індикації, а також обробку помилкових спроб аутентифікації. Програмна логіка побудована за модульним принципом, що спрощує налагодження та подальше розширення функціональності комплексу.

Під час тестування працездатності комплексу було перевірено основні режими роботи: очікування RFID-картки, перевірку дозволеного і невідомого ідентифікатора, введення правильного та неправильного PIN-коду, надання

доступу, відмову в доступі, роботу індикації та реакцію виконавчого пристрою. Результати тестування підтвердили коректність роботи розробленого прототипу та відповідність його функціональних можливостей поставленій меті.

В кваліфікаційній роботі досягнуто поставленої мети – розроблено апаратно-програмний комплекс контролю доступу з багатофакторною аутентифікацією на базі Arduino. Запропоноване рішення є доступним, зрозумілим для практичної реалізації, придатним для навчального використання та може бути основою для подальшого вдосконалення. У перспективі комплекс можна розширити шляхом додавання сканера відбитків пальців, модуля журналювання подій, SD-карти, мережевого модуля для віддаленого моніторингу або більш захищених методів зберігання ідентифікаторів та PIN-кодів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Digital Identity Guidelines: Authentication and Authenticator Management : NIST Special Publication 800-63B-4. *National Institute of Standards and Technology*. URL: https://pages.nist.gov/800-63-4/sp800-63b.html (дата звернення: 15.01.2026).

2. Multifactor Authentication Cheat Sheet. *OWASP Cheat Sheet Series*. URL: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html (дата звернення: 18.01.2026).

3. Authentication Cheat Sheet. *OWASP Cheat Sheet Series*. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (дата звернення: 22.01.2026).

4. Implementing Phishing-Resistant MFA. *Cybersecurity and Infrastructure Security Agency*. URL: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf (дата звернення: 27.01.2026).

5. FIDO Alliance: Free Yourself From Passwords with Passkeys. *FIDO Alliance*. URL: https://fidoalliance.org/fido-alliance-free-yourself-from-passwords-with-passkeys/ (дата звернення: 03.02.2026).

6. Babii A., Samila A. Dual Authentication Technique for RFID Access Control Systems with Increased Level of Protection. Security of Infocommunication Systems and Internet of Things. 2023. Vol. 1, No. 1. Article 01011. https://doi.org/10.31861/sisiot2023.1.01011.

7. Ramzan A., Farhan W., Malahat I., Afzal N. Double-Layered Authentication Door-Lock System Utilizing Hybrid RFID-PIN Technology for Enhanced Security. Materials Proceedings. 2025. Vol. 23, No. 1. Article 19. https://doi.org/10.3390/materproc2025023019.

8. Shetye V., Shetty A., Shetty T., Samdani K. Intelligent Door Entry: RFID-Based Authentication with Pin and Keystroke Profiling. Proceedings of International Conference on Computer Science and Communication Engineering (ICCSCE 2025). Atlantis Press, 2025. P. 1555-1570. https://doi.org/10.2991/978-94-6463-858-5_127.

9. Akshith S. P. та ін. IoT Enabled Multi Factor Authentication Lock System. Journal Information and Technology Management. 2025. Vol. 10, No. 39. https://doi.org/10.35631/JISTM.1039013.

10. Arduino UNO R3 : datasheet. *Arduino Documentation*. URL: https://docs.arduino.cc/resources/datasheets/A000066-datasheet.pdf (дата звернення: 03.03.2026).

11. Getting Started with Arduino UNO R3. *Arduino Documentation*. URL: https://docs.arduino.cc/tutorials/uno-rev3/getting-started/ (дата звернення: 07.03.2026).

12. Getting Started with Arduino IDE 2. *Arduino Documentation*. URL: https://docs.arduino.cc/software/ide-v2/tutorials/getting-started-ide-v2/ (дата звернення: 12.03.2026).

13. MFRC522. *Arduino Documentation*. URL: https://docs.arduino.cc/libraries/mfrc522/ (дата звернення: 18.03.2026).

14. SPI. *Arduino Documentation*. URL: https://docs.arduino.cc/language-reference/en/functions/communication/SPI/ (дата звернення: 24.03.2026).

15. MatrixKeypad. *Arduino Documentation*. 2024. URL: https://docs.arduino.cc/libraries/matrixkeypad/ (дата звернення: 30.03.2026).

16. LiquidCrystal_I2C. *Arduino Documentation*. URL: https://docs.arduino.cc/libraries/liquidcrystal_i2c/ (дата звернення: 05.04.2026).

17. Servo Motor Basics with Arduino. *Arduino Documentation*. URL: https://docs.arduino.cc/learn/electronics/servo-motors/ (дата звернення: 12.04.2026).

18. EEPROM Library. *Arduino Documentation*. URL: https://www.arduino.cc/en/Reference/EEPROM (дата звернення: 20.04.2026).