Вінницький національний технічний університет
(повне найменування вищого навчального закладу)
Факультет інформаційних технологій та комп'ютерної інженерії
(повне найменування інституту)
Кафедра обчислювальної техніки
(повна назва кафедри)

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Апаратно-програмні засоби віддаленого керування доступом до об'єктів через веб-інтерфейс»

ПОЯСНЮВАЛЬНА ЗАПИСКА

08-23.МКР.029.00.000 ПЗ

Виконав: студент 2 курсу, групи 2КІ-21м
спеціальності 123 — «Комп'ютерна інженерія»
_____ Тарновський А. М.

Керівник: к.т.н., доц.каф. ОТ
_____ Крупельницький Л. В.
«15» 12 2022 р.

Опонент: к.т.н., доц. каф. ЗІ
_____ Коваленко О. О.
«18» 12 2022 р.

Допущено до захисту

Завідувач кафедри ОТ
_____ д.т.н., проф. Азаров О. Д.
«15» 12 2022 р

Вінниця ВНТУ - 2022 рік

Вінницький національний технічний університет
Факультет Інформаційних технологій та комп'ютерної інженерії
Кафедра Обчислювальної техніки
Рівень вищої освіти ІІ-ий (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 123 – «Комп'ютерна інженерія»
Освітньо-професійна програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
обчислювальної техніки
д.т.н., проф. Азаров О. Д.
«15» 09 2022 року

З А В Д А Н Н Я
НА МАГІСТРСЬКУ КВАЛІФІКАЦІЙНУРОБОТУ

студенту Тарновському Артему Миколайовичу

1 Тема роботи «Апаратно-програмні засоби віддаленого керування доступом до об'єктів через веб-інтерфейс» керівник роботи Крупельницький Леонід Віталійович, к.т.н., доцент затверджено наказом Вінницького національного технічного університету від "15" 09 2022 року №205-А

2 Строк подання студентом роботи 20.12.2022 р.

3 Вихідні дані до роботи: призначення — керування доступом до об'єктів; надання доступу — за ідентифікатором, що надсилається зі смартфона; надання ідентифікатора — віддалено через Інтернет; об'єкт керування — електромеханічний пристрій; струм керування — не менше 2 А; потужність керування — до 4 кВт.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): обґрунтування доцільності розробки; аналіз сучасних управління доступом; розгляд принципів та технологій віддаленого керування доступом; розробка структурної схеми контролера керування доступом; розробка схеми електричної функціональної контролера керування доступом; розробка веб-додату та додатку для смартфона для керування доступом; економічна частина.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): схема системи віддаленого керування доступом, структурна схема контролера керування доступом; функціональна схема контролера керування доступом; блок-схема алгоритму роботи контролера доступу; блок-схема алгоритму роботи додатку адміністратора; блок-схема алгоритму роботи мобільного додатку; блок-схема алгоритм роботи у веб-сервера

6. Консультанти розділів роботи приведені в таблиці 1

Таблиця 1 — Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1,2,3	Крупельницький Л. В. к.т.н., доцент		
4	Небава М. І. к.е.н., проф.		

7.Дата видачі завдання _____

8 Календарний план виконання МКР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів МКР	Строк виконання	Підпис
1	Постановка задачі	06.09.22	Вик.
2	Огляд існуючих рішень	20.09.22	Вик.
3	Розробка структурної схеми	20.10.22	Вик.
4	Розробка функціональної схеми	01.12.22	Вик.
5	Розрахунок економічної частини	05.12.22	Вик.
6	Оформлення пояснювальної записки та ілюстративного матеріалу	12.12.22	Вик.
7	Перевірка якості виконання магістерської кваліфікаційної роботи та усунення недоліків	16.12.22	Вик.
8	Підписи супроводжувальних документів у керівника, опонента, нормоконтролера	17.12.22	Вик.
9	Перевірка «антиплагіат»	17.12.22	Вик.
10	Попередній захист	24.11.22	Вик.

Студент _____ (підпис) Тарновський А. М. (прізвище та ініціали)

Керівник роботи _____ (підпис) Крупельницький Л. В. (прізвище та ініціали)

АНОТАЦІЯ

Тарновський А. М. Апаратно-програмні засоби віддаленого керування доступом до об’єктів через веб-інтерфейс. Магістерська кваліфікаційна робота зі спеціальності 123 Комп’ютерна Інженерія, Вінниця: ВНТУ, 2022.

На укр. мові. Бібліогр.: 42 назв; рис.: 32; табл. 22.

У роботі розглянуто принципи побудови системи віддаленого управління доступом за мобільним ідентифікатором, що надається віддалено через Інтернет. В роботі проведений аналіз сучасних технологій управління доступом, розглянуті основні принципи побудови систем управління доступом, вибрано та проаналізовано аналоги, розглянуто принципи та технології віддаленого керування доступом, визначено підходи до побудови системи віддаленого керування доступом з розширеними функціональними можливостями, що забезпечує керування доступом при втраті зв′язку з Інтернет. Розроблено структурну та функціональні схеми контролера керування доступом, веб-додаток адміністратора системи та мобільний додаток користувача, тощо.

Ключові слова: управління доступом, контролер управління доступом, мобільна ідентифікація, Bluetooth з’єднання, хмарний сервер, веб-додаток

.

ABSTRACT

Tarnovskyi A. M. Hardware and software tools for remote control of access to objects through a web interface. Master's thesis on the specialty 123 Computer Engineering, Vinnytsia: VNTU, 2022.

In Ukrainian language Bibliogr.: 42 titles; fig.: 32; table 22.

The work considers the principles of building a remote access management system based on a mobile identifier provided remotely via the Internet. The paper analyzes modern access control technologies, considers the main principles of building access control systems, selects and analyzes analogues, considers the principles and technologies of remote access control, defines approaches to building a remote access control system with extended functionality, which provides access control in case of loss of communication Internet connection. Developed structural and functional diagrams of access control controller, system administrator web application and user mobile application, etc.

Keywords: access control, access control controller, mobile identification, Bluetooth connection, cloud server, web application

ЗМІСТ

					08-23.МКР.029.00.000 ПЗ			
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*				
Розробив		Тарновськи А.М.			Апаратно-програмні засоби віддаленого керування доступом до об’єктів через веб-інтерфейс Пояснювальна записка	*Літ.*	*Аркуш*	*Аркушів*
Перевірив		Крупельницький Л. В.					6	122
Рецензент		Коваленко О.О.				ВНТУ, гр. 2КІ-21м		
Н.контр.		Швець С. І.						
Затвердж.		Азаров О.Д						

.

ВСТУП

Під системою управління доступом розуміють комплекс апаратно-програмних та організаційно-методичних засобів, спрямованих на забезпечення безпеки об′єктів за рахунок обмеження та контролю доступу на них [1]. Сучасні системи управління доступом дозволяють вирішувати цілий ряд задач, таких як обмеження проникнення людей і транспорту на територію об'єкта, що охороняється, проведення обліку робочого часу персоналу та контроль за його переміщенням у певний час доби, обмеження проникнення в окремі зони.

Актуальність теми дослідження полягає в тому, що на теперішній час усе більшого значення набувають питання забезпечення безпечного функціонування об'єктів бізнесу, житлових будівель, виробництва, об'єктів соціального призначення. Одним із найефективніших і цивілізованих підходів до вирішення завдання комплексної безпеки об'єктів різних форм власності є використання систем контролю та управління доступом. Такі системи дозволяють закрити несанкціонований доступ на територію, у будівлю, окремі поверхи та приміщення. У той самий час вони не створюють перешкод для проходу персоналу та відвідувачів у дозволені для них зони.

До основних вимог, які пред'являються до систем управління доступом сьогодні слід відносити максимально можливу ефективність та незалежність від людського фактору. Відповідно до цього, сьогодні системи управління доступом є одним з найбільш розвинених сегментів ринку безпеки. Не зважаючи на період кризи падіння у цьому сегменті ринку було незначним. Це, перш за все, пов′язано з тим, що системи управління доступом є тим з небагатьох засобів безпеки, які не лише дозволяють підвищити рівень запобігання потенційним загрозам, а й приносять значний економічний ефект [2].

Стійкий динамічний розвиток індустрії безпеки сьогодні обумовлений не лише зростанням світової економіки, а й активізацією окремих галузей, що пов′язані з такими системами, наприклад, роздрібна торгівля, готельний бізнес, автотранспортна сфера, будівництво. Будучи невід'ємною складовою систем безпеки, системи управління доступом мають значний потенціал. Вони можуть

взаємодіяти і інтегруватися з іншими інформаційними системами, перш за все з системами відеоспостереження, охоронної сигналізації, управління персоналом.

Як і всі інші електронні інформаційні системи системи управління доступом постійно розвиваються та вдосконалюються. Розвиток мікроконтролерної елементної бази, сенсорних елементів та різноманітних технологій зв’язку дозволяє отримати нові функціональні можливості в управлінні доступом. Останні тенденції розвитку у цій галузі пов’язані з впровадженням IP-технологій. Майже усі провідні виробники закладають у своєму обладнанні можливість прямого підключення до мережі Ethernet. Завдяки цьому отримуються нові додаткові можливості, основними з яких є зручність використання обладнання, простота та мала вартість впровадження подібних систем на об'єктах з розвиненою IT-інфраструктурою [3].

Об’єктом дослідження є процеси віддаленого керування доступом.

Предметом дослідження є методи та засоби ідентифікації з використанням смартфону.

Метою роботи є розширення функціональних можливостей системи віддаленого керування доступом через веб-інтерфейс за рахунок підтримки можливості роботи в офлайн режимі.

Для досягнення поставленої мети в роботі розв′язані такі задачі:

аналіз сучасних технологій управління доступом;

аналіз сучасних технологій мобільної ідентифікації;

визначення принципів побудови системи віддаленого керування доступом з розширеними функціональними можливостями.

Для досягнення поставленої в роботі мети використовуються такі **методи дослідження:**

— системний аналіз;

— методи схемотехнічного проектування;

— методи алгоритмічного проектування.

Наукова новизна полягає в тому, що набула подальшого розвиту технологія віддаленого керування доступом з мобільною ідентифікацією, в якій,

на відміну від існуючих, ідентифікатори за допомогою веб-додатку адміністратора зберігаються у контролері керування доступом, що дозволило керувати доступом в офлайн режимі.

Практичне значення роботи полягає в тому, що на основі запропонованих підходів до побудови та функціонування системи віддаленого керування доступом були розроблені контролер керування доступом та програмні засоби для взаємодії з ним, що дозволяє здійснити віддалене керування правами доступу через веб-додаток та забезпечити можливість доступу в офлайн режимі.

Апробація результатів роботи здійснена в доповіді на XV Міжнародній науково-технічній конференції «Перспективи телекомунікацій» ПТ-2021 (12–16 квітня 2021 р., Київ), Всеукраїнській науково-практичній Інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2023)» (ВНТУ)

Матеріали роботи доповідались та опубліковувались:

Тарновський А. М. Система віддаленого керування доступом / А. М. Тарновський, К. В. Коляда // XV Міжнародна науково-технічна конференція «Перспективи телекомунікацій» ПТ-2021 (12 16 квітня 2021 р., Київ) : Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2021. С. 356-358. Режим доступу: http://conferenc.its.kpi.ua/2021/paper/view/23085/12502.

Тарновський А. М. Система віддаленого керування доступом з ідентифікацією через Bluetooth / А. М. Тарновський, Л. В. Крупельницький // Всеукраїнська науково-практична Інтернет-конференція студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2023)» (15 листопада 2022 р. 12 травня 2023 р., Вінниця) : Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2023/paper/viewFile/16888/14078

1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ ДОСТУПОМ

1.1 Основні принципи побудови систем управління доступом

Електронне управління доступом найсучасніший напрямок у галузі безпеки. Застосування електронних систем управління доступом забезпечує зручність та гнучкість функціонування об'єкта, дозволяє організувати розмежування доступу та контролювати доступ як на комерційних об'єктах, так і у приватних приміщеннях. Відповідно до цього основними завданнями системи керування та управління доступом є ідентифікація осіб, які мають право доступу, та управління доступом на заданий об′єкт або на задану територію. Поряд із цим можуть вирішуватися і додаткові завдання, основними серед яких є такі [4]:

облік робочого часу;

розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку);

ведення бази персоналу/відвідувачів;

інтеграція із системою безпеки, наприклад, з системою відеоспостереження, з системою охоронної сигналізації для обмеження доступу до приміщень, для автоматичного зняття та постановки приміщень на охорону;

з системою пожежної сигналізації для отримання інформації про стан пожежних сповіщувачів, автоматичне розблокування евакуаційних виходів та закриття протипожежних дверей у разі пожежної тривоги.

Незалежно від конфігурації, будь-яка система управління доступом містить у своєму складі чотири основні компоненти [5]:

контролер один з головних пристроїв системи, що зберігає інформацію, за якою здійснюється ідентифікація прав доступу та управління ним; саме контролер приймає рішення про надання чи заборони доступу; залежно від типу системи контролер може працювати автономно або в об’єднанні з іншими засобами під керуванням головного комп’ютера;

ідентифікатори засоби, які дають право доступу; ідентифікатор

містить інформацію, що підтверджує повноваження прав його власника для отримання доступу;

зчитувачі пристрої, які забезпечують зчитування кодової інформації, що зберігається в ідентифікаторах, та її перетворення в стандартний формат, що передається для аналізу та прийняття рішення до контролера;

загороджувальні пристрої пристрої, за допомогою яких відбувається управління фізичним доступом; це можуть бути турнікети, електроприводні ворота, шлагбауми, електромеханічні замки дверей і т.п.

Додатковими компонентами систем управління доступом є програмне забезпечення та різні допоміжні елементи, такі як датчики, пульти, кнопки, блоки безперебійного живлення та ін.

Залежно від особливостей реалізації конкретної системи управління доступом окремі з перерахованих вище основних компонентів можуть бути об'єднані в один блок або бути відсутні. Так, наприклад, контролер може бути об’єднаний зі зчитувачем.

Основним принципом роботи будь-якої системи управління доступом є порівняння ознак ідентифікації певного об'єкта з характеристиками, що зберігаються у пам'яті системи. За допомогою зчитувача відбувається введення інформації для ідентифікації, яка передається на контролер. На підставі отриманих даних контролер приймає рішення про надання доступу. Якщо доступ дозволено, контролер посилає відповідний сигнал на загороджувальний пристрій, який безпосередньо забезпечує фізичний доступ.

Усі системи управління доступом можна поділити на автономні (локальні), централізовані (мережеві) та комбіновані [5].

Автономні системи управління доступом спрямовані на керування одним або декількома засобами пропуску. Автономна система, зазвичай, складається з самостійного контролера, який зберігає базу даних ідентифікаторів і забезпечує керування іншими компонентами системи, та виконавчого пристрою. Автономні системи призначені для забезпечення контролю і управління доступом в окреме приміщення, та широко використовуються в адміністративних, громадських та

освітніх закладах, приватних будівлях тощо. Деякі автономні системи передбачають накопичення інформації про всі проходи через точку доступу дату, час, ідентифікаційний номер [6].

Головними перевагами автономних систем є порівняно низька вартість, простота встановлення та експлуатації, легке керування та надійність. Проте вони не дозволяють створювати звіти і передавати інформацію щодо подій, не передбачають можливості дистанційного управління, тощо [6].

Мережеві системи будуються з використанням кількох контролерів, які об’єднуються в єдину мережу із загальним централізованим керуванням з боку комп’ютера. Такі системи дозволяють здійснювати одночасне керування багатьма пунктами пропуску, оперативно вносити зміни у процес функціонування та додавати нові функції, вести облік робочого часу та контролювати переміщення персоналу та відвідувачів. Використовуване програмне забезпечення дозволяє не лише накопичувати інформацію, а й аналізувати її.

Як правило, мережеві системи управління доступом інтегруються із системами відеоспостереження, пожежної та охоронної сигналізації. Вони використовуються на об′єктах з великою кількістю співробітників та відвідувачів. Питома вартість однієї точки проходу в мережевій системі завжди вище, ніж в автономній.

До основних переваг мережевих систем можна віднести: можливість інтеграції з іншими підсистемами безпеки (відеоспостереженням або пожежною сигналізацією), підтримку функцій контролю та управління у реальному часі, підтримку дистанційного управління, введення журналу подій, можливість організації обліку робочого часу та контролю трудової дисципліни [6].

В залежності від номенклатури вирішуваних завдань сучасні системи управління доступом можна поділити на три класи. До першого класу відносять прості автономні системи, функціонал яких полягає у забезпеченні контрольованого доступу через один пункт пропуску. Час відвідування та інші деталі, при цьому не реєструються. Доступ надається за індивідуальним

ідентифікатором, інформація про який зберігається в контролері. Системи цього класу є однорівневими, оскільки ідентифікація здійснюється за однією ознакою. Ідентифікатори додаюпься або видаляються адміністратором з використанням, наприклад, майстер-картки.

До другого класу відносяться системи, які можуть бути багаторівневими та мережевими. Вони забезпечують більш високий рівень безпеки, ніж системи першого класу, та будуються на базі кількох контролерів. Основним елементом таких систем є комп'ютера, за допомогою якого здійснюється програмування всіх контролерів, збір та аналіз інформації, складання звітів, відстеження ситуації на об'єкті. Такі системи надають можливість налаштовувати допуск за часовими інтервалами або датами, проводити реєстрацію осіб, які входять на закриту зону, та виходять із неї, подавати сигнал тривоги на пост охорони або до інших пристроїв у разі несанкціонованого проникнення.

Третій клас складають багаторівневі мережеві комплекси, побудовані з використанням технології локальних мережі, з урахуванням робочого часу, з великою кількістю функцій, складними ідентифікаторами та багаторівневою взаємодією. Використовуються при необхідності контролю часу проходу із застосуванням складних електронних ідентифікаторів. Такі системи крім повної підтримки функціоналу систем попереднього класу надають додаткові можливості, а саме:

можливість інтеграції з протипожежними системами та системами відеоспостереження на апаратному рівні через спеціальний модуль;

ведення докладного обліку щодо кожного відвідувача;

постійна автоматична самодіагностика щодо цілісності складових системи.

Інтеграції з протипожежними системами та системами відеоспостереження здійснюється на релейному рівні, що передбачає наявність додаткового модуля в контролері (або додаткових входів/виходів у контролері), що забезпечує підключення охоронних або пожежних сповіщувачів та керування телекамерами та іншими пристроями через релейні виходи. Подібна інтеграція застосовується

переважно на малих об'єктах, що характеризуються малою інтенсивністю взаємодій між його системами. Цей рівень інтеграції є простим, універсальним та досить надійним.

Системи четвертого класу це багаторівневі системи великої ємності. Відмінними рисами великих систем є наявність розвиненого програмного забезпечення, що дозволяє реалізовувати велику кількість функціональних можливостей і високий рівень інтеграції на програмному (системному) рівні з іншими системами охорони та безпеки. Програмний рівень передбачає поєднання різних систем на основі єдиної програмно-апаратної платформи, з єдиним комунікаційним протоколом та загальною базою даних.

1.2 Технології ідентифікації

Однією з основних задач, що вирішуються системами управління доступом, є ідентифікація відвідувачів, яка здійснюється за ідентифікаційними ознаками. Під ідентифікаційною ознакою розуміють властивість, значення якої певним чином характеризує суб'єкта доступу. Ідентифікатором є унікальний набір значень ідентифікаційних ознак суб'єкта доступу, що використовується для ідентифікації. Процедура ідентифікації полягає у розпізнаванні користувача за ідентифікаційними ознаками. При цьому виконується порівняння ідентифікатора, що пред'являється користувачем, з вмістом бази даних. Для здійснення цієї процедури повинна бути створена база даних образів ідентифікаторів.

Для ідентифікації при наданні доступу можуть використовуватися різні технології. В сучасних системах управління доступом найбільше поширення отримали радіочастотна, мобільна та біометрична ідентифікації [4].

Радіочастотна ідентифікація (Radio Frequency Identification) здійснюється з використанням безконтактних RFID карток EM-Marin та Mifare, інформація з яких може бути зчитана на відстані від 5 до 90 см. При цьому зчитувач може бути скрито розміщений за антивандальною неметалевою перегородкою. Відповідно до цього, безконтактні картки доступу на основі технології

радіочастотної ідентифікації дозволяють швидко здійснювати доступ до системи, не вимагаючи конкретного положення мітки в просторі. Крім того, RIFD-картки дозволяють працювати в агресивному середовищі, здійснювати ідентифікацію на порівняно великій відстані та мають тривалий термін служби.

Картки EM-Marin це Proximity-картки (тільки читання), що працюють на частоті 125 кГц. За своєю суттю, Proximity картка це дистанційний електронний пропуск з вбудованим мікрочіпом, що має унікальний ідентифікаційний код, який широко використовується в системах контролю як фізичного, так і логічного доступу при безконтактній радіочастотній ідентифікації. Картки цього стандарту отримали широке поширення насамперед через зручність використання при досить малій вартості.

Обмін інформацією між Proximity карткою та зчитувачем здійснюється за відкритим протоколом, що робить їх досить вразливими для зловмисників. Крім того, такі картки ні як не захищені від копіювання, а тому не забезпечують належного рівня захисту. Для запобігання несанкціонованому доступу за копією ідентифікатора зазвичай використовують додаткові засоби захисту доступ за карткою у поєднанні з введенням PIN-коду, доступ з підтвердженням, доступ за двома картками і т. п. [4], [5].

Більш захищеними від копіювання є безконтактні високочастотні RIFD-картки (High Frequency), що працюють на частоті 13,56 МГц. Найбільше поширення серед них отримали smart-картки форматів Mifare та iCLASS. За останні кілька років їх вартість знизилася в кілька разів і впритул наблизилася до вартості карток форматів EM-Marine.

Завдяки ширшій смузі пропускання високочастотні RIFD-картки дозволяють забезпечити більший рівень безпеки та швидкодії. Картки доступу, що працюють на частоті 13,56 МГц, дозволяють реалізувати взаємну автентифікацію між карткою та зчитувачем, а також використовувати алгоритми шифрування даних.

Ще однією перевагою високочастотних RIFD-карток є наявність світового стандарту ISO14443, на відміну від низькочастотних карток доступу, що не

підлягають стандартизації.

Чіпи таких карток крім серійного номер чіпа (UID), мають пам'ять для багаторазового запису та читання, і доступ до цієї пам'яті захищений ключами, що практично унеможливлює копіювання таких карток або несанкціоноване зчитування інформації з них. Серійний номер чіпа завжди відкритий для читання, його не можливо змінити або закрити для читання. Тому для підтримки високого рівня захисту від несанкціонованого проникнення як дані для ідентифікації краще використовувати інформацію, що записана у пам′ять картки [5].

Використання вбудованої пам'яті smart-карток та її зростаюча місткість дозволяють зберігати на ній не тільки ідентифікаційні ознаки, а й іншу інформацію. За рахунок збільшення сумарного об’єму ідентифікаційної інформації повністю виключається ситуація її збігу в різних картах. При цьому суттєво змінюється функціонал та знижується вартість стаціонарного обладнання системи контролю та управління доступом.

Для читання захищеної інформації унікальний ключ доступу до даних зберігається в зчитувачі. Для цього використовується двосторонній обмін інформацією контролера зі зчитувачем або запис ключів доступу до даних спеціально підготовленою майстер-карткою при її пред'явленні до зчитувача. Перше рішення є більш зручним, проте вимагає застосування спеціальних зчитувачів і контролерів. Друге рішення дозволяє використовувати стандартні контролери з інтерфейсом Wiegand, але ускладнює настройку та модифікацію параметрів системи. При розподілі інформаційного функціоналу між карткою і стаціонарним обладнанням найбільш перспективними представляються системи зі збереженням на карті ідентифікаційних ознак та централізованим зберіганням прав доступу і персональних даних користувачів [6].

Ще одним типом RIFD-карток є ультрависокочастотні картки доступу (Ultra High Frequency), які працюють на частоті 860-960 МГц. Використання UHF RIFD-карток дозволяє значно збільшити відстань зчитування. Найчастіше технології UHF використовуються для організації віддаленого зчитування RIFD-міток при проїзді автотранспорту. Крім того, ультрависокочастотні карти

доступу можуть застосовуватись у мультитехнологічних рішеннях для організації в'їзду на територію та входу до будівлі по одній картці.

Наступною технологією ідентифікації є мобільна ідентифікація, при якій для отримання прав використовується смартфон. Мобільна ідентифікація останнім часом набуває усе більшого поширення, що обумовлено високою популяризацією смартфонів, їх універсальністю та багатозадачністю. Крім того, використання смартфона як ідентифікатора виключає випадки клонування, втрати або передачі ідентифікатора іншій особі. Відсутня необхідність придбання та персоналізації карт доступу, а впровадження відбувається з мінімальними часовими витратами. До того ж, на відміну від безконтактних карток, самі смартфони підтримують багатофакторну автентифікацію, біометричну ідентифікацію та інші функції безпеки [7], [8].

Мобільний доступ за допомогою смартфону в основному передбачає використання двох технологій: NFC (Near field communication) технологія близької ідентифікації та BLE (Bluetooth Low Energy) технологія низького енергоспоживання Bluetooth [8].

NFC є новою стандартизованою технологією бездротового зв'язку малого радіусу дії, яка є одним з найбільш популярних сучасних трендів у галузі використання мобільних пристроїв як ідентифікаторів. Серед основних особливостей цієї технології слід зазначити безконтактну передачу даних, можливість обміну інформацією з іншими пристроями або пасивними мітками, низьку вартість рішення, мале енергоспоживання [8], [9].

Bluetooth Low Energy є специфікацією ядра популярної бездротової технології Bluetooth, найбільш сттєвими перевагами якої при використанні в системах управління доступу є надмале енергоспоживання, відсутність необхідності у попереднього сполученні пристроїв, використання алгоритму шифрування даних AES з ключем розміром 128 біт [8].

Ідентифікація за біометричними ознаками використовує найрізноманітніші біометричні ознаки людини. Такими ознаками можуть бути як відкриті, такі як обличчя, долоні, відбитки пальців, рогівка ока, так і приховані, такі як

розташування вен долоні, голос, унікальність будови внутрішніх органів тощо [10].

Біометричну ідентифікацію часто називають чистою або реальною, оскільки використовується не віртуальна, а біометрична ознака (ідентифікатор), що реально має відношення до людини. Специфічною особливістю біометричної ідентифікації є великий розмір біометричної бази даних: кожен з біометричних зразків має бути зіставлений з усіма наявними записами в базі даних (порівняння 1: N або «один до багатьох»). Для використання в реальному житті така система потребує високої швидкості зіставлення біометричних ознак [10].

У цілому біометричні системи ідентифікації поділяються на статичні та динамічні. При статичній ідентифікації використовуються фізіологічні характеристики:

відбитки пальців або малюнок папілярних ліній;

райдужна оболонка ока;

сітківка ока;

малюнок вен;

обличчя;

геометрія руки;

серцевий ритм;

ДНК.

Динамічна ідентифікація здійснюється за поведінковими характеристиками такими, як:

почерк та динаміка підпису;

серцевий ритм;

голос та ритм мови;

розпізнавання жестів

швидкість та особливості роботи на клавіатурі комп'ютера (або набору коду на кодонабірній панелі);

хода [10], [11].

Основною перевагою біометричної ідентифікації є ідентифікація безпосередньо самої особи, а тому високий рівень надійності і точності розпізнавання без можливості передачі ідентифікаторів іншим особам. Системи розпізнавання обличчя в цьому списку отримують все більше поширення як найбільш зручний і швидкий спосіб безконтактної ідентифікації. Через дуже високу вартість, малу оперативність і великий необхідний об′єм машинної пам'яті, займаної одним таким ідентифікатором вони застосовуються надзвичайно рідко, в основному в установах з підвищеною секретністю [10].

Основною проблемою при біометричній ідентифікації є співставлення біометричних показників. Якщо біометричні показники змінились чи були пошкоджені, представлені не звичним чином, то співставлення може бути невдалим, що веде до відмови у доступі коректному користувачеві. З’являється ризик помилкового прийняття однієї людини за іншу. Іншою проблемою є загроза атак відтворення. Атакуючий може отримати біометричні ознаки або за допомогою зовнішнього записуючого пристрою, або шляхом копіювання показників у двійковому коді [11].

З проведеного аналізу витікає, що з точки зору перспектив та більш широких можливостей використання найбільш привабливою є технологія мобільної ідентифікації. По-перше, використовується віртуальний ідентифікатор, який є або безкоштовним, або майже безкоштовним у порівнянні, наприклад з карткою. По-друге, на одному смартфоні можна зберігати кілька ідентифікаторів. По-третє, отримується високий ступінь захисту ідентифікаторів від несанкціонованого використання, оскільки смартфони підтримують різноманітні методи аутентифікації, під якою розуміють визначення достовірності користувача за ідентифікаційними ознаками. Нарешті, мабуть саме головне, лише мобільна ідентифікація дозволяє здійснити дистанційне керування правом доступу за рахунок віддаленого надання/відкликання ідентифікатора.

1.3 Аналіз аналогів

Одними з аналогів розглядуваних засобів є універсальний IP контролер

доступу NDC F18IP від компанії Forter (Україна), призначений для керування доступом у приміщення через двері у складі системи контролю та управління доступу, побудованої на основі мережі Ethernet. Пристрій підтримує автономний режим роботи – при відсутності зв′язку з сервером він продовжує виконувати завантаженні у нього права доступу. Ідентифікація доступу здійснюється за безконтактними картками, для роботи з якими контролер передбачає підключення до 2 зчитувачів з інтерфейсом Wiegand [12]. Основні характеристики контролера NDC F18IP наведені у таблиці 1.1.

Таблиця 1.1 Основні характеристики контролера NDC F18IP

Параметр	Значення
Підключення	Ethernet 100Mbit
Підключення зчитувачів -	2 порта Wiegand
Кількість підтримуваних ідентифікаторів	31 768 постійних карток і 1000 тимчасових карток відвідувачів
Журнал подій	47000 записів
Незалежна пам'ять	250 часових зон, 250 тижневих розкладів, 250 вихідних, підтримка плаваючих розкладів
Кількість входів	8, з контролем по струму для підключення датчиків, кнопок і т.д.
Кількість виходів управління зовнішніми пристроями	4 («сухий контакт»): два реле (C NO NC) 24В 5А, два реле (C NO) 24В 1А
Живлення	12В
Мережеві налаштування	Через порт mini USB B вручну, або за допомогою процедури автоконфігурації

Перевагами контролера NDC F18IP є універсальність, підтримка різних зчитувачів карт, протоколу TCP/IP та значної кількості ідентифікаторів. Основними недоліками є керування доступом лише за допомогою карт, що

робить не можливим надання прав доступу дистанційно та порівняно висока вартість, яка складає біля 6,5 тис. грн. на один пункт пропуску.

Ще одним з аналогів є зчитувач-контролер SameKey Card Control від компанії SameKey, призначений для застосування в системах управління доступом, побудованих з використанням інтерфейсів Wi-Fi та Ethernet. Доступ може здійснюватися за NFC-мітками або через мобільний додаток через Bluetooth. Пристрій призначений для надання прав доступу, адміністрування доступу та відвідуваності в офісних та складських приміщеннях, бізнес центрах, будівлях з великою кількістю точок проходу і т .п. Працює через хмару, синхронізуючи дані в реальному часі. Контрольна панель зі статистикою також розташована у хмарі. Підключається до інтернету через мережний кабель Ethernet або бездротове підключення Wi-Fi [13].

До складу хмарної системи контролю доступу крім контролерів SameKey входять хмарна Веб-панель та мобільний додаток. Основні особливості контролера SameKey:

підтримка підключення до мережі Інтернет по Wi-Fi / Ethernet;

надання доступу багатьма способами: NFC-мітки, банківські картки, мобільний додаток через Bluetooth;

безкоштовні мобільні ідентифікатори;

підтримка підключення до електромагнітних і електромеханічних замків;

адміністрування користувачів, пристроїв та прав доступу через Веб-панель;

синхронізація необмеженої кількості користувачів та пристроїв в одному акаунті;

розмежування прав доступу;

гостьовий доступ за посиланням з обмеженням за часом або кількістю;

пам'ять на 5 120 ключів і 16 384 події.

Основні характеристики зчитувач-контролера SameKey представлені у табл. 1.2 [13].

Таблиця 1.2 Основні характеристики контролера SameKey

Параметр	Значення
Тип контролера	Автономний
Інтерфейс підключення	Ethernet, Bluetooth, Wi-Fi
Призначення	Управління дротовими замками
Тип ідентифікації	Картка NFC
Вбудована пам'ять карток	5 120
Вбудована пам'ять подій	16 384
Живлення	5-24 В
Діапазон робочих температур	Від -20°С до + 70°С

До основних переваг зчитувач-контролера SameKey можна віднести підтримку підключення до Інтернету по Wi-Fi/Ethernet, зручне масштабування в на об′єктах зі значною кількістю точок проходу, підтримка можливості організації дистанційного управління доступом.

Основними недоліками є наявність лише одного каналу керування навантаженням та неможливість реалізації зворотного зв′язку з виконавчими пристроями.

Найбільш близьким до розглядуваних засобів є комплекс мобільного керування автоматикою пропуску LOKKYY [14], призначений для використання з різноманітними автоматизованими системами контролю доступу й пропуску транспортних засобів і людей: з воротами, шлагбаумами, ролетами тощо.

Комплекс LOKKYY може застосовуватись на об’єктах побутового, громадського, офісного, промислового, транспортного, телекомунікаційного, банківського, освітнього, медичного та іншого призначення з метою контролю та обмеження пропуску на територію чи з території цих об’єктів. Керування здійснюється через мережі Інтернет, Bluethooth, Wi-Fi за допомогою відповідного мобільного додатка LOKKYY APP, який встановлюється на смартфони користувачів. Цим забезпечується: відсутність будь-яких апаратних ключів, відсутність додаткового апаратного сервера (пристрою централізованого

керування), простота надання довготривалого й короткотермінованого доступу, оперативність зміни ключів, розширена функціональність віддаленого керування й моніторингу. Основні характеристики комплекса LOKKYY наведені у табл. 1.3 [14].

Таблиця 1.3 Основні характеристики комплекса LOKKYY

Параметр	Значення
Підтримувані інтерфейси	Автономний
Інтерфейс підключення	Bluetooth SIG version 5.0, Wi-Fi 802.11 b/g
Кількість вихідних ліній керування навантаженням	4 (2 канали)
Тип виходів	Гальванічно розв’язані нормально розімкнені контакти електромагнітного реле
Максимальна комутована напруга навантаження	60 В постійного струму
Максимальний струм комутації в навантаженні	1 А
Тип датчиків контролю	Магнітні герконові, нормально розімкнені
Номінальна напруга живлення від зовнішнього джерела	24 В постійного або змінного струму частотою 50 Гц
Максимальний струм споживання при спрацюванні реле	200 мА
Споживана потужність в колі вхідної напруги +12 В	не більше 6 Вт
Загальний час спрацювання від подачі команди зі смартфона до спрацювання реле	Від 0,1 с до 10 с

Перевагами комплекса LOKKYY є можливість контролю й керуванням через мережі Інтернет, Bluethooth, Wi-Fi, що не вимагає будь-яких апаратних ключів та додаткового апаратного сервера, простота надання довготривалого й

короткотермінованого доступу, оперативність зміни ключів, розширена функціональність віддаленого керування й моніторингу. Головний недолік необхідність наявності постійного підключення до Інтернет.

З проведеного аналізу аналогів витікає, що розроблювані засоби повинні підтримувати Bluethooth та Wi-Fi підключення, мати до двох каналів керування навантаженням, підтримувати можливість організації зворотного зв′язку з виконавчими елементами.

2 ПРИНЦИПИ ТА ТЕХНОЛОГІЇ ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ

2.1 Аналіз можливих підходів до віддаленого управління доступом

Як було зазначено за результатами проведеного у попередньому розділі аналізу лише технології мобільної ідентифікації можуть надати найбільш широкі можливості в організації управління доступом, зокрема впровадити віддалене керування доступом. Це, перш за все, пов′язано зі швидким розвитком технологій мобільних пристроїв, які сьогодні для багатьох користувачів стали незамінними технічними засобами постійного використання. Відповідно можна спостерігати широке використання мобільних пристроїв та мобільних додатків для вирішення багатьох задач у тому числі і у системах управління доступом.

Сучасні смартфони є багатофункціональним пристроями, що дозволяє організувати віддалене керування доступом кількома способами. Оскільки головним призначенням смартфону є його використання як мобільного телефону, одним з підходів до дистанційного керуання є використання GSM (Global System for Mobile Communications) глобального цифрового стандарту мобільного зв'язку, відповідно до якого для передачі інформації здійснюється в 4-ох частотних діапазонах: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц [15].

Сьогодні пропонується велике різноманіття технічних засобів, що використовують GSM для дистанційного керування з мобільного телефону або смартфона різними пристроями автоматики, у тому числі і тими, що обмежують доступ: воротами та шлагбаумами. Сигнал управління виконавчим пристроєм формується після надходження телефонного дзвінка з певного номера, що знаходиться у базі даних. Тривалість процедури дзвінка, а також можливі збої в роботі операторів зв'язку обмежують сферу застосування подібних систем об'єктами, що характеризуються невисокою інтенсивністю проходу відвідувачів. Крім низької швидкості функціонування, подібна схема забезпечує низький рівень захищеності, оскільки ідентифікаторами є номери абонентів [16].

Типове рішення при реалізації керування доступом з використанням GSM

являє собою цифровий програмно керований засіб, що містить GSM-модуль зі встановленою SIM-картою мобільного оператора. Прийом сигналів з GSM-модуля та вироблення сигналів керування виконавчими пристроями здійснюється блоком керування, який, як правило, будується на мікроконтролері. Номери телефонів, за якими повинен надаватися доступ, записуються у пам′ять мікроконтролера або за допомогою SMS-команд, або за допомогою спеціального програмного забезпечення, наприклад, через USB підключення [16], [17].

Під час виклику від користувача мікроконтролер отримує сигнал від GSM-модуля та порівнює номер абонента з номерами в базі даних. Якщо такий номер є у базі, мікроконтролер формує сигнал керування, після чого скидає вхідний виклик. Якщо такого номера в базі даних немає, мікроконтролер скидає виклик і ніяких дій не виконує. Крім здійснення функцій безпосереднього керування доступом як правило надається можливість віддаленої перевірки стану системи, видавати «гостьові» ключі доступу, а також програмувати сценарії роботи [17].

Головною перевагою використання GSM є те, що стільниковий зв'язок характеризується майже суцільним покриттям, а тому отримується можливість подавати команди та виконувати налаштування практично з будь-якої точки світу.

При іншому підході до керування доступом за допомогою смартфона можна використати те, що сучасні мобільні пристрої функціонують на базі операційних систем. Це надає можливість встановлювати різне програмне забезпечення. Тому ще одним з варіантів є розробка спеціалізованих клієнтських додатків, які дозволяють користувачу самостійно відправляти команди на контролер, що управляє доступом. Головною перевагою такого підходу є відсутність потреби у використанні зчитувачів, що дозоляє спростити архітектуру системи і, як наслідок, знизити її вартість. Саме тому, говорячи про мобільний доступ, найчастіше мають на увазі використання спеціальних мобільних додатків для забезпечення взаємодії із системою керування доступом або застосування телефону як ключа.

Оскільки права доступу можуть надаватися багатьма клієнтам, контролер

повинен підтримувати обробку запитів на доступ від додатків, що використовуються різними користувачами. Тому взаємодія між смартфоном та контролером повинна відбуватися відповідно до принципів, що визначаються архітектурою клієнт-сервер. Архітектура клієнт-сервер є сучасною технологією, що передбачає розподіл завдань між тими, хто надає послуги, та тим, хто їх використовує. Сьогодні принципи клієнт-серверної взаємодії використовуються для організації обміну даними не лише між розподіленими додатками, а й між додатками, що одночасно виконуються в межах одного обчислювального засобу.

Взаємодія між смартфоном та контролером з використанням мобільного додатку може бути організована або напряму, або через віддалений сервер. При прямому доступі контролер є сервером, оскільки він є тим ресурсом, що надає доступ, а мобільний додаток є клієнтом, оскільки він надсилає запити на вирішення задачі щодо отримання можливості доступу. При такому підході програма адміністратора повинна підтримувати два режими роботи: режим сервера та режим клієнта. В режимі сервера обробляються запити клієнтських мобільних додатків на реєстрацію в системі та на отримання ідентифікаторів для доступу. В режимі клієнта ідентифікатори зареєстрованих клієнтів передаються в контролер.

Перевагами прямої взаємодії між мобільним додатком та контролером є висока автономність, малі затримки в отриманні фізичного доступу на об′єкті, відсутність витрат на сервер. Проте такий підхід ускладнює програмне забезпечення контролера, вимагає оренди статичного IP–адресу для нього, що є створює проблеми при розгортанні систем з багатьма точками доступу.

При іншому варіанті взаємодія між смартфоном та контролером здійснюється з використанням віддаленого серверу, який є зв′язувальною ланкою між мобільним додатком та програним забезпеченням контролера. При такому підході мобільний додаток та програмне забезпечення контролера будуть реалізовувати функції клієнта. Серверна частина, що забезпечує переадресацію команд, запитів та відповідей між смартфоном та контролером, розташовується на відділеному сервері.

Такий підхід є доволі перспективним, оскільки відповідає сучасним трендам до часткового або повного переходу в онлайн у багатьох сферах. У зв’язку з цим обсяги використання можливостей та сервісів, що надають Інтернет-технології, постійно зростають, що значно полегшує впровадження зазначеного підходу, дозволяючи отримати нові можливості в керуванні доступом. Крім того, використання віддаленого серверу надає високу гнучкість системі, робить легким її масштабування, дозволяє змінювати права доступу та контролювати роботу системи і переміщення користувачів у режимі реального часу, надає можливість просто оновлювати програмне забезпечення. Головними недоліками використання віддаленого серверу є необхідність постійного надійного Інтернет зв′язку як з боку смартфона, так і з боку контролера, можливі значні затримки у реакції системи, збільшений ризик несанкціонованого втручання в її роботу, тощо.

Підвищити автономність дозволяє застосування мобільного телефону як носія ідентифікатора, що передається від смартфона до контролера керування доступом через Bluetooth або NFC за допомогою мобільного додатку. Передача ідентифікатора у смартфон та запис його до бази даних у контролері доступу здійснюється адміністратором через віддалений сервер за допомогою Веб-додатку. Таким чином отримується можливість управляти правами доступу віддалено. Однак при цьому необхідність у наявності Інтернет зв′язку потрібна лише на час взаємодії віддаленого сервера з мобільним додатком та програмним забезпеченням контролера.

Найпоширеніші способи комунікації між різноманітними сервісами, ресурсами та пристроями в мережі Інтернет реалізуються на основі протоколів HTTP та HTTPS. Протокол HTTP (HyperText Transfer Protocol) є протоколом передачі даних у вигляді гіпертексту, тобто для передачі даних використовується текст. Незважаючи на це повідомлення,що передаються, можуть містити і відео, і аудіо, і картинки. HTTP є протоколом клієнт-серверної взаємодії, що означає ініціювання запитів до сервера з боку клієнта. HTTP є протоколом прикладного рівня, який найчастіше використовує можливості протоколу TCP, проте будь-

який інший надійний транспортний протокол теоретично може бути використаний для доставки таких повідомлень [18].

Протокол HTTPS (HTTP Secure) це зашифрована версія протоколу HTTP. Він забезпечує безпечну передачі даних в Інтернет. Обмін даним здійснюється за тими самими, що й у HTTP, з тією різницею, що перед відправкою дані додатково шифруються, а потім розшифровуються на сервері. Зазвичай HTTPS використовує криптографічні протоколи SSL або TLS для шифрування з'єднання між клієнтом та сервером. Це безпечне з'єднання дозволяє клієнтам безпечно обмінюватися конфіденційними даними із сервером, наприклад, для банківських операцій або онлайн-покупок [18].

Реалізувати систему, де взаємодія між різними компонентами буде реалізовуватись за допомогою HTTP та/або HTTPS протоколів можна використовуючи два різні підходи:

з використанням локального серверу;

з використанням хмарного серверу.

Локальний сервер запускається в одній мережі з користувачами або пристроями, що ним обслуговуються. Це окремий фізичний комп′ютер, що вимагає постійного обслуговування та підтримки.

Хмарні сервери працюють за рахунок віртуалізації фізичних серверів. При віртуалізації за допомогою відповідного програмного забезпечення фізичний сервер поділяється на ізольовані логічні сутності. Таким чином, один фізичний сервер перетворюється на кілька віртуальних серверів, кожен з яких може працювати незалежно від інших і підтримувати кілька додатків, що одночасно працюють. Ці віртуальні сервери можуть бути доступні для користувачів через підключення до Інтернету з будь-якого фізичного місця. Головною перевагою хмарного серверу є висока гнучкість використання. Клієнт вибирає саме те, що потрібно під його потреби.

Хмарні рішення пропонуються у вигляді послуг LaaS, SaaS, PaaS (рис. 2.1). Ці моделі пов'язані між собою. Через послугу LaaS (інфраструктура як послуга) надають інфраструктуру, яка потрібна для керування інструментами SaaS

(сховище та мережеві ресурси). PaaS (платформа як послуга) це хмарне середовище надається розробникам. Сюди входять база даних, операційна система та інші інструменти. Оскільки за роботою платформи стежать провайдери, розробники можуть повністю присвятити свій час розроблюваним додаткам.

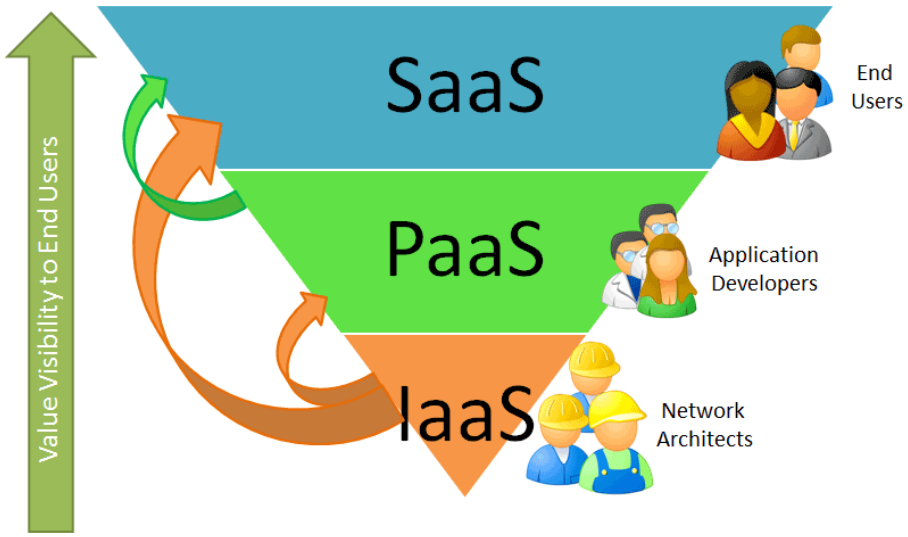

Рисунок 2.1 Моделі хмарних рішень

З точки зору безпеки, у хмарному середовищі використовуються ті самі методи захисту даних, що і в локальному середовищі: виявлення загроз, шифрування, моніторинг у режимі реального часу, багаторівнева ідентифікація. Оскільки дані зберігаються у хмарі, то відповідальність за безпеку розподіляється між користувачем і постачальником послуг.

У дата-центрі, який виділяє потужності під хмарні сервери є вся необхідна інженерна інфраструктура для забезпечення безперебійної та безпечної роботи обладнання, включаючи безперервне електропостачання, кондиціювання та вентиляцію, системи підведення зв'язку та диспетчерські служби.

Порівнюючи особливості використання локального та хмарного серверів можна виділити кілька аспектів. По-перше, це економічна складова. У випадку локального серверу перше, що потрібно зробити — інвестувати у потужний сервер. Потім буде потрібна низка інших IT-послуг, а також залучення фахівців

із сертифікації та внутрішніх IT-аудиторів з метою забезпечення відповідності вимогам безпеки та конфіденційності.

З хмарним середовищем не потрібні великі початкові капіталовкладення, сподіваючись, що вони окупляться в майбутньому. Необхідно платити лише за використані ресурси провайдера у реальному часі. Система оплати у всіх різна. При запуску сервера визначається початковий обсяг пам'яті, ємність, тип дисків і кількість ядер процесора. У процесі експлуатації ці параметри можна легко змінити, відповідно зміниться вартість. За все те, що пов'язане з обслуговуванням обладнання та системами безпеки, бере відповідальність компанія, що надає послугу.

Другий аспект пов'язаний з об'ємом доступних ресурсів. Застосування власного серверу надає можливість його налаштування з урахуванням конкретних завдань при повному використанні усіх наявних апаратних та програмних ресурсів.

У випадку хмарного середовища усе контролюється провайдером. Проте усе більше компаній, що пропонують послуги хмарного сервера, використовують принцип «прозорості», надаючи клієнтам інформацію щодо зовнішнього аудиту, оцінки безпеки тощо.

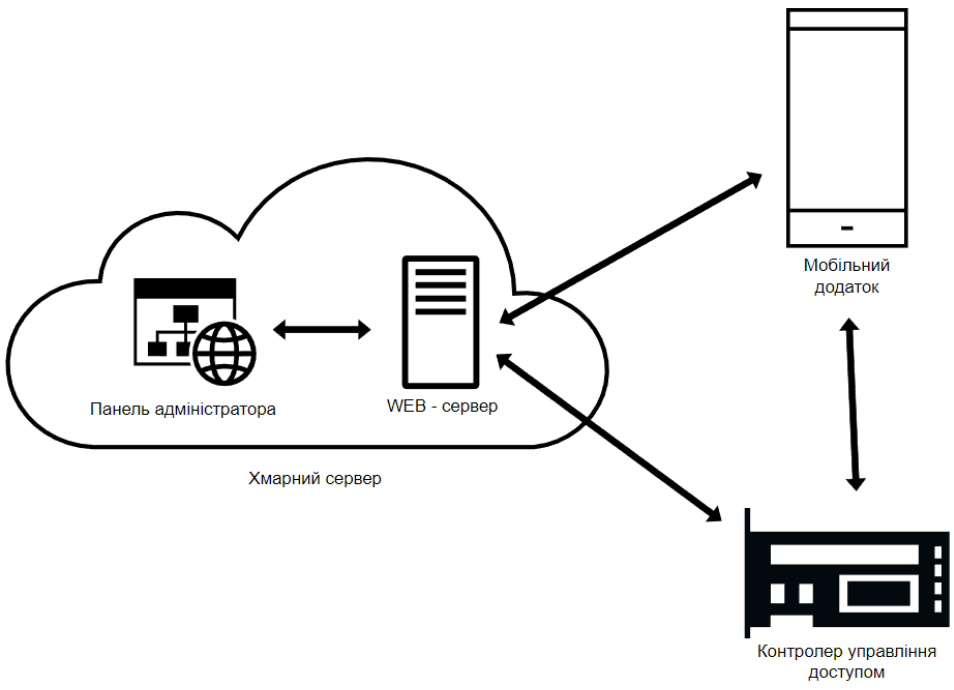

Рисунок 2.2 Принципи віддаленого керування доступом

Підводячи підсумки можна зазначити, що використання хмарного середовища є більш привабливим варіантом, оскільки не вимагає значних витрат, пов′язаних з розгортанням серверу та забезпечення безперебійного доступу до нього через Інтернет. З врахуванням усього викладеного вище, процес віддаленого керування доступом у розроблюваній системі буде таким, що схематично зображений на рис. 2.2.

2.2 Технології мобільної ідентифікації NFC та BLE

Як було зазначено вище достатній рівень автономності системи віддаленого керування доступу може бути досягнений за рахунок передачі ідентифікатора від мобільного пристрою до контролера керування доступом через NFC або Bluetooth. Для вибору, яку з цих технологій найбільш доцільно застосувати, проведемо їх аналіз.

Технологія обміну даними NFC, подібно до технології RIFD, заснована на використанні індуктивного зв'язку між електронними пристроями, що перебувають у безпосередній близькості. Сьогодні NFC набула широкого поширення через популярність мобільних платежів та інших додатків. Головною особливістю NFC є простота використання та дуже малий час встановлення з'єднання [9], [19].

Технологія NFC використовує частоту 13,56 МГц та забезпечує передачу даних зі швидкістю до 424 кбіт/с на відстані приблизно до 10 сантиметрів. На відміну від звичайних безконтактних технологій у даному частотному діапазоні, що дозволяють здійснювати тільки активно-пасивний зв'язок, обмін даними між NFC-пристроями може бути як активно-активним (одноранговим), так і активно-пасивним, тому в стандарті NFC простежуються тісний зв'язок з радіочастотною ідентифікацією RFID.

В технології NFC підтримуються три основні режими роботи пристроїв. Перший, найпоширеніший, пасивний режим емуляції RFID картки, в якому NFC-пристрій працює як безконтактна картка. Це режим використовується при здійсненні безконтактних банківських платежів.

Другий режим, який називають режимом peer-to-peer, є одноранговим і використовується для організації обміну інформацією між двома NFC-пристроями, кожний з яких працює в активному режимі.

Третій режим це режим читання або запису, в якому NFC-пристрій є активним та обмінюється даними з пасивною RFID сумісною міткою [19].

Основним стримувальним фактором до реалізації мобільної ідентифікації з використанням NFC для отримання прав доступу є можливі проблеми при використанні мобільних пристроїв на базі операційної системи iOS. Це обумовлено тим, що тривалий час доступ до NFC в пристроях від Apple для сторонніх розробників був закритий і NFC використовувався лише для здійснення безконтактних платежів за допомогою Apple Pay. Навіть тепер, починаючи з iOS 11, доступ до NFC забезпечується лише в режимі Read Only, що не дозволяє забезпечити повноцінну взаємодію між мобільним додатком та зчитувачем для керування доступом [19].

До основних переваг NFC можна віднести низьке енергоспоживання, швидке встановлення з'єднання, можливості з'єднання з об'єктом без електроживлення, інтуїтивність роботи з пристроями, відповідність промисловим стандартам та взаємодія з існуючими безконтактними технологіями. Мінімальний радіус дії знижує вимоги до захисту від несанкціонованого перехоплення даних. Завдяки цьому у сфері безпеки NFC у майбутньому здатна замінити більшість безконтактних технологій: електронну ідентифікацію особистості, контроль доступу на об'єкт, захист доступу до електронних пристроїв.

Технологія Bluetooth Low Energy (BLE) є інтелектуальною та економічною версією технології бездротової передачі даних Bluetooth, яка з’явилась специфікації Bluetooth 4.0. Технологія BLE широко застосовується там, де вимагається низьке енергоспоживання або там, де передаються невеликі об′єми даних з великими перервами між передачами. Широка інтеграція BLE в персональні електронні пристрої, яку підтримувала більшість виробників смартфонів і комп'ютерів, робить її привабливим вибором для малопотужних і

недорогих додатків Інтернету речей. Стандарт надає швидкість передачі даних в 1 Мбіт/с при розмірі пакета даних 8-27 байт. Дальність зв′язку складає до 300 м при потужності передавача 10 дБм [20].

Так само як і в класичному Bluetooth в BLE використовується ISM-діапазон (англ. Industry, Science and Medicine) від 2,4 ГГц до 2,4835 ГГц, а при встановленні один з пристроїв є ведучим (master), а інший веденим (slave). Один ведучий пристрій може підтримувати кілька з'єднань з веденими, тоді як ведений пристрій може мати лише одне підключення до ведучого. У цьому полягає відмінність BLE від Bluetooth, в якому ведений пристрій міг бути ведучим для інших [20].

Для економії енергії ведений пристрій за замовчуванням знаходиться в сплячому стані, періодично прокидаючись для перевірки наявності пакетів даних від ведучого. Ведучий визначає для своїх ведених пристроїв моменти часу, в які кожен з ведених прокидається, регулюючи тим самим доступ пристроїв до середовища передачі за схемою поділу часу. Завдяки такому підходу активна споживана потужність в BLE за порівнянням з Bluetooth знижена у десяти разів.

У BLE, як і в Bluetooth, використовується технологія адаптивної стрибкоподібної перебудови частоти (AFH). Несуча частота сигналу протягом однієї секунди стрибкоподібно змінюється 1600 разів між 40 частотними каналами шириною 2 МГц. Для кожного з'єднання послідовність перемикання між частотними каналами відома тільки ведучому та веденим. Тому одночасно працюючі поруч пари пристроїв не перешкоджають один одному. Крім того, завдяки такому підходу забезпечується надійна передача даних в умовах зашумленого ефіру [20].

Виділяють два типи каналів канали оголошення та канали даних. Канали оголошення використовуються для пошуку пристроїв, встановлення з'єднання та широкомовної передачі. Канали даних використовуються для обміну даними між пристроями. Для каналів оголошення виділено три частотні канали, інші 37 каналів використовуються для обміну даними.

Порівнюючи технології NFC та BLE треба зазначити, що технологія NFC

надає набагато меншу швидкість передачі, проте забезпечує менший час встановлення з'єднання та має менший радіус дії. Останній фактор можна розглядати як недолік, так і як перевагу, оскільки, як було зазначено вище, мала відстань фактично унеможливлює перехоплення пакетів даних, що гарантує високий рівень безпеки. Крім того, на відміну від Bluetooth, NFC сумісна з технологією RFID, а тому може використовуватися тоді, коли один з пристроїв не має джерела живлення або вимкнений.

На завершення необхідно додати, що NFC не дає ніяких реальних практичних сценаріїв використання або рішень. На відміну від Bluetooth, профілі якого чітко описують як передати файл, як підключити гарнітуру або забезпечити мережний доступ, NFC є лише базою. Безпосереднє використання забезпечується додатковим програмним забезпеченням, яке працює через NFC. З одного боку, це відкриває широкі можливості для розробників, а з іншого — є для них проблемою при забезпеченні взаємодії різних додатків та пристроїв.

Оскільки технологія бездротового зв′язку Bluethooth на відміну від технології NFC підтримується як в пристроях, що використовують Android, так і в тих, що працюють на базі iOS, для передачі ідентифікатора від мобільного пристрою та контролера доступу доцільно здійснювати через Bluethooth.

2.3 Методи та протоколи аутентифікації у веб-додатках

Оскільки розроблювана система має забезпечувати доступ за ідентифікаторами, які можуть змінюватись у режимі реального часу, необхідно забезпечити безпеку даних, що передаються від додатків до апаратної частини, а також розподілити права доступу для різних користувачів. Ці завдання вирішуються за допомогою аутентифікації, під якою розуміють визначення достовірності за ідентифікаційними ознаками. Інакше кажучи аутентифікацію є надання доказів того, що той хто звертається, є тим чим ідентифікувався.

Розглянемо ті з методів аутентифікації, які можуть бути застосовані у розроблюваній системі. Для аутентифікації користувачів у користувачів у додатках використовується аутентифікація за паролем. Одним з найбільш

широко використовуваних протоколів аутентифікації за паролем є протокол HTTP Authentication, що описаний в стандартах HTTP 1.0/1.1. Він існує вже дуже давно, проте і сьогодні користується великою популярністю. Працює протокол за наступним принципом [21]:

сервер при зверненні неавторизованого клієнта (користувача) до захищеного ресурсу надсилає HTTP статус ―401 Unauthorized‖ та додає заголовок ―WWW-Authenticate‖ із зазначенням схеми та параметрів аутентифікації;

браузер при отриманні такої відповіді автоматично показує діалог введення ім’я користувача та паролю; користувач вводить деталі свого облікового запису;

у всіх наступних запитах до веб-сайту браузер автоматично додає HTTP заголовок ―Authorization‖, в якому передаються дані користувача для аутентифікації сервером;

сервер аутентифікує користувача за даними цього заголовка; рішення про надання доступу (авторизація) здійснюється окремо на підставі ролі користувача, ACL або інших даних облікового запису.

Весь процес стандартизований та добре підтримується всіма браузерами та веб-серверами. Існує кілька схем аутентифікації, що відрізняються за рівнем безпеки:

Basic — найпростіша схема (рис. 2.3), коли ім’я користувача (Username) та пароль (Password) користувача передаються в заголовку Authorization в незашифрованому вигляді (base64-encoded); однак при використанні протоколу HTTPS, є відносно безпечним;

Рисунок 2.3 – Приклад аутентифікації з використанням Basic схеми

Digest — Challenge-Response-схема, коли сервер посилає одноразовий числовий код (nonce), а браузер передає MD5 хеш пароля користувача, обчислений з допомогою зазначеного nonce;

NTLM (відома як Windows Authentication) також заснована на Challenge-Response підході, при якому пароль не передається в чистому вигляді; ця схема не є стандартом HTTP, але підтримується більшістю браузерів та веб-серверів; переважно використовується для аутентифікації користувачів Windows Active Directory у веб-застосунках і є вразливою до pass-the-hash-атак;

Negotiate — ще одна схема із сімейства Windows authentication, яка дозволяє клієнту вибрати між NTLM та Kerberos автентифікацією; Kerberos безпечніший протокол, заснований на принципі Single Sign-On, проте він може функціонувати тільки якщо клієнт і сервер знаходяться в зоні intranet і є частиною домену Windows [21].

При використанні HTTP-аутентифікації у користувача немає стандартної можливості вийти з веб-програми, крім закрити всі вікна браузера [22].

Ще одним протоколом аутентифікації за іменем користувача та його паролем є протокол Forms Authentication. Для даного типу аутентифікації не існує єдиного стандарту, тому його реалізація є довільна. Працює Forms Authentication за таким принципом (рис. 2.4): у веб додаток на сторінку монтується HTML-форма, що містить поля вводу ім’я користувача та паролю. Користувач вводить дані та відправляє їх на сервер для аутентифікації через POST-запит. Якщо сервер дозволяє доступ, то формує спеціальний Access Token та відправляє його у відповідь на запит. На стороні клієнту Token зберігається у сховищі браузера. При наступних запитах він автоматично підставляється у запит та дозволяє серверу отримати інформацію про користувача.

Треба зазначити, що перехоплення Token дозволяє отримати несанкціонований доступ, тому при використанні протоколу аутентифікації Forms Authentication обмін даними повинен відбуватися із застосуванням протоколу HTTPS [21], [22].

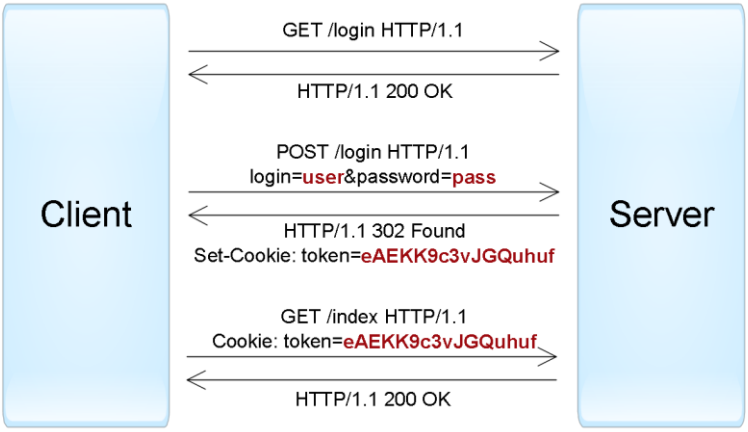

Рисунок 2.4 Приклад Forms Authentication

Протоколи HTTP Authentication та Forms використовуються для аутентифікації користувачів на веб-сайтах. Проте при розробці клієнт-серверних програм з використанням веб-сервісів (наприклад, iOS або Android), поряд з HTTP аутентифікацією, часто застосовуються нестандартні протоколи, в яких дані для аутентифікації передаються в інших частинах запиту [21], [22].

При звертанні пристроїв та додатків до веб-сервісів використовується аутентифікація за ключами. Ключі доступу (Access Key чи API key) — довгі унікальні рядки, що містять довільний набір символів, які по суті замінюють комбінацію Username/Password.

У більшості випадків сервер генерує ключі доступу на запит користувачів, які далі зберігають ці ключі в клієнтських додатках. При створенні ключа також можливо обмежити термін дії та рівень доступу, який отримає клієнтська програма під час аутентифікації за допомогою цього ключа.

Гарний приклад застосування аутентифікації за ключом є хмарні сервіси Amazon Web Services. Припустимо, користувач має веб-додаток, що дозволяє завантажувати і переглядати фотографії, і він хоче використовувати сервіс Amazon S3 для зберігання файлів. У такому випадку, користувач через консоль AWS може створити ключ, що має обмежений доступ до хмари: лише читання/запис його файлів у Amazon S3. Цей ключ можна застосувати для аутентифікації веб-програми в хмарі AWS (рис. 2.5) [21].

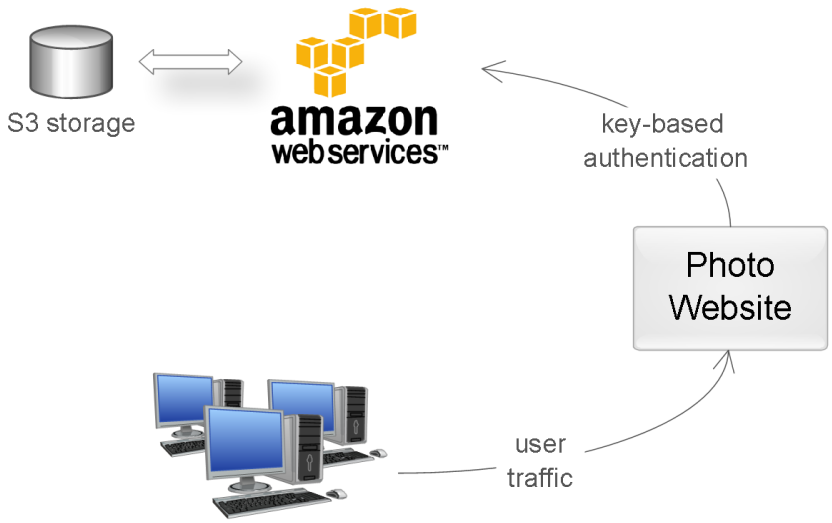

Рисунок 2.5 Приклад аутентифікації за ключем доступу

Використання ключів дозволяє уникнути передачі пароля користувача стороннім програмам (у прикладі вище користувач зберіг у веб-програмі не свій пароль, а ключ доступу). Ключі мають значно більшу ентропію в порівнянні з паролями, тому їх практично неможливо підібрати. Крім того, якщо ключ був розкритий, це не призводить до компрометації основного облікового запису користувача достатньо лише анулювати цей ключ і створити новий.

Враховуючи основні принципи функціонування системи керування доступом, що були визначені у підрозділі 2.1 і відображені на рис. 2.2, будемо застосовувати як аутентифікацію за паролем для аутентифікації клієнтів та адміністраторів у відповідних додатках, так і аутентифікацію за ключем для аутентифікації контролера управління доступом у хмарному сервісі. При аутентифікації за паролем будемо використовувати протокол Forms Authentication.

3 РОЗРОБКА АПАРТНО-ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ

З результатів попереднього розділу витікає, що одним з основних компонентів системи віддаленого керування доступом є контролер, який безпосередньо забезпечує дозвіл/блокування доступу. Тому наступним кроком є розробка контролера керування доступом.

3.1 Розробка структурної схеми контролера керування доступом

Основним завданням контролера керування доступом є надання прав доступу за ідентифікатором, що надсилається через Bluetooth зі смартфона. Для проведення ідентифікації зразок ідентифікатора записується у контролер з використанням ресурсів, що надають Інтернет технології. Підключення контролера до Інтернет можна забезпечити з використанням дротового або бездротового каналу зв′язку. У теперішній час для організації дротового зв′язку в основному використовується або вита пара, або оптичний кабель. Основними перевагами дротового зв′язку є стабільність роботи та надійність, висока швидкість, гарна захищеність. Головний недолік полягає у необхідності прокладання кабелю та викликаними цим додатковими витратами [23].

Бездротовий зв′язок здійснюється за допомогою радіохвиль. Основною перевагою бездротових технологій зв′язку є відсутність потреби у прокладанні кабелю, що надає зручність у використанні, оскільки майже повністю знімаються обмеження на розташування обладнання, простоту та низьку вартість інсталяції. Поряд з цим, бездротовий зв′язок у порівнянні з дротовим забезпечує менші швидкості передачі даних, характеризується порівняно низькою надійністю та поганою захищеністю [23].

З врахуванням переваг та недоліків обох технологій, у розроблюваному контролері доцільно підтримати можливість як дротового, так і бездротового підключення до Інтернет.

На сьогодні найбільш поширеною технологією для дротових підключень мережевого обладнання є технологія Ethernet, що описується стандартами IEEE 802.3. Група стандартів 802.3 описує канальний та фізичний рівні моделі

OSI (Open System Interconnection). Основні відмінності між різними версіями Ethernet полягають у швидкості та використовуваному середовищі передачі даних [24].

Канальний рівень складається з двох підрівнів: підрівня MAC, що відповідає за управління доступом до середовища передачі даних, та підрівня LCC, що забезпечує управління логічним каналом. Незалежно від версій підрівнем MAC є метод множинного доступу з контролем несучої та виявленням колізій CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Метод CSMA/CD дозволяє комп'ютерам спільно використовувати загальне середовище передачі даних без їх втрати. Кожен комп′ютер у будь який момент часу може використати канал для передачі даних. Відповідно до цього канал може бути вільним, зайнятим або перебувати у стані колізії, яка виникає при одночасній спробі кількох комп′ютерів здійснити передачу. Відповідно до цього, головний недолік CSMA/CD полягає в тому, що при зростанні трафіку збільшується число колізій, що знижує продуктивність мережі [24], [25].

Як середовище передачі даних може використовуватися коаксіальний кабель, вита пара або оптоволоконний кабель. Використання коаксіального кабелю є морально застарілим, а тому зараз майже не практикується. Оптоволоконний кабель забезпечує найкращі параметри швидкості та завадостійкості, проте є доволі дорогим для масового використання. Тому найпоширенішим варіантом є використання витої пари [25].

Більшість Ethernet контролерів дозволяють підтримати кілька швидкостей передачі даних, за рахунок автоматичного визначення швидкості та дуплексності. Так, наприклад, контролер Ethernet 10/100 підтримує технології 10BASE-T та 100BASE-TX, що передбачають швидкості передачі 10 Мбіт/с та 100 Мбіт/с, відповідно,а контролер Ethernet 10/100/1000 підтримує стандарти 10BASE-T, 100BASE-TX та 1000BA-T зі швидкостями передачі даних 10 Мбіт/с, 100 Мбіт/с та 1000 Мбіт/с, відповідно [25].

Найпопулярнішою технологією бездротового зв′язку є технологія Wi-Fi, яка фактично є бездротовим аналогом Ethernet. Спочатку Wi-Fi була орієнтована на реалізацію бездротового підключення до точки доступу, що знаходиться в безпосередній близькості. Відповідно до цього ця технологія знайшла

застосування при створенні мереж для забезпечення бездротових з'єднань між комп'ютерами, що розташовані на незначній відстані один від одного. На сьогодні Wi-Fi набула популярності та широкого поширення завдяки доволі широкими можливостям застосування та відносно низькій вартості обладнання [26].

Технологія Wi-Fi описується сімейством стандартів бездротової передачі даних IEEE 802.11x (802.11a, 802.11b, 802.11g, 802.11n і т. д.), які визначають фізичний та канальний рівні моделі OSI. Фізичним рівнем IEEE 802.11x є радіоканал. Канальний рівень забезпечує управління доступом до радіоканалу та управляє обміном пакетами даних між будь-якими двома пристроями бездротової мережі. На канальному рівні використовується метод множинного доступу до середовища з контролем несучої і попередженням колізій CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).

Сьогодні у бездротових мережах Wi-Fi найбільш широко використовуються стандарти IEEE 802.11a, IEEE 802.11b та IEEE 802.11g. Специфікація 802.11a забезпечує швидкість передачі до 54 Мбіт/с в смузі частот 5 ГГц. При цьому максимальна швидкість забезпечується на відстані до 12 метрів для закритих приміщень, і до 30 метрів на відкритому просторі.

Стандарт IEEE 802.11b, відомий також як 802.11 High Rate на сьогоднішній день отримав найбільшого поширення. Він забезпечує трохи нижчу швидкість передачі даних, 11 Мбіт/с, і працює на частоті 2,4 ГГц. Проте відстань впевненого прийому значно більша до 30 метрів в закритих приміщеннях та до 120 метрів на відкритому просторі.

В стандарті IEEE 802.11g збережені переваги двох попередніх стандартів та усунуті їх недоліки. Як і в стандарті 802.11a максимальна швидкість передачі даних складає 54 Мбіт/с, а дальність надійного зв′язку як в стандарті IEEE 802.11b: до 30 метрів в закритих приміщеннях і до 120 метрів на відкритому просторі. Робоча частота - 2,4 ГГц [27], [28].

Головною перевагою технології Wi-Fi є її широке поширення, що обумовлює наявність на ринку широкого різноманіття відповідного обладнання, що забезпечує її легке впровадження. Проте є і недоліки.

По-перше, у різних країнах висуваються різні вимоги до можливості

використання частотного діапазону та до параметрів передавачів/приймачів. Так, наприклад, в одних країнах потрібна реєстрація всіх Wi-Fi мереж, що розгортаються поза приміщеннями, в інших обмежується використання певних частот та потужність передавача. В Україні без дозволу Українського державного центру радіочастот використання Wi-Fi можливо лише за умови, якщо точка доступу обладнана стандартною все спрямованою антеною при потужності сигналу не більшій за 100 мВт на 2,4 ГГц і не більшій за 200 мВт на 5 ГГц. У разі сигналу більшої потужності або при наданні послуг доступу до Інтернет або інших ресурсів, потрібно реєструвати передавач та отримувати ліцензію.

По-друге, найбільш широко використовуваний у Wi- Fi стандарт шифрування WEP може бути відносно легко зламаний через слабку стійкість алгоритму. Проте, слід зазначити, що у нових пристроях підтримується більш досконалий протокол шифрування даних WPA і WPA2.

По-третє, при накладенні сигналів відкритої та закритої точок доступу, що працюють на одному або сусідніх каналах, доступ до відкритої точки доступу може стати неможливим. Крім того, обладнання різних виробників може не у повній мірі відповідати стандарту, що робить його неповністю сумісним. Це призводить до обмеження швидкості передачі даних або можливостей з'єднання [28].

Іншими популярними технологіями бездротового з′єднання є Bluetooth та Zigbee. Як було зазначено вище Bluetooth може забезпечити швидкість передачі даних до 1 Мбіт/с, що набагато менше, ніж для Wi-Fi. Тому застосування Bluetooth для підключення до Інтернет не є доцільним через можливі значні часові затримки при обміні даними.

Технологія Zigbee набула популярності у промислових застосуваннях при організації бездротового зв′язку між датчиками, контролерами та іншими пристроями. На відміну від Wi-Fi або Bluetooth, що передбачають застосування мережевої топології зірка, Zigbee підтримує не лише прості топології бездротового зв'язку, такі як «точка-точка» або «зірка», а й складні бездротові мережі з ретрансляцією та маршрутизацією повідомлень з топологіями «дерево» або «комірчаста мережа». Це надає можливість здійснювати обмін даними між

пристроями, які не лише знаходяться на значних відстанях один від одного, а й в умовах відсутності прямого зв′язку з роутером [29].

Технологія Zigbee заснована на стандарті IEEE 802.15.4, відповідно до якого середовищем зв′язку є радіоканал з частотою 2,4 ГГц. Стандарт передбачає радіус покриття в межах від 10 до 75 м. Пропускна здатність каналу може досягати до 250 кбіт/с [29]. Така мала швидкість робить неможними використання Zigbee для обміну даними між розроблюваним контролером та віддаленим сервером через Інтернет.

Отже, не зважаючи на те, що у розроблюваному контролері буде використовуватися Bluetooth для забезпечення взаємодії зі смартфоном, підключення до віддаленого сервера через Інтернет будемо здійснювати з використанням технології Wi-Fi. Доцільність такого рішення обумовлена не лише більшою пропускною здатністю Wi-Fi за порівнянням з Bluetooth, а й тим, що Wi-Fi підключення є типовим рішенням для організації доступу до Інтернет, що спрощує його реалізацію.

Відповідно до викладеного вище приходимо до структурної схеми контролера віддаленого керування доступом, яка наведена Додатку В. Основними структурними блоками контролера є: мікроконтролер, Bluetooth-модуль, Ethernet-модуль, Wi-Fi модуль, блок комутації та блок індикації.

Головним блоком пристрою є мікроконтролер. Він забезпечує функціонування контролера віддаленого керування доступом, а саме: надання доступу за ідентифікатором, що надсилається мобільним пристроєм через Bluetooth з′єднання. Для виконання цього завдання мікроконтролер забезпечує взаємодію з віддаленим сервером за протоколом TCP/IP у режимі клієнта для отримання ідентифікаторів, що надають права доступу, та керує роботою виконавчого пристрою, за допомогою якого надається фізичний доступ. За допомогою Веб-додатка для чергового клієнта на сервері реєструється ідентифікатор, який записується в пам′ять мікроконтролера через Інтернет.

Підключення до Інтернет може здійснюватися з використанням або дротового з′єднання на основі витої пари, або бездротового з′єднання через Wi-Fi. Дротове та бездротове підключення до мережі забезпечуються модулями Ethernet та Wi-Fi, відповідно, основним завданням яких є реалізація

взаємодії із середовищем передачі даних. Модулі Ethernet та Wi-Fi забезпечують підтримання функцій фізичного рівня та підрівня MAC канального рівня моделі OSI. Функції вищих рівнів будуть реалізовуватися програмним забезпеченням мікроконтролера, зокрема підтримкою стека протоколів TCP/IP.

Право доступу надається мікроконтролером за результатами порівняння ідентифікатора, що надсилається зі смартфону, з ідентифікаторами, що були отримані через Інтернет та зберігаються в його енергонезалежній пам′яті. Прийом ідентифікатора зі смартфону здійснюється мікроконтролером через радіоканал Bluetooth, що використовується у режимі симетричного з′єднання «точка-точка». Обмін даними між стартфоном та мікроконтролером через Bluetooth забезпечується за допомогою Bluetooth-модуля. Основним елементом модуля є радіоблок, який здійснює перетворення цифрових даних в аналоговий радіосигнал у режимі передачі, та зворотне перетворення в режимі прийому. Таким чином, Bluetooth-модуль забезпечує фізичне з′єднання між смартфоном та мікроконтролером. Створення логічного каналу та організація обміну даними через нього здійснюється програмним забезпеченням мікроконтролера та смартфона.

Надання доступу на фізичному рівні здійснюється за допомогою пристроїв загородження, таких як двері, ворота, шлагбауми і т. і. Підтримання закритого стану, наприклад, дверей здійснюється виконавчим пристроєм, який за принципом своєї дії може бути електромеханічним та електромагнітним. Електромеханічний принцип дії виконавчого механізму заснований на переміщенні елементів, що закривають (запорів, ригелів замків і т. і.), за допомогою вмикання на час їх пересування електромотора або електромагніту.

У виконавчих механізмах з електромагнітним принципом дії рухомі механічні елементи, що закривають, відсутні, а блокування засобів загородження, наприклад, дверей, здійснюється за допомогою сил магнітного тяжіння, створюваних потужним магнітом. Часто у виконавчих пристроях застосовується електромагнітне блокування елементів, що закривають, наприклад, магнітні засувки.

Оскільки керування і електромеханічними, і електромагнітними виконавчими пристроями здійснюється за рахунок прикладання до них

електричної напруги, до структурної схеми контролера введений блок комутації. За сигналом, що формується мікроконтролером, блок комутації забезпечує подау на виконавчий пристрій напруги, потрібної для його спрацювання.

Основним елементом блоку комутації є електронний прилад, що може перебувати у двох станах: високоомному або розімкненому, та низькоомному або замкненому Перемикання між станами відбувається за електричним сигналом керування. Такий електронний прилад може бути напівпровідниковим або електромагнітним. Основними напівпровідниковими або твердотільними елементами, що широко використовуються для комутації силових електричних кіл, є тиристори та симістори. Вони надають можливість здійснити безконтактну комутацію електричних кіл зі значеннями напруг від 24 В до 480 В постійного або змінного струмів.

Електромагнітне реле є електромеханічними елементом, в основу роботи якого покладено явище електромагнітної індукції. Реле складається з електромагніту та механічних електричних контактів, замикання яких відбувається під дією магнітного поля, що виникає у котушці електромагніту при прикладанні до неї електричної напруги.

Електромагнітні реле бувають нейтральні, поляризовані та імпульсні. Нейтральні реагують лише на значення струму у котушці, поляризовані на полярність сигналу керування. Керування імпульсними або бістабільними реле, здійснюється імпульсним сигналом, що переводить контакти реле з одного стану в інший. Після зняття електричного імпульсу контакти реле залишаються в стані замкнено або розімкнено, що відрізняє їх від звичайних реле, в яких увімкнений стан зберігається лише на час прикладання напруги керування [30].

За порівнянням з електромагнітними реле тиристори або симістори характеризуються меншим часом спрацювання та набагато більшим ресурсом роботи, тоді як ресурс роботи електромагнітних реле обмежується кількістю можливих перемикань його контактів. З іншого боку, електромагнітні реле забезпечують можливість комутації набагато більшої електричної потужності, мають кращу стійкість до імпульсів перенапруги, не мають електричного зв′язку між колом керування та колом комутації, характеризуються малим тепловиділенням, мають меншу вартість [30].

З врахуванням цього керування виконавчим пристроєм будемо здійснювати за допомогою електромагнітного реле. Серед різних типів реле для побудови блоку комутації будемо використовувати імпульсне реле, оскільки воно споживає електричну потужність лише у момент перемикання та не змінює свій стан при вимиканні напруги.

Для отримання інформації про те, чи знаходиться пристрій загородження у зачиненому стані, передбачимо можливість підключення відповідних датчиків. Сигнали з виходів датчиків надходять на входи мікроконтролера. Стан буде визначатися мікроконтролером за логічним значенням сигналу на виході датчика.

Останнім блоком контролера віддаленого доступу є блок індикації, основним завданням якого є надання інформації користувачеві про результат ідентифікації та стан виконавчого пристрою: зачинений чи відкритий. Це завдання можна вирішити за допомогою двох світлодіодів: червоного та зеленого кольору світіння. При зачиненому механізмі, що надає фізичний доступ, буде активним світлодіод червоного кольору випромінювання, при відкритому зеленого. Ці самі світлодіоди можна використати і для індикації результату ідентифікації. Позитивний результат ідентифікації буде відображатися вимиканням червоного світлодіода та вмиканням зеленого. Оскільки при негативному результаті ідентифікації виконавчий пристрій залишається у зачиненому стані, тобто режим світіння червоного світлодіода не змінюється. Для того, щоб користувач розумів, що пристрій реагує на пред′явлення ідентифікатора, негативний результат ідентифікації будемо відображати короткочасним вимиканням світлодіода червоного кольору світіння.

3.2 Аналіз можливої реалізації структурних блоків та вибір елементної бази

Головним структурним блоком контролера керування доступом є мікроконтролер. Сучасний ринок мікроконтролерів наповнений різними моделями з різною архітектурою та від різних виробників. Найбільш поширеними та популярними серед них є RISC мікроконтролери з Гарвардською

архітектурою. До недавнього часу найпоширенішими і доступнішими були два сімейства 8-и бітних мікроконтролерів: AVR та PIC. Сьогодні усе більшої популярності набувають 32-ох розрядні ARM мікроконтролери на ядрі Cortex-M3. На даний час ціна на них знизилася настільки, що за цим показником вони вже можуть конкурувати з 8-ми та 16-ти бітними мікроконтролерами. При цьому продуктивність та функціональні можливості ARM мікроконтролерів є набагато більшими.

Мікроконтролерне ядро ARM (Advanced RISC Machines) було розроблено англійською компанією ARM Limited, яка займається тільки розробкою архітектури та засобів розробки (компіляторів та IDE) і не має виробничих потужностей з випуску мікроконтролерів, а тому продає ліцензії іншим компаніям. Клієнтами ARM Limited є понад 60 компаній-виробників напівпровідникової продукії, серед яких можна виділити таких популярних виробників як Altera, Analog Devices, Atmel, Cirrus Logic, Fujitsu, Intel, Motorola, National Semiconductor, Philips , ST Microelectronics та Texas Instruments [31].

Основні особливості ядра Cortex-M3, що виділяють ARM мікроконтролери серед конкурентів [32]:

повністю 32-бітна архітектура: усі регістри 32-бітові, арифметичні операції працюють з 32-бітними даними; операція множення виконується за 1 такт, ділення за 2-12 тактів;

велика кількість (від 16) регістрів загального призначення, характерна для архітектури RISC;

відмінна підтримка режимів енергозбереження; у режим сон може бути переведений як весь мікроконтролер, так і його окремі підсистеми;

24-бітний таймер SysTick, що надає можливість задавати інтервал його спрацьовування в широких межах для організації кінцевих автоматів і планувальника RTOS;

повноцінне налагодження JTAG або SWD, що надає можливість ставити точки зупинки (breakpoints), переглядати вміст змінних та регістрів, покроково виконувати програму тощо.

контролер переривань NVIC підтримує до 240 переривань та до 256 пріоритетів;

наявність контролера прямого доступу до пам′яті DMA дозволяє периферії обмінюватися даними з оперативною пам′яттю без участі ядра;

загальна орієнтованість набору інструкцій на компілятори С, що в сприяє більш ефективній оптимізації коду компіляторами С, а значить і більш високій швидкості роботи.

Найбільш популярним сімейством ARM мікроконтролерів на ядрі Cortex-M3 є сімейство STM32 від компанії ST Microelectronics. Одна з причин його світової популярності максимальний комфорт розробника. Якщо універсальність ядра Cortex-M3 дозволяє змінювати виробника з мінімальними витратами на програмний код, то pin-to-pin сумісність усередині сімейства STM32 дозволяє змінювати об′єми флеш-пам'яті та ОЗП, а також периферію, не змінюючи друкованої плати. «Pin-to-pin сумісність» означає, що для одного розміру корпусу усі сигнали зберігаються на тих самих входах/виводах для різних варіантів мікроконтролерів сімейства. Крім того, STM32 мають багату периферію [32]:

кілька багатоканальних швидкісних 12-бітних АЦП;

двоканальний ЦАП, що підтримує 8-ми та в 12-бітнні режими роботи;

12-канальний контролер DMA, що обслуговує до 12 запитів, має 4 рівні пріоритетів, незалежні розміри блоків даних для прийому та передачі (8, 16 та 32 біти), підтримує кільцевий буфер, передачу даних у режимах пам'ять-пам'ять, пам'ять-периферія, периферія-пам'ять та периферія-периферія;

кілька 16-бітних таймерів з довільними дільниками (не тільки ступеня двійки, як у AVR) з різноманітними режимами роботи;

модуль RTC (Real-Time Clock) годинник реального часу з лічильником та будильником;

кілька Watchdog-таймерів для більшої надійності;

FSMC — Flexible Static Memory Controller, що забезпечує прозорий доступ до кількох видів пам'ят: SRAM, ROM, NOR Flash, NAND Flash, PSRAM і 16-бітових PC Card-сумісних пристроїв.

SDIO — Secure Digital I/O interface для читання/запису на карти пам'яті MMC та SD, що дає можливість легко та просто забезпечити підтримку FAT та повноцінно працювати з файлами на картках.

контролер USB, що забезпечує повну підтримку стандарту USB 2.0 Full-Speed, до 8 кінцевих точок та режим USB OTG (On-The-Go) для зв'язування USB-пристроїв без участі хоста;

контролер Ethernet з повною підтримкою MAC-рівня та швидкості 10/100 Мбіт/с;

шина I2S — шина цифрового аудіо пристрою;

UART, SPI, I2C, CAN.

Ще одним з факторів, що сприяють популяризації STM32, є велика кількість різноманітних засобів розробки як платних, так і безкоштовних, а також великий вибір безкоштовних бібліотек з документацією із застосування [32].

З врахуванням викладеного ще як мікроконтролер будемо використовувати мікроконтролер серії STM32. Для реалізації підключення до Ethernet будемо вибирати мікроконтролер з контролером Ethernet. При цьому будемо орієнтуватися на готові модулі, що сприятимемо зменшенню кількості використовуваних компонентів та спрощенню фізичної реалізації контролера керування доступом. Серед різних варіантів будемо вибирати той, що має найменші габаритні розміри та меншу вартість.

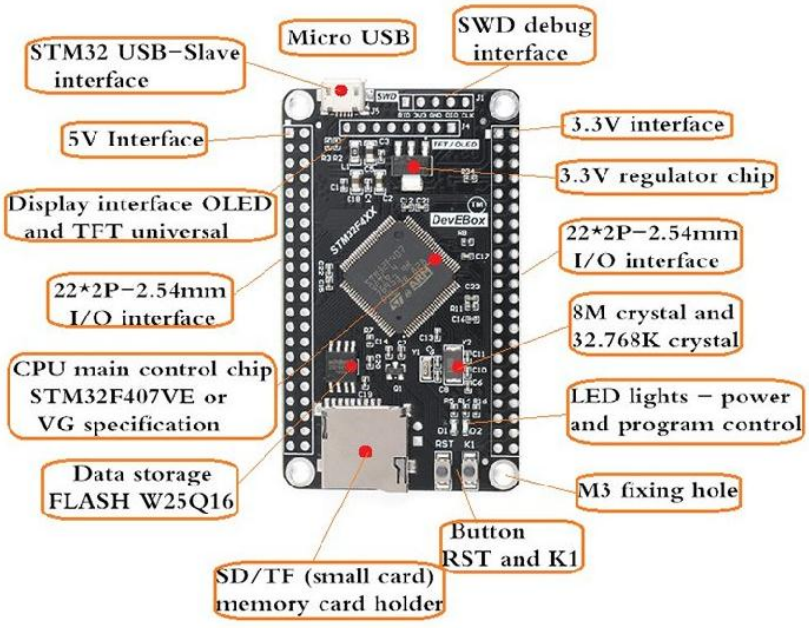

Рисунок 3.1 Модуль STM32F407VET6-Mini

Відповідно до цього вибираємо модуль STM32F407VET6-Mini (рис. 3.1),

побудований на високопродуктивному мікроконтролері STM32F407VET6. Робоча частота ядра становить 168 МГц. На платі модуля розміщені: додаткова FLASH пам'ять на 16Mbit, роз'єм підключення модуля бездротового зв'язку NRF24L01, TFT LCD дисплея з FSMC інтерфейсом, SD карти, батарейний відсік годинника реального часу. Основні характеристики модуля STM32F407VET6-Mini наведені у табл. 3.1 [33].

Таблиця 3.1 Характеристики модуля STM32F407VET6-Mini

Параметр	Значення
Мікроконтролер	STM32F407VET6, ядро ARM Cotrex M4
Максимальна частота	168 МГц
Об'єм пам'яті програм (FLASH)	512 кБайт
Об'єм пам'яті даних (RAM)	192 кБайт
Зовнішня пам'ять	W25Q16/16Мбіт
Кварцові резонатори	HSE - 8МГц і RTC - 32.768Гц
Контролер DMA	16-ти потоковий з FIFO та пакетною підтримкою
Кількість доступних виводів	96 шт.
Таймери загального призначення	12 шт., 16 біт 2 шт., 32 біт
Розширений таймер з ШІМ управління двигуном	1 шт.
Генератор випадкових чисел	1 шт.
Системний таймер	1 шт.
Сторожові таймери	2 шт.
АЦП	3 шт., 12 біт
АЦП	2 шт., 12 біт
UART	4 шт.
SPI	3 шт.
I2S	3 шт.

Продовження табл. 3.1

I2C	2 шт.
FSMC	1 шт.
SDIO	1 шт.
CAN	2 шт.
USB	2 шт.
Ethernet	1 шт., 10/100 Мбіт/с
Роз'єм 32-pin для підключення TFT LCD дисплея з інтерфейсом FSMC	1 шт.
Роз'єм 8-pin підключення модуля бездротового зв'язку NRF24L01	1 шт.
Роз'єм SD картки	1 шт.
JTAG/SWD debug	1 шт.
Модуль RTC із низьким енергоспоживанням	1 шт.
Кнопки користувача	3 шт.
DC-DC перетворювач	5В в 3.3В
Напруга живлення мікроконтролера	3,3 В
Напруга живлення плати	5 В
Розміри плати	72мм × 85 мм

На рис. 3.2 наведена схема з призначенням контактів роз′ємів модуля STM32F407VET6-Mini.

Підключення контролера керування доступом до локальної мережі Ethernet буде здійснюватися з використанням наявного у мікроконтролері STM32F407VET6 модуля Ethernet. Ethernet-модуль відповідає стандарту IEEE802.3 і забезпечує передачу даних на швидкостях 10 і 100 Мбіт/с через стандартний інтерфейс MII або скорочений інтерфейс RMII. Крім того забезпечена підтримка протоколу IEEE1588 на апаратному рівні, VLAN (віртуальна локальна мережа), режимів Half-duplex і Full-duplex підрівня

управління доступом до середовища (підрівня MAC) [34].

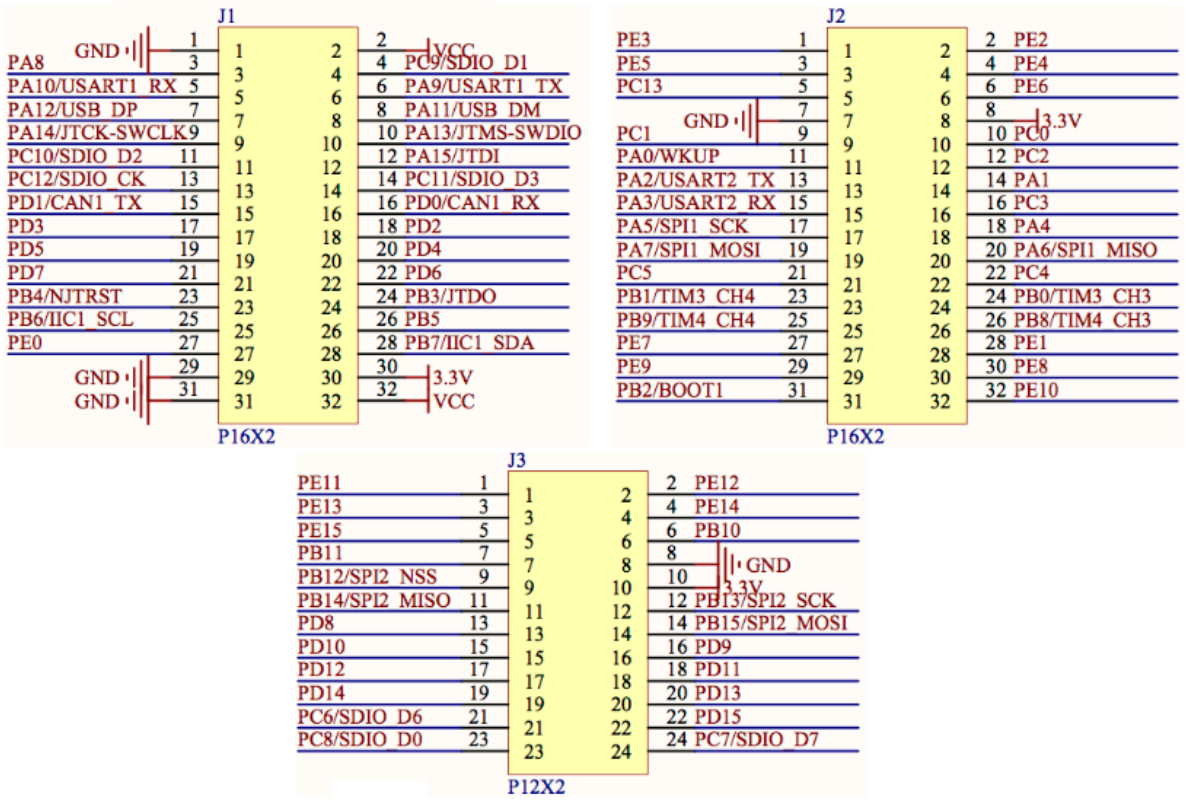

Рисунок 3.2 Призначення контактів роз′ємів модуля STM32F407VET6-Mini

Для полегшення процесу розробки Ethernet-додатків компанія STMicroelectronics представила на сайті кілька рекомендацій із застосування. Наприклад, описано застосування lwIP TCP/IP- і NicheLiteTM TCP/IP-стеків.

Для підключення до фізичної шини LAN мікроконтролер STM32F407xx потребує зовнішнього фізичного інтерфейсного пристрою трансивера фізичного рівня (PHY). Трансивер забезпечує кодування даних, що передаються від Ethernet-модуля для передачі їх у транспортне середовище, синхронізацію даних, що передаються, а також їх прийом і декодування.

Підключення трансивера до мікроконтролера здійснюється за інтерфейсами SMII, MII або RMII. Інтерфейс SMII утворює службовий канал, що використовується для доступу до регістрів управління або статусу трансивера. Він складається лише з двох сигналів:

MDIO — двонаправлений послідовний канал даних для зв'язку з регістрами трансивера;

MDC тактовий сигнал послідовного каналу даних MDIO.

Інтерфейс MII (рис. 3.3) забезпечує взаємодію між підрівнем MAC, що підтримується Ethernet-модулем, та трансивером на швидкостях передачі даних 10 Мбіт/с або 100 Мбіт/с. Усі операції інтерфейсу MII виконуються в синхронному режимі [34].

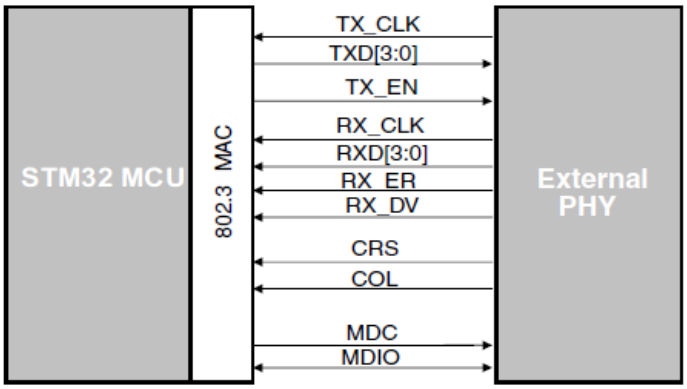

Рисунок 3.3 Схема підключення трансивера за інтерфейсом MII

Канал передачі даних MII містить наступні сигнали:

MII_TXD (3..0) група паралельних сигналів даних, які надходять в трансивер з MAC;

MII_TX_CLK тактовий сигнал для передачі даних; виробляється в трансивері і передається в MAC: 2,5 МГц для операцій 10 Мбіт/с, 25 МГц для операцій 100 Мбіт/с;

MII_TX_EN дозвіл передачі; MAC встановлює цей сигнал, коли встановлені достовірні дані для передачу;

MII_CRS опитування несучої; при напівдуплексних операціях трансивер встановлює цей сигнал, коли передає або приймає пакети даних; при дуплексних операціях CRS встановлюється при прийомі;

MII_COL детектування колізії; встановлюється трансивером коли виявлено колізію на лінії; залишається високим на час колізії; цей сигнал є асинхронним і неактивним при дуплексних операціях;

MII_RXD (3..0) група паралельних сигналів даних, що видаються з трансивера в MAC-контроллер;

MII_RX_CLK тактовий сигнал для прийому даних; виробляється в трансивері і передається в MAC: 2,5 МГц для операцій 10 Мбіт/с, 25 МГц для

операцій 100 Мбіт/с;

MII_RX_DV достовірність прийнятих даних; встановлюється трансивером, коли він отримує достовірний пакет даних і, відповідно, видає достовірні дані на RXD;

MII_RX_ER помилка прийому; встановлюється трансивером при виявленні помилки у потоці даних, що приймаються [34].

Інтерфейс RMII (Reduced MII) (рис. 3.4) — це «скорочений» варіант MII. Трансивер, що підтримує RMII, має можливість працювати зі скороченим набором сигналів інтерфейсу MII. У такому режимі роботи розрядність шин RXD і TXD скорочується вдвоє, але відповідно вдвоє збільшується частота синхронізації [34].

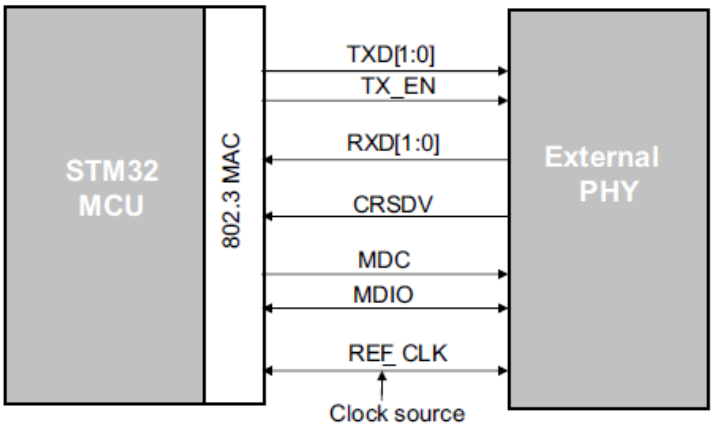

Рисунок 3.4 Схема підключення трансивера за інтерфейсом RMII

Вибір способу підключення, MII чи RMII, здійснюється 23-ім бітом (MII_RMII_SEL), в регістрі SYSCFG_PMC мікроконтролера. У табл.3.2 наведений перелік ліній портів введення/виведення мікроконтролера STM32F407VET6, альтернативними функціями яких є сигнали інтерфейсів MII та RMII [34].

Таблиця 3.2 Ліній портів введення/виведення мікроконтролера STM32F407VET6 з альтернативними функціями MII та RMII

Порт	Ethernet
PA0	WKUP ETH_MII_CRS
PA1	ETH_MII _RX_CLK / ETH_RMII _REF_CLK

Продовження таблиці 3.2

PA2	ETH_MDIO
PA3	ETH_MII_COL
PA7	ETH_MII _RX_DV/ETH_RMII _CRS_DV
PB0	ETH_MII_RXD2
PB1	ETH_MII_RXD3
PB5	ETH_PPS_OUT
PB8	ETH_MII_TXD3
PB10	ETH_MII_RX_ER
PB11	ETH_MII_TX_EN/ETH_RMII_TX_EN
PB12	ETH _MII_TXD0/ETH_RMII_TXD0
PB13	ETH _MII_TXD1/ETH_RMII_TXD1
PC1	ETH_MDC
PC2	ETH_MII_TXD2
PC3	ETH_MII_TX_CLK
PC4	ETH_MII_RXD0/ETH_RMII_RXD0
PC5	ETH_MII_RXD1/ETH_RMII_RXD1
PE2	ETH_MII_TXD3
PG8	ETH_PPS_OUT
PG11	ETH_MII_TX_EN/ETH_RMII_TX_EN
PG13	ETH_MII_TXD0/ETH_RMII_TXD0
PG14	ETH_MII_TXD1/ETH_RMII_TXD1
PH2	ETH_MII_CRS
PH3	ETH_MII_COL
PH6	ETH_MII_RXD2
PH7	ETH_MII_RXD3
PI10	ETH_MII_RX_ER

Як трансивер вибрано модуль DP83848 Ethernet Board (рис. 3.5), що конструктивно об′єднує Ethernet-трансивером фізичного рівня DP83848, роз'ємом

RJ-45 та роз′єм керуючого інтерфейсу для підключення до мікроконтролерів з вбудованим Ethernet-модулем. Основні характеристики модуля DP83848 Ethernet Board наведені у табл. 3.3 [35].

Рисунок 3.5 Модуль DP83848 Ethernet Board

Таблиця 3.3 Характеристики модуля DP83848 Ethernet Board

Параметр	Значення
Підтримувані мережеві підключення	10/100МБіт
Стандарт	802.3u RMII
Напруга живлення	3.3 В
Споживана потужність	не більше 270 мВт

Для підтримання підключення до бездротової мережі WiFi також скористаємося готовими рішеннями, які за рахунок реалізованої у них підтримки сімейства протоколів TCP/IP дозволяють суттєво спростити процес розроби. На сьогодні найбільш популярними є ESP модулі WiFi, побудовані на мікросхемі ESP8266.

Модулі випускаються компанією Espressif Systems (Китай) і відрізняються серед конкурентів найнижчою вартістю при достатньо значних можливостях. Існує кілька модифікацій, що в основному відрізняються кількістю флеш-пам'яті, типами роз′ємів і т. і.

Конструктивно модулі ESP об′єднують мікросхему ESP8266EX, мікросхему SPI Flash-пам'яті ємністю 2 Мбайт та інтегровану PCB-антену. Мікросхема ESP8266EX інтегрує у собі 32-бітний мікроконтролер Tensilica L106 з тактовою частотою 80 МГц та ультранизьким енергоспоживанням і

радіотракт. В режимі максимальної продуктивності тактова частота мікроконтролер Tensilica L106 може збільшуватися до 160 МГц. Мікросхема ESP8266EX забезпечує підтримку IPv4, TCP/UDP/HTTP/FTP та режими Wi-Fi-з'єднання Wi-Fi-клієнт, Wi-Fi-точка доступу, точка доступу плюс клієнт. Для забезпечення надійності бездротової передачі даних (Wi-Fi 802.11b/ g/n) підтримуються зтехнології WPA/WPA2, WEP/TKIP/AES [36], [37].

За даними виробника підтримка мережі Wi-Fi забирає лише 20% процесорного часу. Увесь інший час може бути використаний на додаток користувача. Модуль працює на операційній системі RTOS, що полегшує інтеграцію користувацьких додатків у його програмне забезпечення [36].

Серед різних модифікацій модулів ESP вибираємо модель ESP-07 (рис. 3.6), оскільки вона не лише має керамічну антену, а й передбачає можливість підключення зовнішньої, що дозволить збільшити відстань та якість зв'язку. Взаємодія з модулем відбувається з використанням АТ-команд. Зовнішній вигляд модуля ESP-07 наведений на рис. 3.1, а його основні технічні характеристики представлені у табл. 3.4 [37].

Рисунок 3.6 –Wi-Fi модуль ESP-07

Таблиця 3.5 – Характеристики Wi-Fi модуля ESP-07

Процесорне ядро	Tensilica L106, 32 біт
Wi-Fi-протоколи	802.11 b/g/n
Частотний діапазон	2.4 – 2.5 ГГц
Режими WiFi	Station / SoftAP / SoftAP + Station
Безпека	WPA/WPA2
Шифрування	WEP/TKIP/AES
Підтримувані мережеві протоколи	IPv4, TCP/UDP/HTTP/FTP

Продовження табл. 3.5

Підтримка	WiFi Direct (P2P), P2P Discovery, P2P GO (Group Owner) mode, GC (Group Client) mode, P2P Power Management.
Інтерфейс для підключення	UART
Напруга живлення	від 2.5 В до 3.6 В
Середній струм споживання	80 мА

Для забезпечення взаємодії контролера керування доступом зі смартфоном через Bluetooth з′єднання також скористаємося готовим Bluetooth-модулем. Серед різних моделей Bluetooth-модулів вибираємо модуль HC-05 (рис. 3.8), що користується найбільшою популярністю, а тому широко представлений на ринку. Модуль HC-05 призначений для реалізації двостороннього зв'язку за протоколом Bluetooth і може використовуватися у режимах Master, та Slave. Завдяки цим двом режимам модуль може самостійно виявляти Bluetooth пристрій та налагоджувати зв’язок з ним.

Підключення модуля здійснюється за послідовним асинхронним ТТЛ сумісним інтерфейсом UART. Основним елементом модуля є мікросхема CSR BC417, яка підтримує зв'язок Bluetooth версії 2.0. Швидкість передачі даних становить до 3 Мбіт/с. Взаємодія з модулем відбувається за допомогою АТ-команд. Основні характеристики модуля HC-05 наведені в табл. 3.6 [38].

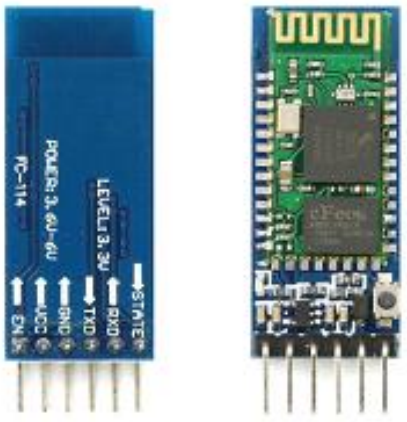

Рисунок 3.7 Bluetooth-модуль HC-05

Таблиця 3.6 Характеристики Bluetooth-модуля HC-05

Параметр	Значення
Робоча напруга	+3,3 В або +5 В
Споживаний струм	50 мА
Основна частота	2,4 ГГц
Антена	Інтегрована
Потужність	≤ 4дБм, клас 2
Чутливість	≤ 84дБм, при 0,1%
Швидкість синхронної передачі даних	1 Мбіт/с
Швидкість асинхронної передачі даних	2,1 Мбіт/с
Захист	Авторизація та шифрування
Розміри (Д × Ш × В)	17 мм × 43 мм × 7,5 мм

Плата модуля HC-05 має 6 контактів для підключення (табл. 3.7).

Таблиця 3.7 Функціональне призначення контактів модуля HC-05

Контакт	Символ	Призначення
1	EN	Вхід дозволу Активний рівень низький
2	VCC	Живлення
3	GND	Контакт «земля»
4	TXD	Вихід послідовних даних
5	RXD	Вхід послідовних даних
6	STATE	Вихід індикації стану Перемикання між логічними рівнями встановлення зв′язку Високий рівень зв'язок встановлено

Керування виконавчим пристроєм, що перешкоджає/дозволяє фізичний доступ, буде здійснюватися за допомогою імпульсного (бістабільного)

електромагнітного реле. Такі реле мають дві обмотки імпульсного керування. Імпульс струму в одній з них викликає замикання контактів реле, в іншій їх розмикання. Відповідно до цього керування імпульсним реле здійснюється за допомогою двох транзисторних ключів, що забезпечують формування імпульсів струмів в обмотках (рис. 3.8).

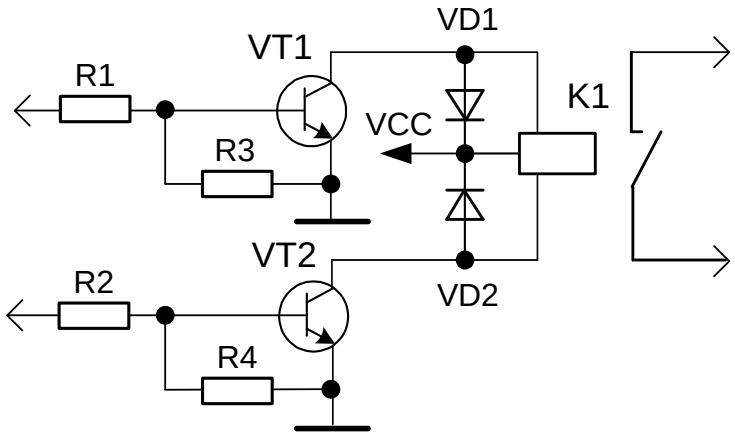

Рисунок 3.8 Схема керування імпульсним реле

Основними критеріями при виборі реле є комутована потужність не менша за 2 кВт та напруга керування +5 В. Відповідно до цих критеріїв вибираємо реле G2RL145DC, основні параметри якого представлені у табл. 3.8 [39].

Таблиця 3.8 Основні характеристики реле G2RL145DC

Параметр	Значення
Комутована потужність	12 А, 250 В змінного струму 12 А, 24 В постійного струму
Напруга керування	5 В
Струм керування	80 мА
Кількість перемикань	20 млн

Транзисторні ключові каскади будемо будувати на широко використовуваних транзисторах BC817-25, що мають максимальний струм колектора більший за струм керування реле, що складає 80 мА, а напругу .

колектор-емітер більший за 5 В. Основні характеристики транзистора BC817-25 наведені у табл. 3.9 [40].

Таблиця 3.9 - Основні характеристики транзистор BC817-25

Параметр	Значення
Тип	n-p-n
Максимальний струм колектора	500 мА
Максимальна напруга колектор-база	50 В
Максимальна напруга колектор-емітер	45 В
Статичний коефіцієнт передачі струму бази	не менше 160
Гранична частота	200 МГц

Ці самі транзистори будуть використовуватися для керування світлодіодами, за допомогою яких буде відображатися стан елемента блокування пристрою загородження. Положення пристрою загородження, відчинене чи зачинене, визначатиметься за допомогою датчиків, сигнали з яких будуть аналізуватися мікроконтролером.

Найпростішим типом датчика, що дозволяє зафіксувати перебування пристрою загородження у крайньому положенні, є магнітно-контактний датчик. Конструктивно він складається з двох частин, одна з яких містить постійний магніт і розміщується на рухомому елементі пристрою загородження, наприклад, на двері, а інша герконовий елемент, утворений двома електричними контактами, і розміщується на нерухомому елементі, наприклад, дверному одвірку. Коли обидві частини датчика знаходяться поруч (двері зачинені), магніт утримує контакти геркона у замкнутому стані. При відкритті дверей елемент датчика, що містить магніт, віддаляється і контакти геркона розмикаються.

Для захисту входів мікроконтролера від пробою підключення датчика будемо здійснювати з використанням оптоелектронного розв′язування кіл датчиків та входів мікроконтролера за допомогою оптронів, наприклад EL817

серії. Параметри оптрона EL817 наведені в табл. 3.10 [41].

Таблиця 3.10 Основні характеристики оптрона EL817

Параметр	Значення
Тип оптрона	транзисторний
Напруга ізоляції	5000 В
Вхідний прямий струм світлодіода	60 мА
Вхідна пряма напруга на світлодіоді	1,2 В
Вихідний струм колектора	50 мА
Напруга колектор-емітер	35 В

Підключення герконового датчику через оптрон будемо здійснювати за схемою, що наведена на рис. 3.9.

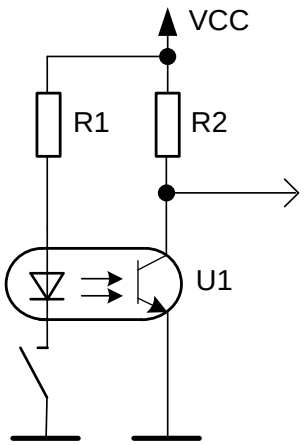

Рисунок 3.9 Схема підключення герконового датчика через оптрон

3.3 Розробка схеми електричної функціональної

З використанням вибраних у попередньому підрозділі компонентів та розглянутих схемних рішень було розроблено функціональну схему контролера керування доступом, що наведена у додатку Г. Контролер побудований на мікроконтролерному модулі STM32F407VET6-Mini DD2, основою якого є 32-ох

бітний високопродуктивний мікроконтролер STM32F407VET6. Модуль STM32F407VET6-Mini є завершеним функціональним блоком, оскільки крім самого мікроконтролера містить усі необхідні компоненти для підтримання його роботи. Модуль забезпечує виконання таких завдань:

обмін повідомленнями з хмарним сервером через Інтернет, використовуючи мережеве Ethernet або WiFi підключення;

взаємодію зі смартфоном через Bluetooth з′єднання та визначення прав доступу;

керування в виконавчими елементами загороджувальних пристроїв для надання доступу.

Підключення до мережі Ethernet забезпечується наявним у мікроконтролері STM32F407VET6 Ethernet контролером та модулем трансивера фізичного рівня Ethernet DD1. Контролер Ethernet, що входить до складу мікроконтролера STM32F407VET6, забезпечує підтримання функцій підрівня MAC канального рівня моделі OSI відповідно до стандарту IEEE802.3. Основу модуля трансивера DD1 складає мікросхема DP83848 приймача-передавача фізичного рівня, що забезпечує кодування та декодування даних, їх безпосередні прийом та передачу по витій парі. Підключення трансивера DD1 до модуля DD2 (контролера Ethernet мікроконтролера STM32F407VET6) здійснюється за RMII інтерфейсом, сигнали якого виведенні на роз′єми J2 та J3 модуля DD2. Фізичне підключення до кабелю Ethernet здійснюється через 8-ми контактний роз′єм RJ45, розташований на платі модуля DD1. Обмін даними з хмарним сервером через мережу Ethernet відбувається з використанням стеку протоколів TCP/IP, що підтримується програмним забезпеченням мікроконтролера STM32F407VET6.

Підключення до мережі WiFi здійснюється за допомогою WiFi модуля DA1, що забезпечує обмін даними по радіоканалу відповідно до стандарту 802.11x. Модуль DA1 підтримує стек протоколу TCP/IP, а тому реалізує не лише функції фізичного та канального рівнів, а й мережевого, транспортного та прикладного. Завдяки цьому взаємодія з хмарним сервером через WiFi підключення до точки доступу відбувається з використанням простих AT

команд, що пересилаються між мікроконтролерним модулем DD2 та WiFi модулем DA1. Команди передаються через послідовний асинхронний канал з′язку, утворений лініями послідовних даних RxD та TxD з використанням вбудованого у мікроконтролер STM32F407VET6 універсального асинхронного передавача/приймача UART1. Високий рівень сигналу на вході CH_PD модуля DA1, що формується на лінії PA12 мікроконтролера, переводить модуль в активний режим. Сигнал низького рівня на вході RST, що підключений до лінії PA8 мікроконтролера, забезпечує перезапуск модуля.

Надання прав доступу відбувається за ідентифікатором, що передається зі смартфона в контролер керування доступом через Bluetooth з′єднання, яке встановлюється за допомогою Bluetooth модуля DA2. Модуль DA2 забезпечує двосторонній зв'язок між смартфоном та мікроконтролерним модулем DD2 за протоколом Bluetooth. Підключення модуля до мікроконтролера STM32F407VET6 здійснюється через послідовний асинхронний інтерфейс. Мікроконтролер обмінюється даними з модулем за допомогою асинхронного приймача/передавача UART2 через лінії послідовних даних Tx та Rx.

Управління виконавчими пристроями засобів загородження забезпечується електромагнітними реле. У розроблюваному контролері керування доступом передбачені два канали управління виконавчими елементами, вмикання/вимикання яких здійснюється за допомогою імпульсних реле K1 та K2. Для управління кожним реле використовуються два імпульсні сигнали. За одним з них контакти реле замикаються, за іншим розмикаються. У статичному стані, в якому контакти реле замкнені або розімкнені, сигнал управління має рівень логічного нуля.

Управління реле здійснюється через лінії PD0…PD3 мікроконтролера STM32F407VET6, сигнали з яких подаються на ключі каскади на транзисторах VT1…VT4. Сигнали на лініях PD0, PD1 забезпечують керування реле K1, на лініях PD2, PD3 реле K2. Високий рівень сигналу забезпечує переведення підключеного до неї транзистора у відкритий стан. Це створює умови для протікання струму через обмотку реле, що увімкнена у колекторне коло цього

транзистора. Це, у свою чергу, призводить до зміни стану контактів реле. Діоди VD1…VD4 захищають транзистори VT1…VT4 від ЕРС самоіндукції, яка виникає у котушці реле в момент перемикання транзистора у закритий стан.. Резистори R5… R8 обмежують базові струми транзисторів VT1…VT4. Їх опір знаходиться з виразу:

$$R5...R8 \approx \frac{U^1_{ВИХ} - U_{БЕ}}{I_Р} \; h21, \qquad (3.1)$$

де $U^1_{ВИХ}$ напруга на логічної одиниці на виході мікроконтролера;

$U_{БЕ}$ напруга база-емітер транзистора;

$I_Р$ струм керування реле;

$h21$ коефіцієнт підсилення струму бази транзистора в схемі із загальним емітером.

Резистори R11 та R14, що увімкнені між загальною шиною та базами транзисторів, забезпечують закритий стан транзисторів у момент вмикання живлення, коли ліній введення/виведення мікроконтролера перебувають у високоомному стані. Вихідні контакти реле вмикаються у розрив кола живлення виконавчого пристрою через роз′єми X3 або X4.

Індикація стану загороджувального пристрою забезпечується світлодіодами HL1 та HL2 червоного та зеленого кольорів світіння. Світіння червоного світлодіода відповідає зачиненому стану, зеленого відчиненому. Керування світлодіодами відбувається за допомогою ключових каскадів на транзисторах VT5 та VT6, що підключені до ліній PC10 та PC11 мікроконтролера. Вмикання світлодіода відбувається за сигналом високого логічного рівня на виході мікроконтролера STM32F407VET6, який переводить транзистор у відкритий стан, створюючи умови для протягання струму через світлодіода, що увімкнений у його колекторне коло.

Резистори R9 та R10 обмежують базові струми транзисторів VT5 та VT6. Їх опір також знаходиться за виразом (3.1), в який замість значення струм керування реле $I_Р$ треба підставити значення рямок струму світлодіода $I_{СД}$.

Резистори R15 та R16 служать для обмеження прямого струму світлодіодів. Їх опір знаходиться з виразу:

$$R15,.R16 \approx \frac{VCC \} U_{СД}}{I_{СД}}, \qquad (3.2)$$

де VCC напруга живлення (VCC = 5 В);

$U_{СД}$ пряма напруга на світлодіоді;

$I_{СД}$ прямий струм світлодіода.

Для контролю положення загороджувального засобу передбачена можливість підключення двох герконових датчиків. Контакти герконів вмикаються між контактами 2, 4 та 3, 4 роз′єму X1. Стан контактів визначається за рівнем сигналів на ходах PB5 та PB6 мікроконтролера STM32F407VET6. Для захисту виводів мікроконтролер, підключення датчиків здійснюється через транзисторні оптрони U1 та U2.

Вхідні кола оптронів, що утворені світлодіодом, при зазначеному підключені герконів будуть увімкнені послідовно до їх контактів. При розімкненому стані контактів струм через світлодіод не протікає. Тому вихідний фототранзистор оптрона буде закритий, і напруга на його колекторі буде відповідати високому логічному рівню. При замкнених контактах геконів, вхідне коло оптрона замикається, і через світлодіод буде протікати струм, викликаючи світіння світлодіода. У цьому випаду фототранзистор буде відкритий, а тому його колекторі буде напруга низького логічного рівня. Резистори R1 та R2 обмежують прямий струм світлодіодів. Їх опір знаходиться з виразу (3.2), в якому VCC є напругою від якої буде живитися вхідне коло оптрона. Резистори R3 та R4 є навантаженням фототранисторів. Їх опір вибирається рівним кілька кОм.

Живлення засобу відбувається від зовнішнього джерела постійної напруги +5В, що підключається через роз′єм X2. Напруга живлення Ethernet трансивера DD1 та WiFi модуля DA1складає 3,3 В. Ця напруга береться з плати мікроконтролерного модуля DD2, який містить DC-DC перетворювач вхідною

напругою для якого є напруга +5 В, а вихідною +3,3 В.

3.4 Розробка алгоритму роботи системи віддаленого керування доступом

Перед тим як переходити безпосередньо до розробки програмного забезпечення, необхідно визначити загальний алгоритм роботи системи. Знання алгоритму дозволяє визначити вимоги до мов програмування та необхідного програмного забезпечення.

Як було визначено у підрозділі 2.1 розроблювана система складається з чотирьох компонентів (рис. 2.2): додатку адміністратора, додатку клієнта, веб-серверу та контролера керування доступом. Причому додаток адміністратора та веб-сервер запускаються у вигляді окремих сервісів на хмарному сервері. Розглянемо алгоритми роботи кожного з цих компонентів системи. Почнемо з алгоритму роботи контролера управління доступом.

Контролер керування доступом є тим засобом, що дозволяє отримати фізичний доступ за ідентифікатором, який надсилається до нього зі смартфона через Bluetooth. Для забезпечення працездатності системи при відсутності зв′язку з Інтернет, ідентифікатори доступу зберігаються у пам′яті контролера. Проте для отримання можливості віддаленого керування правами доступу, необхідно забезпечити онлайн оновлення бази даних ідентифікаторів у контролері. Це можна забезпечити за рахунок періодичного відправлення контролером до веб-серверу запиту на оновлення даних про ідентифікатори. У ролі ідентифікатора пропонується використовувати MAC-адрес (UUID) Bluetooth модуля, яким обладнаний смартфон.

Процес отримання доступу на об′єкті буде відбуватися таким чином. Контролер керування доступом постійно знаходиться в режимі очікування на підключення Bluetooth. При надходженні запиту на встановлення Bluetooth з′єднання контролер вилучає з нього UUID пристрою, що робить цей запит, та перевіряє чи збігається він з одним із тих, що зберігаються в його пам′яті. Якщо так, то доступ дозволено. Якщо ж подібного ідентифікатора немає, то контролер відправляє веб-серверу запит на синхронізацію, після чого знову перевіряє

ідентифікатор на відповідність. Якщо збігу знову немає, доступ не надається.

Необхідно відзначити, що встановлення повноцінного Bluetooth з’єднання між смартфоном чи планшетом та контролером керування доступом не відбувається. Після отримання запиту на встановлення з′єднання та прийняття рішення надавати чи не надавати доступ, контролер відмовляє у з’єднанні. Блок-схема алгоритму роботи контролера доступу наведена у додатку Д.

Перш ніж розглядати алгоритм роботи мобільного додатку, необхідно визначити як працюватиме додаток адміністратора та виконання яких функцій він повинен забезпечити. Основним завданням панелі адміністратора є надання можливості записати до пам′яті контролера керування доступом UUID пристроїв, за якими повинен надаватися доступ. Першим кроком для вирішення цього завдання є активація контролера, під якою розуміється «прив′язування» до панелі адміністратора одного чи кількох контролерів. Таке «прив′язування» здійснюється за ID контролера, що присвоюється йому виробником. Надалі адміністратор лише редагує список користувачів, які мають права доступу, тобто формує так званий white-list (білий список) користувачів. Доступ до панелі адміністратора надається після аутентифікації за логіном та паролем.

При додаванні користувача у білий список контролера керування доступом пристрою необхідно створити новий запис у базі даних, що знаходиться на веб-сервері. Для цього адміністратор через певну форму вводить дані для нового користувача та відправляє запит на сервер про створення нового запису. У випадку, коли операція проходить вдало, адміністратор отримує код доступу, який надсилається користувачеві. Використовуючи цей код користувач реєструється в системі. Під час реєстрації відбувається запис UUID Bluetooth модуля смартфона користувача до відповідного поля у базі даних. Блок-схема алгоритму роботи додатку адміністратора представлена у додатку Е.

Далі розглянемо алгоритм роботи мобільного додатку клієнта, а саме тієї його частини, яка безпосередньо пов′язана з отриманням прав доступу. Після завантаження додатку на смартфон чи планшет користувач повинен зареєструвати акаунт, або увійти у вже існуючий. Після входу у додатку

відображається перелік об′єктів, на яких йому дозволений доступ. Під об′єктом розуміється місце, через яке надається доступ. З точки зору системи це ID контролера, в пам′ять якого записаний UUID Bluetooth модуля смартфона користувача.

Для додавання нового об’єкту, клієнту необхідно на відповідній сторінці ввести спеціальний код, що був наданий адміністратором. Таким чином, якщо код вірний, то новий «замок» додається до списку дозволених.

Для отримання доступу необхідно вибрати з переліку потрібний об’єкт. При виборі об’єкту у додатку активізується екран керування, через який здійснюється розблокування загороджувального засобу. При переході на екран керування на пристрої автоматично вмикається Bluetooth. Якщо додаток «бачить», що у зоні покриття є Bluetooth, то кнопка запиту дозволу стає зеленою. При натисканні на кнопку, додаток відправляє до контролера керування доступом запит на встановлення на Bluetooth з’єднання. Контролер вилучає із запиту UUID Bluetooth модуля смартфона та використовує його як ідентифікатор прав на доступ. Далі контролер відмовляє у встановленні Bluetooth з′єднання, що використовується додатком для вмикання Bluetooth у смартфоні. Блок-схему алгоритму роботи мобільного додатку наведено у додатку Ж.

Взаємний зв′язок та взаємодія між усіма компонентами системи забезпечується веб-сервером. Саме на веб-сервері відбувається реєстрація адміністратора та користувача, здійснюється «прив′язування» контролера керування доступом до панелі адміністратора. Крім того, через веб-сервер забезпечується запис ідентифікаторів користувачів до пам′яті контролера керування доступом. додатку клієнта, веб-серверу та контролера керування доступом. Додаток адміністратора та веб-сервер запускаються у вигляді окремих сервісів на хмарному сервері. Блок-схема алгоритм роботи веб-сервера наведена у додатку К.

3.5 Аналіз можливих засобів реалізації додатків та веб-серверів

Існує велика кількість мов програмування, які дозволяють вирішувати

величезний спектр задач. Майже на будь-якій мові програмування можна написати програму, яка у своїй роботі не буде відрізнятись від такої ж програми, але написаної з використанням іншої мови програмування. Але приступаючи до виконання певної задачі необхідно пам’ятати, що кількість мов обумовлена специфікою задач які вони мають вирішувати. Так на мові JavaScript буде складно реалізувати нейромережу, а на мові C веб-сервер для обслуговування REST-запитів.

Для початку визначимо перелік критеріїв для вибору набору інструментів, необхідних для розробки додатку адміністратора, додатку клієнта та веб-сервера.

Додаток адміністратора повинен бути доступний з будь-якої точки світу а також має запускатись на будь-якому пристрої. Також, необхідно, щоб користувачеві не потрібно було робити якихось складних налаштувань перед використанням додатку. Враховуючи вище сказане, найліпшим способом реалізації такого додатку є реалізація його у вигляді веб-сайту. Оскільки для хостингу додатку буде використовуватись хмарний сервер, то немає необхідності в написанні власного веб-серверу для хостингу веб-сторінок, оскільки він входить до усіх базових конфігурацій хмарних серверів у всіх провайдерів таких послуг. Відкинувши необхідність написання веб-серверу для хостингу веб-сторінок, можна викреслити зі списку такі мови як PHP, Java чи Python. Отже, окрім як JavaScript для написання додатку адміністратора нам більше нічого не знадобиться.

Наступним кроком є вибір бібліотеки чи фреймворку, які дозволять спростити та прискорити розробку. Для JavaScript існує велетенська кількість бібліотек та фреймворків: jQuery, Vue.js, React, Angular, Ember.js, тощо. Відразу викинем зі списку бібліотеку jQuery. Хоча на jQuery написаний великий відсоток веб-сайтів, але бібліотека є доволі старою, а при написані нових продуктів для веб-сегменту її намагаються уникати.

Vue.js та Angular є фреймворками, а отже беруть на себе більшість задач в процесі розробки. Додаток адміністратора є доволі простий у контексті кількості сторінок та можливих функцій, тому максимальна автоматизація нам не

потрібна, оскільки вимагає чималих зусиль у процесі початкового налаштування.

Ember.js також фреймворк, але окрім недоліків (для нашої задачі), описаних вище, має ще один. Сам по собі, фреймворк не новий, його було створено у 2011 році, але великої популярності набув лише кілька років тому. Таким чином, підтримка додатку буде не легкою задачею, оскільки профільних спеціалістів сьогодні мало.

Методом виключення приходимо до бібліотеки React. Бібліотека була створена відносно недавно у 2013 році. За час свого існування здобула великої популярності, а розробників, що володіють цією бібліотекою досить багато, це дозволить спростити підтримку додатку. Також, оскільки React – бібліотека, а не фреймворк, є можливість мати повний контроль над розробкою та конфігурувати додаток в процесі розробки.

Основними вимогами до додатку клієнта є портативність та можливість роботи за відсутності Інтернет зв′язку. Крім того, додаток має працювати на будь-якому пристрої під будь-якою операційною системою та мати доступ до системної інформації.

Оскільки додаток має бути портативний, то необхідність написання повноцінної програми під комп’ютери відпадає. Отже, нам необхідний додаток для смартфонів та планшетів. Ми могли б розробити ще один веб-додаток, але такі додатки не мають змоги отримати системну інформацію. Таким чином, під наші критерії підходить лише варіант з розробкою повноцінної програми саме для смартфонів та планшетів.

Згідно з інформацією з порталу Statcounter.com серед найбільш поширених операційних систем мобільних пристроїв, таких як смартфони та планшети, лідером у 2022 році є Android OS, яка використовується у 70,29% пристроїв (рис. 3.10). Друге місце займає операційна система iOS, яку встановлено на 29,05% приладів. Таким чином, можна сказати, що майже 98% від усіх операційних систем займають iOS та Android, а отже, ми можемо сфокусувати свою увагу лише на них.

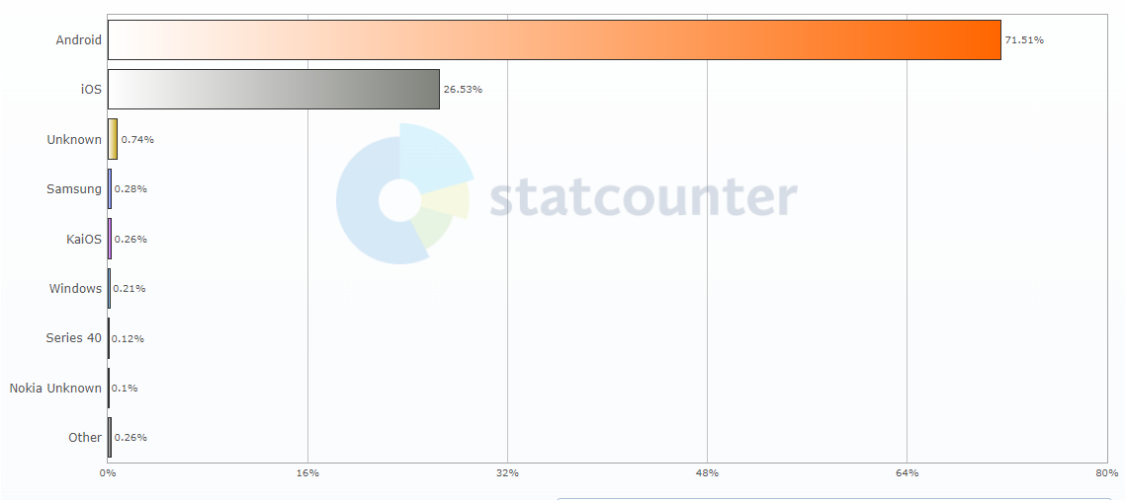

Рисунок 3.10 Розподіл операційних систем на смартфонах та планшетах

Сьогодні, найбільш поширеним варіантом для написання кросс-платформеного додатку для iOS та Android є мова програмування Kotlin у поєднані з фреймворком Flutter. Завдяки такому поєднанню можна швидко та якісно писати додатки для вибраних нами операційних систем. Але є один недолік для кожної OS необхідно буде писати власний код, а процес конфігурації займає дуже багато часу.

Окрім Kotlin чи Java існує ще один спосіб писати додатки для планшетів та смартфонів JavaScript та вже відома нам бібліотека React, а точніше її модифікація у вигляді фреймворку React-Native. Оскільки React-Native використовує такі самі принципи та підходи як React, то рішенням використовувати React-Native дозволяє нам використовувати одних і тих самих розробників для підтримки додатків та, в майбутньому, легко портувати веб-додаток адміністратора під Android чи iOS додаток і навпаки – клієнтський додаток під веб-інтерфейс.

Слід зазначити, що сам по собі React-Native це лише кодова база, тобто набір інструментів. Для повноцінної роботи необхідно користуватись однією з двох можливих надбудов: React-Native-CLI чи Expo. Порівняння цих двох надбудов представлене у таблиці 3.11 [42].

Незважаючи на певні недоліки Expo, такі як розмір пустого проекту чи можливість додавання сторонніх модулів на інших мовах програмування, надамо

перевагу саме йому, оскільки плюси від його використання переважують мінуси, які взагалі не вплинуть на розроблюваний додаток.

Таблиця 3.11 Порівняльний аналіз надбудов Expo та React-Native-CLI

Назва	React-Native-CLI	Expo
Ви можете додати власні модулі, написані на Java/Objective-C	Так	Ні
Вага стандартної програми Hello World	5 мБ	25 мБ
Потрібно Android Studio та XCode для запуску проектів	Так	Ні
Шрифти необхідно імпортувати вручну в XCode	Так	Ні
Спільне використання програми (за допомогою QR-коду або посилання), вам не потрібно надсилати весь файл .apk або .ipa	Складніше	Простіше
Якщо ви хочете поділитися цією програмою, вам потрібно надіслати весь файл .apk / .ipa	Так	Ні
Надає JS API з коробки, наприклад, Push-Notifications, Asset Manager	Ні	Так

Отже, для розробки обох додатків будемо використовувати мову JavaScript. Для мобільного додатку з використанням фреймворку React-Native з надбудовою Expo, а для веб-додатку - бібліотеку React.

Після визначення засобів для розробки додатків адміністратора та клієнта, залишається питання взаємодії останніх між собою та контролером керування доступом. Як було сказано у розділі 2.2, комунікацію між усіма компонентами системи буде забезпечувати хмарний сервер та протокол HTTP.

Реалізувати веб-сервер можна на багатьох мовах програмування, але найбільш економним варіантом є, знову ж таки, мова JavaScript та середовища виконання NodeJS, що дає змогу виконувати програми JS не тільки в браузері, але й на комп’ютері.

NodeJS привабливий тип, що у процесі виконання не потребує багато оперативної пам’яті (на відміну від Java), а отже кінцева програма має нижчі системі вимоги до апаратної частини. Окрім системних вимог NodeJS зручний тим, що розробка як додатку клієнта, так і веб-серверу буде здійснюватися з використанням однієї і тієї самої мови програмування.

3.7 Розробка веб-серверу

Розробку розпочнемо з веб-серверу. У веб сервері можна виділити 4 основні блоки (рис. 3.11):

REST-Interface інтерфейс доступу, через який проходять усі запити до серверу; на цьому рівні сервер проводить аутентифікацію ресурсу, що надіслав запит; якщо ресурс аутентифікований, то запит надсилається до відповідного контролеру;

контролери запитів на цьому рівні визначається з чим та яку операцію необхідно провести;

обробники запитів рівень, на якому виконуються задані операції з заданими сутностями;

сховище даних база даних чи файлова система, яка відповідає за зберігання даних.

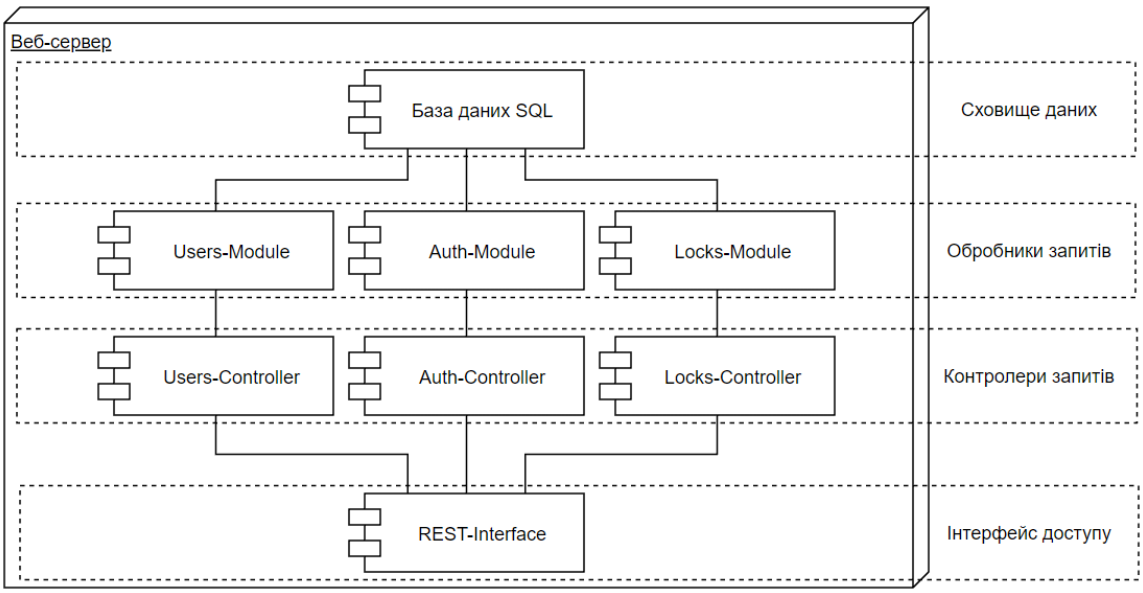

Рисунок 3.11 Структура веб-серверу

Усі 4 рівні працюють у певній послідовності за певним алгоритмом. Наприклад: на сервер надійшов запит за адресую /lock/activate/b627bc3289. Перш за все REST контролер перевірить accessToken (див. розділ 2.3). Якщо токен дійсний, то запит передається на рівень контролерів запитів. Оскільки перший параметр в адресі запиту lock, отже операція відбувається з «замками», таким чином запит відправляється в Locks-Module. Другий параметр в запиті activate. Параметр activate відповідає за активацію нового пристрою. В Lock-Module спрацює функція initLock, яка перевірить коректність серійного номеру пристрою (третій параметр - b627bc3289) та, якщо серійний номер існує та досі не активований, зробить запит до сховища даних та обновить відповідні записи.

Оскільки функцій та методів на кожному рівні дуже багато, розглянемо основні функції на рівні обробників запитів.

Для створення нового користувача використовується функція createUser(String: username, String: password, String: email). Якщо username, password та email відповідають усім вимогам, то заносить у базу даних інформацію про нового користувача.

За ініціалізацію адміністратора, тобто при його першому вході у систему відповідає функція initAdmin(String: passcode, String: username, String: password). Passcode унікальний ідентифікатор клієнта, що видається при придбанні першого пристрою. Якщо passcode існує та ще не був активований, створює нового адміністратора з відповідним ім’ям та паролем;

Після реєстрації нового користувача чи ініціалізації нового адміністратора, за вход у систему відповідає функція login(String: username, String: password). Якщо username и password збігаються із існуючими даними, то за допомогою функції generateToken формується новий accessToken.

Функція generateToken(Int: userId) створює accessToken, який представляє собою зашифровану інформацію про користувача. У подальшому цей токен відповідає за аутентифікацію користувача.

Функція checkToken(String: accessToken) є функцією, що працює на рівні REST інтерфейсу. За допомогою приватного ключа, який зберігається на сервері

розшифровує accessToken та отримує необхідну інформацію про користувача. Якщо користувач має необхідний рівень доступу, то запит йде далі. Якщо ж токен не існує, містить в собі помилки, чи рівень користувача не відповідає тому запиту, що він надіслав запит відхилюється.

Запит на активацію нового пристрою обробляється функцією initLock(String: lockSerial). Якщо пристрій з серійним номером lockSerial ще не активований, то активує пристрій та закріплює його за певним адміністратором.

За допомогою фунцій disableLock(Int: lockId) та enableLock(Int: lockId) можна змінити статус пристро. Якщо пристрій з таким id належить користувачеві, який надіслав запит, перемикає статус пристрою у «Вимкнений» та у «Ввімкнений» відповідно.

Функція assingUser(Int: lockId, Date: startDate, Date: expDate) відповідає за створення нового ключа доступу до пристрою. Якщо пристрій з таким id належить користувачеві, який надіслав запит, створює запис у базі даних про додавання користувача, який активує цей код, до білого списку потрібного пристрою.

Функція disableUser(Int: lockId, Int: userId) функція, що робить протилежне попередній. Якщо пристрій з таким id належить користувачеві, який надіслав запит, створює запис у базі даних про видалення користувача з відповідним id із білого списку потрібного пристрою.

За активацію коду у мобільному додатку відповідає функція activateCode(String: code) Якщо код коректний та він існує, додає до списку доступних ідентифікаторів для відповідного пристрою ідентифікатор користувача, який надіслав запит. При цьому код видаляється з бази даних;

Функція myLocks() робить з бази даних вибірку усіх пристроїв до яких у користувача є доступ.

Запит на оновлення даних на пристрої обслуговується функцією syncData(). Вона робить вибірку для пристрою, який надіслав запит, про його поточний статус («Увімкнений», «Вимкнений») та список ідентифікаторів для яких доступ дозволено.

Аби мати змогу відслідковувати коли та ким був отриманий доступ, пристрій при активації надсилає запит, на який реагує функція newAction(LockAction: action). Вона додає до історії певного пристрою інформацію про останню дію, що була виконана на пристрої. Параметр action містить у собі інформацію про те, коли та ким був отриманий доступ.

3.8 Розробка додатку адміністратора

Наступним етапом після розробки веб-сервера є розробка додатку адміністратора. Знову ж таки, розробку розпочнемо з розробки архітектури додатку.

У додатку адміністратора мона виділити два основні рівні: Business Layout (рівень бізнес логіки) та Representative Layout (представницький рівень) (рис. 3.12). Рівень бізнес логіки відповідає за отримання, зберігання, обробку та постачання даних до компонент, які знаходяться на представницькому рівні, який їх відображає. Так, наприклад, запит POST /auth (авторизація користувача) виконується наступним чином: на сторінці Login, що знаходиться на представницькому рівні, користувач натискає на кнопку «Увійти». Натискання на кнопку викликає функцію, що звертається до менеджеру даних, який знаходиться на рівні бізнес логіки. Менеджер даних робить запит на веб-сервер для отримання інформації чи був користувач авторизований. Коли від веб-серверу надійде відповідь, то менеджер даних наддасть про це інформацію представницькому рівню, який в свою чергу відобразить користувачеві відповідний інтерфейс.

Розробку додатку адміністратора розпочнемо з розробки сторінки авторизації (рис. 3.13). На цій сторінці є три основні функції: login(), switchMode() та registration(). Видно, що жодна функція не приймає ніяких параметрів. Це тому, що всі необхідні дані для них лежать на бізнес рівні.

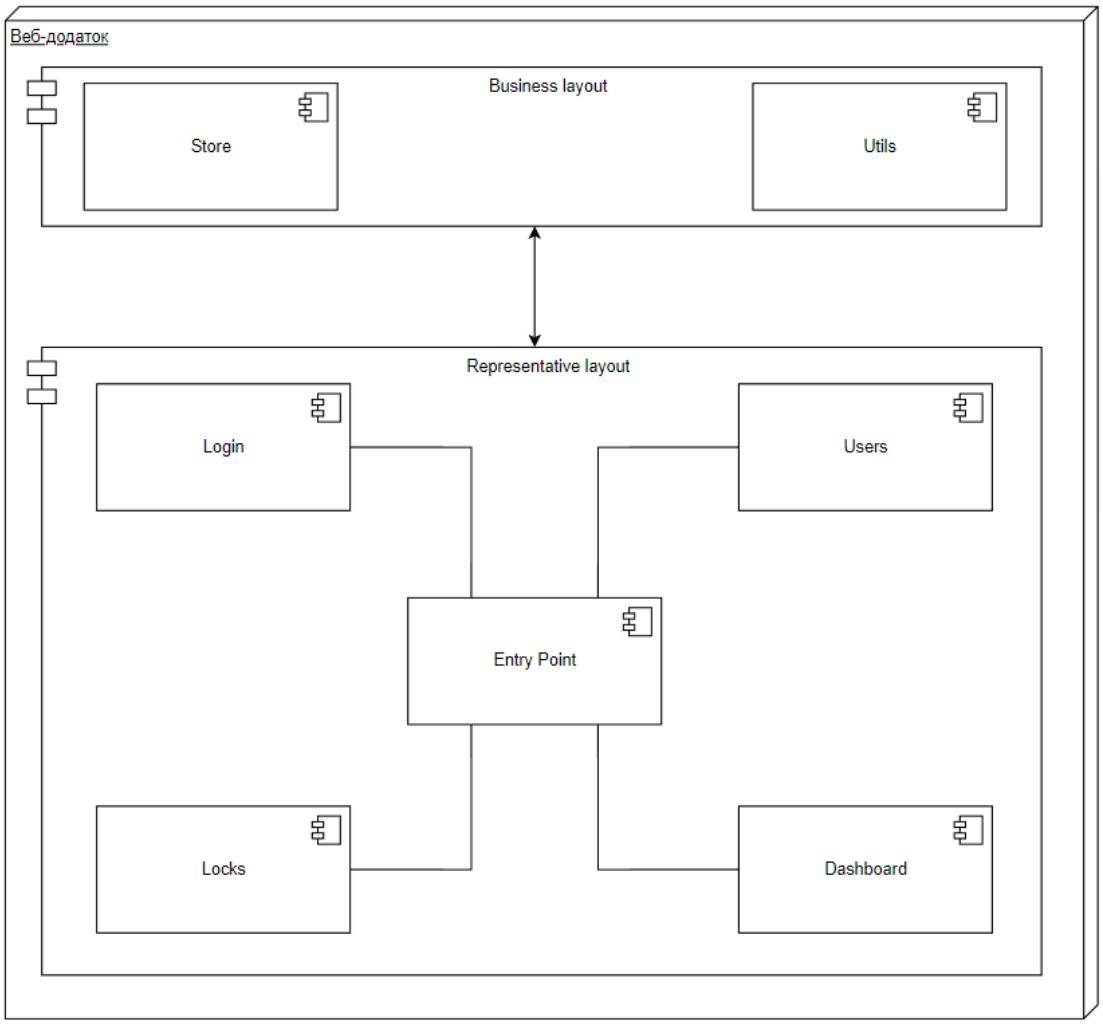

Рисунок 3.12 Структура веб-додатку адміністратора

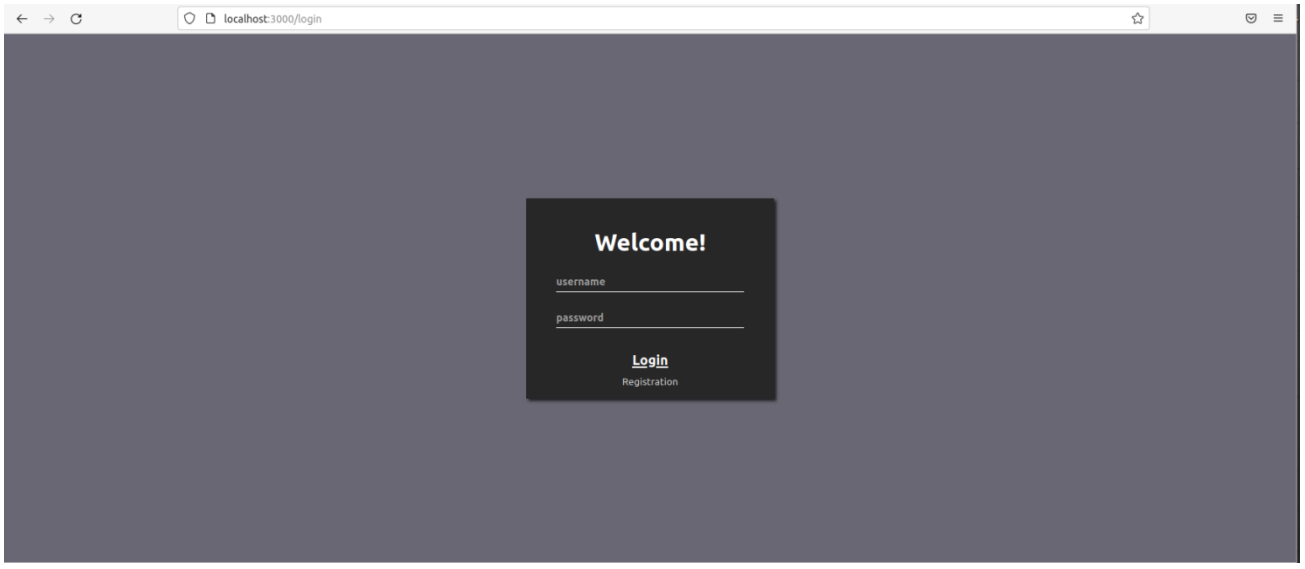

Рисунок 3.13 Сторінка авторизації

Функція login() ініціалізує запит POST /auth на сервер. У тілі запиту

містяться username та password які ввів користувач.

Щоб ініціалізувати адміністратора використовується функція switchMode(). При натисканні на кнопку Registration компонент авторизації змінюється компонентом ініціалізації (рис. 3.14)

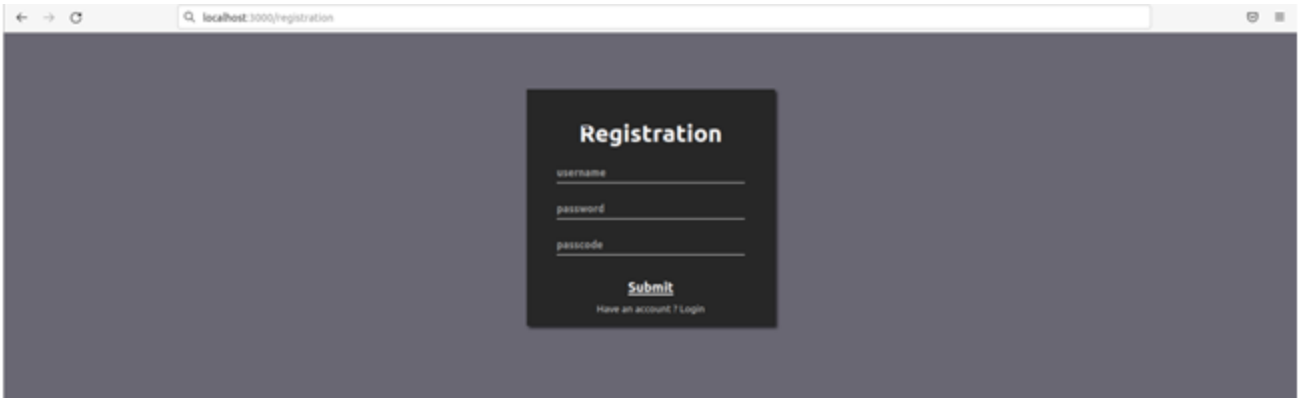

Рисунок 3.14 Сторінка ініціалізації

При натисканні на кнопку Submit викликається функція registration(), що ініціалізує запит PUT/auth. Як відбувається процес ініціалізації адміністратора було сказано на початку підрозділу.

Після успішної авторизації адміністратор потрапляє на сторінку Dashboard (рис. 3.15). На цій сторінці адміністратор має змогу зробити швидкий огляд усіх доступних йому пристроїв та користувачів, що мають права доступу. Оскільки ця сторінка є лише інформативною, то ніяких цікавих для розгляду функцій вона не використовує.

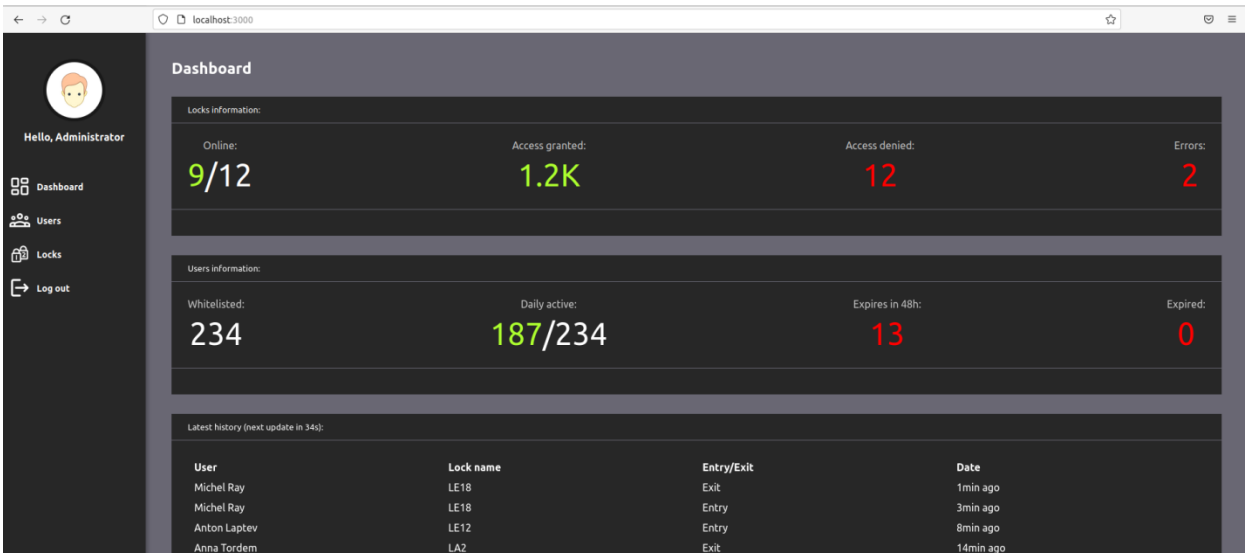

Рисунок 3.15 Сторінка Dashboard

Розглянемо сторінку Users (3.16), що відповідає за відображення усіх користувачів, у яких є права доступу до пристроїв, які закріплені за певним адміністратором. Також на цій сторінці можна надати користувачеві до певного пристрою.

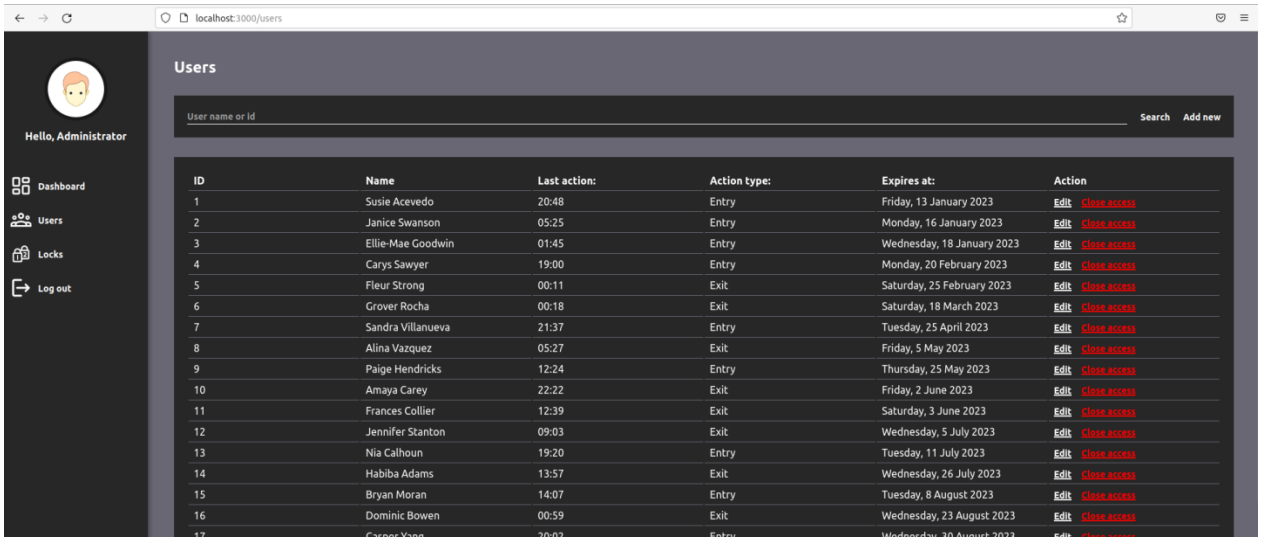

Рисунок 3.16 Сторінка Users

При натисканні кнопки Add New змінюється стан додатку та відкривається вікно діалогу (рис. 3.17), на якому пропонується додати нового користувача, який буде мати доступ до вибраного нам пристрою. У першому полі вводиться ім’я користувача, у другому - дата, до коли доступ буде наданий, третє поле для вибору пристрою, через який буде здійснюватися доступ.

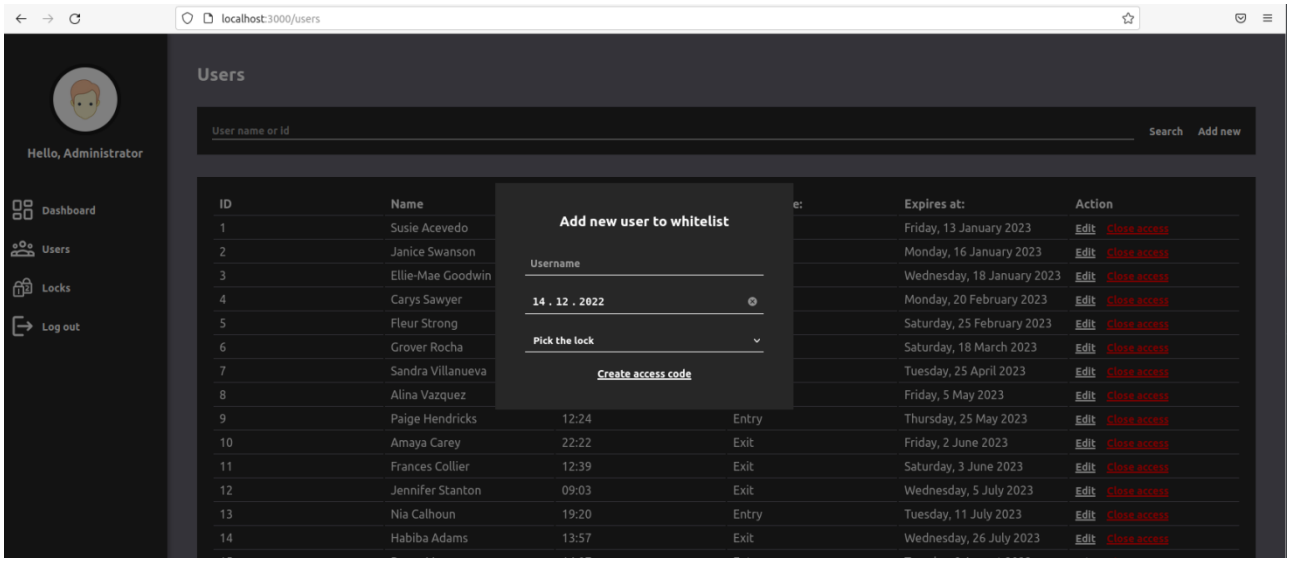

Рисунок 3.17 Вікно діалогу для додавання нового користувача

При натисканні на кнопку Create Access Code на сервер відправляється запит PUT /lock/generate. Якщо запит успішний, то адміністратору виведеться на екран код підтвердження (рис. 3.18).

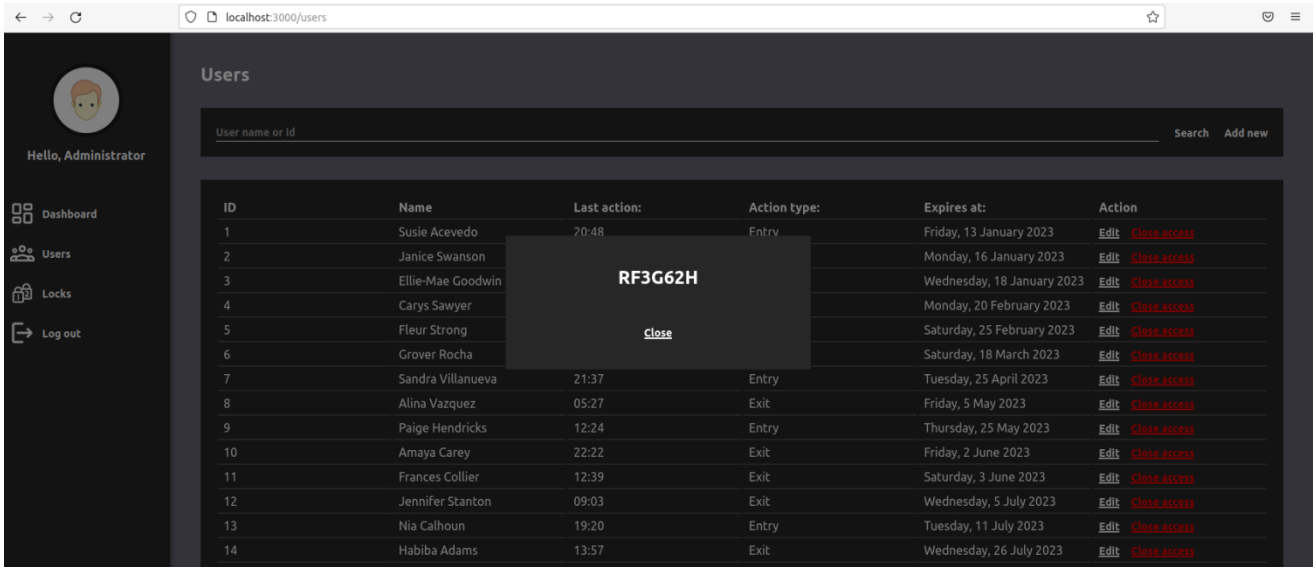

Рисунок 3.18 Вікно діалогу з відображенням коду доступу

Остання сторінка Locks (рис. 3.19). На цій сторінці відображаються усі пристрої, які належать адміністратору. Також, тут можна додати новий пристрій.

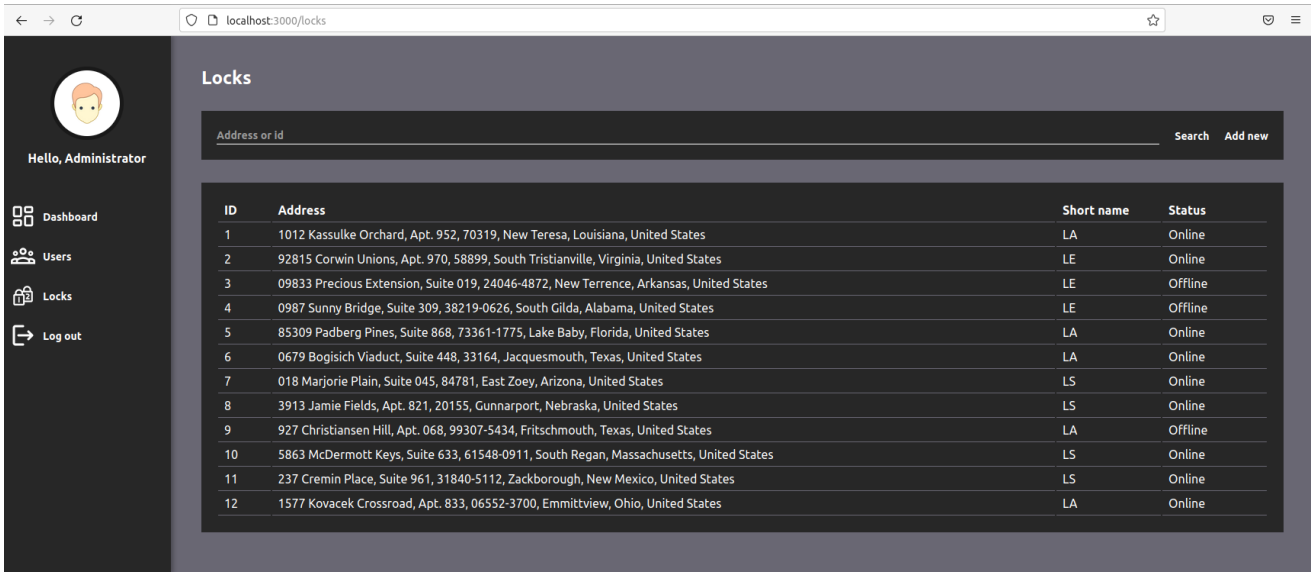

Рисунок 3.19 Сторінка Locks

Так само, як і на сторінці з користувачами, для активації нового пристрою необхідно скористатись діалоговим вікном (рис. 3.20), яке відкривається при натисканні на кнопку Add New. У вікні необхідно ввести адресу, де знаходиться

об'єкт, до якого буде надаватись доступ; ключове слово для пристрою, за яким буде зручніше орієнтуватись між великою кількістю пристроїв; серійний номер пристрою, саме за цим номером відбувається активація. При натисканні на кнопку Connect Lock відправляється запит POST /lock/activateю Якщо запит пройде успішно, то у переліку доступних адміністратору пристроїв з’явиться тільки но доданий.

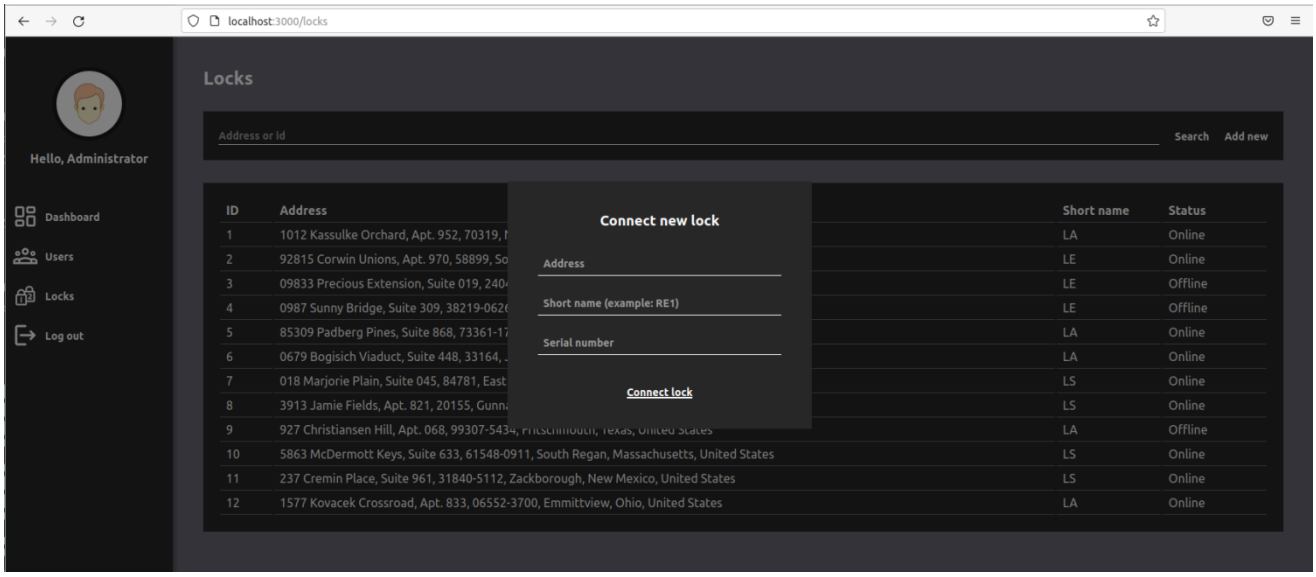

Рисунок 3.20 Вікно діалогу для активації нового пристрою

3.9 Розробка додатку користувача

В кінці розглянемо клієнтський додаток для смартфонів та планшетів. За традицією почнемо із структурної схеми (рис. 3.21). Оскільки технології, які використовувались для написання додатку такі ж самі, як і у випадку з додатком адміністратора, то і схема буде дуже схожа. Так, у схемі знову ж таки видно два основні рівні:бізнес та рівень презентації. Єдине, що відрізняє схему веб-додатку та додатку для смартфону/планшету екрани на презентаційному рівні.

Функції бізнес рівня були розглянуті під час розроби додатоку адміністратора, тому відразу перейдемо до представницького рівня. Сторінка Login (рис. 3.22) працює за тими самими принципами, що й сторінка Login на веб-панелі. Сторінка реєстрації наведена на рисунку 3.23.

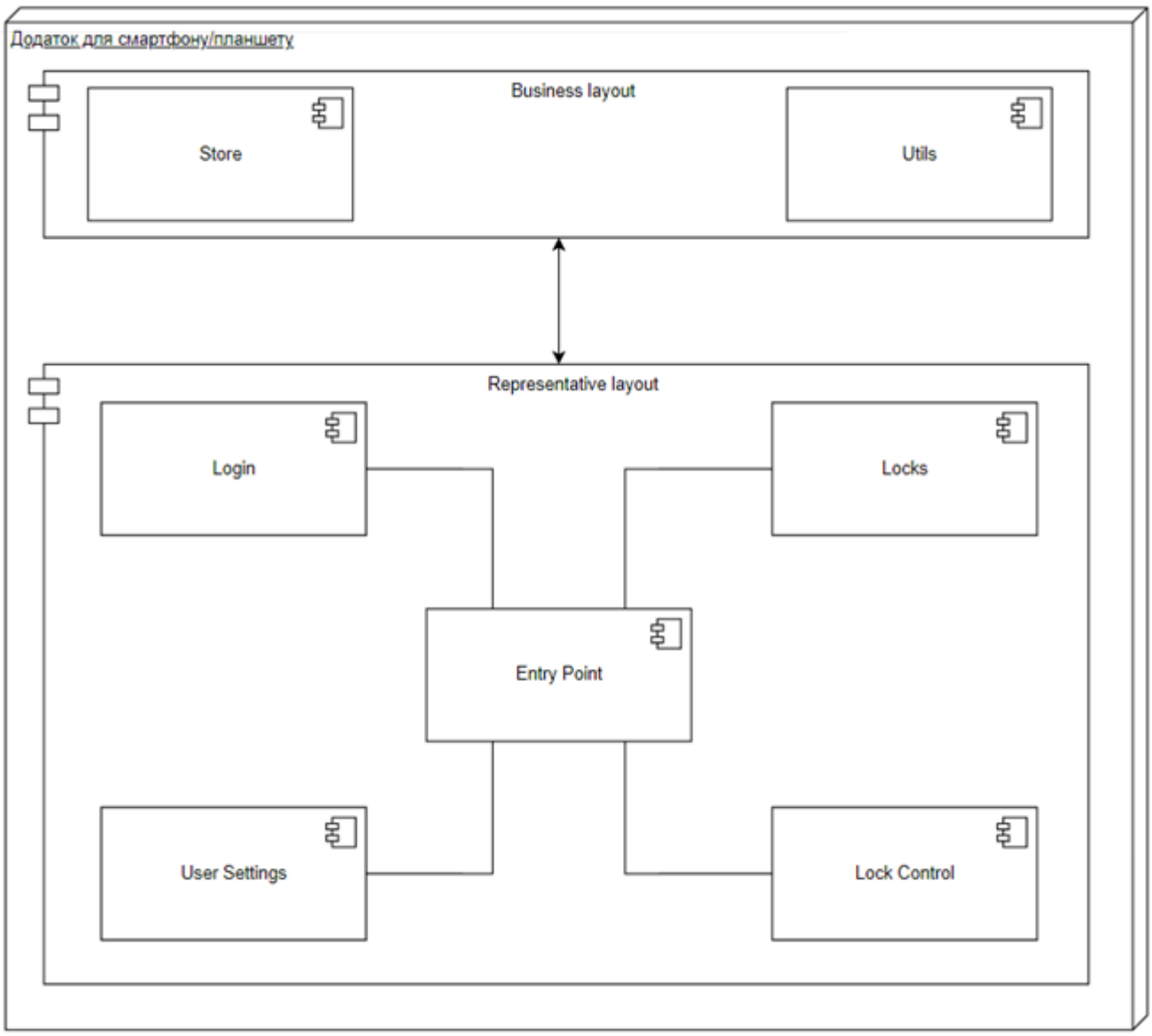

Рисунок 3.21 Структурна схема додатку для смартфону/планшету

На сторінці Locks нас зустрічає два основних блоки: перелік пристроїв, що зроблені у вигляді каруселі та історія дій користувача. Між цими блоками є перемикач, який змінює тип історії. Якщо вибраний режим «Selected», то відображається історія лише для вибраного пристрою (рис. 3.24). Якщо режим «All», то відображається уся історія користувача (рис. 3.25)

Для керування пристроєм загородження необхідно натиснути на картку потрібного пристрою. Після натискання користувача перенаправляє на екран керування (рис. 3.26). При натисканні на головну кнопку до контролера управління доступом надсилається запит на отримання доступу. Як працює алгоритм було описано у підрозділі 3.4.

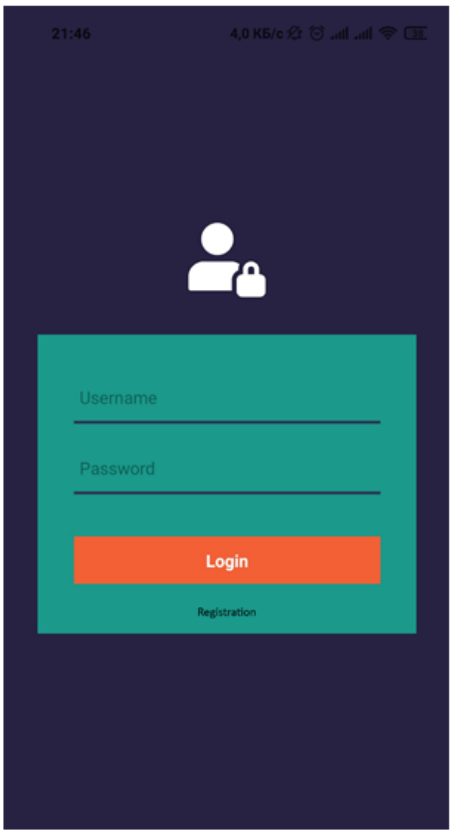

Рисунок 3.22 Сторінка Login

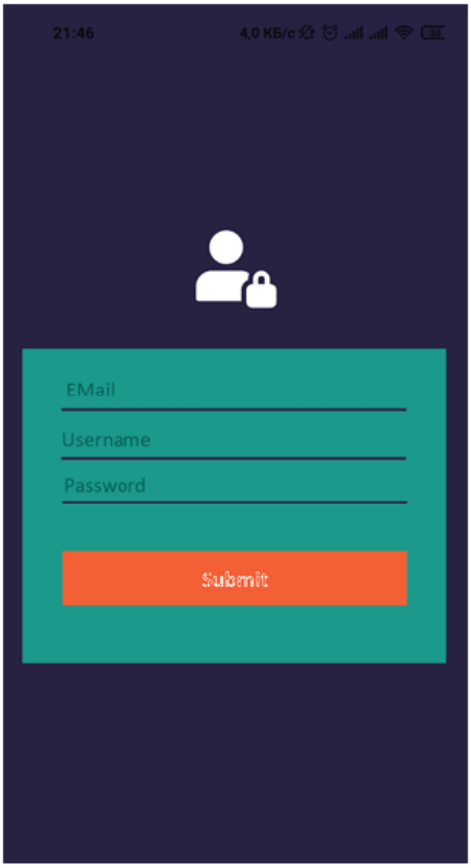

Рисунок 3.23 Сторінка реєстрації

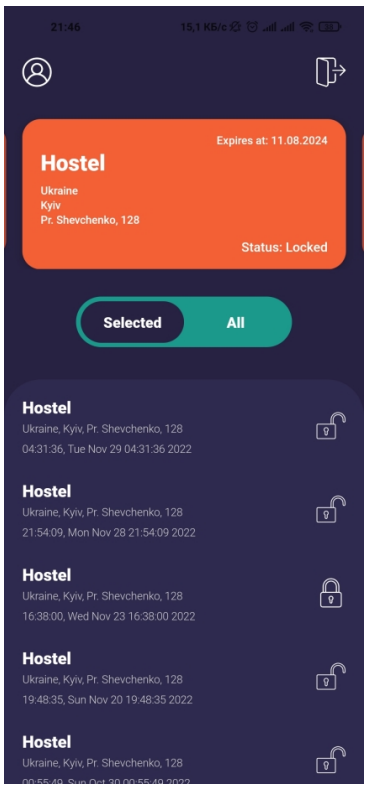

Рисунок 3.24 Сторінка історії для пристрою

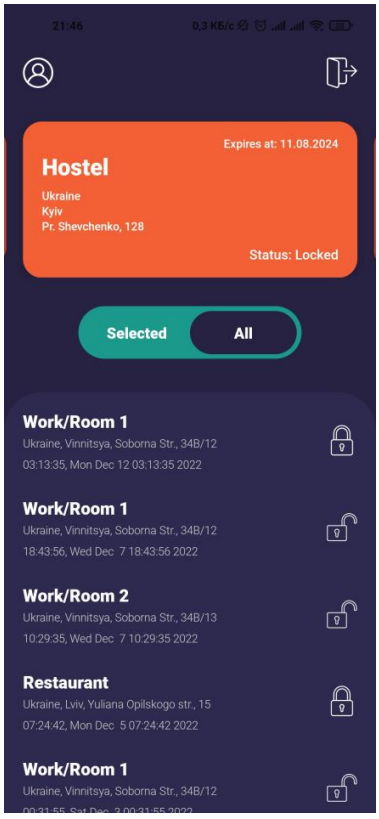

Рисунок 3.25 Сторінка загальної історії

Для додавання нового пристрою у додаток, необхідно зайти в

налаштування та вибрати пункт «Add new lock». Після з'явиться можливість для введеня коду (рис. 3.27), який був надісланий адміністратором. Якщо код корректний, то пристрій з'явиться у переліку доступних на головній сторінці.

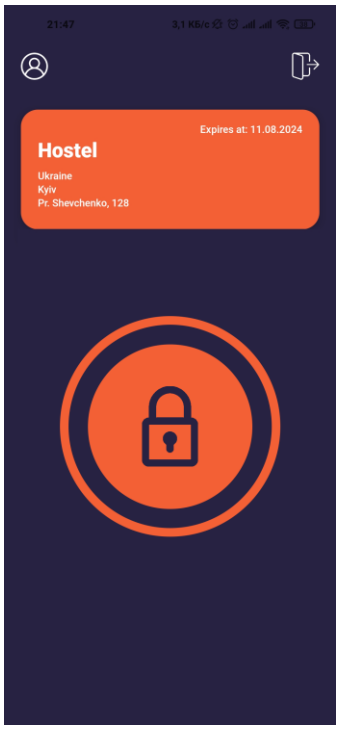

Рисунок 3.26 Сторінка керування контролером доступу

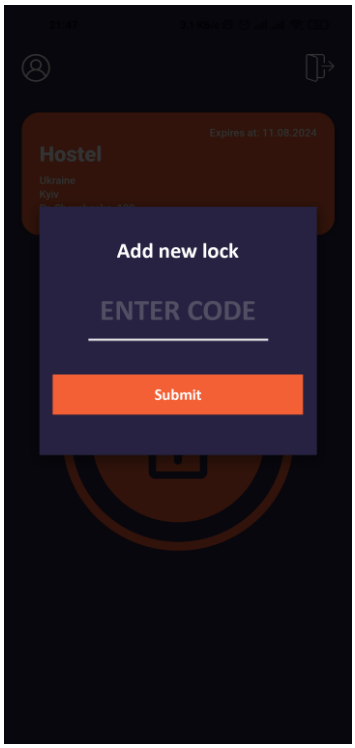

Рисунок 3.27 Меню додавання нового пристрою

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку нового виробу, а саме апаратно-програмного засобу віддаленого керування доступом до об’єктів через веб-інтерфейс. Особливістю виробу є розширення функціональних можливостей системи управління доступом за рахунок підтримки WEB-сервісі. Одним із найефективніших і цивілізованих підходів до вирішення завдання комплексної безпеки об'єктів різних форм власності є використання систем контролю та управління доступом. Такі системи дозволяють закрити несанкціонований доступ на територію, у будівлю, окремі поверхи та приміщення. Поряд із цим можуть вирішуватися і додаткові завдання, такі як облік робочого часу, ведення бази персоналу/відвідувачів, інтеграція з системами відеоспостереження та пожежної сигналізації.

Аналогом розробки є комплекс мобільного керування автоматикою пропуску LOKKYY, вартість 5800 грн.

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п’ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 4.1.

Таблиця 4.1 Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Крите-рій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздат-ність в реальних умовах

Продовження табл. 4.1

Ринкові переваги					
2	Багато аналогів на малому ринку	Ринкові п Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так із комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження табл. 4.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в табл. 4.2

Таблиця 4.2 Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	4	2
Наявність аналогів на ринку	2	2	2
Цінова політика	4	4	4
Технічні та споживчі властивості виробу	3	3	3
Експлуатаційні витрати	4	2	3
Ринок збуту	2	3	2
Конкурентоспроможність	3	4	4
Фахівці з технічної і комерційної реалізації	2	3	2
Фінансування	2	2	3
Матеріально-технічна база	3	3	3
Термін реалізації ідеї	4	4	4
Супровідна документація	4	3	3
Сума	36	37	35
Середньоарифметична сума балів	(36+37+35) / 3 = 36		

За даними таблиці 4.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 4.3.

Таблиця 4.3 - Рівні комерційного потенціалу розробки

Середньоарифметична сума балів СК розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 - 1 0	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового виробу є вище середнього, що досягається за рахунок розширення функціональних можливостей системи управління доступом за рахунок підтримки Веб-сервісі. Такі системи дозволяють закрити несанкціонований доступ на територію, у будівлю, окремі поверхи та приміщення. Поряд із цим можуть вирішуватися і додаткові завдання, такі як облік робочого часу, ведення бази персоналу/відвідувачів, інтеграція з системами відеоспостереження та пожежної сигналізації.

4.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

Розраховуємо основну заробітну плату розробників:

$$З_о = \frac{М}{Т_р} \cdot t, \qquad (4.1)$$

де М місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ число робочих днів в місяці, 20 днів;

t число днів роботи розробника (дослідника).

Результати розрахунків зведемо до табл. 4.1.

Таблиця 4.1 Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	21000	1050,00	30	31500,000
Інженер	20000	1000,00	30	30000,000
Всього				61500,00

Витрати на основну заробітну плату робітників ($З_р$) розраховуються на основі норм часу, які необхідні для виконання даної роботи, розраховуються за формулою:

$$З_р = \sum_{1}^{n} t_i \ C_i \ K_c, \qquad (4.2)$$

де t_i норма часу (трудомісткість) на виконання конкретної роботи, годин;

n число робіт по видах та розрядах;

K_c коефіцієнт співвідношень, який установлений в даний час Генеральною тарифною угодою між Урядом України і профспілками;

Сі погодинна тарифна ставка робітника відповідного розряду, який виконує відповідну роботу, грн./год.

C_i визначається за формулою:

$$C_i = \frac{M_м \ K_i}{T_р \ T_{зм}}, \qquad (4.3)$$

де $M_н$ мінімальна місячна оплата праці, грн., $M_н$ = 6700 грн.

K_i тарифний коефіцієнт робітника відповідного розряду;

$T_р$ число робочих днів в місяці, $T_р$ = 20 дні;

$T_{зм}$ тривалість зміни, $T_{зм}$ = 8 годин.

Погодинна тарифна ставка згідно чинного законодавства у грудні 2022 року = 40,46 грн./год.

Розрахунки заносимо до табл. 4.5.

Таблиця 4.5 Витрати на основну заробітну плату робітників

Найменування робіт	Трудомісткість, год.	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн.	Величина оплати на робітника грн.
Заготівельні	6	3	1,35	54,621	327,726
Слюсарно-збиральні	22	3	1,35	54,621	1201,662
Налагоджувальні та контрольні	3,5	5	1,7	68,782	240,737
Всього					1770,13

Розраховуємо додаткову заробітну плату розробників, які приймали участь в розробці обладнання. Додаткова заробітна плата прийнято розраховувати як 10% від основної заробітної плати розробників та робітників:

$$З_д = (З_{о.роз} + З_{о.роб}) \cdot 10\% /100\% \quad (4.4)$$

$$З_д = (61500,00 + 1770,13) \cdot 10\%/100\% = 6327,01 \text{ (грн.)}$$

Визначаємо нарахування на заробітну плату розробників. Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_{о.роз} + З_{о.роб} + З_{д.}) \cdot 22\%/100\% \quad (4.5)$$

$$Н_з = (61500,00 + 1770,13 + 6327,01) \cdot 22\%/100\ \% = 14921,94 \text{ (грн.)}$$

Розраховуємо витрати на амортизацію обладнання, яке використовувалось

для проведення розробки. Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді амортизація обладнання, що використовувалась для розробки розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (4.6)$$

де Ц балансова вартість обладнання, грн.;

Т термін корисного використання обладнання згідно податкового законодавства, років

$t_{вик}$ термін використання під час розробки, місяців.

Розрахуємо, для прикладу, амортизаційні витрати на комп'ютер балансова вартість якого становить 20500 грн., термін його корисного використання згідно податкового законодавства – 2 роки, а термін його фактичного використання – 1,5 місяців.

$$A_{обл} = \frac{20500}{2} \cdot \frac{1{,}5}{12} = 1281{,}25 \text{ (грн.).}$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до табл. 4.6.

Таблиця 4.6 Амортизаційні відрахування матеріальних і нематеріальних ресурсів для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія	20500	2	1,500	1281,250
Офісне обладнення (меблі)	22000	4	1,500	687,500
Приміщення	750000	20	1,500	5302,734
Всього				7271,48

Амортизація обладнання, що використовувалось робітниками, розраховується аналогічно, результати розрахунків зведено в табл. 4.7 і враховуються при розрахунку виробничої собівартості виробу.

Таблиця 4.7 – Амортизаційні відрахування матеріальних і нематеріальних ресурсів для робітників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання		Амортизаційні відрахування, грн.
			год.	міс.	
Комп’ютер	20500	2	3,5	0,0219	18,6849
Спеціалізоване обладнання (меблі)	22000	4	3,5	0,0219	10,0260
Приміщення	750000	20	31,5	0,1969	615,2344
Всього					643,9453

Оскільки вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних ресурсів, а також спеціалізованого обладнання менше 20000 грн (операційна система – безкоштовно, осцилограф – 8000 грн., мультиметр – 380грн.), то даний нематеріальний актив не амортизується, а його вартість включається у вартість розробки повністю, $B_{спец.\ обл..}$ = 8380 грн.

Розраховуємо витрати на комплектуючі. Витрати на комплектуючі, що були використані на виготовлення розраховуються за формулою

$$K = \sum_{i=1}^{n} H_i \ Ц_i \ K_i, \qquad (4.7)$$

де H_i кількість комплектуючих i-го виду, шт.,

$Ц_i$ роздрібна ціна комплектуючих i-го виду, грн.,

K_i коефіцієнт транспортних витрат, K_i=1,1,

n кількість видів матеріалів.

Проведені розрахунки зводимо до табл. 4.8 без врахування транспортних витрат.

Таблиця 4.8 – Витрати на комплектуючі

Найменування комплектуючих	Кількість	Ціна за штуку, грн.
Bluetooth-модуль HC-05-SPP-C	1	140
Wi-Fi модуль ESP-07	1	150
Світлодіод індикаторний	2	2
Оптрон EL817	2	4,5
Резистори	10	0,8
Реле G2RL145DC	2	108
Транзистори BC817	6	2,5
Корпус	1	600
Bluetooth-модуль HC-05-SPP-C	1	140
Всього		1146,00

Витрати на комплектуючі, що були використані на розробку з врахуванням транспортних втрат:

$$H = 1146 \cdot 1,1 = 1260,60 \text{ (грн.)}$$

Визначаємо витрати на електроенергію. Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП).

Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В П Ф К_п, \quad (4.8)$$

де В — вартість 1 кВт-години електроенергії, В = 6,2 грн./кВт;

П — встановлена середня потужність обладнання, кВт. П = 0,4 кВт;

Ф — фактична кількість годин роботи обладнання, годин.

$К_п$ — коефіцієнт використання потужності, $К_п$ = 0,8.

$$В_е = 0,8 \cdot 0,4 \cdot 8 \cdot 30 \cdot 6,2 + 0,8 \cdot 0,4 \cdot 7,0 \cdot 6,2 = 476,16 + 13,888 =$$
$$= 490,05 \text{ (грн.)}$$

Визначаємо інші витрати та загальновиробничі витрати. До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \qquad (4.9)$$

де $Н_{ів}$ норма нарахування за статтею «Інші витрати».

$$I_в = (61500,00 + 973,57) \cdot 55\% / 100\% = 34798,57 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} \cdot (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \qquad (4.10)$$

де $Н_{нзв}$ норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$H_{нзв} = (61500,00 + 1770,13) \cdot 110\% / 100\ \% = 69597 \text{ (грн.)}$$

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи:

$$B_{заг} = 61500,00+1770,13+6327,01+14921,94+7271,48+ 643,9453+8380+$$
$$+1260,60+490,05+34798,57+69597 = 206960,86 \text{ (грн.)}.$$

Розраховуємо загальні витрати на науково-дослідну (науково-технічну) роботу та оформлення її результатів. Загальні витрати на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються *ЗВ*, визначається за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \qquad (4.11)$$

де η коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Оскільки науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 206960,86 / 0,5 = 413922 \text{ (грн.)}.$$

4.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить

потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

а) вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

б) зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

в) кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб’єктів (зацікавлених осіб) цього попиту;

г) визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

абсолютного економічного ефекту (чистого дисконтованого доходу);

внутрішньої економічної дохідності (внутрішньої норми дохідності);

терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об’єднати, враховуючи визначені ситуації з відповідними умовами.

В роботі здійснюється вдосконалення апаратно-програмного засобу для використання масовим споживачем. У цьому випадку майбутній економічний

ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot (1 - \frac{\lambda}{100}), \qquad (4.12)$$

де $\pm\Delta Ц_o$ зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_o$ основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_o = Ц_б \pm \Delta Ц_o$;

$Цб$ вартість програмного продукту у році до впровадження результатів розробки;

ΔN збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

p коефіцієнт, який враховує рентабельність продукту;

ϑ ставка податку на прибуток, у 2022 році ϑ =18%.

Припустимо, що при прогнозованій ціні *2500* грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *250* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року – на 1000 шт., протягом другого року – на 1500 шт., протягом третього року на 2000 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$$\Delta П_1 = (0*250 + (2500 + 250)*1000)* 0{,}8333*0{,}2) * (1 - 0{,}18) = 341666{,}653 \text{ (грн.)}.$$

$$\Delta П_2 = (0*250 + (2500 + 250)*(1000+1500)* 0{,}8333*0{,}2) * (1 - 0{,}18) =$$

= 939583,296 (грн.).

$\Delta П_3$ = (0*250 + (2500 + 250)*(1000+1500+2000)* 0,8333*0,2) * (1 - 0,18) =

= 1691249,932 (грн.).

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 2972499,88 грн.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Розраховуємо приведену вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.13)$$

де $\Delta П_i$ збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, *= 0,05…0,15;*

t період часу (в роках).

Збільшення прибутку ми отримаємо починаючи з першого року:

ПП = (341666,653/(1+0,1)[1])+(939583,296/(1+0,1)[2])+(1691249,932/(1+0,1)[3]) =

= 310606,05 + 776515,12 + 1270661,11 = 2357782,275 (грн.).

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (4.14)$$

де $k_{інв}$ коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

ЗВ загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 413922 = 827844 \text{ (грн.)}.$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \quad (4.15)$$

$$E_{абс} = 2357782{,}275 - 413922 = 1943860{,}55 \text{ (грн.)}.$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої но-рми дохідності *(IRR, Internal Rate of Return)* вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в > \sqrt[T_ж]{1 + \frac{E_{обс}}{PV}} - 1, \quad (4.16)$$

$T_ж$ життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{1 + 1943860{,}55/413922} - 1 = 0{,}786$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$d + f, \tag{4.17}$$

де d середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d = (0,09…0,14);

f показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{4.18}$$

$$T_{ок} = 1 / 0{,}786 = 1{,}27 \text{ (р.)}.$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 1,27 роки, то фінансування даної наукової розробки є доцільним.

Висновки до розділу: економічна частина даної роботи містить розрахунок витрат на розробку нового продукту, сума яких складає 413922 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений продукт за ціною

дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 1,27 роки.

ВИСНОВКИ

Систем керування доступом є сучасним та ефективним підходом до вирішення завдань комплексної безпеки. Інноваційні рішення у цій галузі пов’язані із застосуванням IP-технологій, що надає зручність використання, забезпечує легкість та гнучкість впровадження, дозволяє отримати нові функціональні можливості, зокрема можливості віддаленого керування.

Віддалене керування правами доступу може бути забезпечене лише за рахунок застосування технологій мобільної ідентифікації, при якій ідентифікатор пред′являється за допомогою смартфону.

Розроблений контролер керування доступом дозволяє віддалено визначати права доступу через Ethernet або WI-FI підключення до хмарного сервера, надаючи доступ в режимі офлайн за ідентифікатором, що надсилається зі смартфона через Bluetooth.

Розроблені додатки адміністратора, веб-сервера та мобільного додатку користувача дозволяють побудувати на основі розробленого контролера гнучку ієрархічну систему віддаленого керування доступом через веб-інтерфейс для будь-якого об′єкта.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Системи контролю та управління доступом. [Електронний ресурс]. Режим доступу: https://evertech.ua/access-controll-systems/.

2. Виды систем контроля и управления доступом. [Електронний ресурс]. Режим доступу: https://karabiner.ua/stati/vidy-sistem-kontrolya-i-upravleniya-dostupom-skud/.

3. Капинос, И. С. Современные тенденции в построении систем контроля и управления доступом / И. С. Капинос // Молодой ученый. — 2019. — № 22 (260). — С. 49-51.

4. Системи контролю і управління доступом від А до Я. [Електронний ресурс]. Режим доступу: https://deps.ua/ua/knowegable-base/reference-information/7824.html.

5. Системи контролю та управління доступом. [Електронний ресурс]. Режим доступуhttps://www.rim2000.com/equipment/networks/access-control/.

6. СКУД - система контролю та управління доступом. [Електронний ресурс]. Режим доступу: http://www.centrebespek.com/articles/ELEMENT_ID_14787/.

7. Gean Davis Breda New Era of Mobile Access Control System / Gean Davis Breda, Raul Mariano Cardoso, Felipe André Cordeiro Pirotta // International Journal of Computer Science and Network Security, VOL.15, No.8, 2015, P. 6 – 15.

8. Rajashree S. Bluetooth and NFC Enabled Contactless Access Control System / S.Rajashree, S. Kaushik, K. Varman // ScieXplore: International Journal of Research in Science, 2015, № 2, P. 1 32.

9. NFC: умные метки. [Електронний ресурс]. Режим доступу: https://itc.ua/articles/nfc_umnye_metki_53544/.

10. Бідюк П. Сучасні методи біометричної ідентифікації / Петро Бідюк, Володимир Бондарчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2009. Випуск 1(18). С. 137 146.

11. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих

навчальних закладів] / Р.Ю. Царьов, Т. М. Лемеха. Одеса: ОНАЗ ім. О.С. Попова, 2016. 140 с.

12. Контроллер доступа NDC F18IP(U-Prox IP400). [Електронний ресурс]. Режим доступу: https://www.forter.com.ua/kontrollery-dostupa/u-prox-ip-400/.

13. Зчитувач-контролер SameKey Card Control. [Електронний ресурс]. Режим доступу: https://secur.ua/kontroller-schityvatel-samekey-card-control.html.

14. Комплекс мобільного керування автоматикою пропуску LOKKYY[Електронний ресурс]. Режим доступу: https://lokkyy.com/#about.

15. GSM. [Електронний ресурс]. Режим доступу: http://www.smartphone.ua/w_gsm.html.

16. GSM-модуль RC-25 пристрій для управління автоматикою воріт і шлагбаумів з мобільного телефону. [Електронний ресурс]. Режим доступу: https://novi-vorota.com.ua/ua/avtomatika-gsm-module.html.

17. Дистанційне управління зі смартфона з WI-FI, Bluetooth, LTE, GSM. [Електронний ресурс]. Режим доступу: https://dtb.com.ua/ua/g91671568-upravlenie-smartfona-kanalam.

18. Протокол передачи гипертекста. [Електронний ресурс]. Режим доступу: https://developer.mozilla.org/ru/docs/Web/HTTP/Overview.

19. Технология NFC в смартфонах и ее практическое использование. [Електронний ресурс]. Режим доступу: https://www.ixbt.com/mobile/nfc-2018.shtml.

20. Bluetooth Technology Overview. [Електронний ресурс]. Режим доступу:https://www.bluetooth.com/learn-about-bluetooth/tech-overview/.

21. Обзор способов и протоколов аутентификации в веб-приложениях. [Електронний ресурс]. Режим доступу: https://habr.com/ru/company/dataart/blog/262817/.

22. Аутентификация и авторизация в микросервисных приложених. [Електронний ресурс]. Режим доступу: https://habr.com/ru/company/dataart/blog/311376/

23. Проводные и беспроводные локальные сети преимущества и

недостатки. [Електронний ресурс]. Режим доступу: http://alternativa.dp.ua/provodnye-i-besprovodnye-lokalnye-seti-preimushhestva-i-nedostatki/

24. Комп’ютерні мережі : підручник / Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.. − Вінниця : ВНТУ, 2020, 378 с.

25. Обзор технологии Ethernet. [Електронний ресурс]. Режим доступу: https://bg.net.ua/content/obzor-tekhnologii-ethernet.

26. Внедрение на сети доступа технологий WI-FI. [Електронний ресурс]. Режим доступу: http://www.incore.me/svyaz/vnedrenie-na-seti-dostupa-texnologij-wi-fi/.

27. Беспроводная технология Wi-Fi. [Електронний ресурс]. Режим доступу: https://www.lessons-tva.info/articles/net/003.html.

28. Стрельцов Д. Устройство и принцип работы Wi-Fi сети (преимущества и недостатки). [Електронний ресурс]. Режим доступу: https://hobbyits.com/ustrojstvo-i-princip-raboty-wi-fi-seti.

29. Лящук О. М. Безпровідні мережі. Стандарт ZigBee. / О. М. Лящук // Вісник Національного технічного університету України «КПІ», №44, 2011, С. 157 – 163.

30. Види і призначення електромагнітного реле, пристрій і принцип роботи, переваги і недоліки. [Електронний ресурс]. Режим доступу: https://sitemasters.com.ua/elektroobladnannja/vidi-i-priznachennja-elektromagnitnogo-rele/

31. Рожненко Ж. Г. Використання мікропроцесорів на базі arm cortex в електромеханіці / Ж. Г. Рожненко, О. К. Данилейко, Г.В. Коломіц, А. В. Ятчук // Гірничий вісник, вип. 109, 2021, С. 98 – 106.

32. STM32: Эпоха 32-битных микроконтроллеров наступила. [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/data/stm32/stm32new.php.

33. Отладочная плата STM32F407VET6-Mini. [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/el.php?name=STM32F407VET6-Mini.

34. STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced Arm-based 32-bit MCUs. [Електронний ресурс]. Режим доступу: https://www.st.com/resource/en/reference_manual/dm00031020-stm32f405-415-stm32f407-417-stm32f427-437-and-stm32f429-439-advanced-arm-based-32-bit-mcus-stmicroelectronics.pdf.

35. Ethernet модуль DP83848 Waveshare. [Електронний ресурс]. Режим доступу: https://miniboard.com.ua/modules/764-ethernet-modul-dp83848-waveshare.html.

36. ESP8266: микросхема Wi-Fi. [Електронний ресурс]. Режим доступу: http://microsin.net/adminstuff/hardware/esp8266-wifi-ic.htm.

37. Wi-Fi модуль ESP8266 версія ESP-07. [Електронний ресурс]. Режим доступу: https://arduino.ua/prod1444-wi-fi-modyl-esp8266-versiya-esp-07.

38. Модуль Bluetooth HC-05. [Електронний ресурс]. Режим доступу: https://foton.ua/catalog/arduino/modul-bluetooth-hc-05.html

39. PCB Relay G2RL. . [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/pdf/G2RL.pdf.

40. BC817 45 V, 500 mA NPN general-purpose transistors. [Електронний ресурс]. Режим доступу: https://assets.nexperia.com/documents/data-sheet/BC817_SER.pdf.

41. 4 PIN DIP PHOTOTRANSISTOR PHOTOCOUPLER Everlight Electronics Co., Ltd. 1 http://www.everlight.com Document No： DPC-0000046 Rev.10 April, 21 2010 EL817 Series

42. React Native init VS Expo [Електронний ресурс]. Режим доступу: https://habr.com/ru/post/480258/

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ_____

проф., д.т.н.. Азаров О.Д.

_____

" ____ " _____ 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

«Апаратно-програмні засоби віддаленого керування доступом до об’єктів через веб-інтерфейс**»**

08-23.МКР.029.00.000 ТЗ

Науковий керівник: доцент к.т.н.

_____ Крупельницький Л. В.

Виконав: студент групи 2КІ-21м

_____ Тарновський А. М.

ВНТУ 2022

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Необхідність побудови гнучкої та легко впроваджувальної системи віддаленого керування правами доступу з підтримкою можливості надання доступу в автономному режимі з використанням технологій мобільної ідентифікації.

1.2 Наказ про затвердження теми МКР.

2 Мета МКР і призначення розробки

2.1 Мета робота — розширення функціональних можливостей системи віддаленого керування доступом через веб-інтерфейс за рахунок підтримки можливості роботи в офлайн режимі;

2.1 Призначення розробки — визначення підходів до побудови апаратних та програмних засобів системи віддаленого керування доступом через веб-інтерфейс.

3 Вихідні дані для виконання МКР

3.1 Функціональне призначення — віддалене керування доступом з використанням хмарних та мобільних технологій;

3.2 Організація доступу за ідентифікатором, що надсилається зі смартфону або планшету;

3.3 Реєстрація в системі — відділена через веб-інтерфейс;

3.4 Інтерфейси Ethernet, WI-FI та Bluetooth;

3.5 Протоколи TCP/IP, HTTP, Bluetooth;

3.6 Вихід контролера — 2 комутовані канали потужністю до 4 КВт;

3.7 Вхід контролера — 2 оптично розв′язані канали;

3.8 Живлення контролера — джерело постійної напруги +5 В потужністю до 3 Вт.

4 Вимоги до виконання МКР

4.1 Провести обґрунтування доцільності розробки;

4.2 Провести аналіз сучасних технологій управління доступом;

4.3 Визначити підходи до реалізації апаратних та програмних засобів системи віддаленого керування доступом через веб-інтерфейс з підтримкою можливості роботи в режимі офлайн;

4.4 Оцінити комерційний потенціал розробки.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ ета-пу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз сучасних сучасних технологій управління доступом			Вступ Розділ 1
2	Огляд принципів та технологій віддаленого керування доступом			Розділ 2
3	Розробка структурної схеми контролера керування доступом			Розділ 3, Структурна схема
4	Аналіз можливої реалізації структурних блоків та вибір елементної бази. Розробка функціональної схеми			Розділ 3, Функціо-нальна схема
5	Розробка алгоритмів роботи системи та її компонентів. Розробка веб-серверу, додатку адміністратора та мобільного додатку користувача			Розділ 3, Блок схеми алгоритмів, додатки
6	Оцінка комерційного потенціалу розробки			Розділ 4
7	Оформлення пояснювальної записки, графічного матеріалу і презентації			Поясню-вальна записка, графічний матеріал, презентація

6 Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні

матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, довідка про відповідність оформлення МКР діючим вимогам.

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Единa система конструкторської документації. Основні написи»;

— методичні вказівки. Кафедра обчислювальної техніки 2022;

— документами на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21».

ДОДАТОК Б

Схема системи віддаленого керування доступом

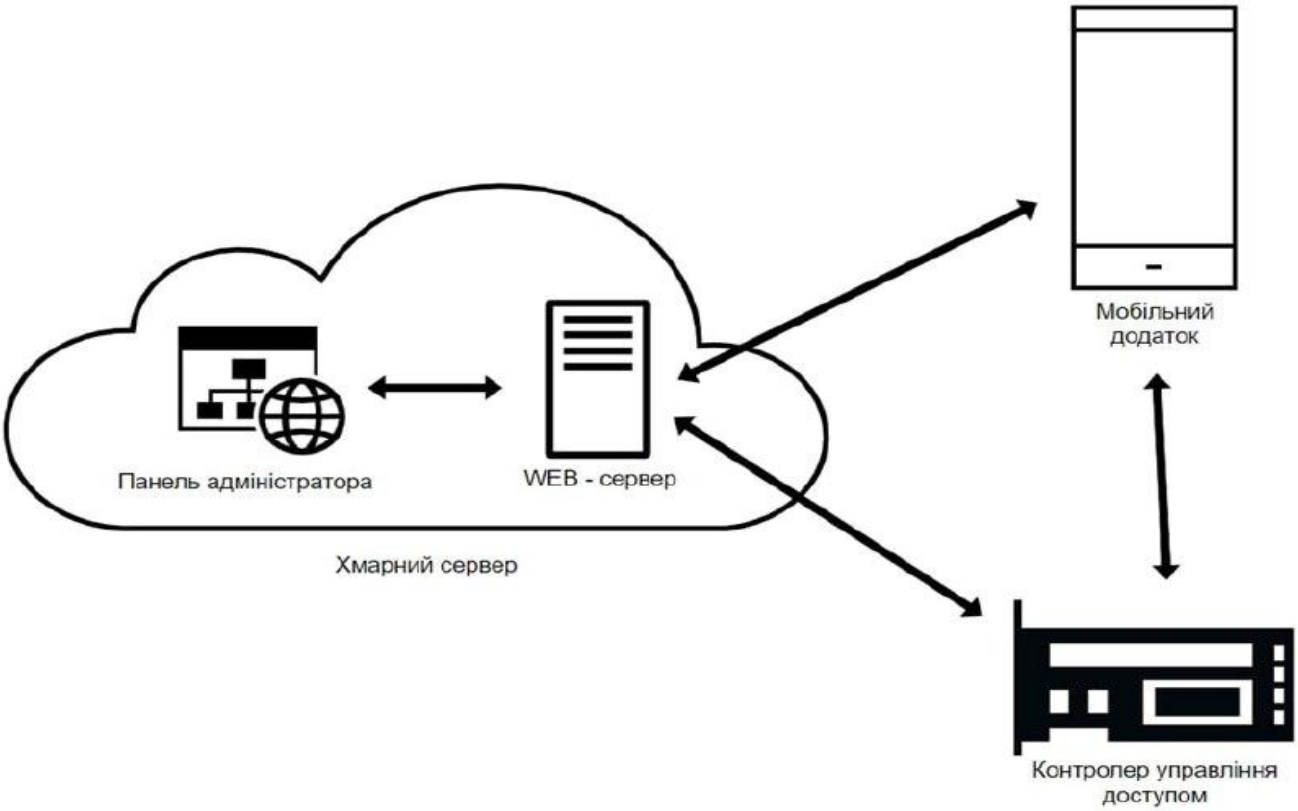

Рисунок Б.1 — Схема системи віддаленого керування доступом

ДОДАТОК В

Структурна схема контролера керування доступом

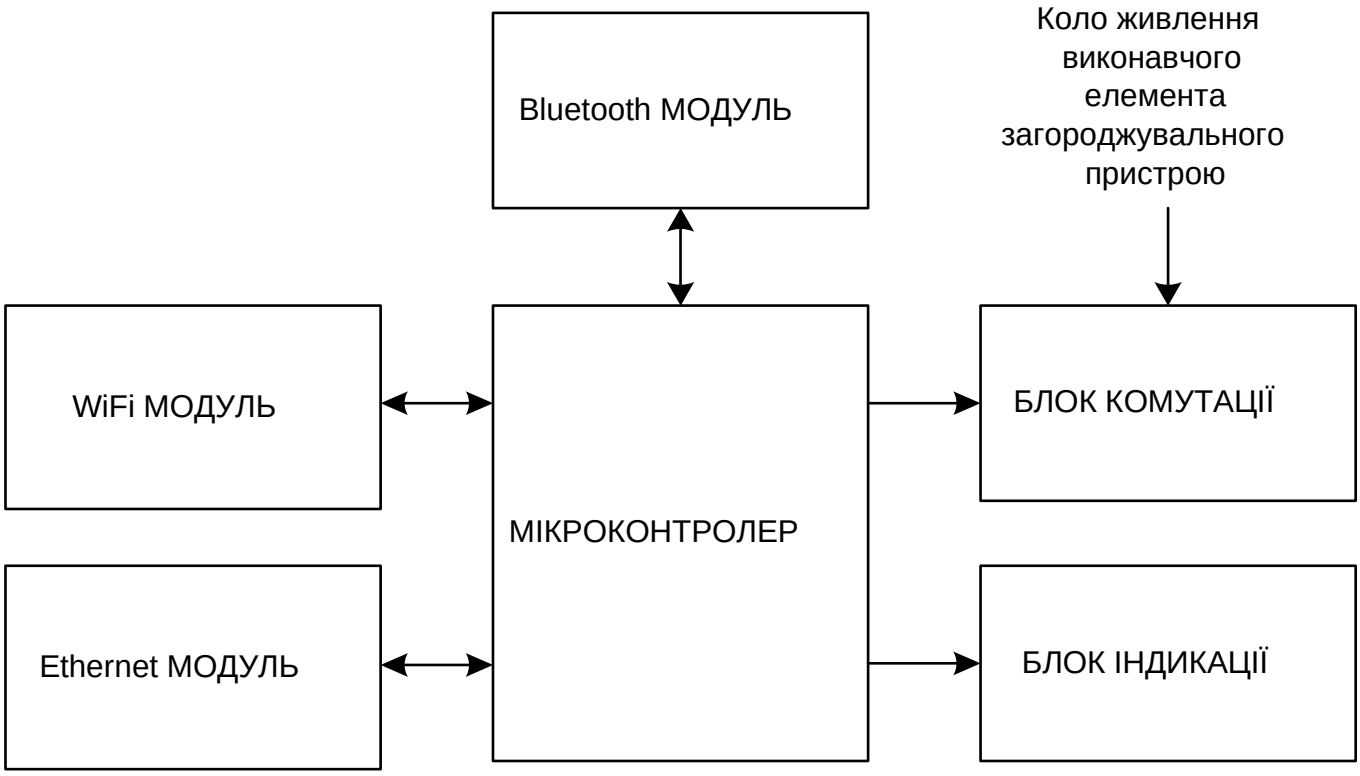

Рисунок В.1 — Структурна схема контролера керування доступом

ДОДАТОК Г

Функціональна схема контролера керування доступом

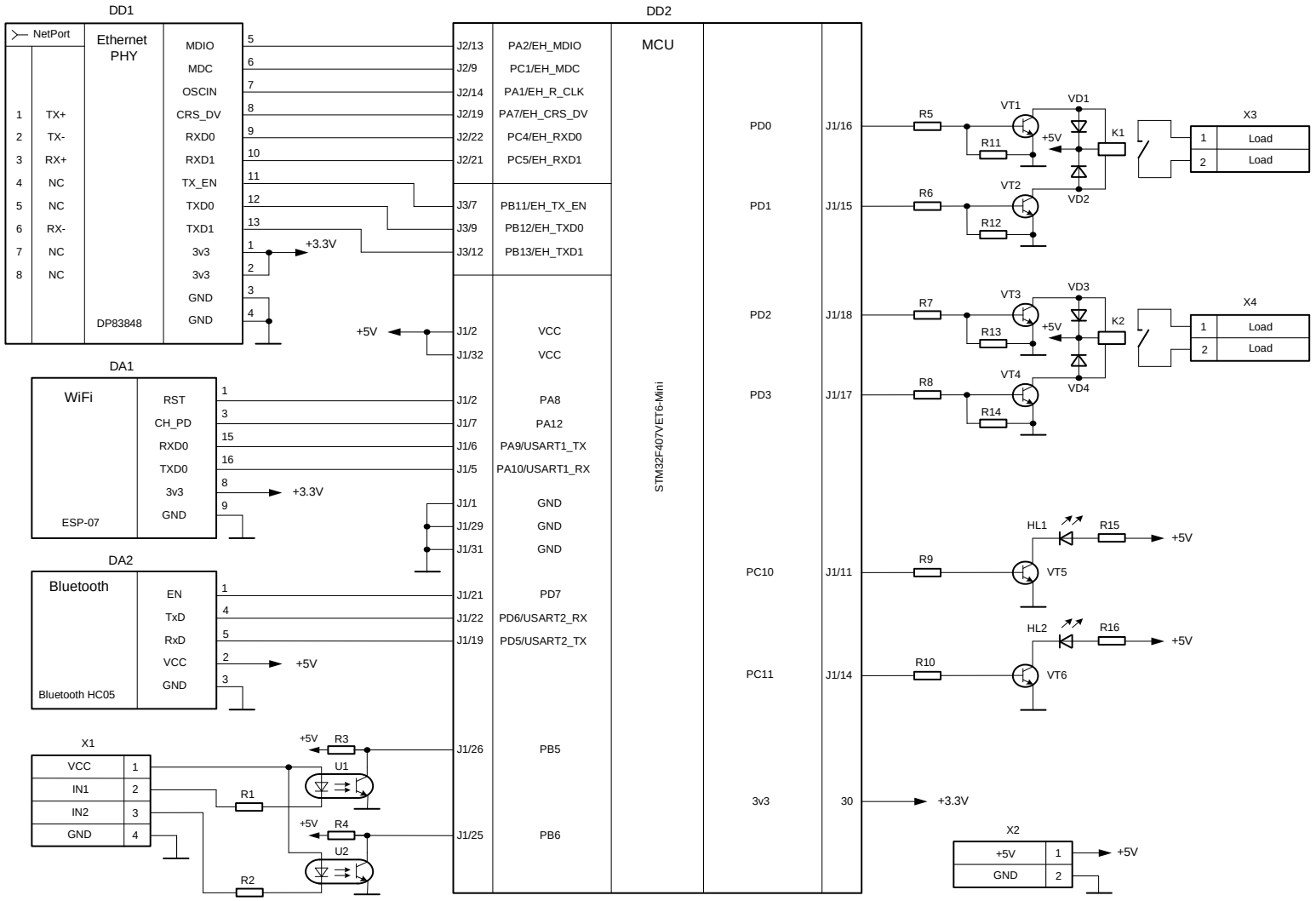

Рисунок Г.1 — Функціональна схема контролера керування доступом

ДОДАТОК Д

Блок-схема алгоритму роботи контролера доступу

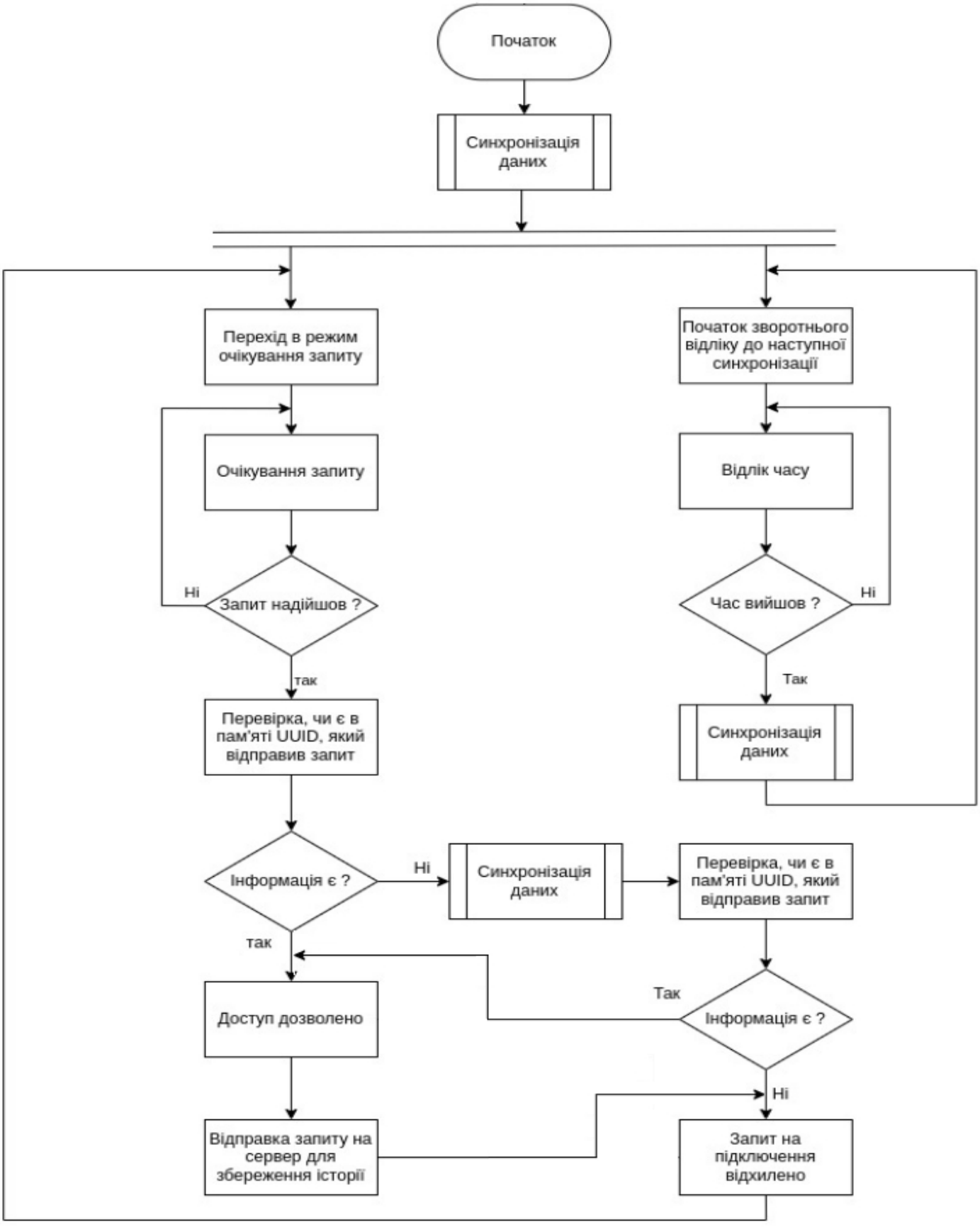

Рисунок Д.1 — Блок-схема алгоритму роботи контролера доступу

ДОДАТОК Е

Блок-схема алгоритму роботи додатку адміністратора

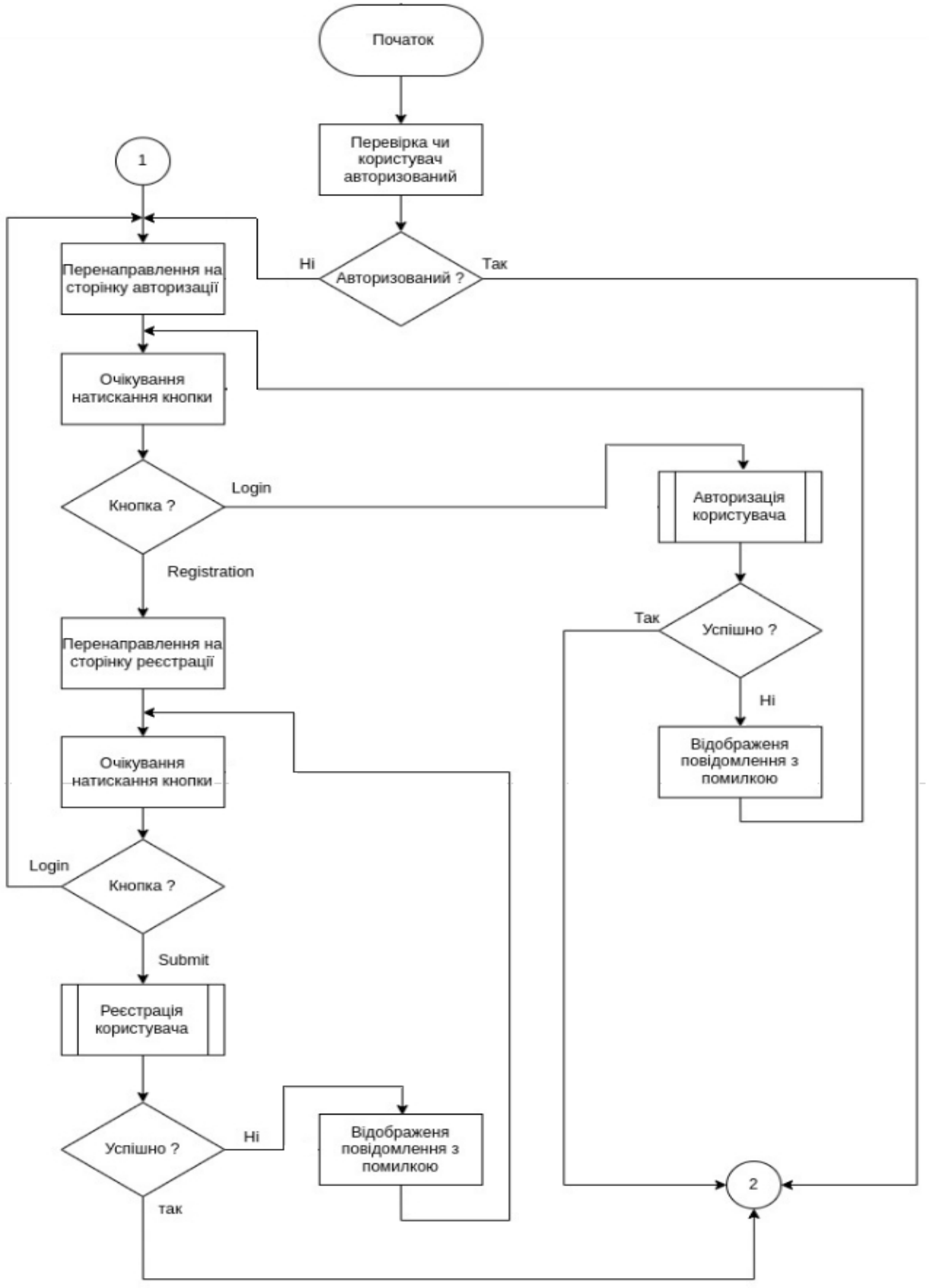

Рисунок Е.1 — Блок-схема алгоритму роботи додатку адміністратора

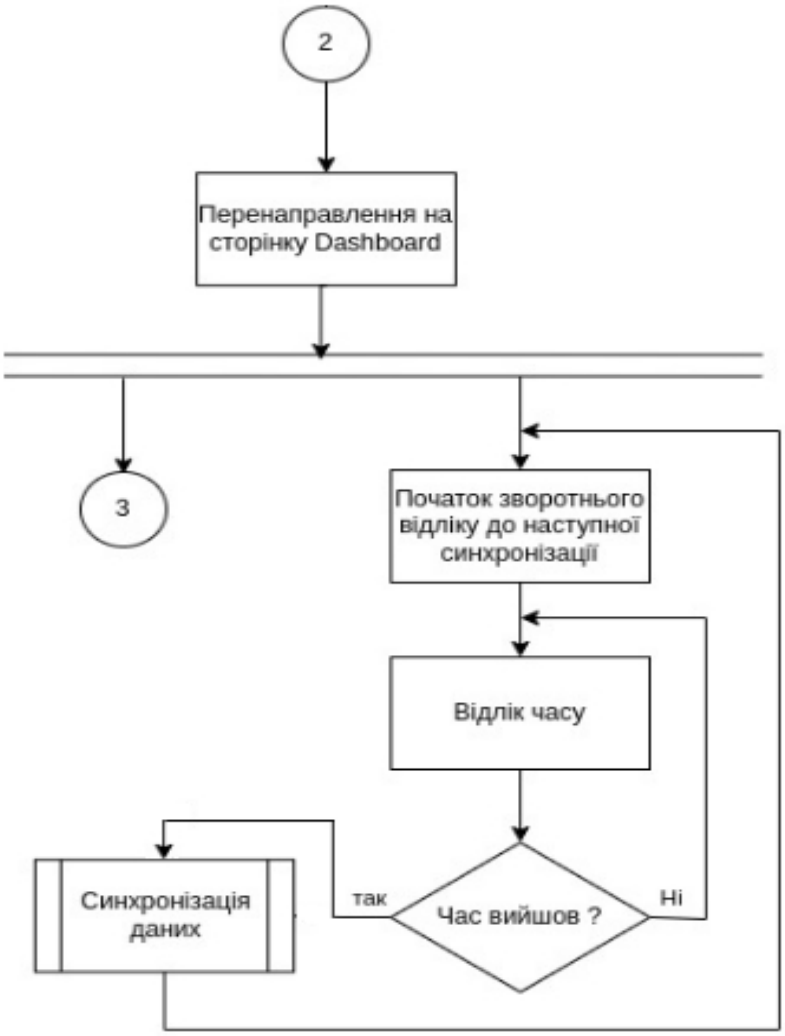

Рисунок Е.1 — Аркуш 2

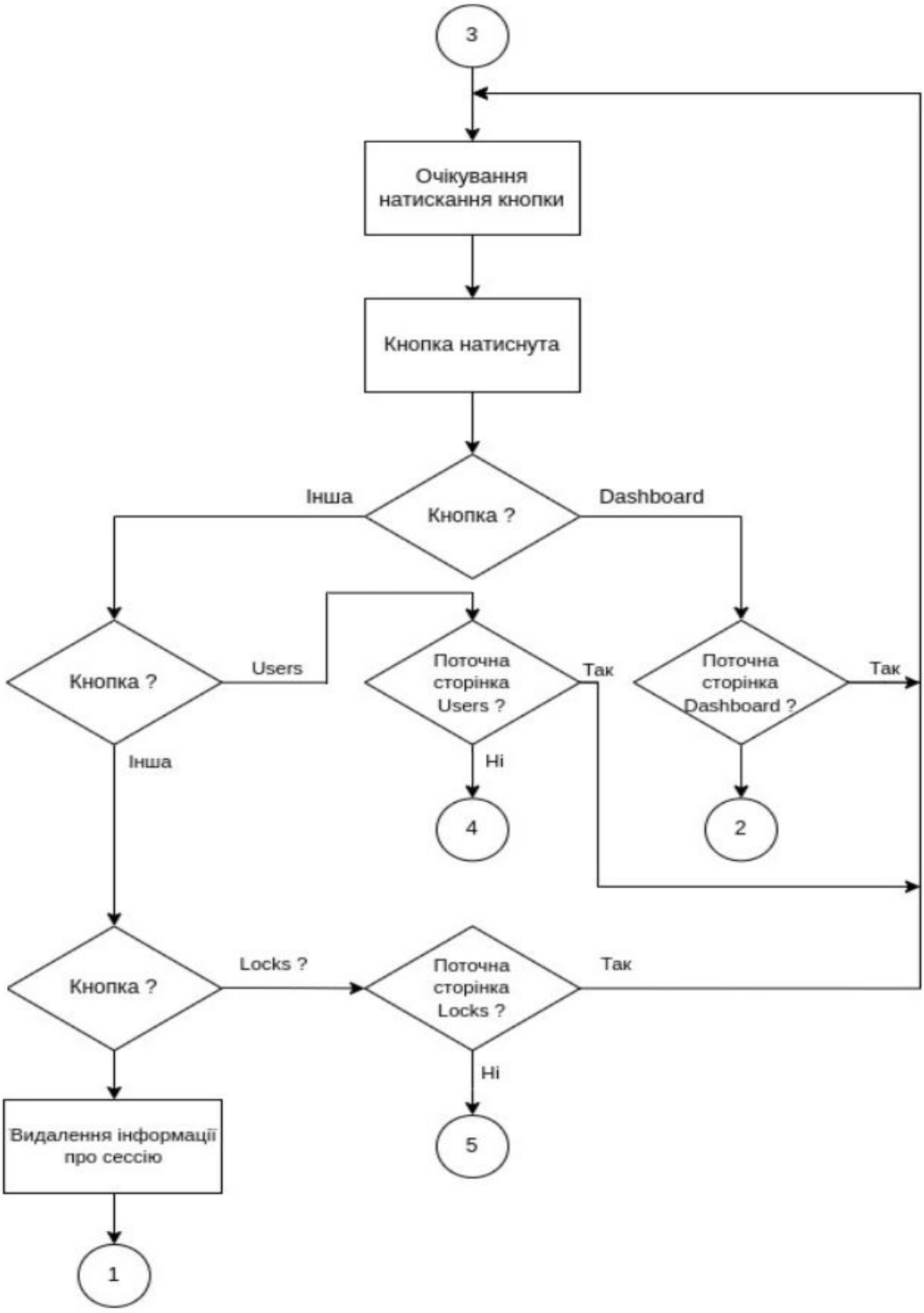

Рисунок Е.1 — Аркуш 3

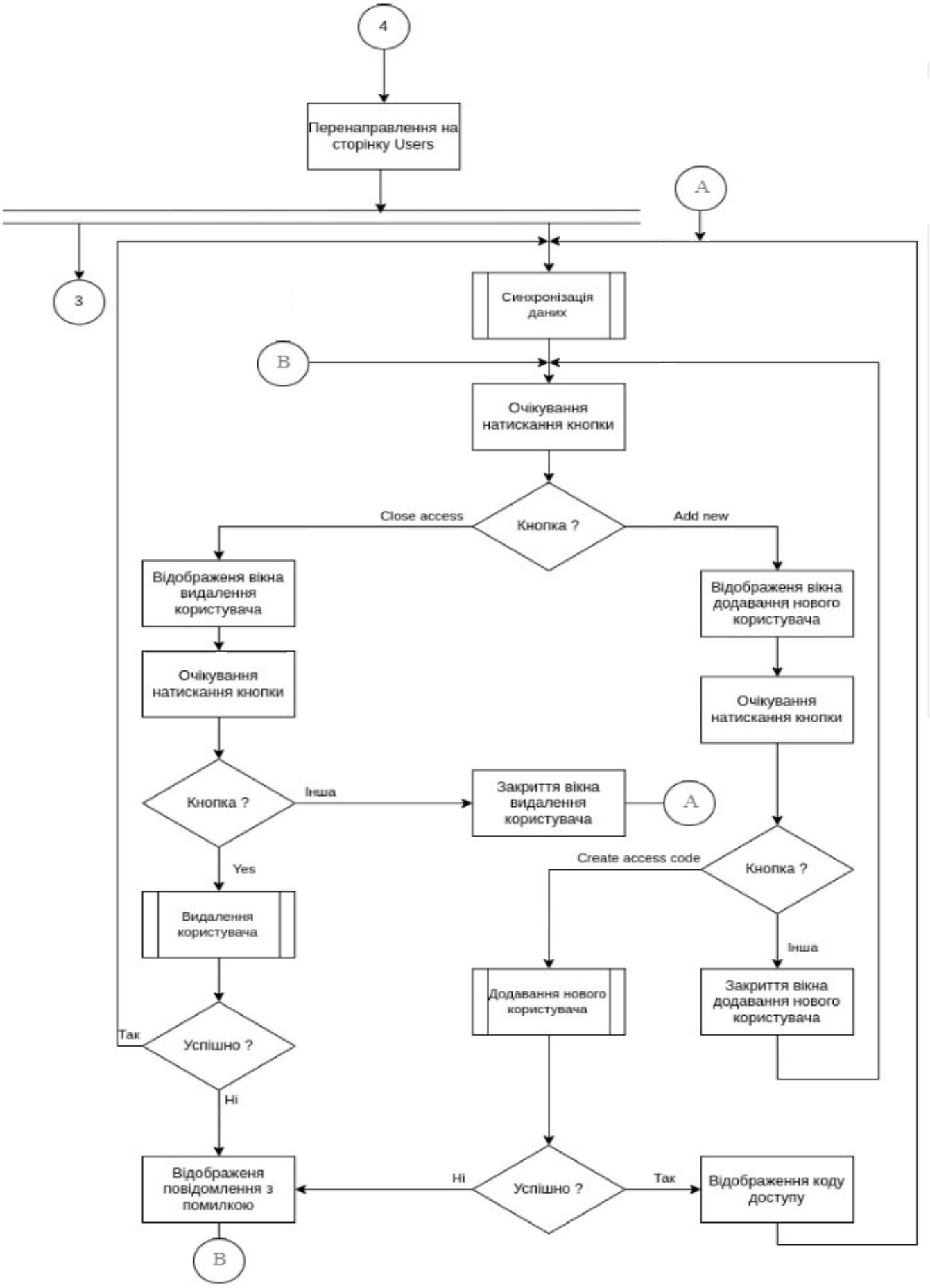

Рисунок Е.1 — Аркуш 4

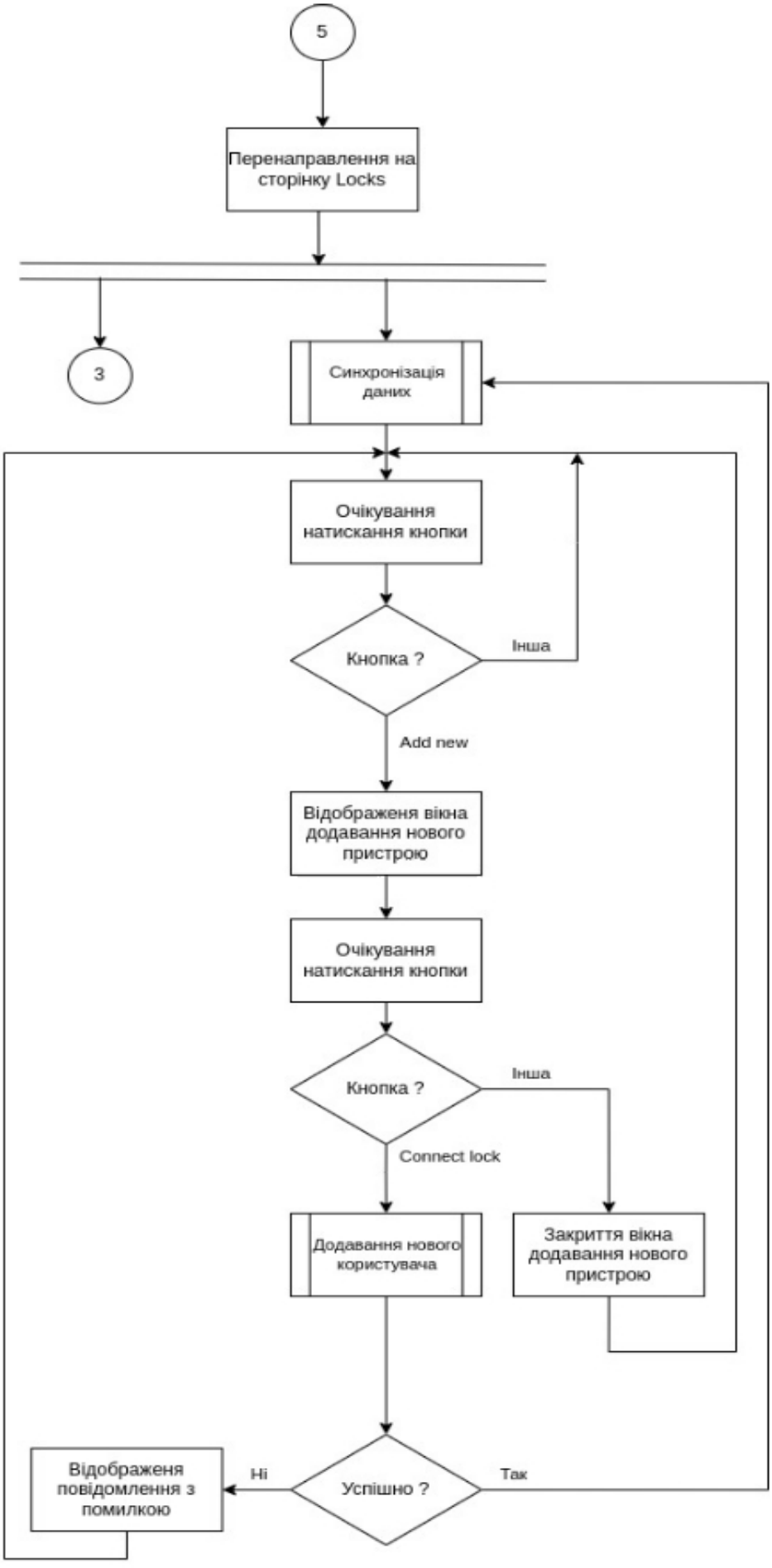

Рисунок Е.1 — Аркуш 5

ДОДАТОК Ж

Блок-схема алгоритму роботи мобільного додатку

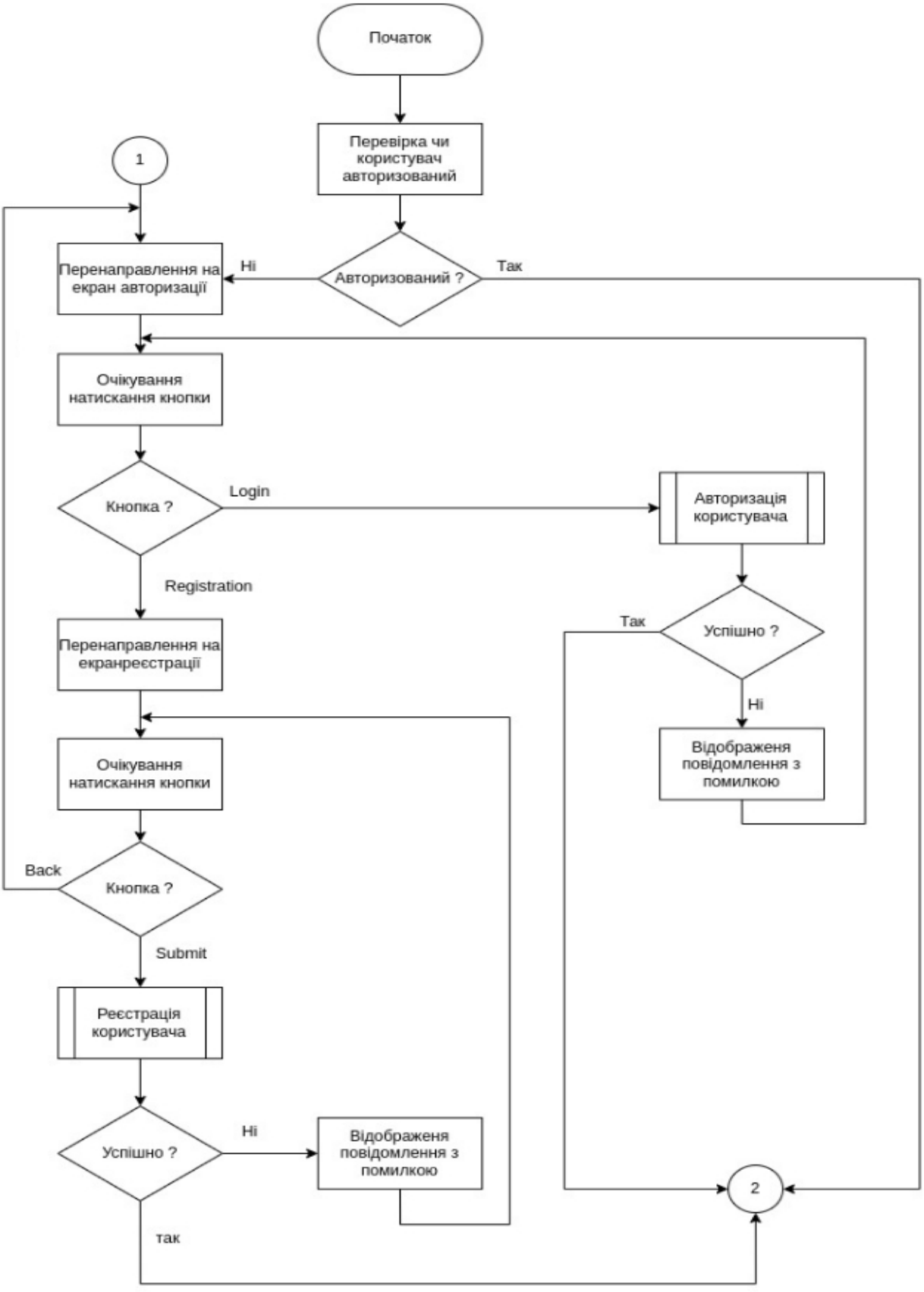

Рисунок Ж.1 — Блок-схема алгоритму роботи мобільного додатку

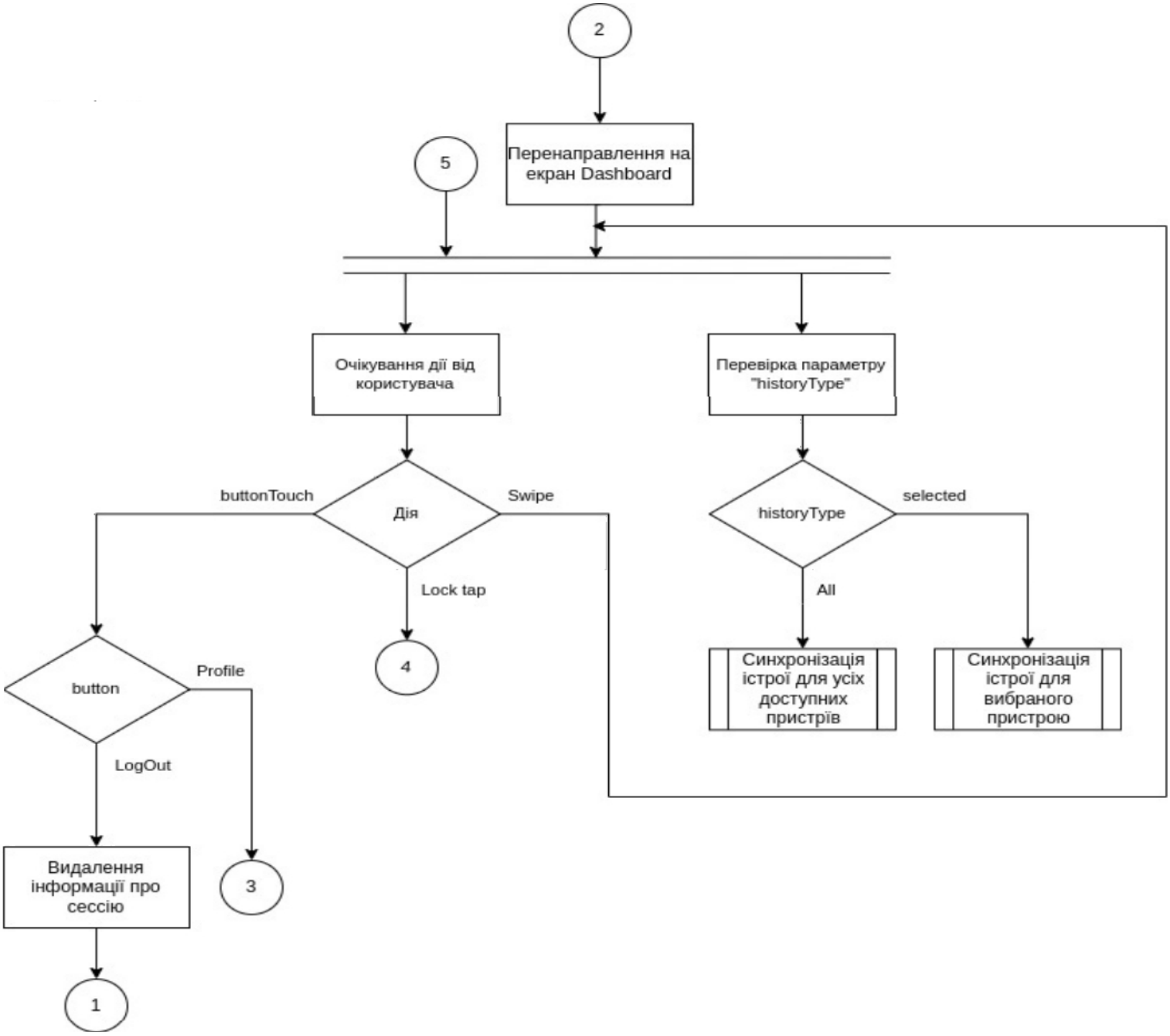

Рисунок Ж.1 — Аркуш 2

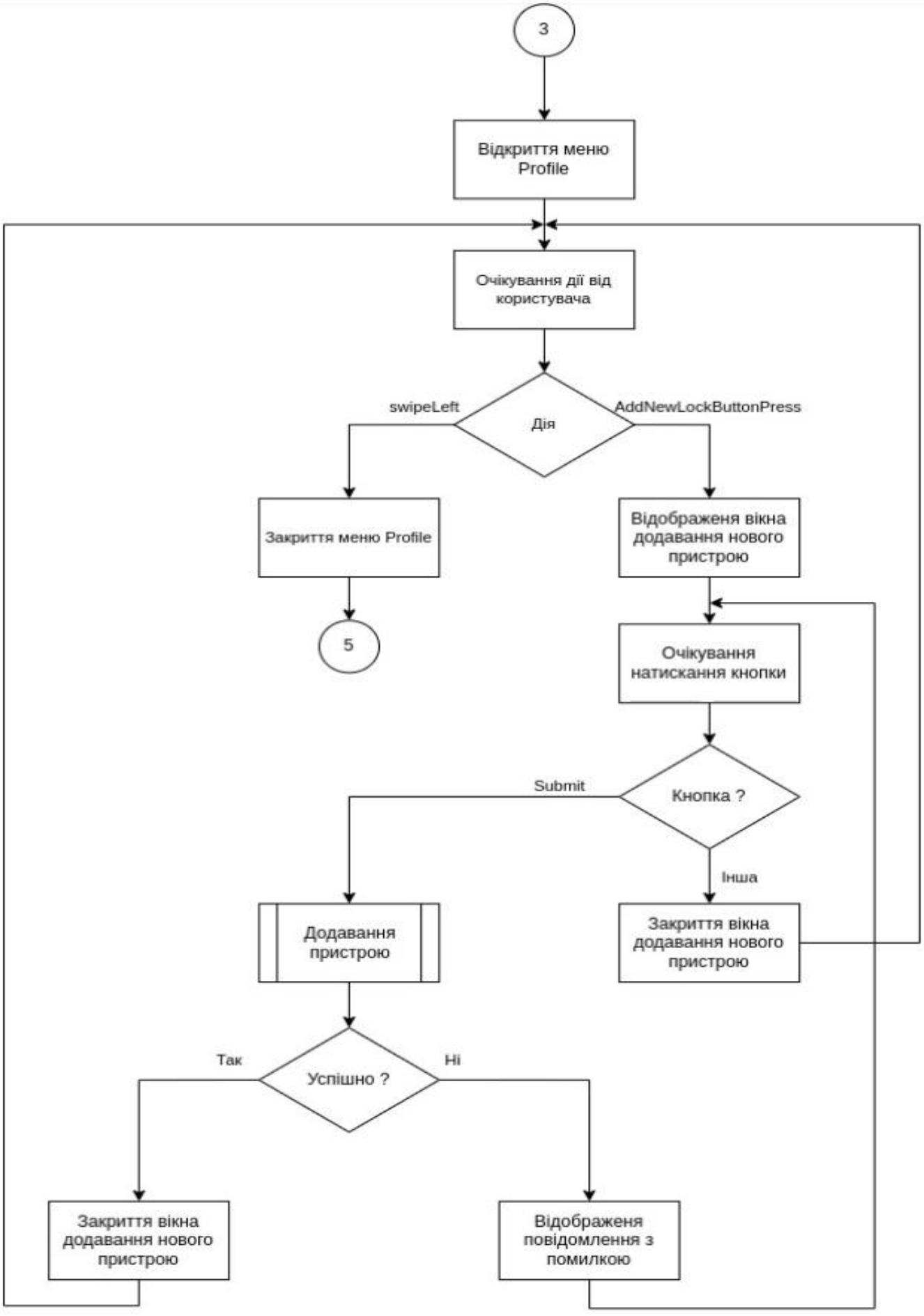

Рисунок Ж.1 — Аркуш 3

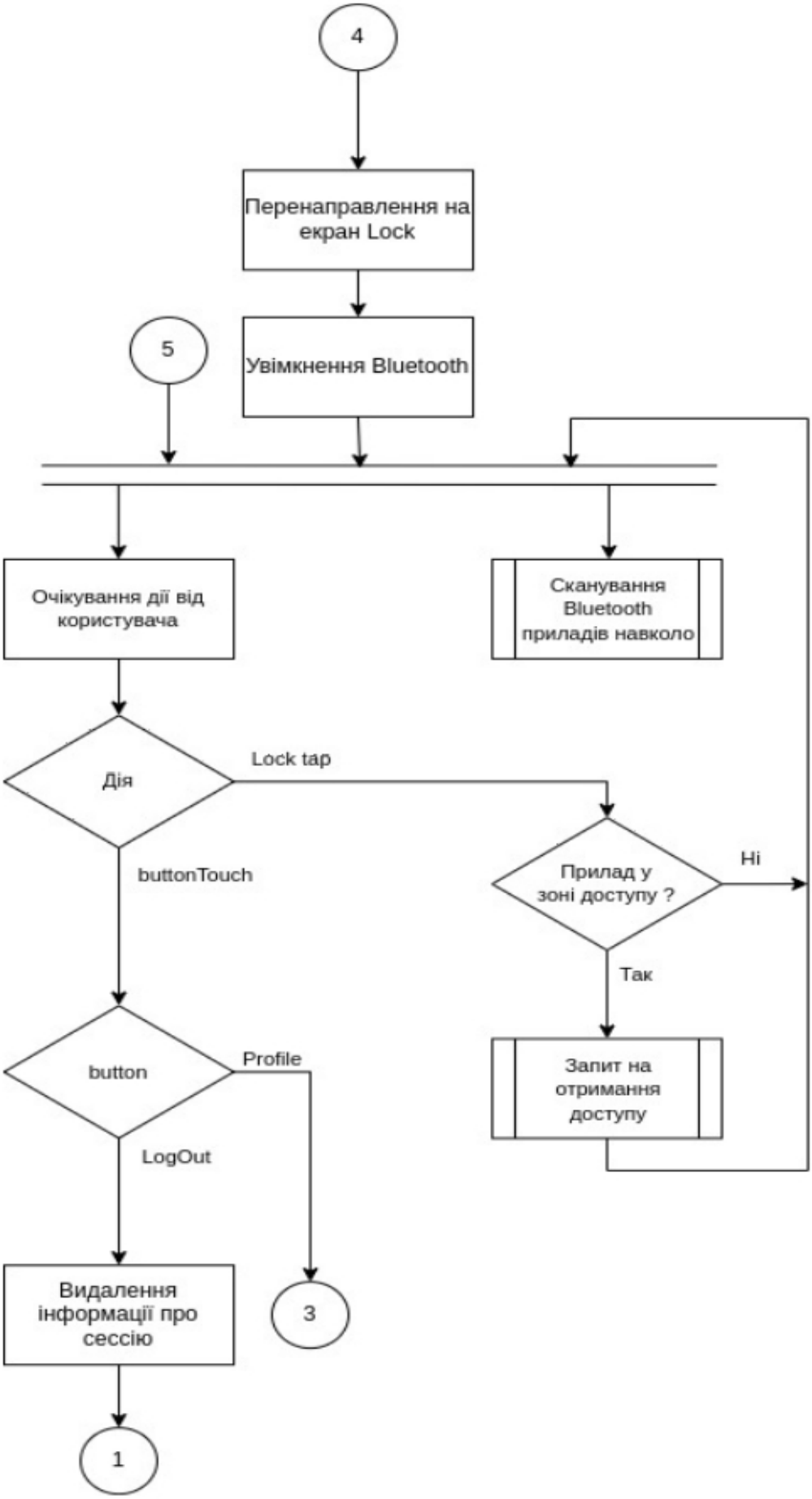

Рисунок Ж.1 — Аркуш 4

ДОДАТОК К

Блок-схема алгоритму роботи веб-сервера

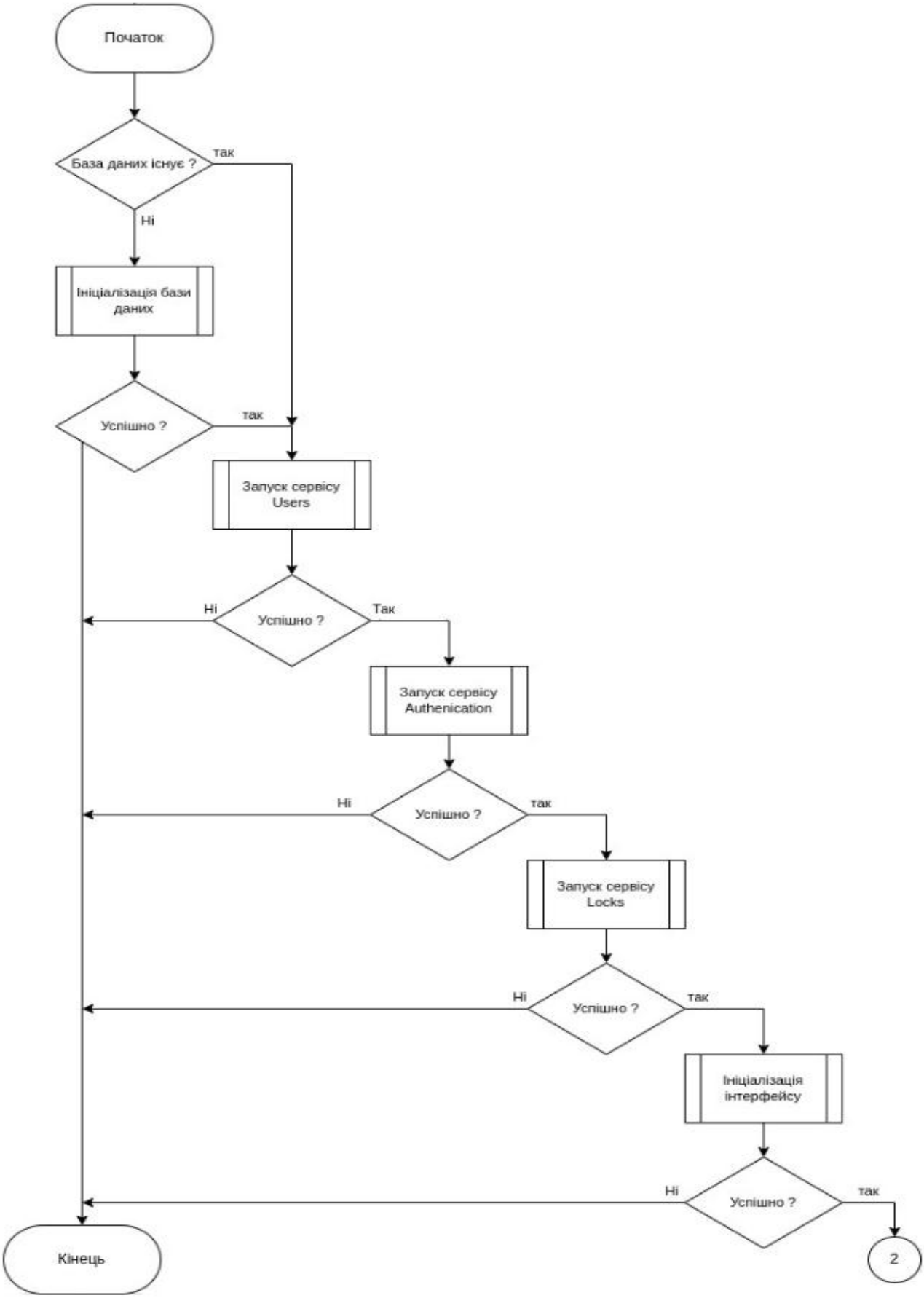

Рисунок К.1 — Блок-схема алгоритму роботи веб-сервера

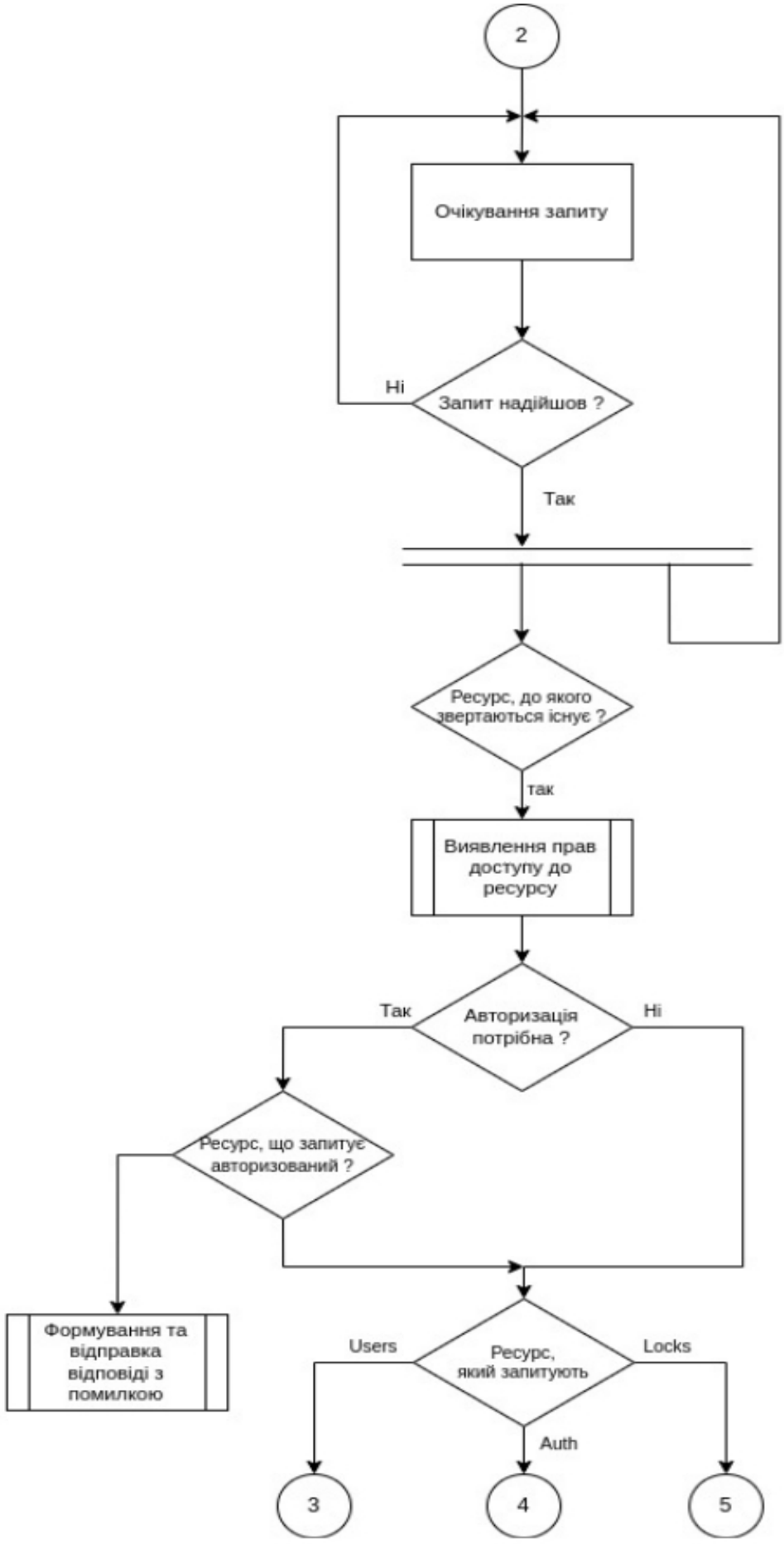

Рисунок К.1 — Аркуш 2

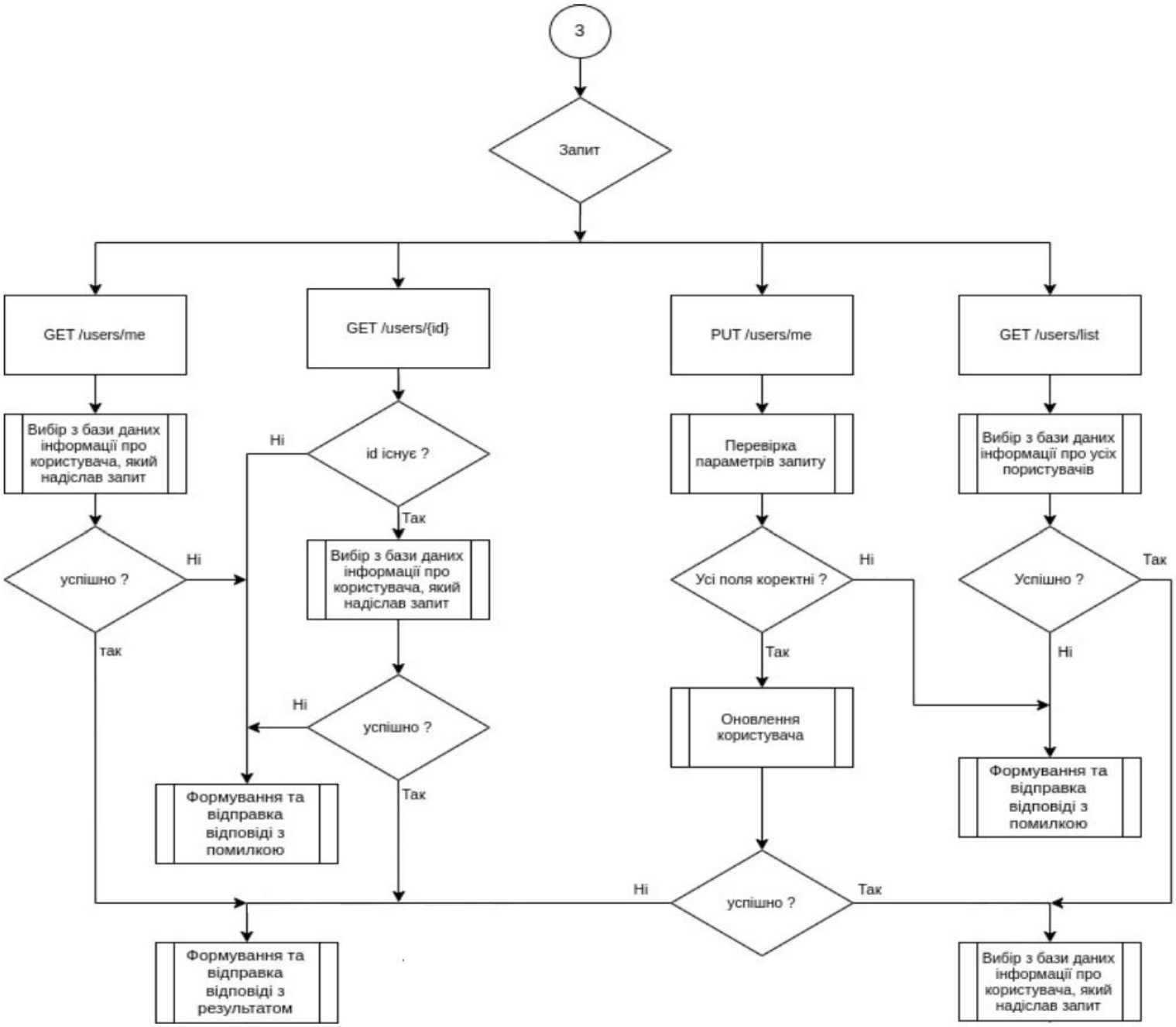

Рисунок К.1 — Аркуш 3

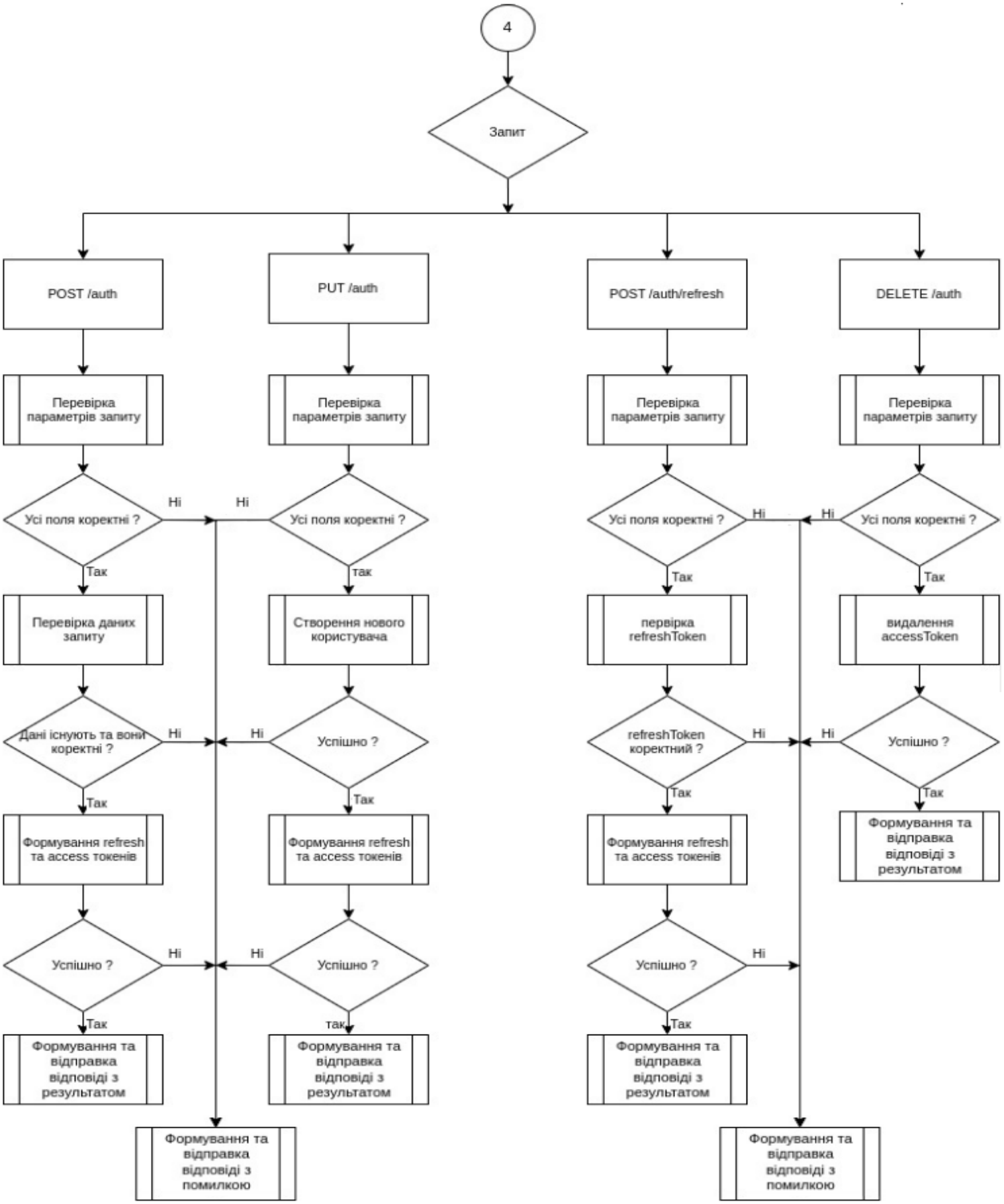

Рисунок К.1 — Аркуш 4

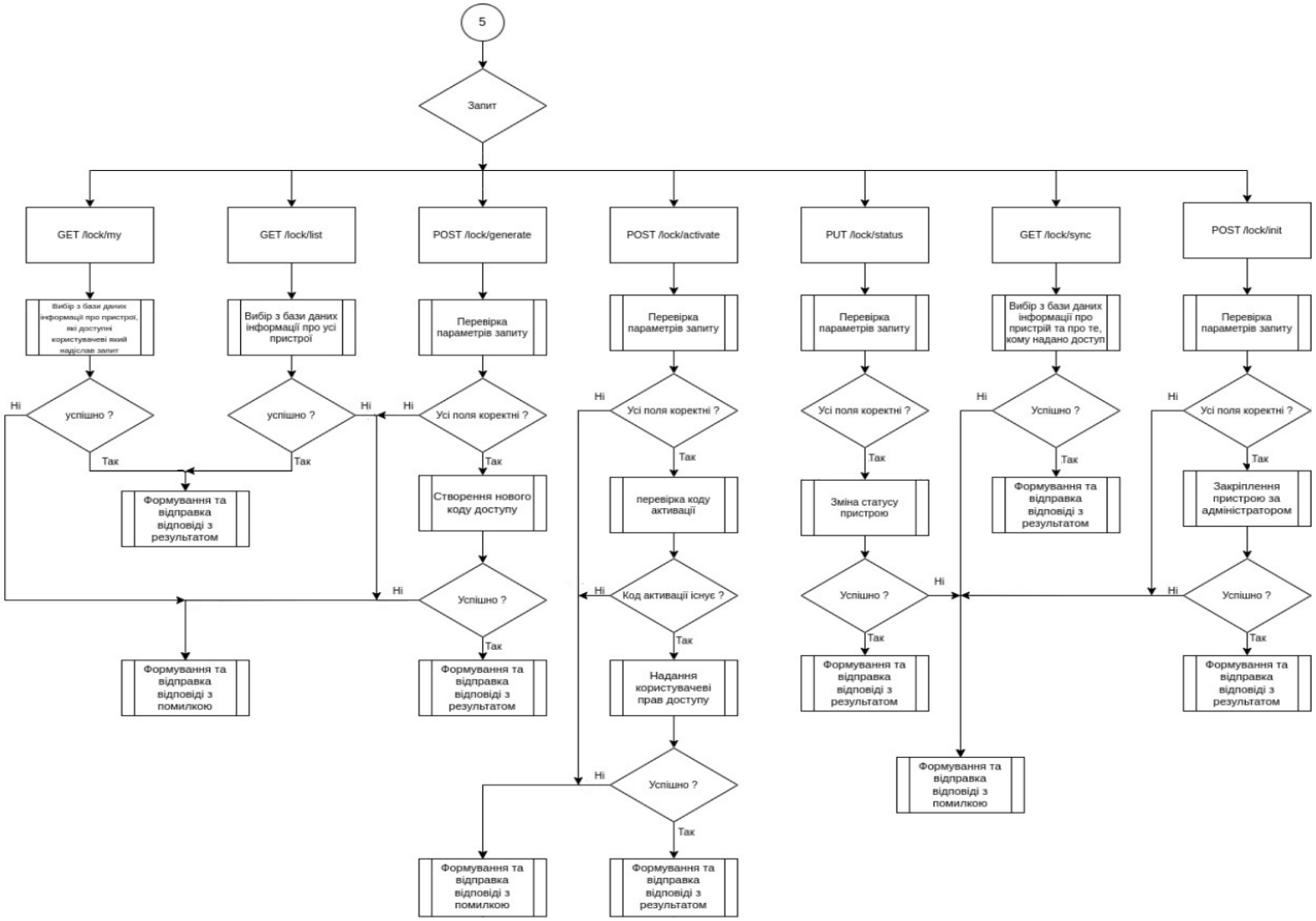

Рисунок К.1 — Аркуш 5

ДОДАТОК Л

Протокол перевірки кваліфікаційної роботи

Назва роботи: Апаратно-програмні засоби віддаленого керування доступом до об’єктів через веб-інтерфейс

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності
Unicheck

Оригінальність 92.7% Схожість 7.3%

Аналіз звіту подібності (відмітити потрібне):

- ☒ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Тарновський А. М.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Крупельницький Л. В.
(підпис) (прізвище, ініціали)