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 безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

СИСТЕМА КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ ARDUINO NANO

ACCESS CONTROL SYSTEM BASED ON ARDUINONANO

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Павлюк Ілля Вадимович

(підпис)

Керівник:к.ф.-м.н,
Бурбан Олександр Вікторович

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 10 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 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
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Павлюку Іллі Вадимовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Система контролю доступу на основі ARDUINO NANO*

Керівник роботи *к.ф.-м.н., Бурбан Олександр Вікторович*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

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 та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз предметної області та наявних рішень
Вибір методів та технологій для реалізації проєкту
Практична реалізація системи контролю доступу
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Існуючі рішення систем безпеки
Використання технології у проєкті
Схема електричних з'єднань системи
Інтерфейс системи контролю доступу

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз предметної області та наявних рішень	*Бурбан О.В., (керівник)*		
Вибір методів та технологій для реалізації проєкту	*Бурбан О.В., (керівник)*		
Практична реалізація системи контролю доступу	*Бурбан О.В., (керівник)*		
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 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз проблемної області на наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Вибір методів та технологій для реалізації проєкту*	до 02.03.2025 р.	Виконано
3.	*Практична реалізація системи контролю доступу*	до 02.04.2025 р.	Виконано
4.	*Висновки та загальні результати дослідження*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 15.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 30.05.2025 р.	Виконано
10.	*Інструментальна перевірка на академічний плагіат*	до 03.06.2025 р.	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ Павлюк І.В.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Бурбан О.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Павлюк І.В. Система контролю доступу на основі Arduino Nano. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

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

Перший розділ присвячено огляду предметної олбасті, тут розглядаються основні поняття про системи безпеки їх види та сфери їх використання, зокрема, як частини розумного будинку, наведено практичні приклади. Також в цьому розділі здійснено огляд систем-аналогів (ZKTeco, KONE Access, SALTO SVN, Hundure Technology).

В другому розділі здійснено вибір та обгронтування елементної бази та схемотехнічних рішень. Обрано засоби: технологію RFID, Arduino Nano. Описано складові компоненти системи.

Третій розділ присвячено опису процесам проектування та розробки системи: проектування електричної схеми у сервісі Wokwi, виготовлення пристрою та написанню керуючої програми. .

Ключові слова: Arduino Nano, система контролю доступу, RFID, система безпеки, розумний будинок.

ANNOTATION

Pavliuk I. Access control system based on Arduino Nano.

Qualifying work of a bachelor of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2024.

Qualification work consists of an introduction, three sections, conclusions, a references, appendices.

The first section is devoted to an overview of the subject area, it considers the basic concepts of security systems, their types and areas of use, in particular, as parts of a smart home, practical examples are given. This section also reviews similar systems (ZKTeco, KONE Access, SALTO SVN, Hundure Technology).

In the second section, the selection and design of the element base and circuit solutions are carried out. The means are selected: RFID technology, Arduino Nano. The components of the system are described.

The third section is devoted to the description of the design and development processes of the system: designing an electrical circuit in the Wokwi service, manufacturing the device and writing the control program.

Keywords: Arduino Nano, access control system, RFID, security system, smart home.

ЗМІСТ

ВСТУП

Потреба у забезпеченні безпеки зростає як у побуті, так і в промисловості. У зв’язку з цим широко впроваджуються автоматизовані системи контролю доступу. Вони дозволяють надійно обмежити доступ до приміщень або обладнання лише для уповноважених осіб [1]. Це підвищує рівень захисту об’єктів.

Актуальність теми. Мікроконтролери є ефективним засобом для реалізації таких систем. Вони дозволяють створювати гнучкі рішення з можливістю адаптації під конкретні умови. Також мікроконтролери легко інтегруються з іншими елементами системи і мають невисоку вартість. Сучасні мікроконтролери підтримують роботу з різними засобами ідентифікації: клавіатурами, RFID-мітками, біометричними датчиками [2, 3]. Це збільшує функціональні можливості систем контролю доступу та розширює сферу їх застосування. Отже, дослідження особливостей роботи таких систем на базі мікроконтролерів є досить важливим. Воно дозволяє підвищити їх ефективність, надійність та зручність у використанні.

Метою роботи є створення недорогої та ефективної системи контролю доступу на основі мікроконтролера.

Об’єкт дослідження – методи реалізації та використання сучасних систем безпеки.

Предмет дослідження – система контролю доступу побудована на базі мікроконтролера.

Завдання, які необхідно виконати:

– дослідити технології та методи створення сучасних систем безпеки;

– спроектувати модель електричної схеми системи контролюдоступу в симуляторі;

– реалізувати систему контролю доступу використовуючи оптимальні схемотехнічні рішення та елементну базу.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА НАЯВНИХ РІШЕНЬ

1.1 Системи безпеки їх типи та види

Сучасні системи безпеки призначені для виконання низки функціональних завдань, зокрема: підтримки безпечного стану охоронюваного об’єкта, превентивного запобігання потенційним загрозам і несанкціонованим втручанням, а також оперативної нейтралізації та ліквідації актуальних ризиків [4]. Із методологічної точки зору, сучасні системи безпеки можна інтерпретувати як інтегральні комплекси, спрямовані на забезпечення безпеки життєдіяльності суб’єктів, збереження їх майнових активів і матеріальних цінностей.

Структурно такі системи класифікуються на: індивідуальні системи безпеки призначені для житлових приміщень – будинків, квартир та комерційні системи захисту орієнтовані на охорону офісних, промислових, торгових об’єктів, територіальних зон.

Проектування систем безпеки має ґрунтуватися на принципах проактивності, що передбачає ідентифікацію та усунення загроз на докризових етапах їхнього формування [5]. Сучасні технологічні рішення інтегрують гетерогенні пристрої, сенсори, програмні інструменти та алгоритмічні механізми, що забезпечують універсальність функціоналу. Це робить можливим реалізацію практично будь-якої захисної процедури в межах єдиного комплексу [6].

Ключовою метою таких систем є антропоцентричний захист (збереження життя та здоров’я особи) та протекція матеріальних ресурсів. Високий рівень технологізації, спеціалізовані можливості (наприклад, біометрична аутентифікація, автоматизований моніторинг) сприяють їхньому масовому впровадженню в різних сферах – від приватного житла до промислових підприємств і громадської інфраструктури.

На сьогодні системи безпеки є обов’язковим компонентом інженерної інфраструктури будь-якого об’єкта, а прогнозується, що майбутнє належатиме крос-функціональним комплексам, які поєднують фізичний, кібернетичний та організаційний рівні захисту.

Сучасні системи безпеки демонструють універсальність застосування, охоплюючи різноманітні операційні контексти: житлові приміщення (квартири, приватні будинки, дачні котеджі), промислові об’єкти (заводи, фабрики, склади), комерційні структури (магазини, супермаркети, банки, ресторани), громадські установи (школи, готели, офісні центри). Незалежно від специфіки об’єкта, системи безпеки класифікуються на два концептуальних типи: комплексні (орієнтовані на багаторівневий захист) та інтегровані (здатні взаємодіяти з іншими технологічними підсистемами).

Ефективність таких систем визначається їх здатністю превентивно ідентифікувати та нівелювати загрози, зокрема: несанкціонований доступ, матеріальні втрати, акти вандалізму, порушення установлених протоколів. Оптимально спроектована система передбачає інтеграцію інженерно-технічних засобів, що забезпечують цілісний моніторинг охоронюваної зони, включаючи периметр та внутрішні простори. Ключовим функціональним імперативом є оперативна детекція зовнішніх і внутрішніх ризиків з подальшою їхньою нейтралізацією, що мінімізує ймовірність реалізації негативних сценаріїв.

З точки зору архітектури управління, системи поділяються на автономні, які функціонують із закритим контуром контролю та централізовані, які підпорядковані диспетчерським пунктам. Процес їхнього проектування базується на формалізації цілей, що враховують унікальні загрози об’єкта: від техногенних аварій (пожежі, протікання) до соціальних ризиків (крадіжки, терористичні акти) [7]. На промислових підприємствах акцент зміщується на автоматизацію робочих процесів, зокрема контроль доступу персоналу, моніторинг трудової дисципліни, запобігання витоку конфіденційних даних.

Для оптимізації витрат пропонуються модульні рішення – стандартизовані комплекси, що дозволяють швидко впровадити базовий рівень захисту. Такі

системи набувають популярності завдяки економії ресурсів, однак їх ефективність обмежена порівняно з індивідуально розробленими схемами.

Фундаментальна мета будь-якої системи безпеки – антропоцентричний захист (збереження життя та здоров'я) та збереження матеріальних активів. Це досягається через забезпечення стабільності (стійкості до тривалих зовнішніх впливів), цілісності (відсутності критичних вразливостей) та гомеостазу (здатності підтримувати функціональні параметри в умовах дестабілізуючих факторів).

Створення систем безпеки є об'єктивним наслідком потреби у забезпеченні екзистенційних інтересів суб'єктів – від окремих осіб до корпоративних структур. На макрорівні це відображає глобальні тенденції, такі як прагнення держав до стратегічної стабільності, що, зокрема, проявляється у відродженні ядерних програм як інструментів стримування. Таким чином, системи безпеки трансформуються з технічних рішень у соціотехнічні комплекси, що інтегрують технологічні, організаційні та соціальні механізми для досягнення глобальної рівноваги системи.

Фундаментальними цілями побудови системи безпеки є: превентивне запобігання виникненню загроз, захист від їх реалізації через мінімізацію потенційних втрат, а також редукція інтенсивності впливу існуючих ризиків[6]. Ключовим імперативом формування таких систем є інтегроване управління безпекою, що передбачає систематичний контроль загроз і оптимізацію механізмів їх нейтралізації.

Функціонування системи безпеки відбувається в умовах перманентного впливу дестабілізуючих факторів, як ендогенного (внутрішнього), так і екзогенного (зовнішнього) походження. Це зумовлює її стан хронічної напруги, який, однак, є нормативним для конфліктогенного середовища. Критичним аспектом є визначення порогових значень допустимого рівня конфлікту, перевищення яких ініціює перехід потенційних загроз у актуальні.

Засоби безпеки інтерпретуються як сукупність методів і процедур, спрямованих на досягнення цілей системи. Оскільки система є

багатокомпонентною, її функціональність вимагає існування спеціалізованої підсистеми – системи забезпечення безпеки. Ця підсистема виконує роль механізму розробки та імплементації концептуальних, стратегічних і тактичних рішень у сфері безпеки. Вона включає організаційні структури, нормативні протоколи та алгоритми прийняття управлінських рішень, що забезпечують адаптацію системи до динаміки зовнішніх та внутрішніх умов [5].

Відсутність такої підсистеми призводить до системних флуктуацій, які загрожують цілісності як окремих елементів, так і всієї структури. Її функціональна роль полягає у реалізації цілей безпеки через моніторинг, діагностику, ідентифікацію загроз, їх подальше запобігання, мінімізацію наслідків та відновлення стабільності.

Формування системи забезпечення безпеки ґрунтується на оптимізації організаційної структури та аналізу ефективності її елементів, розробці уніфікованого методологічного підходу і нормативно-правової бази, створенні механізмів координації взаємодії підсистем.

Окремий клас становлять електронні системи безпеки, що інтегрують програмні та апаратні рішення для підвищення рівня захисту об’єктів [8, 9]. Вони базуються на автоматизованому зборі даних із сенсорних підсистем, наприклад, охоронної сигналізації, контролю доступу, відеоспостереження. Їх аналізі оператором та оперативному реагуванні на порушення. Такі системи забезпечують високий рівень детермінованості реакцій, зменшуючи антропогенну складову у прийнятті рішень.

Охоронна сигналізація – це комплекс технічних засобів, призначений для виявлення несанкціонованого проникнення на об’єкт або в окреме приміщення, а також для передачі відповідного сповіщення користувачу або диспетчерському пункту [9]. Основне призначення охоронної сигналізації полягає в оперативному виявленні порушення охоронюваної зони, з метою попередження або мінімізації можливих збитків. Система зазвичай включає в себе датчики руху, відкриття дверей і вікон, контролери, сигнальні пристрої (сирени, світлові індикатори) та пристрої зв’язку для передавання тривожних повідомлень. У сучасних системах

часто застосовуються мережеві технології, бездротовий зв’язок, а також інтеграція з мобільними додатками та відеоспостереженням. Охоронні сигналізації можуть бути автономними або частиною комплексних систем безпеки об’єкта. Їх використання є актуальним як у приватному секторі, так і на підприємствах, в установах та державних організаціях. Надійність і ефективність охоронної сигналізації суттєво підвищують рівень захисту матеріальних цінностей і безпеки людей.

Системи контролю доступу – це сукупність технічних і програмних засобів, що забезпечують обмеження, моніторинг та управління доступом осіб до певних зон, об’єктів або інформаційних ресурсів[7,10]. Основною функцією таких систем є ідентифікація та авторизація користувачів з метою запобігання несанкціонованому проникненню або використанню ресурсів. Системи контролю доступу широко застосовуються як у фізичному середовищі – наприклад, для контролю доступу до будівель, офісів або виробничих приміщень, – так і в інформаційній сфері, де вони відповідають за безпечний доступ до комп’ютерних систем і баз даних. Технологічно такі системи можуть включати ідентифікатори у вигляді карт доступу, PIN-кодів, біометричних даних [11], а також електронні замки, зчитувачі, контролери і програмне забезпечення для адміністрування та ведення журналів подій [12,13]. Сучасні системи контролю доступу часто інтегруються з іншими засобами безпеки, зокрема з відеоспостереженням, охоронною сигналізацією та системами управління персоналом. Застосування систем контролю доступу сприяє підвищенню рівня безпеки об’єктів та оптимізації внутрішніх процесів контролю.

Системи відеоспостереження – це комплекс технічних засобів, призначений для візуального контролю та фіксації подій у певному просторі з метою забезпечення безпеки, моніторингу ситуації та документування порушень. До складу таких систем зазвичай входять відеокамери, пристрої запису, монітори, мережеве обладнання та програмне забезпечення для обробки та збереження відеоданих. Сучасні системи відеоспостереження можуть

працювати в реальному часі, підтримувати функції аналітики відеопотоку, розпізнавання облич, виявлення руху, підрахунку осіб та інших інтелектуальних алгоритмів. Відеоспостереження застосовується як у приватному секторі, так і на промислових, комерційних та громадських об’єктах для запобігання правопорушенням, розслідування інцидентів та забезпечення загального контролю за обстановкою. Завдяки розвитку цифрових технологій, мережеві відеосистеми здобули широке розповсюдження, забезпечуючи віддалений доступ до відеопотоку через інтернет, зберігання великих обсягів даних у хмарних сервісах та інтеграцію з іншими системами безпеки.

1.2 Системи контролю доступу як складова розумного удинку

Системи контролю доступу є окремою категорією систем безпеки. Залежно від контексту, їх також можна віднести до таких категорій: фізична безпека, інформаційна безпека, інженерні системи будівель, кіберфізичні системи.

Фізична безпека – коли йдеться про обмеження доступу до будівель, приміщень або зон (наприклад, замки, турнікети, карткові зчитувачі).

Інформаційна безпека – якщо йдеться про доступ до комп’ютерних систем, мереж, даних (наприклад, паролі, біометрія, двофакторна аутентифікація).

Інженерні системи будівель – як складова автоматизації будівель або систем «розумного будинку».

Кіберфізичні системи – коли система контролю доступу поєднує IT-рішення та фізичні пристрої, наприклад, мережевий замок, керований через мережу Інтернет.

Система контролю доступу є технологічним комплексом, що інтегрує апаратні засоби та програмне забезпечення для регулювання та адміністрування фізичного або логічного доступу до об’єктів різного призначення – від державних установ і медичних закладів до промислових підприємств та приватних територій. Проектування таких систем передбачає вибір оптимальної схеми ідентифікації, яка враховує специфіку рівня безпеки, бюджетні обмеження

та можливість інтеграції з іншими інженерними системами, такими як опалення, протипожежний захист, охоронні мережі. Архітектура рішення може варіюватися від локального обмеження доступу до окремих зон до масштабних комплексів із централізованим управлінням.

Ефективність системи визначається типом використовуваного обладнання, що впливає на її надійність і функціональність. Серед сучасних варіантів виділяють біометричні, мережеві та автономні системи. Біометричні платформи базуються на ідентифікації унікальних фізіологічних параметрів (відбитки пальців, структура райдужної оболонки), що усуває ризик підробки автентифікаційних даних. Незважаючи на високу точність і швидкість верифікації, такі системи мають суттєві недоліки, зокрема високу вартість впровадження та відсутність механізмів тимчасового доступу.

Мережеві системи орієнтовані на використання централізованих контролерів, інтегрованих із серверними модулями [14,15]. Їхня перевага полягає у взаємодії з підсистемами відеоспостереження або пожежної сигналізації, що дозволяє автоматизувати евакуаційні протоколи (наприклад, розблокування дверей під час надзвичайних ситуацій). Однак застосування ключ-карт створює потенційні ризики компрометації при їх втраті або крадіжці.

Автономні системи, що функціонують у локальному режимі, пропонують економічне рішення для обмеження доступу до конкретних зон. Вони керуються контролерами з вбудованою пам’яттю для зберігання кодів доступу, але не забезпечують моніторингу трудової дисципліни або журналу відвідувань. Технічні обмеження включають необхідність повного скидання даних при видаленні компрометованих ключів, що знижує гнучкість управління [15].

Таким чином, вибір типу системи контролю доступу обумовлений балансом між рівнем безпеки, бюджетними можливостями та операційними вимогами, що визначає її роль як критичного компоненту інфраструктурного захисту.

Функціональність системи контролю доступу визначається наявністю керуючого контролера, який інтегрує базу даних авторизованих користувачів,

уповноважених на переміщення через контрольовані точки об’єкта [17]. Даний модуль виконує роль центрального процесора, аналізуючи запити на активацію механізмів доступу (двері, ворота, шлагбауми) та приймаючи рішення про їхнє схвалення або блокування. Ключовим інтерфейсом взаємодії є зчитувач, призначений для отримання біометричних або цифрових даних з ідентифікаційних носіїв та їх подальшої передачі до контролера для верифікації.

Ідентифікація реалізується через спеціалізовані носії, такі як ключ-карти, RFID-браслети або проксі-брелоки, що містять унікальні коди, інтегровані з профілями користувачів. Виконавчі компоненти системи, зокрема електромеханічні замки, турнікети та автоматизовані бар’єри, активуються виключно після отримання санкції від контролера. Ці механізми функціонують у двох режимах: автоматичному (на основі програмних алгоритмів) або ручному (з участю оператора), залежно від конфігурації та рівня складності системи.

Найбільш релевантне застосування таких систем спостерігається в сегментах, де критичними є ідентифікація особи та контроль переміщень. До них належать: промислові об’єкти (виробничі цехи, складські комплекси), інституційні установи (медичні заклади, освітні організації, музеї), транспортна інфраструктура (паркінги, логістичні хаби), а також інтелектуальні середовища типу «розумного будинку». Системи забезпечують не лише фізичний захист, а й оперативний аудит усіх спроб доступу, що є ключовим для запобігання несанкціонованим діям та підвищення рівня безпеки об’єкта.Сучасна концепція інтелектуального житла базується на інтеграції сенсорів та пристроїв у єдину мережу, яка забезпечує дистанційне керування через смартфони, планшети, комп’ютери або інші гаджети. Центральним компонентом таких систем є контрольний блок, відповідальний за комунікацію між усіма підключеними пристроями, збір даних та їх передачу власнику через спеціалізовані програми. Цей блок підтримує підключення сотень пристроїв, що формує комплексну інфраструктуру автоматизації.

До ключових функціональних модулів інтелектуального житла належать системи клімат-контролю (регулювання опалення, вентиляції, освітлення та

вологості), засоби безпеки (контроль доступу, сигналізація, датчики руху, відеоспостереження з трансляцією на мобільні пристрої), динамічне освітлення (налаштування інтенсивності та кольору), управління мультимедіа (програмоване включення техніки, голосовий контроль аудіосистем) та автоматизація побутових приладів, наприклад, планування роботи пральних машин, зволожувачів тощо.

Керування системою здійснюється через спеціалізоване програмне забезпечення, доступне у вигляді мобільних додатків, десктопних програм або спеціальних панелей. Пристрої комунікують через Wi-Fi, що дозволяє користувачам керувати ними дистанційно. Наприклад, інтелектуальні розетки дають змогу активувати або деактивувати техніку на відстані. Система автономно моніторить стан кожного елемента, усуваючи потребу в постійному ручному контролі.

Важливою перевагою інтелектуального житла є оптимізація енергоспоживання. Автоматизоване регулювання освітлення, теплопостачання та водокористування зменшує витрати на комунальні послуги до 20%. Крім того, система забезпечує реальний моніторинг усіх компонентів: частина пристроїв використовує локальні радіоканали для зв’язку в межах приміщення, тоді як інші інтегровані з Інтернетом дозволяють отримувати дані з будь-якої точки світу. Наприклад, користувач може активувати бойлер або кондиціонер перед поверненням додому, забезпечуючи оптимальні умови [15].

Зростання комфорту пов’язане з усуненням необхідності фізичного взаємодії з приладами. Користувач може керувати освітленням, кранами або сигналізацією через смартфон, що особливо корисне в екстрених ситуаціях. Системи безпеки фіксують зовнішні загрози (наприклад, фіксують обличчя відвідувачів або сповіщають про незамкнені двері), а датчики газу чи води запобігають аваріям.

Незважаючи на переваги, впровадження інтелектуальних систем має обмеження. Висока вартість обладнання та складність інсталяції вимагають залучення кваліфікованих фахівців, оскільки помилки під час монтажу можуть

порушити функціональність усієї мережі. Окрім того, окремі компоненти (наприклад, кабелі для клімат-контролю чи розумного освітлення) потребують інтеграції на етапі будівництва або капітального ремонту. Це обумовлює необхідність ретельного планування ще до впровадження системи.

1.3 Приклади існуючих систем контролю доступу

На даний час існують багато методів реалізації систем контролю доступу: біометрична ідентифікація, RFID-технології, мобільна інтеграція, IP-мережі та хмарні технології.

Біометрична ідентифікація включає в себе використання біометричних даних (відбитки пальців, розпізнавання обличчя) забезпечує високий рівень безпеки. Наприклад, система Inbio інтегрує двофакторну автентифікацію: співпадіння обличчя та картки. При спробі використання чужих ідентифікаторів система блокує прохід та сповіщає охорону. Цей метод ефективний для критично важливих об’єктів, таких як серверні або лабораторії.

RFID-технології засновані на використанні Безконтактних карток або брелоків. Безконтактні картки або брелоки з мікросхемами є найпоширенішим рішенням. Наприклад, система ZKTeco ZKAccess використовує зчитувачі KR503, що передають дані через Ethernet-контролери [18]. Кожна картка має унікальний код, який зіставляється з базою даних. Для великих організацій передбачено USB-персоналізатори для масового запису карток. Ця система поєднує апаратні компоненти (електромагнітні замки, турнікети) з програмним забезпеченням для обліку робочого часу. Контролери C3-100 підключаються через Ethernet, що дозволяє розміщувати точки доступу на великих відстанях. Функція Anti-Pass Back запобігає повторному проходу через один пункт, а SDK-інструменти дозволяють інтегрувати систему з іншими платформами.

Ще одне рішення ждя систем контролю доступу це мобільна інтеграція. Сучасні системи, такі як KONE Access, дозволяють керувати доступом через смартфони [19]. Користувачі можуть викликати ліфт або відкривати двері через

додатки, інтегровані з панелями керування будівлею. Це підвищує зручність для мешканців офісних комплексів або житлових будинків. Рішення від фінської компанії KONE спеціалізується на інтеграції з ліфтами та дверима. Використовуючи зчитувачі карток біля панелей виклику ліфтів, система автоматично направляє користувачів на потрібні поверхи. Турнікети синхронізуються з програмним забезпеченням для моніторингу пасажиропотоку, що критично важливо для торгових центрів або офісних веж.

Деякі системи використовують IP-мережі та хмарні технології. Наприклад, IP-системи, такі як SALTO, забезпечують централізоване управління через інтернет [20]. Вони підтримують віддалене налаштування прав доступу, генерацію звітів у реальному часі та інтеграцію з відеоспостереженням. Наприклад, платформа SALTO SVN дозволяє об’єднувати до 100 000 пристроїв у єдину мережу. Іспанська платформа SALTO пропонує бездротові СКД з підтримкою біометрії та мобільних додатків. Система XS4 дозволяє керувати тисячами дверей через централізований інтерфейс. Ключова перевага – автономність: навіть при збоях мережі замки зберігають останні налаштування в локальній

Схожиі рішення створені компанією Belintech Ukraine. Компанія розробляє інтегровані системи з багаторівневою ідентифікацією. Їхні рішення включають шифрування даних, інтеграцію з відеоспостереженням та автоматичне блокування дверей при виявленні порушень [21]. Наприклад, при несанкціонованому доступі до серверної система активує тривогу та надсилає сповіщення на пошту адміністратора.

Також існують системи з інтеграцією HVAC та відеоспостереження. Системи керування доступом від Hundure Technology інтегруються з системами опалення, вентиляції та кондиціювання (HVAC). Наприклад, при відкритті дверей у неробочий час система автоматично вимикає кондиціонери для енергозбереження. Інтеграція з ONVIF-сумісними камерами забезпечує синхронізацію журналів подій, що покращує аналіз інцидентів.

РОЗДІЛ 2
ВИБІР МЕТОДІВ ТА ТЕХНОЛОГІЙ ДЛЯ РЕАЛІЗАЦІЇ ПРОЄКТУ

2.1 Технологія RFID

Для реалізації процесу ідентифікації користувачів буде використовуватись технологія RFID.

RFID – це один з методів автоматичного ідентифікування об’єктів, принцип якого полягає у зчитуванні або записуванні даних за допомогою радіосигналів. Дані при цьому збережені в спеціальних пристроях – RFID-мітках або транспондерах [22].

Всі RFID-системи складаються зі зчитуючого пристрою і транспондеру. Іноді RFID-мітку ще називають RFID-тегом. Усі RFID-мітки складаються із двох компонентів [23].

Перший компонент являє собою інтегральну схему, що призначена для обробки та зберігання інформації, а також для демодуляції та модуляції відповідного радіосигналу та виконання певних інших функцій. Другий компонент – це антена яка забезпечує прийом та передачу радіосигналу. Для забезпечення функціонування таких міток необхідне також відповідне програмне забезпечення. Фактично це програми, які збирають та аналізують інформацію, що одержується з RFID-міток.

RFID-мітки поділяються на два види: активні і пасивні. Мітки, що відносяться до активних мають вбудоване джерело енергії, відповідно вони мають можливість самі відсилати сигнал і можуть бути зчитані зі значної відстані. Мітки, які відносяться до пасивних не мають вбудованого джерела живлення і тому можуть активізуватись тільки після надходження сигналу від активного пристрою і тільки тоді можуть передавати поміщені в них дані.

Теги RFID складаються з двох основних компонентів: електронного чіпа для зберігання інформації про ідентичність об’єкта та власне антени, яка забезпечує спілкування чіпу з пристроями зчитування тегів. Для зв’язку тега і зчитувача тегів використовуються радіохвилі.

Областями застосування RFID-міток можуть бути системи контролю доступу або контроль часових точок у спортивних змаганнях [2]. RFID-тегами можна застосовувати навіть у фермерських господарствах, зокрема маркувати велику рогату худобу для фіксації даних про проходження певних процедур конкретними тваринами. У транспортній галузі такі рішення можуть допомагати ідентифікувати транспорт, який рухається на великій швидкості. У авіаперевезеннях використовують мітки для відстеження багажу при великих його потоках. Також RFID-чіпи вбудовані у сучасні біометричні паспорти, та сучасні кредитні картки, що забезпечує безпечний доступ до захищених областей.

Існують теги які можна зчитати на відстані декількох метрів від пристрою зчитування, якщо він знаходиться у зоні видимості. Переважна кількість тегів містять також на собі текстовий запис та штрих-код що є довненням призначеним для зчитування мітки у випадку несправності зчитуючого обладнання.

В RFID-мітці зберігається унікальний ідентифікатор який називають електронним кодом продукту (EPC) за яким і ідентифікують та відслідковують елементи в потрібних сценаріях керування. Електронний код продукту був розроблений організацією EPCglobal. Дана організація також розробляє та забезпечує підтримку стандартів, пов’язаних з технологіями RFID та EPC. Стандарти EPCglobal широко застосовуються у сфері роздрібної торгівлі, охорони здоров’я, транспортування та логістики. Також технологія RFID дуже часто використовується у пристроях інтернету речей. До корисних властивостей, що роблять цю технологію корисною для пристроїв інтернету речей можна віднести такі:

– відкритість;

– масштабованість;

– надійність;

– можливість підтримки ідентифікаторів об’єктів.

2.2 Обгрунтування вибору керуючого мікроконтролера

Для керуючого пристрою було вирішено використату платформу Arduino. Це інтерактивна платформа для створення простих і складніших електронних пристроїв. Вона включає в себе мікроконтролер (мікропроцесор), який можна програмувати для виконання різноманітних завдань, таких як керування світлодіодами, читання сенсорів, управління моторами тощо. Arduino надає простий інтерфейс для програмування, що робить його доступним навіть для початківців [24].

Одна з ключових особливостей Arduino полягає в його відкритості. Це означає, що всі документація, схеми, вихідний код програмного забезпечення та інші ресурси доступні для вільного використання та модифікації. Це сприяє швидкому розвитку та інноваціям, оскільки користувачі можуть спільно працювати над проектами, ділитися знаннями та вдосконалювати програмне та апаратне забезпечення.

Багато людей використовують Arduino для розвитку різноманітних проектів, таких як робототехніка, автоматизація побутових пристроїв, мистецтво та багато іншого. Його популярність полягає в простоті використання, доступності та широкому спектрі можливостей.

Платформа Arduino відрізняється універсальністю, що дозволяє реалізовувати широкий спектр електронних систем та пристроїв. Її конкурентні переваги включають: економічну доступність (низьку вартість порівняно з аналогами), кросплатформену сумісність (підтримка Windows, Mac OS та інших ОС, на відміну від більшості платформ, орієнтованих на моноплатформні рішення), інтуїтивне середовище розробки, оптимізоване для початківців завдяки наявності численних навчальних матеріалів, а також відкриту архітектуру. Остання передбачає можливість модифікації програмного забезпечення та апаратних компонентів, що робить платформу привабливою для просунутих розробників, які потребують кастомізації під специфічні завдання.

Ці характеристики сприяють демократизації доступу до електронного прототипування, поєднуючи простоту освоєння з гнучкістю для професійного застосування. Відкритий код та модульна структура забезпечують еволюційний потенціал платформи, дозволяючи інтегрувати сторонні бібліотеки та апаратні розширення, що відкриває шлях до створення нішевих технічних рішень.Arduino - це не лише плата, але й ціла платформа для розробки електронних проектів. Основою плат Arduino є мікроконтролери Atmel AVR та деякі інші типи мікроконтролерів. Плати мають вбудовані елементи, що спрощують процес програмування та інтеграції з іншими пристроями.

Багато плат Arduino мають вбудований лінійний стабілізатор напруги, який забезпечує стабільність живлення на рівні +5В або +3,3В. Тактовий сигнал генерується за допомогою кварцового резонатора на частоті 16 або 8 МГц.

Особливістю плат Arduino є наявність завантажувача (bootloader) у мікроконтролері, що дозволяє програмувати його без використання зовнішнього програматора. Це значно спрощує процес розробки та відладки програмного забезпечення для пристроїв на базі Arduino.

На початковому етапі в розвитку платформи Arduino для програмування використовувалася комунікація через RS-232, що є послідовним з’єднанням. Проте з розвитком технологій та відповідно до потреб ринку, новіші платформи Arduino перейшли на програмування через USB.

Завдяки використанню мікросхеми конвертера USB-to-Serial, такої як FTDI FT232R, більшість сучасних плат Arduino можуть програмуватися через USB. Наприклад, у платформі Arduino Uno в якості конвертера використовується контролер Atmega8 у SMD-корпусі, що забезпечує можливість розпізнавання платформи як миші, джойстика чи іншого пристрою, якщо це необхідно для розробки.

Проте, існують варіанти Arduino, такі як Arduino Mini або неофіційний Boarduino, де для програмування потрібно використовувати окрему плату USB-to-Serial або кабель. Це може бути зумовлено розмірами або специфічними вимогами проекту.

Отже, розвиток та різноманітність платформ Arduino дозволяють користувачам вибирати оптимальний спосіб програмування відповідно до їх потреб та умов проекту.

Плати Arduino дійсно надають можливість використовувати значну кількість виводів мікроконтролера для різноманітних цілей у зовнішніх схемах. Наприклад, у платі Decimila є доступно 14 цифрових входів/виходів, із яких 6 можуть генерувати ШІМ (широтно-імпульсну модуляцію) сигналу, а також 6 аналогових входів. Ці виводи можуть бути використані для підключення до різноманітних сенсорів, актуаторів, індикаторів та інших пристроїв.

Сигнали доступні на платі через контактні площадки або штиреві роз'єми, що робить їх легкими у використанні та підключенні до зовнішніх схем.

Крім того, існують різноманітні зовнішні плати розширення, які називаються «shields» («щити»), які можуть бути приєднані до плати Arduino через штиреві роз'єми. Ці щити можуть містити різноманітні модулі та компоненти, такі як сенсори, мотори, дисплеї, Ethernet-порти, бездротові модулі та багато іншого. Вони спрощують розширення можливостей платформи Arduino та дозволяють швидко та легко реалізувати різноманітні проекти.

Arduino та сумісні з ним плати спроєктовані таким чином, щоб їх можна було розширювати за необхідності, додаючи до пристрою нові компоненти, відомі як «shields» (плати розширення). Ці плати розширень підключаються до Ардуіно за допомогою встановлених на них спеціальних роз'ємів. Існує ряд стандартизованих плат, які дозволяють конструктивно з'єднувати процесорну плату та плати розширень в стопку через шину. Крім того, доступні плати зі зменшеним розміром (наприклад, Nano, Lilypad) і спеціальні форм-фактори для використання в робототехніці. Ця можливість розширення дозволяє створювати різноманітні пристрої з різним функціоналом на базі плат Arduino.

На ринку існує значна кількість датчиків та виконавчих пристроїв, які можуть бути використані разом із платами Arduino. Також доступні набори електромеханічних елементів, спеціально адаптованих для використання з Arduino за допомогою спеціальних драйверних плат. Саме ці елементи, такі як

двигуни та електромагніти, можуть бути інтегровані у проекти з використанням Arduino.

Порівняння плати Arduino Nano з іншими моделями, такими як Uno, Mega та Due, дозволить краще зрозуміти її переваги та особливості. Наведена нижче таблиця 2.1 містить докладну інформацію про характеристики кожної моделі, що дозволяє розглянути їх детальніше та визначити, яка з них краще підходить для виконання проєкту кваліфікаційної роботи.

Таблиця 2.1 – Порівняння характеристик плат Arduino [24]

Характеристика	Arduino Uno	Arduino Nano	Arduino Mega	Arduino Due
Мікроконтролер	ATmega328P	ATmega328P	ATmega2560	SAM3X8E
Пам’ять (флеш)	2 КБ	2 КБ	256 КБ	512 КБ
Пам’ять (SRAM)	0.5 КБ	0.5 КБ	8 КБ	4 КБ
Пам’ять (EEPROM)	1 КБ	1 КБ	512 КБ	4 КБ
Вхідні/вихідні порти	14 (6 ШІМ)	14 (6 ШІМ)	54 (15 ШІМ)	54 (12 ШІМ)
Аналогові входи	6	6	16	12
Цифрові порти	6 (5 ШІМ)	6 (5 ШІМ)	39 (9 ШІМ)	42(12 ШІМ)
ШІМ	6	6	15	12
UART	1	1	3	3
I2C	1	1	1	1
SPI	1	1	1	1
USB	1	1	1	1
Розмір плати	68 х 53 мм	43 х 25 мм	103 х 53 мм	104 х 53 мм

Порівнявши та проаналізувавши загальні характеристики різних платформ для виконання проекту було вирішено використати плату Arduino Nano. Розглянемо докладніше її характеристики.

Arduino Nano – це компактна плата, основана на мікроконтролері AtMega328. Функціонально плата схожа на Arduino Uno, але виконана в значно меншому форм факторі, незважаючи на це вона сумісна з макетними платами (рис. 2.1).

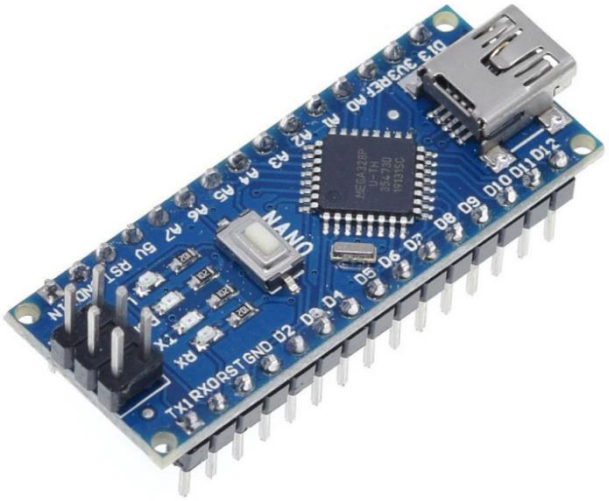

Рисунок 2.1 – Arduino Nano [25]

Для програмування використовується вбудований на платі micro-USB порт.

Характеристики плати Arduino Nano:

– мікроконтролер Atmel AtMega328;

– робоча напруга – 5В;

– вхідна напруга (рекомендована) – 7-12В;

– вхідна напруга (гранична) – 6-20В;

– цифрові входи/виходи – 14 (6 з яких можуть використовуватися як ШІМ);

– аналогові входи – 8;

– постійний ток через входи/виходи – 40мА;

– флеш память – 32кБ, 2 з яких використовуються для завантажувача;

– оперативний запам’ятовуючий пристрій – 2кБ;

– енергонезалежна память – 1кБ;

– тактова частота – 16МГц;

– розмір – 1.85х4.2 см.

Arduino Nano живиться через mini-B USB, зовнішнього живлення 6-20В(30 пін) або від стабілізованого 5В джерела живлення (27 пін). Плата автоматично підбирає джерело живлення з найбільшою напругою.

Кожен із 14 цифрових виходів, використовуючи функції pinMode(), digitalWrite(), та digitalRead(), може налаштовуватися як вхід чи вихід. Виходи працюють при напрузі 5 В. Кожен з них має резистор навантаження (стандартно відключений) 20-50 кОм і може пропускати до 40 мА.

Деякі виходи Arduino Nano мають особливі функції:

– піни послідовної шини 0 (RX) та 1 (TX) використовуються для отримання (RX) та передачі (TX) даних TTL;

– піни зовнішнього переривання 2 і 3 можуть бути налаштовані на виклик переривання або на молодшому значенні, або на передньому або задньому фронті, або при зміні значення;

– піни з доступною ШІМ 3, 5, 6, 9, 10 і 11 забезпечують ШІМ з роздільною здатністю 8 біт за допомогою функції analogWrite().

– за допомогою пінів SPI 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). здійснюється зв’язок SPI, який, хоч і підтримується апаратною частиною, але не включений у мову Arduino;

– пін LED 13 відповідає за вбудований світлодіод, підключений до цифрового виводу 13, якщо значення виводу має високий потенціал, то світлодіод світиться.

На платі Arduino Nano встановлено 8 аналогових входів, кожен роздільною здатністю 10 біт (тобто може набувати 1024 різних значення). Стандартно виходи мають діапазон виміру до 5 В щодо землі, проте є можливість змінити верхню межу за допомогою функції analogReference(). Деякі виходи мають додаткові функції:

– за допомогою пінів I2C A4 (SDA) та A5 (SCL) здійснюється зв’язок I2C (TWI);

– на пін AREF подається опорна напруга для аналогових входів, яка використовується з функцією analogReference().

– функція піну Reset полягає в наступному: низький рівень сигналу на виводі перезавантажує мікроконтролер, зазвичай використовується для

підключення кнопки перезавантаження на платі розширення, що закриває доступ до кнопки на платі Arduino.

2.3 Опис складових елементів системи

Для оптимізації електричних з’єднань було використано плату розширення Arduino Nano I/O Shield (рис. 2.2). Вона призначена для полегшення підключення зовнішніх компонентів до Arduino Nano. Плата розширення слугує проміжною ланкою між мікроконтролером та периферійними пристроями, забезпечуючи зручний доступ до виводів цифрового та аналогового введення/виведення. Завдяки оптимізованому розміщенню контактів користувач отримує можливість швидкого з’єднання сенсорів, сервоприводів, модулів зв’язку та інших електронних елементів без потреби у пайці або використанні макетної плати. Крім того, плата включає стандартні роз’єми, такі як роз’єми типу Grove, що сприяє швидкому прототипуванню та інтеграції у навчальних або експериментальних проєктах.

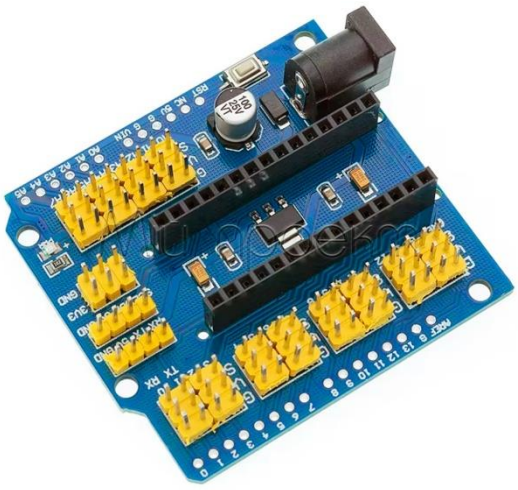

Рисунок 2.2 – Arduino Nano I/O Shield [26]

Конструкція Arduino Nano I/O Shield передбачає підключення мікроконтролера Arduino Nano у відповідне гніздо, після чого всі його пінові виводи виводяться на окремі клеми або роз’єми, позначені відповідно до

нумерації плати Arduino. Додатково плата може містити роз’єми живлення, кнопки керування, світлодіоди індикації та інші допоміжні елементи, що розширюють функціональність базової плати. Це забезпечує не лише зручність під час налагодження схем, а й підвищує стабільність підключень у порівнянні з традиційними макетними рішеннями.

Для реалізації можливості використання цифрових паролів було вибрано матрична клавіатуру для Arduino (рис. 2.3).

HC-SR501 використовується в системах «розумного будинку» для автоматизації освітлення, в охоронних сигналізаціях, а також у проектах, де потрібна активація пристроїв при присутності людини. Наприклад, він може керувати вентиляцією у ванній кімнаті або активувати камеру спостереження при проникненні до приміщення.

Рисунок 2.3 – Матрична клавіатура для Arduino [27]

Матрична клавіатура – це пристрій введення даних, який використовує матричну структуру для зменшення кількості займаних GPIO-пінів мікроконтролера. Вона складається з кнопок, організованих у вигляді рядів і стовпців, що утворюють електричну сітку. Така конструкція дозволяє підключати велику кількість кнопок, використовуючи мінімальну кількість

портів. Наприклад, клавіатура 4×4 потребує 8 пінів (4 для рядків, 4 для стовпців) для керування 16 кнопками.

Функціонування матричної клавіатури ґрунтується на методі послідовного сканування рядків і стовпців. Рядки підключаються до цифрових виходів мікроконтролера, а стовпці – до входів з підтягуючими резисторами, які забезпечують високий рівень сигналу (HIGH) у стані спокою. Процес сканування включає два етапи.

По-перше, мікроконтролер перемикає кожен рядок у стан LOW, послідовно активуючи їх. По-друге, система аналізує рівень напруги на стовпцях. Якщо кнопка на перетині активованого рядка та стовпця натиснута, стовпець отримує низький рівень сигналу (LOW). Комбінація активного рядка та стовпця з LOW-сигналом дозволяє визначити координати натиснутої кнопки. Для усунення ефекту дрижання контактів, спричиненого механічними коливаннями, застосовуються програмні методи. До таких методів можна віднести, наприклад, введення затримки 10-50 мс. Або апаратні фільтри, такі як RC-кола.

Розмір матриці визначається кількістю рядків і стовпців. Найпоширеніші конфігурації – 3×4 (12 кнопок) та 4×4 (16 кнопок). Для платформи Arduino Uno, яка має 14 цифрових пінів, клавіатура 4×4 є оптимальною через баланс між кількістю кнопок і використанням ресурсів.

Тип кнопок впливає на довговічність і тактильний відгук. Мембранні клавіатури, виготовлені з гнучких матеріалів, відрізняються низькою вартістю та стійкістю до вологості, проте мають обмежений термін служби. Механічні кнопки забезпечують точний відгук і високу надійність, але потребують додаткового простору для монтажу.

Напруга живлення матричних клавіатур зазвичай становить 3.3-5 В, що відповідає робочим параметрам більшості мікроконтролерів, включаючи Arduino. Підключення здійснюється безпосередньо до GPIO-пінів через дроти або роз’єми. Для спрощення інтеграції можна використовувати спеціалізовані

шилди, такі як Keypad Shield, які поєднують клавіатуру з додатковими компонентами, наприклад, LCD-дисплеєм.

Програмне забезпечення для роботи з матричною клавіатурою базується на бібліотеках, таких як Keypad.h для Arduino IDE. Ці бібліотеки автоматизують процеси сканування, обробки сигналів та перетворення їх у символи. Приклад реалізації включає визначення мапи кнопок, налаштування пінів для рядків і стовпців, а також функцію постійного моніторингу стану клавіатури.

Швидкість сканування матриці зазвичай становить 10-100 мс. Цей параметр визначає частоту оновлення стану кнопок і повинен бути оптимізований для уникнення пропусків натискань або затримок у відгуку системи.

В якості екрана вибрано LCD - дисплей 1602 з модулем шини I2C/IIC (рис. 2.4). Дисплей Arduino 1602 може показувати інформацію в 16 символах, які розміщуються на два рядки.

Рисунок 2.4 – Рідкокристалічний дисплей LCD1602 [28]

Під час підключення графічного дисплея використовується модуль I2C, який дуже сильно спрощує підключення і водночас використовує тільки 4 піна для під’єднання. Два використовуються для живлення і два для передавання даних.

Параметри LCD - дисплея 1602:

– LCD-контролер: HD44780;

– 16 символів;

– 2 рядки;

– напруга живлення: 5 В;

– висота 36 мм;

– ширина 80 мм.

У якості сканера RFID-міток було вибрано RFID-модуль RC522 (рис.2.5).

Рисунок 2.5 – RFID-модуль RC52 [29]

Він є компактним радіочастотним зчитувачем, який працює на частоті 13,56 МГц і призначений для безконтактної ідентифікації об’єктів за допомогою радіочастотної технології. Він реалізує протокол ISO/IEC 14443 типу A і підтримує роботу з картками, брелоками та мітками стандарту MIFARE. Модуль RC522 часто використовується у проєктах на базі Arduino завдяки своїй доступності, низькому енергоспоживанню та простоті інтеграції.

Основними елементами модуля є мікросхема MFRC522, антена у вигляді спіралі на платі, а також набір контактів для підключення до мікроконтролера через інтерфейс SPI. Також можливе використання I²C або UART, хоча SPI є найпоширенішим способом зв’язку через його високу швидкість. Живлення модуля здійснюється від джерела 3,3 В, а логічні рівні також відповідають цьому стандарту, що вимагає використання понижуючих перетворювачів при підключенні до Arduino, яке працює на 5 В.

Принцип дії модуля полягає в генерації електромагнітного поля, яке активує RFID-мітку, що потрапляє в зону дії антени. Після цього відбувається обмін даними між міткою та зчитувачем, під час якого мікроконтролер отримує унікальний ідентифікаційний код або інші збережені на мітці дані. RC522 забезпечує надійне зчитування інформації на відстані до 5 см, що залежить від типу мітки та умов навколишнього середовища.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1 Проектування електричної схеми пристрою

Для проектування електричної схеми пристрою та подальшої симуляції роботи пристрою було використано сервіс Wokwi. Це сучасна онлайн-платформа, яка дозволяє моделювати та симулювати електронні проєкти прямо у веббраузері. Вона добре підходить для розробки та тестування схем на базі Arduino, ESP32, Raspberry Pi Pico та інших популярних мікроконтролерів [30].

Використовуючи даний сервіс користувач може створити електронну схему, додати необхідні компоненти, написати програму на мові Arduino (C++) та одразу побачити, як система буде працювати без використання фізичного обладнання.

Сервіс підтримує найпоширеніші компоненти: датчики температури і вологості, такі як DHT22, LCD-дисплеї з інтерфейсом I2C, кнопки, світлодіоди, реле, серводвигуни та інше. Також можлива симуляція обміну даними через I2C, SPI та UART, що відкриває шлях до створення складніших систем.

Окрім моделювання з’єднань, Wokwi має низку корисних можливостей:

– симуляція роботи у реальному часі;

– можливість налагодження;

– гнучке налаштування;

– автоматичне підключення бібліотек вказаних у коді програми;

– збереження і спільна робота.

Особливістю цього сервісу є наявність файлу diagram.json в якому описуються всі графічні елементи та з’єднання. Саме згідно цього файлу формуються візуальне представлення та електричні з’єднання симульованої схеми. Даний файл автоматично формується при створенні візуальної схеми методом «Drag-and-drop». Цей файл також можна редагувати в текстовому режимі. Вміст файлу diagram.json для спроектованої схеми подано у Додатку В.

Електрична схема зібрана у сервісі Wokwi зображена на рисунку 3.1.

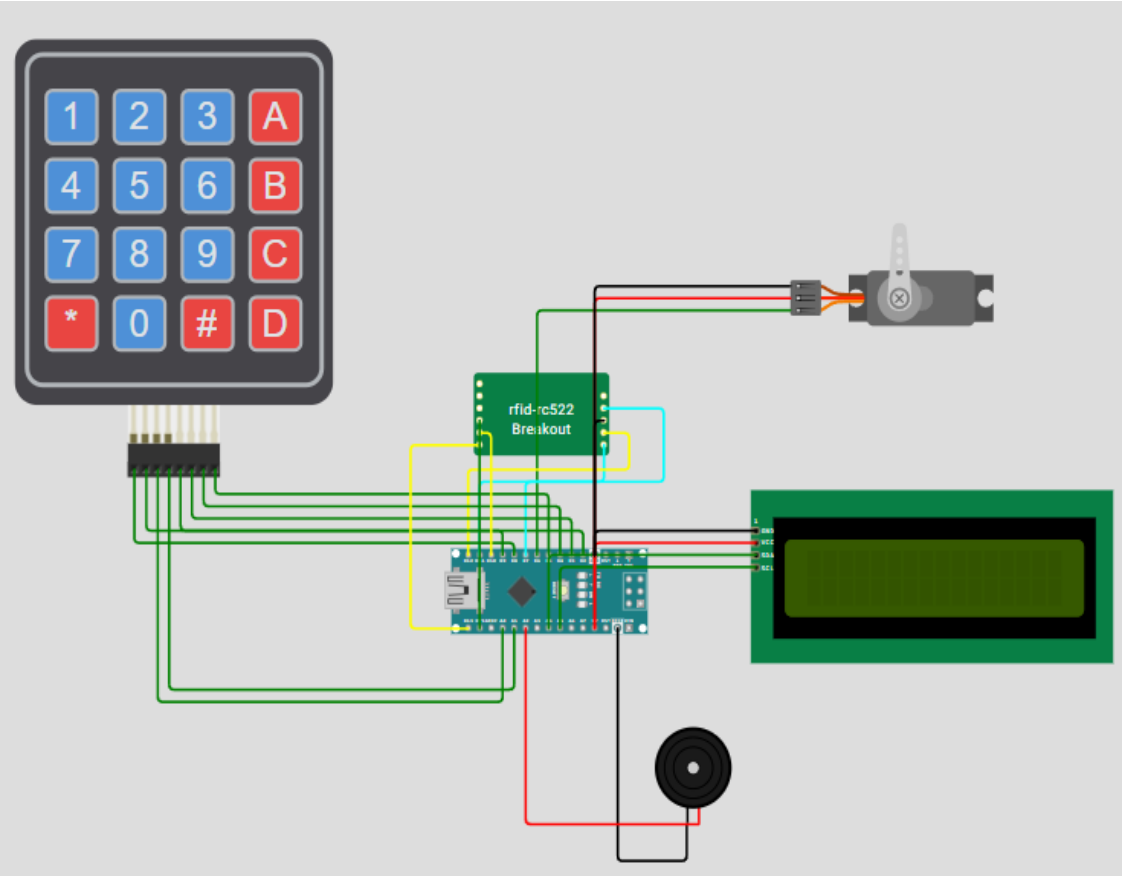

Рисунок 3.1 – Електрична схема у сервісі Wokwi

У даній схемі елементи з’єднані між собою згідно таблиці 3.1.

Таблиця 3.1 – З’єднання елементів схеми

Найменування елемента	Найменування контакту	Найменування елемента	Найменування контакту
1	2	3	4
Arduino	GND	LCD	GND
Arduino	5V	LCD	VCC
Arduino	A4	LCD	SDA
Arduino	A5	LCD	SCL
Arduino	2	Keypad	C1
Arduino	3	Keypad	C2
Arduino	4	Keypad	C3
Arduino	5	Keypad	C4
Arduino	8	Keypad	R1
Arduino	9	Keypad	R2
Arduino	A0	Keypad	R3
Arduino	A1	Keypad	R4
Arduino	GND	Servo	GND
Arduino	5V	Servo	VCC
Arduino	6	Servo	PWM
Arduino	GND	RFID	GND
Arduino	3.3V	RFID	3.3V

Продовження таблиці 3.1

1	2	3	4
Arduino	10	RFID	SDA
Arduino	13	RFID	SCK
Arduino	7	RFID	RESET
Arduino	12	RFID	MISO
Arduino	11	RFID	MOSI
Arduino	GND	BUZZER	GND
Arduino	A2	BUZZER	Signal

У сервісі Wokwi відсутня модель RFID-модуля для зчитування RFID-міток. Тому для створення моделі RFID-модуля було використано Custom Chips API. Цей API дозволяє створювати відсутні в бібліотеках сервісу електронні елементи.

3.2 Виготовлення пристрою

Всі компоненти були змонтовані в пластиковому корпусі. В корпусі було зроблено отвори для розміщення екрану. Сенсорна клавіатура розміщувалась на поверхні корпусу, а її виводи через спеціально відведений отвір проводились в середину пристрою та під’єднувались до відповідних пінів Arduino.

Всі комплектуючі кріпились до корпусу задопомогою гвинтів та в окремих випадках фіксувались із використанням термоклею.

Задля спрощення процесу електричного монтажу компоненти монтувались без виготовлення друкованої плати та під’єднувались задопомогою провідників у відповідності до таблиці 3.1. Для більш зручної організації електричних з’єднань та оптимізації використання простору в корпусі було використано плату розширення для Arduino NANO. Таке рішення дозволило спростити монтаж та електричну розв’язку компонентів, а також додало додатковий вбудований лінійний стабілізатор напруги.

RFID-мітка кріпилась з внутрішньої сторони корпусу. Стінка корпусу досить тонка, тому зчитування UUID RFID-мітки відбувається безперешкодно.

Зовнішній вигляд зібраного пристрою показано на рисунку 3.3.

Рисунок 3.3 – Зовнішній вигляд пристрою

Після завершення монтажу проводилось завантаження керуючої програми в мікроконтролер.

3.3 Створенння програми керуваня пристрою

Написання програми відбувалось у вбудованому IDE сервісу Wokwi на мові програмування Arduino. Блок-схема алгоритму програми наведена на рисунку В.1.

При написанні програми було використано три бібліотеки: Keypad.h, LiquidCrystal_I2C.h та Servo.h.

Бібліотека Keypad.h забезпечує зручну роботу з матричною клавіатурою, LiquidCrystal_I2C.h призначену для керування LCD-дисплеєм через інтерфейс I2C та Servo.h дозволяє керувати положенням сервоприводу.

На початку коду виконується ініціалізація клавіатури (лістинг 3.1).

Лістинг 3.1 – Ініціалізація клавіатури

```
const byte ROWS = 4;
const byte COLS = 4;
```

```
    char keys[ROWS][COLS] = { {‘1’, ‘2’, ‘3’, ‘A’}, {‘4’, ‘5’, ‘6’, ‘B’}, {‘7’, ‘8’, ‘9’, ‘C’}, {‘*’, ‘0’, ‘#’, ‘D’} };
    byte rowPins[ROWS] = {8, 9, A0, A1};
    byte colPins[COLS] = {2, 3, 4, 5};
    Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);
```

кінець лістингу 3.1

Масив keys визначає символи, що відповідають кожній клавіші клавіатури 4×4. Масиви rowPins та colPins вказують, до яких цифрових і аналогових виводів мікроконтролера підключено рядки та стовпці клавіатури відповідно. Далі створюється об’єкт keypad, який використовується для зчитування натискань клавіш.

Наступним кроком є ініціалізація дисплея та сервоприводу (лістинг 3.2).

Лістинг 3.2 – Ініціалізація дисплея та сервоприводу

```
LiquidCrystal_I2C lcd(0x27, 16, 2);
Servo myServo;
const int SERVO_PIN = 6;
```

кінець лістингу 3.2

LCD-дисплей типу 1602 із I2C-адресою 0x27 ініціалізується через об’єкт lcd. Об’єкт myServo використовується для керування сервоприводом, підключеним до цифрового виводу 6.

Далі оголошуються змінні, пов’язані з паролем: correctPassword та inputPassword.

У змінній correctPassword зберігається правильний пароль. Змінна inputPassword слугує для накопичення символів, введених користувачем.

У функції setup() виконується ініціалізація пристроїв (лістинг 3.3).

Лістинг 3.3 – Ініціалізація пристроїв

```
lcd.init();
lcd.backlight();
myServo.attach(SERVO_PIN);
```

```
    myServo.write(90);
    showPrompt();
```

кінець лістингу 3.3

В подальшому ініціалізується дисплей, вмикається підсвітка, сервопривід встановлюється в початкове (нейтральне) положення 90°, і викликається функція showPrompt(), яка виводить запрошення до сканування карти та введення пароля на дисплей.

Основна логіка програми реалізована у функції loop(), де зчитуються UUID RFID-мітки та моніторяться натиснуті клавіши з клавіатури за допомогою команди: char key = keypad.getKey();

Після сканування RFID-мітки UUID порівнюється із переліком дозволених значень. Якщо значення UUID невідоме, то подаються три коротких звукових сигналів, а на екрані на 1 секунду з’являється напис «Filed». Після чого програма повертається до сканування UUID. У випадку, коли UUID коректний відбувається перехід до зчитування паролю.

Якщо клавіша натиснута, то далі обробляється її значення. Якщо це клавіша *, то змінна inputPassword очищується і викликається showPrompt() для повторного введення. Якщо натиснуто клавішу #, то спочатку перевіряється довжина введеного пароля. Якщо вона дорівнює чотирьом символам, то здійснюється порівняння з правильним паролем. У випадку збігу на дисплеї з’являється повідомлення «Open», а сервопривод повертається у положення 180° (відкриття доступу), після чого відбувається затримка на 2 секунди. Якщо пароль неправильний, відображається повідомлення «Failed» (має бути «Failed»), а після затримки в 1 секунду введення скидається. Якщо пароль надто короткий, то на дисплей виводиться повідомлення «Too short».

У випадку, якщо натиснуто цифрову клавішу і довжина введення менша за чотири символи, то символ додається до inputPassword, і на дисплеї у відповідній позиції виводиться символ *, що імітує введення паролю.

Функція showPrompt() реалізується згідно лістингу 3.4.

Лістинг 3.4 – Функція showPrompt()

```
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Enter Password:");
    lcd.setCursor(0, 1);
```

кінець лістингу 3.4

Ця функція очищує дисплей, виводить на перший рядок повідомлення «Enter Password:» і переводить курсор на другий рядок для введення.

3.4 Опис та тестування розробленої системи

Даний пристрій може працювати в двох режимах: «System Armed», «System Disarmed».

Перший режим відповідає зачиненому об’єкту, а другий – відчиненому.

Систему можна повернути в режим «System Disarmed» скануванням RFID-мітки та введенням коду безпеки.

Після сканування RFID-мітки або введенням коду безпеки пристрій буде знаходитись в режимі «System Disarmed» до повторного введення коду безпеки та повторного сканування RFID-мітки.

Для живлення пристрою можна використовувати як живлення від мережі так і живлення від батареї. Для живлення необхідно використовувати адаптер живлення із вихідною напругою 5В та максимальним вихідним струмом не менше 1 А, або портативну батарею із вихідною напругою 5В.

Після підключення живлення відбувається ініціалізація системи. Після підключення живлення, система автоматично ініціалізує всі компоненти. На дисплеї з’явиться повідомлення про готовність.

Для активації системи необхідно просканувати мітку. Якщо RFID-мітка авторизована, система перейде в режим очікування паролю. На дисплеї з’явиться повідомлення «Password».

На наступному етапі необхідно ввести пароль доступу. Для введення паролю необхідно натиснути будь-яку клавішу на клавіатурі, щоб активувати режим введення паролю. Після введення паролю необхідно натиснути «#». Якщо пароль правильний, система перейде в активний режим. На дисплеї з’явиться повідомлення «System Armed».

Для зняття з охорони необхідно піднести RFID-мітку до RFID-модуля. Якщо мітка авторизована, система запросить введення паролю.

Для введення паролю необхідно натиснути будь-яку клавішу на клавіатурі. Введіть свій пароль та натисніть #. Якщо пароль правильний, система зніметься з охорони. На дисплеї з’явиться повідомлення «System Disarmed».

Зміна паролю. Для зміни паролю необхідно перепрограмувати мікроконтролер, замінивши старий пароль у програмному коді на новий.

ВИСНОВКИ

В ході дослідження здійснено комплексний аналіз сучасних технологій і методів побудови систем безпеки. Виконано порівняльне дослідження комерційних рішень (ZKTeco, KONE Access, SALTO SVN, Hundure Technology), що дозволило визначити їхні сильні та слабкі сторони й сформувати технічні вимоги до власної розробки, такі як низька вартість, масштабованість і сумісність із концепцією «розумного будинку».

Спроектовано та візуалізовано модель електричної схеми системи контролю доступу в симуляторі Wokwi, що включає Arduino NANO, RFID-зчитувач, індикатори та виконавчі елементи. Отримано підтвердження коректності апаратних і програмних рішень під час віртуального тестування. Вибрана елементна база забезпечує стабільну роботу системи за мінімальних витрат ресурсів.

Спроектовано та реалізовано прототип системи контролю доступу: змонтовано апаратну частину й розроблено прошивку мікроконтролера мовою C/C++ у середовищі Arduino IDE.

Розроблену систему можна використовувати для обмеження доступу в побутових, освітніх чи малих виробничих об’єктах, де потрібна надійна, економічно доцільна та проста в обслуговуванні система безпеки. Завдяки гнучкості архітектури, систему можна інтегрувати з іншими елементами розумного будинку, такими як системи відеоспостереження, сигналізації, керування освітленням чи вентиляцією.

Окрім основної функції контролю доступу, система може слугувати платформою для подальшого розширення функціональності. Зокрема, можлива реалізація мережевого моніторингу з веденням журналу подій у режимі реального часу, впровадження мобільної авторизації за допомогою смартфонів або смартгодинників, інтеграція з хмарними сервісами для зберігання та аналізу даних, а також підключення до локальної мережі для централізованого адміністрування кількох точок доступу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Система контролю і управління доступом. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом (дата звернення: 08.02.2025).

2. Pal A., Tripathi A., Saigal A. RFID technology: an overview. International Journal of Research -Granthaalayah. 2020. Vol. 5, no. 12. P. 176-182.

3. Levshun D., Chechulin A., Kotenko I. Design of Secure Microcontroller-Based Systems: Application to Mobile Robots for Perimeter Monitoring. Sensors. 2021. Vol. 21, no. 24. P. 8451.

4. Review of Smart-Home Security Using the Internet of Things / G. Vardakis et al. Electronics. 2024. Vol. 13, no. 16. P. 3343.

5. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations / M. K. Hasan et al. Journal of Network and Computer Applications. 2023. Vol. 209. P. 103540.

6. Haque A.K., Bhushan B., Dhiman G. Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Systems. 2021, Vol. 39. P. e12753.

7. Що таке СКУД і як це працює, різновиди систем контролю доступу. idcard.com.ua. URL: https://idcard.com.ua/ua/blog/chto-takoe-skud-i-kak-eto-rabotaet/ (дата звернення: 08.05.2025).

8. Mangla A. Securing Smart Shopping System Using IoT. International Journal for Research in Applied Science and Engineering Technology. 2022. Vol. 10, no. 7. P. 672-674.

9. Сучасні системи охорони та пожежної безпеки. Варта Безпека. URL: https://www.varta-bezpeka.com.ua/okhoronna-syghnalizacija/ (дата звернення: 08.03.2025).

10. Принцип роботи системи контролю доступу. Сучасні системи безпеки бізнесу. URL: https://ssbb.ua/sistemy-kontrolya-dostupa/sistema-kontrolyu-dostupu/princip-raboty-sistemy-kontrolya-dostupa/ (дата звернення: 11.03.2025).

11. Biometrics for Internet-of-Things Security: A Review / W. Yang et al. Sensors. 2021. Vol. 21, no. 18. P. 6163.

12. Kumar V., Chawda R. K. A research paper on smart home. International Journal of Engineering Applied Sciences and Technology. 2020. Vol. 5, no. 3. P. 530-532.

13. Radha R. K. Flexible smart home design: Case study to design future smart home prototypes. Ain Shams Engineering Journal. 2021.

14. Kumar R. P., Kishore E. G., Senthilraja P. Smart home controller using internet of things. International journal of health sciences. 2022. P. 2869-2875.

15. Combinatorial methods for testing Internet of Things smart home systems / B. Garn et al. Software Testing, Verification and Reliability. 2021. Vol. 32, no. 2. P.1805.

16. Marikyan D., Papagiannidis S., Alamanos E. «Smart Home Sweet Smart Home». International Journal of E-Business Research. 2021. Vol. 17, no. 2. P. 1-23.

17. Unisa S. A. Smart Home Control. International Journal for Research in Applied Science and Engineering Technology. 2022. Vol. 10, no. 7. P. 1153-1158.

18. Програмне забезпечення біометричного контролю доступу ZKTeco ZKAccess 3.5. URL: https://zkstore.com.ua/ua/p938101634-programmnoe-obespechenie-biometricheskogo.html?srsltid=AfmBOooxvAjdP70k-KaVcmAX9ThtkcTFiuCKtYxcUf9Fan2rC5g6tahL (дата звернення: 26.03.2025).

19. Kone website. Контроль доступу. URL: https://www.kontakt.com.ua /tehnologiyi-kone/kontrol-dostupa (date of access: 09.04.2025).

20. SALTO Systems. Smart Security. URL: https://smartsec.com.ua /uk/partneri/salto-systems/ (date of access: 18.04.2025).

21. Системи відеоспостереження і контролю доступу. Belintech. URL: https://bitech.com.ua/ua/services/accesscontrol/ (дата звернення: 17.04.2025).

22. Що таке система RFID, в чому її особливості використання | Новини RFID. idcard.com.ua. URL: https://idcard.com.ua/ua/blog/chto-takoe-sistema-rfid-v-chem-ee-osobennosti-

ispolzovaniya/?srsltid=afmbooorh0bkua5bklmhhnauuij93_vtxcuroujfs_h18bvk44ao8wzb (дата звернення: 21.04.2025).

23. Учасники проектів Вікімедіа. Радіочастотна ідентифікація – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Радіочастотна_ідентифікація (дата звернення: 08.04.2025).

24. Arduino. Bitkit. URL: https://bitkit.com.ua/shho-take-arduino?srsltid=AfmBOoorWQ02ALxOB3ydopWbQYOfQwhsKz7H8NaMTKUkygrkAOKxRL-U (date of access: 05.04.2025).

25. Arduino Nano V3.0 AVR ATmega328P з розпаяними роз'ємами. URL: https://arduino.ua/prod166-arduino-nano-v3-0-avr-atmega328p-s-raspayannimi-razemami (дата звернення: 03.04.2025).

26. Плата розширення Arduino Nano I/O Shield. Mini-tech. URL: https://www.mini-tech.com.ua/ua/nano-io-shield (дата звернення: 01.04.2025).

27. Клавіатура мембранна матрична 12 кнопок (4x3). Arduino KIT. URL: https://arduinokit.com.ua/ua/p2277063566-klaviatura-membrannaya-matrichnaya.html (дата звернення: 01.05.2025).

28. LCD 1602 символьний дисплей 16x2 (синій). mehanika.net.ua. URL: https://mehanika.net.ua/product/lcd-1602-simvolnij-displej-16x2-sinij/ (дата звернення: 01.05.2025).

29. RFID Card Reader/Writer RC522. Senith Electronics. URL: http://www.senith.lk/shop/item/1071/rfid-card-reader-writer-rc522 (date of access: 02.05.2025).

30. Wokwi - World's most advanced ESP32 Simulator. Wokwi. URL: https://wokwi.com/ (date of access: 24.04.2025).

ДОДАТКИ

Додаток А

Код керуючої програми

```
#include <Keypad.h>
#include <LiquidCrystal_I2C.h>
#include <Servo.h>
// === Налаштування клавіатури ===
const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};
byte rowPins[ROWS] = {8, 9, A0, A1};  // R1, R2, R3, R4
byte colPins[COLS] = {2, 3, 4, 5};    // C1, C2, C3, C4
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);
// === LCD ===
LiquidCrystal_I2C lcd(0x27, 16, 2);
// === Servo ===
Servo myServo;
const int SERVO_PIN = 6;
// === Пароль ===
const String correctPassword = "1234";
String inputPassword = "";

void setup() {
  lcd.init();
  lcd.backlight();
  myServo.attach(SERVO_PIN);
  myServo.write(90);  // Початкове положення (нейтральне)
  showPrompt();
}

void loop() {
  char key = keypad.getKey();

  if (key) {
    if (key == '*') {
      // Скидання введеного паролю
      inputPassword = "";
```

```
      showPrompt();
    }
    else if (key == '#') {
      if (inputPassword.length() == 4) {
        if (inputPassword == correctPassword) {
          lcd.clear();
          lcd.setCursor(0, 0);
          lcd.print("Open");
          myServo.write(180);  // Відкрити
          delay(2000);
        } else {
          lcd.clear();
          lcd.setCursor(0, 0);
          lcd.print("Filed");
          delay(1000);
        }
      } else {
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Too short");
        delay(1000);
      }
      inputPassword = "";
      showPrompt();
    }
    else if (inputPassword.length() < 4 && isDigit(key)) {
      inputPassword += key;
      lcd.setCursor(inputPassword.length() - 1, 1);
      lcd.print("*");
    }
  }
}

void showPrompt() {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Enter Password:");
  lcd.setCursor(0, 1);
}
```

Додаток Б

Вміст файлу diagram.json

```
{
  "version": 1,
  "author": "Олександр Бурбан",
  "editor": "wokwi",
  "parts": [
    { "type": "chip-rfid-rc522", "id": "chip1", "top": -142.98, "left": 72,
"attrs": {} },
    { "type": "wokwi-arduino-nano", "id": "nano", "top": -4.8, "left": 47.5,
"attrs": {} },
    {
      "type": "wokwi-membrane-keypad",
      "id": "keypad1",
      "top": -405.2,
      "left": -311.2,
      "attrs": {}
    },
    {
      "type": "wokwi-lcd1602",
      "id": "lcd1",
      "top": -51.2,
      "left": 303.2,
      "attrs": { "pins": "i2c" }
    },
    { "type": "wokwi-servo", "id": "servo1", "top": -261.2, "left": 336, "attrs":
{} },
    {
      "type": "wokwi-buzzer",
      "id": "bz1",
      "top": 127.2,
      "left": 222.6,
      "attrs": { "volume": "0.1" }
    }
  ],
  "connections": [
    [ "nano:2", "keypad1:C1", "green", [ "v-19.2", "h-335.9" ] ],
    [ "servo1:PWM", "nano:6", "green", [ "h0" ] ],
    [ "nano:7", "chip1:RESET", "cyan", [ "v-57.6", "h115.2", "v-57.6" ] ],
    [ "nano:11", "chip1:MOSE", "cyan", [ "v-57.6", "h103.79" ] ],
    [ "nano:12", "chip1:MISO", "yellow", [ "v-67.2", "h134.4", "v-28.8" ] ],
    [ "nano:3", "keypad1:C2", "green", [ "v-28.8", "h-316.8" ] ],
    [ "nano:4", "keypad1:C3", "green", [ "v-38.4", "h-297.45" ] ],
    [ "nano:5", "keypad1:C4", "green", [ "v-48", "h-278.1" ] ],
    [ "nano:8", "keypad1:R1", "green", [ "v-9.6", "h-316.8" ] ],
    [ "nano:9", "keypad1:R2", "green", [ "v-19.2", "h-297.2" ] ],
    [ "nano:10", "chip1:SDA", "yellow", [ "v0" ] ],
    [ "nano:13", "chip1:SCK", "yellow", [ "h-48", "v-144" ] ],
    [ "nano:A4", "lcd1:SDA", "green", [ "v0" ] ],
    [ "nano:A5", "lcd1:SCL", "green", [ "v0" ] ],
```

```
    [ "nano:3.3V", "chip1:3.3V", "green", [ "v0" ] ],
    [ "nano:5V", "lcd1:VCC", "red", [ "v0" ] ],
    [ "nano:5V", "servo1:V+", "red", [ "v0" ] ],
    [ "nano:GND.2", "lcd1:GND", "black", [ "v0" ] ],
    [ "nano:GND.2", "chip1:GND", "black", [ "v0" ] ],
    [ "nano:GND.2", "servo1:GND", "black", [ "v0" ] ],
    [ "nano:A0", "keypad1:R3", "green", [ "v57.6", "h-287.7" ] ],
    [ "nano:A1", "keypad1:R4", "green", [ "v48", "h-287.8" ] ],
    [ "bz1:1", "nano:GND.1", "black", [ "v28.8", "h-57.6" ] ],
    [ "bz1:2", "nano:A2", "red", [ "h-144.4", "v-153.6" ] ]
  ],
  "dependencies": {}
}
```