Міністерство освіти і науки України

Луцький національний технічний університет
Факультет комп'ютерних та інформаційних технологій
Кафедра комп'ютерної інженерії та охоронних систем

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

НАВЧАЛЬНО-ЛАБОРАТОРНА УСТАНОВКА СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА БАЗІ BIOTIME ZKBT-DEV-P10

TRAINING AND LABORATORY PHYSICAL ACCESS CONTROL SYSTEM INSTALLATION BASED ON BIOTIME ZKBT-DEV-P10

спеціальність 126 Інформаційні системи та технології
(шифр і назва спеціальності)

освітня програма «Інформаційні системи та технології охорони і безпеки»
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи ІСТО-41
ТРОФИМЧУК Ілля Олегович

_____
(підпис)

Керівник:
д.г.н., професор
ПУГАЧ Сергій Олександрович

_____
(підпис)

Кваліфікаційну роботу допущено до захисту
«___» _____2026 р.
Гарант освітньої програми:
к.т.н., доцент
ТЕРЛЕЦЬКИЙ Тарас Володимирович

_____
(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет: *комп'ютерних та інформаційних технологій*
Кафедра: *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *126 Інформаційні системи та технології*
Освітня програма: «*Інформаційні системи та технології охорони і безпеки*»

ЗАТВЕРДЖУЮ
Завідувач кафедри КІБ
к.т.н., доцент Терлецький Т. В.

_____
«___» _____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

ТРОФИМЧУКУ Іллі Олеговичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: *Навчально-лабораторна установка системи контролю та управління доступом на базі BioTime ZKBT-Dev-P10.*

Керівник роботи: *к.т.н., доцент Кайдик Олег Леонтійович*
затверджені наказом закладу вищої освіти від «16» грудня 2025 р. № 529/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: «30» травня 2026 р.
3. Вихідні дані до роботи: *Схема та конструктивне рішення навчально-лабораторного стенда ДСТУ EN 60839 ДСТУ EN 60839-11-1:2019. ДСТУ EN 60839-11-2:2019 ДСТУ ISO/ IEC 30107-3:2024 ДСТУ IEC 60529:2014. ДБН В.2.5-56:2014 Системи контролю та управління доступом: BioTime ZKBT-Dev-P10 (ZKTeco); Hikvision DS-K1T; Dahua ASI*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити): *Анотація. Вступ. Розділ 1 Аналітичний огляд стану предметної області (хараетеристика об'єкту проєктування; огляд нормативно-правової бази та стандартів у сфері біометричної Ідентифікації й СКУД; порівняльний аналіз архітектур сучасних безконтактних систем контролю доступу; постановка завдань на кваліфікаційну роботу) Розділ 2 Обґрунтування вибору засобів та методів реалізації (обґрунтування вибору базової апаратної платформи мультибіометричного термінала; вибір периферійного обладнання, органів керування та давачів; вибір програмного забезпечення для керування та моніторингу; методика інтеграції та способи взаємодії компонентів системи за архітектурою PUSH-сервера; обґрунтування інженерних методів монтажу). Розділ 3 Практична реалізація (архітектурне структурно-функціональна схема навчально-лабораторної установки; проєктування кабельної інфраструктури, схем комутації силових та сигнальних ланцюгів за принципом Fail-Safe програмно-апаратна інтеграція та конфігурування серверної платформи ZKBio Access IVS експериментальне дослідження точності розпізнавання облич Visible Light та тестування алгоритмів захисту від біометричних підробок Liveness Detection) Загальні висновки та рекомендації. Список використаних джерел. Додатки.*
5. Перелік графічного (ілюстративного) матеріалу: *Презентація на 15 слайдах*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Розділ 1 Аналітичний огляд стану предметної області	*Пугач С. О.*		
Розділ 2 Обґрунтування вибору засобів та методів реалізації	*Пугач С. О.*		
Розділ 3 Практична реалізація	*Пугач С. О.*		
Загальні висновки та рекомендації	*Пугач С. О.*		
Нормоконтроль	*Кайдик О. Л.*		
Гарант ОП	*Терлецький Т. В.*		
Показник запозичень тексту			
Академічна доброчесність	*Кайдик О. Л.*		

7. Дата видачі завдання: «16» грудня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи бакалавра	Строк виконання етапів роботи	Примітка
1.	Обґрунтування теми	До 12.12.2025 р.	
2.	Огляд літератури із досліджуваної проблеми	До 12.12.2025 р.	
3.	Розділ 1 Аналітичний огляд стану предметної області	До 28.02.2026 р.	
4.	Розділ 2 Обґрунтування вибору засобів та методів реалізації	До 31.03.2026 р.	
5	Розділ 3 Практична реалізація	До 30.04.2026 р.	
6.	Загальні висновки та рекомендації	До 16.05.2026 р.	
7.	Формування списку використаних джерел	До 20.05.2026 р.	
8.	Формування додатків.	До 20.05.2026 р.	
9.	Формування презентації за темою кваліфікаційної роботи	До 20.05.2026 р.	
10.	Нормоконтроль	До 21.05.2026 р.	
11.	Інструментальна перевірка на академічний плагіат	До 22.05.2026 р.	
12.	Представлення кваліфікаційної роботи бакалавра до захисту	До 02.06.2026 р.	

Здобувач вищої освіти _____ (Трофимчук І. О.)
(підпис)

Керівник кваліфікаційної роботи _____ (Пугач С. О.)
(підпис

АНОТАЦІЯ

Трофимчук І. О. Навчально-лабораторна установка системи контролю та управління доступом на базі BioTime ZKBT-Dev-P10. Рукопис.

Кваліфікаційна робота бакалавра ОП «Інформаційні системи та технології охорони і безпеки». Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота бакалавра складається зі вступу, трьох розділів, загальних висновків та рекомендацій, списку використаних джерел та додатків.

У пояснювальній записці кваліфікаційної роботи акцентовано увагу на аналітичному огляді стану предметної області, нормативно-правовій базі та міжнародних стандартах у сфері біометричної ідентифікації й систем безпеки, а також проведено порівняльний аналіз архітектур сучасних безконтактних систем контролю та управління доступом. Обґрунтовано вибір базової апаратної платформи мультибіометричного термінала, виконавчих механізмів, периферійного обладнання, датчиків та спеціалізованого програмного забезпечення для централізованого керування й моніторингу подій.

Описано методику комплексної інтеграції, способи мережевої взаємодії компонентів системи, а також інженерні методи їх монтажу, просторового позиціонування та налаштування. У практичній частині представлено архітектурне рішення та структурну схему лабораторного стенда, спроєктовано кабельну інфраструктуру, схеми електричної комутації силових та сигнальних ланцюгів із дотриманням принципів Fail-Safe, а також топологію підключення пристроїв. Особливу увагу приділено процесам програмно-апаратної інтеграції обладнання з серверною платформою, дослідженню ефективності розпізнавання облич у видимому спектрі світла та тестуванню алгоритмів захисту від біометричних підробок.

Ключові слова: система контролю та управління доступом (СКУД), мультибіометричний термінал, розпізнавання облич, Visible Light, Liveness Detection, ZKBio Access IVS, апаратна реалізація, лабораторний стенд, комутація, Fail-Safe, кібербезпека.

ANNOTATION

Trofymchuk I. Training and laboratory physical access control system installation based on BioTime ZKBT-Dev-P10. Manuscript.

Bachelor's qualification work EP «Security and safety information system and technologies». Lutsk National Technical University. Lutsk, 2026.

This bachelor's thesis comprises an introduction, three sections, general conclusions and recommendations, a list of references, and appendices.

The explanatory note of the qualification thesis emphasizes an analytical review of the subject area status, the regulatory framework, and international standards in the field of biometric identification and security systems, as well as a comparative analysis of modern contactless access control and management system architectures. The choice of the baseline hardware platform a multi-biometric terminal, actuators, peripheral equipment, sensors, and specialized software for centralized management and event monitoring has been substantiated.

The methodology of comprehensive integration, methods of network interaction between system components, as well as engineering methods for their mounting, spatial positioning, and configuration are described. The practical part presents the architectural solution and the block diagram of the laboratory stand, the design of the cable infrastructure, electrical commutation schemes for power and signal circuits in compliance with Fail-Safe principles, and the device connection topology. Particular attention is paid to the processes of hardware and software integration of the equipment with the server platform, the investigation of face recognition efficiency in the visible light spectrum, and the testing of biometric presentation attack detection (liveness detection) algorithms.

Keywords: access control and management system (ACMS), multi-biometric terminal, face recognition, Visible Light, Liveness Detection, ZKBio Access IVS, hardware implementation, laboratory stand, commutation, Fail-Safe, cybersecurity.

ЗМІСТ

ВСТУП

Еволюція інженерних рішень у сфері безпеки зумовила поступову відмову від класичних засобів контактної автентифікації, таких як механічні замки чи RFID-картки. Сучасний вектор розвитку СКУД спрямований на інтеграцію інтелектуальних безконтактних технологій. Особливе місце серед них посідають методи розпізнавання обличчя у видимому спектрі світла, які працюють у межах єдиних клієнт-серверних мереж та забезпечують миттєву ідентифікацію користувачів.

Важливою перевагою новітнього біометричного обладнання є застосування вбудованих інструментів перевірки наявності живого об’єкта. Це повністю нівелює ризики обходу системи за допомогою роздрукованих фотокарток чи цифрових зображень із екранів смартфонів. Водночас розгортання та адміністрування таких комплексів вимагає глибоких практичних знань від випускників інженерних спеціальностей. Модернізація навчального процесу шляхом створення автентичних випробувальних стендів на базі промислових контролерів дозволяє детально моделювати реальні сценарії захисту об’єктів і готувати затребуваних фахівців.

Об’єктом дослідження є процеси програмно-апаратної інтеграції, налаштування та експлуатаційного тестування розподілених систем контролю та управління доступом.

Предмет дослідження – архітектура, мережева взаємодія, алгоритми розпізнавання та схеми безперебійного живлення лабораторного стенда СКУД на основі терміналу BioTime ZKBT-Dev-P10.

Мета кваліфікаційної роботи – проєктування, технічне розгортання та експериментальне дослідження параметрів навчально-лабораторної установки СКУД на базі термінала BioTime ZKBT-Dev-P10 для вдосконалення матеріально-технічної бази Луцького національного технічного університету (ЛНТУ) та підвищення якості практичної підготовки студентів.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Концептуальні засади проектування СКУД

Проектування сучасних систем контролю та управління доступом являє собою складний, багатоетапний інженерний процес, спрямований на створення захищеного периметра та внутрішнього простору об’єкта від широкого спектра загроз штучного й техногенного характеру [1]. З точки зору системного аналізу, такі комплекси є невіддільною складовою інтегрованого контуру безпеки будь-якої установи, оскільки вони безпосередньо взаємодіють із підсистемами охоронно-пожежної сигналізації, відеоспостереження, оповіщення та загальною інформаційною інфраструктурою підприємства [2]. Головною концептуальною парадигмою під час розробки архітектури контролю доступу є створення ешелонованого захисту, що передбачає послідовне формування зон безпеки з поступовим посиленням суворості автентифікації суб’єктів на шляху від зовнішнього периметра до критично важливих точок, як-от серверні кімнати, сховища даних або науково-дослідні лабораторії.

Важливим аспектом проектування логічної структури системи є реалізація принципу мінімальних привілеїв, згідно з яким кожному користувачу надається лише той обсяг прав, що необхідний для виконання його безпосередніх функцій, обмежений як просторово, так і в часовому вимірі. При цьому сучасні інженерні стандарти вимагають високого рівня автономності периферійних вузлів. Це означає, що локальні контролери точок проходу повинні зберігати повну працездатність і логіку прийняття рішень навіть у випадку тимчасової втрати зв’язку із центральним сервером або головною базою даних. Окрему увагу при формуванні концепції безпеки приділяють вимогам цивільного захисту: при виникненні будь-яких надзвичайних ситуацій, зокрема при спрацюванні пожежної сигналізації, система повинна автоматично пріоритезувати функцію збереження життя людей, миттєво знеструмлюючи всі виконавчі механізми на шляхах потенційної евакуації [3].

Логіка ухвалення рішень у сучасних системах безпеки спирається на розробку динамічних матриць доступу, які зіставляють унікальні ідентифікаційні ознаки суб’єктів із просторово-часовими параметрами самого об’єкта захисту. Математично цей процес описується функцією предикату, що аналізує вектор запиту, який складається з мноми користувачів, точок проходу та точного часового штампу [4]. Результатом обчислення функції стає бінарний сигнал, який або дозволяє формування керуючого імпульсу для розблокування дверей, або фіксує спробу несанкціонованого проходу із занесенням події до журналу тривог. Класичні підходи, які тривалий час домінували на ринку та базувалися на механічному кодуванні чи радіочастотній ідентифікації, сьогодні демонструють критичні концептуальні недоліки. Основним серед них є відносна легкість відчуження фізичного носія від його законного власника, адже картку чи брелок можна передати іншій особі, викрасти або скопіювати за допомогою дублікаторів, що змушує інженерів переходити до впровадження біометричних ознак людини, які неможливо відокремити від особистості.

1.2 Аналіз сучасних методів біометричної автентифікації

Біометрична автентифікація є технологічним процесом перевірки автентичності суб’єкта шляхом порівняння його пред’явлених фізіологічних характеристик із заздалегідь зареєстрованими цифровими еталонами, що зберігаються в реляційній базі даних [5]. Застосування таких методів дозволяє повністю нівелювати ризики, пов’язані з людським фактором, забезпечуючи високу достовірність ідентифікації. У сучасній інженерній практиці проектування засобів безпеки тривалий час базовим рішенням виступала дактилоскопія, тобто розпізнавання за відбитками пальців. Цей метод базується на аналізі унікального папілярного візерунка шкіри та взаємного розташування особливих точок, відомих як мінуції. Незважаючи на відносно низьку апаратну вартість сенсорів та швидкість обробки даних, дактилоскопія має суттєві

експлуатаційні обмеження, оскільки порізи, забруднення чи вологість шкіри різко підвищують ймовірність відмови в допуску.

На цьому тлі найбільш прогресивним та динамічним напрямом є безконтактне розпізнавання обличчя у видимому спектрі світла, відоме як технологія Visible Light [6]. Сучасні алгоритми цього класу базуються на згорткових нейронних мережах і методах глибокого навчання, що дозволяє здійснювати автентифікацію користувачів на ходу, на відстані до трьох метрів та під великими кутами нахилу голови. Процес функціонування таких інтелектуальних систем складається з кількох послідовних етапів, де спочатку виконується геометрична детекція обличчя в кадрі, після чого за допомогою реперних антропометричних точок відбувається його математичне вирівнювання до еталонної фронтальної площини. Далі нейромережа трансформує графічні дані у компактний цифровий дескриптор, що описує глибокі геометро-текстурні параметри зовнішності, які залишаються стабільними навіть при зміні зачіски, появі бороди чи наявності окулярів. Важливою інженерною перевагою технології Visible Light є наявність вбудованого захисту від атак підробки за допомогою модулів Liveness Detection. Спеціальні здвоєні оптичні сенсори, які поєднують звичайну та інфрачервону камери, аналізують тривимірний об’єм об’єкта, текстуру живої шкіри та природні мікрорухи очей, що дозволяє миттєво відсікати спроби обходу системи за допомогою роздрукованих паперових фотографій високої роздільної здатності чи відеозаписів із екранів мобільних телефонів.

Узагальнену логічну послідовність етапів ідентифікації користувача за допомогою нейромережевих алгоритмів у видимому спектрі світла представлено на рисунку 1.1.

Для об’єктивного порівняння та технічного обґрунтування вибору технології ідентифікації, у таблиці 1.1 наведено зіставлення ключових параметрів дактилоскопічного методу та технології розпізнавання облич Visible Light.

Аналіз даних в таблиці 1.1 демонструє беззаперечні переваги впровадження розпізнавання Visible Light для об’єктів із підвищеними вимогами

до швидкодії та безпеки, оскільки цей метод мінімізує критичні помилки FAR та FRR, забезпечуючи при цьому максимальну захищеність від саботажу.

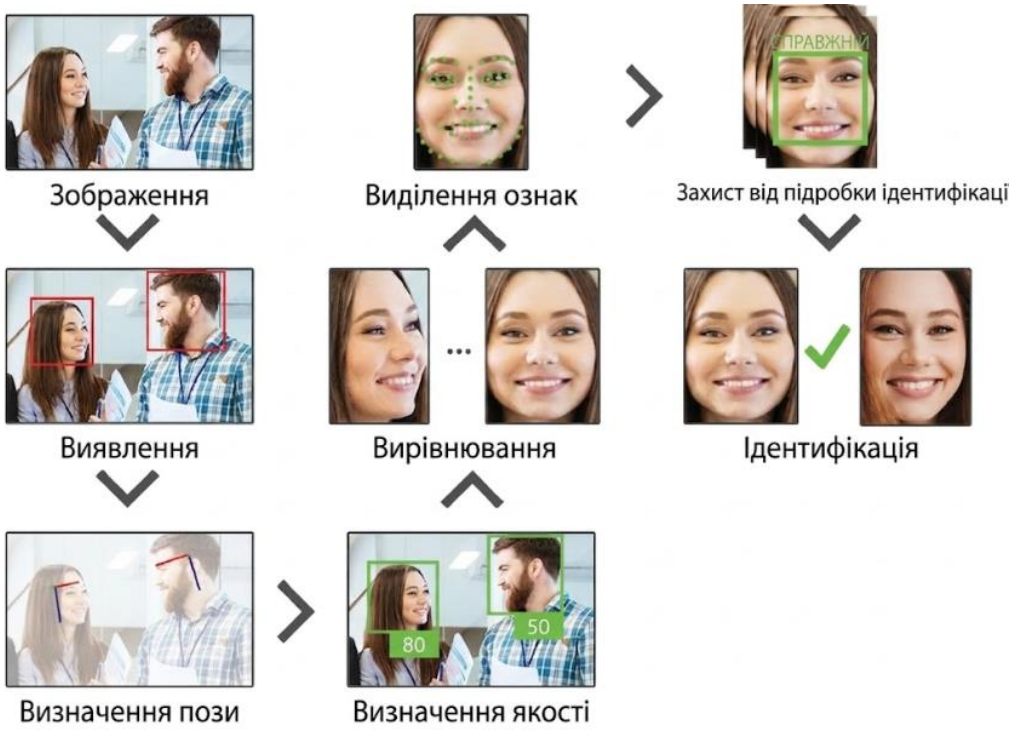

Рисунок 1.2 – Функціональна схема обробки біометричних даних терміналом BioTime

Таблиця 1.1 – Порівняльний аналіз ключових біометричних методів автентифікації

Техніко-експлуатаційний параметр	Метод сканування відбитків пальців	Технологія розпізнавання облич Visible Light
Коефіцієнт помилкового допуску (FAR)	0,001-0,01%	менше 0,0001%
Коефіцієнт помилкової відмови (FRR)	0,1-1,0%	менше 0,01%
Спосіб взаємодії зі зчитувачем	Виключно контактний	Повністю безконтактний
Максимальна відстань сканування	0 см (безпосередній дотик)	від 0,5 до 3,0 метрів
Чутливість до стану середовища	Висока (волога, бруд, температура)	Низька (завдяки вбудованому WDR та ІЧ)
Стійкість до атак підробки	Середня (можливі силіконові муляжі)	Максимальна (апаратний Liveness Detection)
Вплив індивідуальних факторів людини	Порізи, старіння шкіри, стирання візерунка	Зміна зачіски чи макіяжу не впливають

1.3 Апаратна інфраструктура систем контролю доступу

Сучасна апаратна інфраструктура СКУД будується за багаторівневою ієрархічною структурою, яка об’єднує периферійні пристрої зчитування інформації, виконавчі блокувальні механізми, комутаційне обладнання та сервери обробки даних [7]. Для глибокого аналізу побудови технічних засобів охорони [8] у межах цього проєкту розглядається реальний об’єкт – багатомодульний навчально-лабораторний стенд ЛНТУ (рис. 1.2).

Рисунок 1.1 – Структурно-функціональна схема апаратної інфраструктури розподіленого лабораторного стенда

Зазначена установка являє собою повнофункціональну масштабну інженерну модель розподіленої системи безпеки підприємства, апаратна структура якої містить такі елементи:

– вісім незалежних функціональних секцій – кожна з них імітує окрему точку проходу з унікальним компонентним складом обладнання, що дозволяє

всебічно досліджувати різноманітні архітектурні контури, протоколи обміну даних та сценарії захисту об'єктів;

– центральний комутаційно-енергетичний вузол – виступає геометричним та енергетичним ядром лабораторного стенда, розміщеним на загальній монтажній основі;

– герметичний захисний бокс – призначений для безпечного внутрішнього монтажу та інтеграції елементів живлення;

– імпульсне джерело безперебійного живлення – оснащене автоматичним модулем заряджання для підтримки стабільної напруги в системі;

– резервна свинцево-кислотна акумуляторна батарея – має ємність 7 А·год та забезпечує тривалу автономну роботу системи при знеструмленні будівлі;

– багатопортовий мережевий контролер (комутатор) – змонтований поруч із блоком живлення і забезпечує формування ізольованої локальної мережі стенда;

– центральний монітор – встановлений над основним обладнанням для візуалізації поточних подій та відображення графічного інтерфейсу адміністратора в режимі реального часу.

Основну інноваційну функцію захисту на стенді виконує другий модуль, на якому встановлено інтелектуальний біометричний термінал серії BioTime, зокрема модель ZKBT-Dev-P10. Цей термінал оснащений кольоровим сенсорним екранним модулем, здвоєною оптичною системою розпізнавання Visible Light та вбудованими зчитувачами відбитків пальців і безконтактних смарт-карт. Підключення термінала до загальної локальної мережі комплексу здійснюється за допомогою кабелю крученої пари UTP Cat 5e через стандартизований інтерфейс RJ-45.

Інші периферійні модулі установки призначені для імітації альтернативних варіантів точок проходу та виконавчих елементів, що часто зустрічаються на реальних об’єктах цивільного та промислового призначення. Так, п’ятий модуль обладнано цифровою кнопковою кодовою панеллю, а секції по боках стенда

містять автономні карткові зчитувачі та безконтактні оптичні кнопки виходу зі світлодіодною індикацією поточного стану реле.

Як виконавчі механізми на стенді використовуються діючі зразки технічних засобів охорони, серед яких представлені накладні електромагнітні замки з високою силою утримання магнітопроводу та врізні електромеханічні замки із соленоїдними приводами засувок. Таке різноманіття запірних пристроїв дозволяє під час лабораторних досліджень практично відпрацьовувати логіку комутації як нормально відкритих (NO), так і нормально закритих (NC) контактів керуючих реле контролера.

Для розширення дослідницьких можливостей і низькорівневого аналізу сигналів інфраструктура стенда передбачає інтегрований інтерфейсний модуль крос-комутації. Через виділені релейні блоки та сигнальні лінії цей модуль забезпечує гнучку взаємодію з виконавчими механізмами, дозволяючи в реальному часі емулювати роботу датчиків проходу, герконів, сповіщувачів систем безпеки або інтегрувати стенд із суміжними підсистемами охоронно-пожежної сигналізації.

1.4 Аналіз програмного забезпечення та обґрунтування його вибору

Ефективне управління розподіленою апаратною інфраструктурою лабораторного стенда та координація взаємодії між усіма периферійними модулями потребує застосування сучасного серверного програмного забезпечення, що здатне надійно обробляти великі масиви інформації та надавати гнучкі інструменти адміністрування. У межах теоретичного обґрунтування проєкту було введено порівняльний аналіз поширених на ринку програмних комплексів для систем безпеки, за результатами якого для практичної реалізації було обрано веб-орієнтовану платформу ZKBio Access IVS [9], яка базується на передовій архітектурі клієнт-сервер із доступом через стандартний веб-браузер, що дозволяє керувати контуром безпеки з будь-якого комп’ютера локальної мережі кафедри без встановлення додаткового софту.

Результати проведеного системно-компаративного аналізу програмних рішень, що розглядалися як альтернативні варіанти ядра системи, зведено та структуровано у таблиці 1.2.

Таблиця 1.2 – Комплексний порівняльний аналіз програмного забезпечення для СКУД

Функціональний критерій порівняння	Альтернативна платформа А	Альтернативна платформа Б	Веб-платформа ZKBio Access IVS
Тип системної архітектури	Настільний Thick Client	Клієнт-серверна модель	Веб-орієнтована (Web-based)
Репозиторій збереження (СКБД)	SQLite / MS Access	MySQL	Реляційна СКБД PostgreSQL
Базовий мережевий протокол	Циклічне опитування (Pull)	Синхронний HTTP-запит	Асинхронний подійний PUSH-SDK
Інтеграція з Visible Light	Через зовнішні плагіни	Обмежена (лише 2D-фото)	Повна нативна інтеграція пристрою
Управління часовими зонами	Жорсткі глобальні профілі	Лінійні графіки доступу	Динамічна матриця розкладів
Тип ліцензування системи	Платна комерційна версія	Щорічна SaaS-підписка	Безкоштовна базова ліцензія

Аналіз даних в таблиці 1.2 обґрунтовує вибір вебплатформи ZKBio Access IVS. Головним інженерним аргументом є нативна підтримка термінала ZKBT-Dev-P10 та використання асинхронного протоколу PUSH-SDK. На відміну від циклічного опитування пристроїв, модель Push миттєво ініціює TCP-з’єднання та передає дані й кадр фотофіксації безпосередньо в момент верифікації, мінімізуючи мережевий трафік. Інтеграція з СКБД PostgreSQL забезпечує стабільність збереження журналів подій та біометричних шаблонів, а вбудований аналітичний модуль автоматизує облік робочого часу персоналу [10]. Наявність безкоштовної базової ліцензії робить цей комплекс оптимальним для розгортання в університетській лабораторії.

1.5 Постановка завдань на кваліфікаційну роботу бакалавра

На основі проведеного аналітичного огляду стану предметної області, детального порівняльного аналізу сучасних методів біометричної автентифікації, дослідження інженерної структури наданого багатомодульного лабораторного

стенда та обґрунтування вибору програмно-серверної платформи, сформувано такі конкретні науково-технічні завдання на проектування:

1) розробити повну технічну документацію та принципову електричну схему кабельних ліній та комутаційних з’єднань апаратних елементів стенда, забезпечивши правильне об’єднання біометричного терміналу ZKBT-Dev-P10, кнопок виходу та релейних приводів виконавчих замків;

2) виконати інженерні розрахунки підсистеми автономного електроживлення установки, визначивши сумарні струми споживання обладнання в номінальному та піковому режимах, а також підібравши оптимальну потужність імпульсного ДЖБ та ємність резервної АКБ;

3) провести інсталяцію та конфігурацію серверного програмного забезпечення ZKBio Access IVS на базі виділеної робочої станції, ініціалізувати базу даних у СКБД PostgreSQL та виконати оптимізацію параметрів системного кешування для прискорення транзакцій;

4) реалізувати логічну структуру матриці прав доступу, що включає внесення облікових записів і реєстрацію біометричних шаблонів користувачів, а також розробку часових розкладів доступу до точок проходу для різних категорій персоналу кафедри;

5) розробити комплексну методику тестування біометричного розпізнавання Visible Light та провести серію експериментальних випробувань системи за різних умов зовнішнього середовища з метою розрахунку показників FAR/FRR та оцінки стійкості до атак спуфінгу.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Техніко-функціональна характеристика пристрою BioTime ZKBT-Dev-P10

Вибір мультибіометричного термінала ZKBT-Dev-P10 як базового елемента системи обумовлений його архітектурою периферійних обчислень, що дозволяє виконувати детекцію та розпізнавання об’єктів безпосередньо на точці проходу [11].

Ключові функціональні переваги обраної моделі:

– ідентифікація користувачів у русі завдяки технології Visible Light, що не потребує повної зупинки перед сенсором;

– робоча дистанція розпізнавання геометричного шаблону обличчя в діапазоні від 0,5 до 3,0 метрів;

– висока толерантність до просторових відхилень (нахили, повороти голови) у межах до 30 градусів у будь-якій площині;

– апаратна підтримка алгоритмів глибокого навчання за допомогою інтегрованого нейропроцесора NPU.

Технічні параметри апаратного комплексу:

– обчислювальна платформа: чотириядерний процесор ARM Cortex-A53 (1,5 ГГц) під управлінням embedded ядра Linux;

– пам’ять: оперативна 1 Гб (DDR3) та енергонезалежна флеш-пам’ять 8 Гб (eMMC) для локального збереження баз даних;

– гранична ємність сховища: до 10000 еталонів облич та аналогічна кількість відбитків пальців і RFID-карт;

– автономний журнал подій: фіксація до 100000 транзакцій без деградації швидкодії системи

Характеристики оптичної підсистеми та безпеки:

– бінокулярна камера (2 Мп): поєднання RGB-сенсора та ІЧ-сенсора для реалізації захисту Liveness Detection;

– дворівнева перевірка на «живість»: аналіз тривимірної глибини сцени та текстури шкіри для відсікання фото- та відео-підробок;

– розширений динамічний діапазон (WDR до 120 дБ): забезпечення стабільної роботи при зустрічному засвічуванні або в повній темряві;

– швидкість верифікації в режимі 1:N: менше 0,3 секунди на один запит

Для детального інженерного аналізу та систематизації експлуатаційних спроможностей обраного периферійного пристрою, у таблиці 2.1 наведено повну специфікацію його апаратно-програмних та технічних параметрів.

Таблиця 2.1 – Техніко-функціональні параметри термінала BioTime ZKBT-Dev-P10

Категорія параметрів системи	Найменування технічної характеристики	Значення параметрів пристрою
Обчислювальна підсистема	Архітектура та тип процесора	4-ядерний ARM Cortex-A53, 1,5 ГГц
	Керуюче операційне середовище	Оптимізоване embedded ядро Linux
Репозиторій пам’яті	Об’єм оперативної пам’яті (RAM)	1 Гб типу DDR3
	Об’єм енергонезалежної пам’яті	8 Гб типу eMMC Flash
Гранична ємність сховища	Максимальна кількість шаблонів облич	10000 еталонів
	Кількість відбитків пальців (SilkID)	10000 шаблонів
	Кількість безконтактних RFID-карт	10000 ідентифікаторів
	Ємність локального журналу подій	100000 транзакцій
Метрологічні характеристики	Швидкість розпізнавання в режимі 1:N	менше 0,3 секунди
	Робоча дистанція зчитування обличчя	від 0.5 до 3.0 метрів
	Коефіцієнт помилкового допуску (FAR)	менше 0,0001%
	Коефіцієнт помилкової відмови (FRR)	менше 0,01%
Фізичні інтерфейси	Мережевий комунікаційний порт	1 × RJ-45
	Сигнальні периферійні інтерфейси	Wiegand Input / Output, RS-485
	Виконавчий комутаційний вихід	1 × Реле замка
Електричні параметри	Номінальна напруга живлення	12 В постійного струму (DC)
	Максимальний струм споживання	500 мА

Централізоване управління розгорнутою апаратною інфраструктурою лабораторного стенда та координація інформаційних потоків здійснюється за допомогою серверного програмного забезпечення ZKBio Access IVS. Ця програмна платформа побудована за модульним принципом на основі трирівневої веб-орієнтованої архітектури, де взаємодія адміністратора або

диспетчера безпеки з системою відбувається віддалено через стандартний веб-браузер за захищеним протоколом HTTPS.

Як базовий репозиторій для збереження глобальної конфігурації СКУД, персональних карток користувачів, біометричних шаблонів та довгострокових журналів подій платформа використовує реляційну систему керування базами даних PostgreSQL [12]. Дана СКБД обрана завдяки її повній відповідності критеріям надійності транзакцій ACID, високій ефективності обробки складних структурованих запитів та наявності механізмів оптимізації індексів для бінарних об’єктів великого обсягу, що виключає ризики пошкодження або втрати інформації при тривалій безперервній експлуатації комплексу.

2.2 Формування принципової моделі взаємодії елементів

Ефективність, живучість та завадостійкість розподіленої інфокомунікаційної системи контролю та управління доступом у межах розроблюваної навчально-лабораторної установки безпосередньо залежать від раціональної організації інформаційних, логічних та фізичних зв’язків між її компонентами. Архітектурна побудова взаємодії елементів системи реалізована за класичною дворівневою ієрархічною моделлю, яка чітко розмежовує функції централізованого довгострокового адміністрування та оперативного периферійного ухвалення рішень реального часу:

– верхній рівень локалізований на серверній робочій станції, де функціонує програмний комплекс ZKBio Access IVS, інтегрований із реляційним репозиторієм даних СКБД PostgreSQL;

– нижній рівень розгорнутий безпосередньо на фізичній точці проходу лабораторного стенда та концентрований навколо інтелектуального мультибіометричного термінала ZKBT-Dev-P10, який взаємодіє з виконавчими механізмами й датчиками.

Логічна модель міжрівневого мережевого обміну даними між сервером додатків та периферійним біометричним контролером базується на стеку

протоколів TCP/IP з використанням спеціалізованого асинхронного клієнт-серверного механізму передачі інформації за фірмовою технологією PUSH-SDK [9]. Ключова інженерна особливість даної технології полягає в тому, що ініціатором і підтримувачем постійного мережевого з'єднання (Persistent Connection) завжди виступає периферійний термінал ZKBT-Dev-P10, а не центральний сервер. Після подачі напруги живлення та завершення циклу ініціалізації внутрішнього ядра Linux, комунікаційний демон термінала виконує запит на встановлення TCP-сесії у напрямку статичної IP-адреси та визначеного системного порту сервера СКУД. Після успішного рукостискання та авторизації пристрою, канал зв'язку переходить у режим безперервного моніторингу, в якому термінал із жорстко заданою періодичністю відправляє короткі пакети опитування зв'язку (Heartbeat), що дозволяє серверу оперативно діагностувати стан активності точки проходу та синхронізувати системний час.

Транзакційна взаємодія під час реєстрації подій проходу в межах PUSH-архітектури мінімізує навантаження на пропускну здатність локальної обчислювальної мережі кафедри та гарантує миттєву доставку критично важливих логів. У момент, коли користувач підходить до точки проходу і його біометричний дескриптор успішно розпізнається нейромережевим модулем Visible Light, термінал переходить у режим генерації події. Пристрій миттєво формує структурований інформаційний пакет, що містить унікальний числовий ідентифікатор співробітника або студента, точний часовий штамп події (Unix Timestamp) з точністю до мілісекунди, код напрямку проходу, статус успішності автентифікації, а також бінарний масив графічного кадру фотофіксації особи. Цей пакет асинхронно надсилається на сервер додатків, який приймає повідомлення, виконує аналіз логіки відповідності поточним правилам доступу, ініціює SQL-транзакцію для запису події в таблиці бази даних PostgreSQL та повертає терміналу прапорець успішного отримання даних, після чого запис видаляється з поточної оперативної черги пристрою.

Взаємодія сервера додатків із реляційною системою керування базами даних PostgreSQL організована за допомогою оптимізованого пулу з'єднань, що

забезпечує високу швидкість обробки множинних паралельних запитів від декількох точок проходу без ризику виникнення взаємних блокувань таблиць. При отриманні пакета події від термінала, серверний модуль ZKBio Access IVS здійснює синтаксичний розбір даних та викликає відповідні збережені процедури в СКБД. База даних виконує перевірку цілісності, записує подію до довгострокового журналу транзакцій, автоматично оновлює індекси для швидкого пошуку і запускає внутрішні тригери, які відповідають за миттєвий перерахунок параметрів модулів обліку робочого часу, формування аналітичних звітів та відображення картки фотоверифікації користувача на моніторі оператора безпеки в режимі реального часу.

Фізичний та електричний рівень взаємодії елементів у межах точки проходу лабораторної установки реалізований шляхом прямої комутації слабострумових сигнальних ліній та силових ланцюгів живлення безпосередньо через інтерфейсну колодку термінала ZKBT-Dev-P10. Головним виконавчим елементом керування виступає інтегроване в термінал електромагнітне реле з групою перекидних сухих контактів стандарту Form-C, що включає в себе нормально закритий (NC), нормально відкритий (NO) та загальний (COM) виводи. Оскільки накладений електромагнітний замок лабораторного стенда функціонує за принципом Fail-Safe задля утримання дверей у заблокованому стані потрібна постійна присутність напруги, його силова лінія позитивного потенціалу 12 В постійного струму від блоку безперебійного живлення підключається в розрив через пару контактів NC та COM термінала. Коли пристрій ухвалює локальне рішення про легітимність проходу, керуючий сигнал мікроконтролера подає напругу на обмотку реле, контакти переключаються, ланцюг живлення замка розривається, і магнітне поле зникає, звільняючи двері для фізичного відкриття суб’єктом.

Для забезпечення повної інформативності контуру безпеки та можливості ручного керування точкою проходу, загальна модель взаємодії включає підсистему зчитування зворотних сигналів від периферійних пристроїв:

– безконтактна оптична кнопка запиту на вихід підключається до спеціалізованого цифрового входу термінала за схемою контролю сухого контакту. При піднесенні руки користувача вхідна сигнальна лінія замикається на загальну шину заземлення (GND). Логічний модуль фіксує падіння напруги на порту та ініціює стандартний часовий цикл спрацювання реле замка без біометричної ідентифікації;

– магнітоконтактний датчик положення дверей (геркон) безперервно транслює на окремий цифровий вхід термінала інформацію про реальний фізичний стан дверного полотна. Це дозволяє внутрішньому програмному забезпеченню контролювати факт здійснення проходу, а також детектувати тривожні стани наприклад, несанкціонований силовий злом або утримання дверей відкритими понад ліміт, з активацією зумера та надсиланням PUSH-пакета на сервер.

2.3 Обґрунтування та підбір комплектувальних виробів

Практична реалізація фізичного контуру навчально-лабораторної установки системи контролю та управління доступом потребує ретельного інженерного підбору та обґрунтування вибору периферійних пристроїв, виконавчих механізмів та кабельної інфраструктури. Усі елементи системи повинні мати високу експлуатаційну надійність, повну апаратну сумісність за рівнями логічних та силових сигналів, а також відповідати чинним стандартам безпеки.

З метою побудови відмовостійкої архітектури та забезпечення належних експлуатаційних параметрів, підбір ключових елементів стенда виконано за такими інженерними критеріями:

– накладний електромагнітний замок промислового типу із зусиллям утримання на розрив не менше 280 кілограмів обрано як головний виконавчий елемент для фізичного блокування точки проходу таких як дверей. Застосування запірного механізму класу Fail-Safe є базовою вимогою нормативних документів із пожежні безпеки об’єктів цивільного та навчального призначення. На відміну

від пристроїв класу Fail-Secure, електромагнітний замок миттєво відкривається при повному зникненні напруги в силовому ланцюзі, що гарантує безперешкодну та безпечну евакуацію студентів і персоналу з приміщення лабораторії під час надзвичайних ситуацій;

– безконтактна оптична кнопка виходу інфрачервоного типу передбачена у складі комплекту для забезпечення можливості санкціонованого виходу з приміщення без необхідності проходження біометричної ідентифікації. На відміну від механічних кнопок, схильних до зносу контактних груп, оптичний сенсор функціонує за рахунок детекції відбитого сигналу в оптичному спектрі й забезпечує ресурс у понад один мільйон комутацій. Кнопка оснащена двоколірним світлодіодним індикатором стану, де зелений колір при розблокованому замку та синій у режимі очікування, що підвищує ергономічність лабораторної установки;

– екранована кручена пара типу FTP категорії Cat 5e з мідними провідниками перерізом 0,51 мм обґрунтовано застосовується для організації магістрального інформаційного каналу між мережевим інтерфейсом RJ-45 термінала ZKBT-Dev-P10 та комутатором локальної обчислювальної мережі. Наявність загального захисного екрана з алюмінієвої фольги дозволяє повністю нівелювати високочастотні завади від іншого навчального та лабораторного обладнання, розташованого в аудиторії;

– гнучкий з’єднувальний шнур марки ШВВП із двома мідними багатодротовими жилами перерізом 0,75 квадратних міліметрів підібрано для прокладання низьковольтних силових ланцюгів живлення термінала та електромагнітного замка від центрального джерела безперебійного живлення. Такий переріз провідника є оптимальним, оскільки він мінімізує падіння напруги на довжині кабельної лінії при проходженні пікових струмів споживання, запобігаючи збоям в роботі периферійного обчислювального ядра.

Важливим етапом проектування апаратної частини СКУД є математичний розрахунок енергетичного балансу системи та параметрів підсистеми гарантованого живлення. Джерело безперебійного живлення повинно

забезпечувати стабільну номінальну напругу 12 В постійного струму та володіти достатньою потужністю для покриття пікових навантажень усіх підключених споживачів. Сумарний максимальний струм споживання периферійного контуру установки (I_{Σ}) визначається як адитивна сума номінальних струмів кожного окремого елемента за формулою (2.1):

$$I_{\Sigma} = I_{term} + I_{lock} + I_{button} + I_{aux}, \quad (2.1)$$

де: I_{term} – піковий струм споживання мультибіометричного термінала;

I_{lock} – струм утримання обмотки електромагнітного замка;

I_{button} – струм функціонування інфрачервоного датчика та світлодіодної індикації кнопки виходу;

I_{aux} – резерв підсистеми для підключення додаткових датчиків стану дверей.

Підставивши номінальні значення у вихідне рівняння, отримаємо сумарне значення струму:

$$I_{\Sigma} = 0{,}5 + 0{,}4 + 0{,}05 + 0{,}05 = 1 \text{ А}.$$

Відповідно до правил проектування систем безпеки та автоматики, номінальний вихідний струм джерела живлення (I_{psu}) повинен розраховуватися з урахуванням тридцятивідсоткового інженерного запасу для запобігання перегріву та передчасного виходу з ладу силових електронних компонентів при тривалій експлуатації :

$$I_{psu} = I_{\Sigma} \times k_{res} = 1 \times 1{,}3 = 1{,}3 \text{ А}.$$

Виходячи з отриманого розрахункового значення, для інтеграції у лабораторну установку підібрано промисловий імпульсний блок безперебійного живлення в металевому захисному боксі з номінальним вихідним струмом 3 А, що повністю перекриває потреби системи і забезпечує високий коефіцієнт надійності.

Наступним кроком є визначення необхідної електричної ємності резервної акумуляторної батареї, яка здатна підтримувати повнофункціональну автономну

роботу всієї точки проходу протягом нормативних 3 годин у разі повного аварійного вимкнення первинної мережі змінного струму 220 В. Математичний розрахунок ємності виконується за формулою, що враховує коефіцієнт корисної дії перетворювача напруги та глибину розряду батареї (2.2) [13]:

$$Q_{akb} = (Ie \times t) / (\eta \times kd), \quad (2.2)$$

де: η – коефіцієнт корисної дії ББЖ, $\eta = 0,85$;

k_d – коефіцієнт максимальної глибини розряду акумулятора, $k_d = 0,80$.

Проводячи чисельне обчислення, отримаємо:

$$Q_{akb} = (1 \times 3) / (0,85 \times 0,80) \approx 4,41 \text{ А} \times \text{год}.$$

Аналізуючи номенклатурний ряд герметизованих свинцево-кислотних акумуляторів, виготовлених за технологією AGM, для встановлення в бокс джерела живлення обрано стандартну акумуляторну батарею номінальною ємністю 7 А·год із робочою напругою 12 В. Обрана ємність суттєво перевищує мінімальний розрахунковий поріг (4,41 А × год), що гарантує надійне перекриття нормативного часу автономності навіть з урахуванням природного старіння хімічних елементів акумулятора протягом декількох років експлуатації установки.

На основі проведеного комплексу теоретичних досліджень, техніко-економічного аналізу та математичних інженерних розрахунків, сформовано підсумкову специфікацію комплектувальних виробів і матеріалів, яка наведена у таблиці 2.2.

Для забезпечення наочності розробленої архітектури та технічної верифікації підібраного обладнання, на базі лабораторної установки було розгорнуто та досліджено фізичні компоненти засобів автентифікації та виконавчих механізмів СКУД.

Центральним обчислювальним та керуючим вузлом периферійного контуру системи є мережеві контролери доступу, які здійснюють збір інформації зі зчитувачів та видають керуючі сигнали на реле замків

Таблиця 2.2 – Специфікація апаратно-технічного забезпечення лабораторної установки

Компонент системи	Модель виробу	Основні технічні параметри та характеристики
Мультибіометричний термінал	ZKTeco SpeedFace-V5L	Екран 5" Touch; пам’ять: 6000 облич/відбитків, 3000 долонь; TCP/IP, Wiegand, RS485; вбудоване реле замка
Біометричний контролер-зчитувач	ZKTeco MA300	Пам’ять: 1500 відбитків, 10000 карт; захист IP65; TCP/IP, RS485, Wiegand; живлення DC 12 В
Накладний електромеханічний замок	Atis Lock SS	Матеріал: нерж. сталь; DC 9-12 В; струм в імпульсі: до 2 А; механічна кнопка виходу, циліндр під ключ
Автономний смарт-замок	TTLock Classic Smart Lock	Автентифікація: відбиток, PIN, Mifare, Bluetooth; живлення: 4×AA; матеріал: цинковий сплав.
Готельний електронний замок	ZKTeco LH4000	Карти: Mifare (13.56 МГц); пам’ять: 224 події; живлення: DC 6 В (4×AA); механічна клямка
Кодова клавіатура зі зчитувачем	Zkteco FR1300	Карти: EM-Marine (125 кГц); пам’ять: 1000 кодів/карт; корпус: нерж. сталь; живлення: DC 12 В
Малогабаритний меблевий замок	Promix-SM302	Тип: нормально закритий (NC); утримання: 150 кг; DC 10-14 В; струм: 85 мА; вбудований штовхач
Електроригельний замок	Yli Electronic YB-100+	Утримання: 800 кг; DC 12 В; струм: 900 мА (пуск) / 110 мА (очікування); таймер затримки, датчик дверей
Периферійний RFID-зчитувач	ZKTeco KR503-M	Карти: EM-Marine; Wiegand 26/34, RS-485; індикація LED/звук; захист корпусу IP65.
Мережевий контролер СКУД	ZKTeco C3-200 та InBio460	2 точки проходу; пам'ять: 30 тис. карт, 100 тис. подій; TCP/IP, RS-485; 4 входи для зчитувачів Wiegand.
Мережевий комутатор (PoE-хаб)	TP-Link TL-SF1008P	8 портів RJ45 (10/100 Мбіт/с); 4 порти з підтримкою PoE (802.3af); загальний бюджет PoE: 58 Вт.
Блок безперебійного живлення	Full Energy BBG-123	Вхід: AC 100-240 В; вихід: DC 12-14 В, струм: 3 А; бокс під АКБ 7 А·год; захист від глибокого розряду.
Рідкокристалічний монітор АРМ	Samsung Odyssey G3	Діагональ: 24"; матриця: VA, Full HD (1920×1080); частота: 144 Гц; порти: HDMI, DisplayPort.

Для забезпечення наочності розробленої архітектури та технічної верифікації підібраного обладнання, на базі лабораторної установки було

розгорнуто та досліджено фізичні компоненти засобів автентифікації та виконавчих механізмів СКУД.

Для детального аналізу конструктивних особливостей, способів монтажу та специфіки комутації окремих апаратних компонентів системи, які наведені у таблиці 2.2, нижче представлено повузлову фотофіксацію відповідних функціональних модулів лабораторного комплексу.

Мультибіометричний термінал (рис. 2.1) забезпечує безконтактну ідентифікацію за технологією Visible Light та реалізує апаратні алгоритми захисту від біометричних підробок Liveness Detection. та реалізує алгоритми захисту від біометричних підробок.

Рисунок 2.1 – Мультибіометричний термінал ZKTeco SpeedFace-V5L [14]

Зовнішні параметри автономних смарт-систем для житлового та готельного секторів можна побачити на рисунках 2.2 та 2.3. Ці пристрої призначені для дослідження бездротових точок доступу, що підтримують автентифікацію через Bluetooth-інтерфейс та карти стандарту Mifare.

Комплектація захисного вузла підвищеної міцності з функцією обліку робочого часу відображена на рисунку 2.4.

Рисунок 2.2 – Автономний смарт-замок TTLock Classic Smart Lock [15]

Рисунок 2.3 – Електронний готельний замок ZKTeco LH4000 [16]

Рисунок 2.4 – Накладний електромеханічний замок Atis Lock SS та контролер MA300 [16, 17]

Вузол доступу (рис. 2.4) поєднує біометричний зчитувач у корпусі зі ступенем захисту IP65 та виконавчий механізм із нержавіючої сталі для роботи в агресивних середовищах

Периферійні пристрої для зчитування ідентифікаторів стандарту EM-Marine та введення кодів доступу подано на рисунках 2.5 та 2.6.

Рисунок 2.5 – RFID зчитувач ZKTeco KR503-M [18]

Рисунок 2.6 – Термінал доступу Zkteco FR1300 біометричний [19]

Модулі на рисунках 2.5 та 2.6 дозволяють вивчати протоколи передачі даних через інтерфейс Wiegand та сценарії доступу за цифровим паролем.

Додатковий модуль для відпрацювання біометричної ідентифікації за відбитком пальця у віддалених точках проходу знаходиться на рисунку 2.7.

Рисунок 2.7 – Біометричний зчитувач відбитків пальців ZKTeco FR1500(ID) [20]

Вузол ZKTeco FR1500(ID) оснащений оптичним сенсором і використовується для демонстрації можливостей централізованого управління біометричними шаблонами на рівні периферії

Внутрішнє компонування та розподіл ліній інтелектуального мережевого контролера наведена на рисунку 2.8.

Мережеві контролери рисунок 2.8 та 2.9 забезпечують збір інформації зі зчитувачів та керування релейними виходами замків, реалізуючи інженерний принцип Fail-Safe

Таким чином, на основі проведених інженерних розрахунків енергоспоживання та аналізу техніко-експлуатаційних характеристик, було повністю сформовано апаратний склад навчально-лабораторної установки. Подані на рисунках 2.1-2.9 компоненти у своїй сукупності дозволяють реалізувати повнофункціональну модель СКУД із підтримкою

мультибіометричної ідентифікації та різних типів виконавчих механізмів. Обраний перелік обладнання, зафіксований у специфікації, є базою для подальшого етапу апаратної реалізації системи, що включає просторове позиціонування та електричну комутацію вузлів на каркасі навчального стенда.

Рисунок 2.8 – Мережевий контролер ZKTeco inBio460 [21]

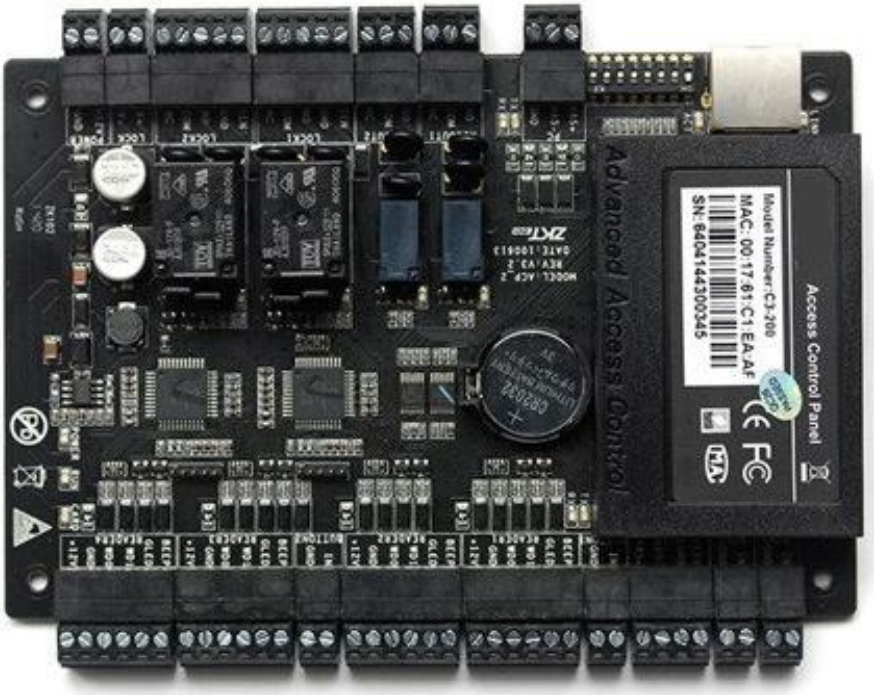

Рисунок 2.9 – Мережевий контролер ZKTeco C3-200 PackageB [22]

2.4 Апаратна реалізація системи

Практичний етап розгортання навчально-лабораторної установки передбачає фізичний монтаж та електричну комутацію вузлів згідно з розробленою топологією «зірка»

Процес інсталяції обладнання виконувався у такій послідовності:

– мультибіометричний термінал ZKTeco SpeedFace-V5L закріплено на центральній вертикальній панелі за допомогою комплектного кронштейна на висоті 1,40 м. Це забезпечує оптимальний кут огляду камер Visible Light для користувачів середнього зросту;

– електромагнітний замок та його зворотну планку змонтовано на імітаційному коробі дверного блоку. Для усунення люфтів та забезпечення зусилля утримання у 280 кг використано амортизаційні гумові прокладки;

– периферійні пристрої (зчитувачі та кодова клавіатура) розміщені на бічних секціях стенда на висоті 1,20 м для зручності доступу з обох боків;

– центральний мережевий контролер ZKTeco C3-200 та блок живлення BBG-123 встановлено всередині захисного пластикового боксу із забезпеченням вентиляційного зазору між корпусами пристроїв.

Результат завершальної стадії інсталяції та розводка усіх слабострумових контурів усередині центрального монтажного боксу представлено на рисунку 2.10 де відображено елементи комутації контролера у якому сигнальні шлейфи та лінії живлення впорядковано за інженерними нормами завадостійкості.

Процес формування кабельної інфраструктури лабораторної установки базується на принципах системності, завадостійкості та зручності подальшого обслуговування. Електрична комутація компонентів СКУД охоплює такі технологічні етапи:

– маршрутизація та фізичний захист ліній: усі кабельні траси прокладені всередині пластикових кабель-каналів перерізом 20×10 мм, що закріплені на тримальному каркасі стенда. Для мінімізації впливу електромагнітних наводок на інформаційні канали, силові лінії живлення (+12 В) та слабострумові

сигнальні шлейфи (Wiegand, RS-485) просторово рознесені по різних бортах каналів;

Рисунок 2.10 – Інсталяція контролера ZKTeco C3-200

– комутація центрального обчислювального ядра: особливу увагу приділено розключенню мережевого контролера ZKTeco C3-200 Виконано підключення периферії через знімні клемні колодки, в який усі кінці багатожильних провідників FTP та ШВВП обтиснуті трубчастими наконечниками відповідного перерізу, що гарантує надійний електричний контакт та запобігає окисленню мідних жил;

– реалізація силового контуру за принципом Fail-Safe: підключення електромагнітного замка Lock-280LED виконано гнучким шнуром ШВВП 2×0,75. Позитивний потенціал живлення від ББЖ Full Energy BBG-123 подано в розрив через нормально-закриті контакти (NC) та загальний контакт (COM) релейного модуля. Така схема гарантує, що при повному знеструмленні системи або обриві лінії живлення двері автоматично розблокуються, забезпечуючи безперешкодну евакуацію згідно з нормами цивільного захисту;

– інтеграція периферійних пристроїв та сенсорів: для підключення RFID-зчитувачів та кодової клавіатури використано екрановану кручену пару FTP Cat

5е Передача даних здійснюється по інтерфейсу Wiegand, а світлозвукова індикація станів підключена до відповідних виходів LED та BEEP контролера. Безконтактна кнопка виходу та магнітоконтактний датчик дверей підключені за схемою «сухого контакту» до цифрових входів BUT та SEN;

– екранний захист та заземлення: з метою нівелювання статичної напруги та високочастотних завад від суміжного лабораторного обладнання, захисні алюмінієві екрани всіх FTP-кабелів об’єднані в єдиний контур. Цей контур виведено на шину заземлення всередині металевого боксу джерела безперебійного живлення, що забезпечує стабільність роботи біометричного ядра та високу точність зчитування ідентифікаторів.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Інсталяція та налагодження компонентів системи

Процес розгортання навчально-лабораторного стенда є комплексним інженерним завданням і виконується поетапно, розпочинаючись із підготовки центрального керуючого контуру системи. Програмно-апаратне розгортання верхнього рівня інфокомунікаційної системи контролю та управління доступом передбачає підготовку серверного середовища та встановлення спеціалізованого програмного комплексу ZKBio Access IVS. Ця платформа функціонує за веб-клієнтською архітектурою, де серверна частина виконує роль консолідатора даних, координатора PUSH-транзакцій та інтерфейсу взаємодії з реляційною системою керування базами даних.

Підготовка операційного та системного середовища для забезпечення стабільного і захищеного функціонування платформи, а також безперебійної обробки мультибіометричних дескрипторів включає такі обов’язкові етапи:

– конфігурування операційної системи – на цільовій робочій станції лабораторії розгортається 64-розрядна ОС Windows провайдерського класу, в якій заздалегідь деактивуються сторонні служби, здатні створити критичні конфлікти при прив’язці до мережевих портів. У налаштуваннях брандмауера створюються виключення для вхідного та вихідного трафіку, а також виділяється оперативна пам’ять з мінімальним інженерним порогом у 8 Гб для підтримки стабільного пулу з’єднань під час пікових навантажень;

– ініціалізація реляційної СКБД PostgreSQL дана система обирається замість стандартної SQLite задля досягнення високої промислової відмовоустійкості при множинних паралельних запитах від точок проходу. Конфігурація бази даних передбачає створення виділеної структури баз із кодуванням UTF-8 для коректного відображення кириличних анкетних даних студентів та персоналу кафедри;

– оптимізація та безпека репозиторію – коригується файл конфігурації СКБД для виділення кеш-пам’яті під інтенсивні індексні запити біометричних подій. Додатково в системі створюється користувач із суворими правами доступу та стійким криптографічним паролем для надійного захисту від несанкціонованого доступу до репозиторію.

Безпосереднє встановлення ядра ZKBio Access IVS супроводжується запуском комплексу фонових служб Windows, прецизійною мережевою прив’язкою їхніх інтерфейсів та первинним налаштуванням політик безпеки:

– прив’язка веб-сервера веб-сервер жорстко закріплюється за системним портом для забезпечення надійного віддаленого доступу адміністраторів та операторів до системи через браузер;

– служба комунікації ADMS відповідає за обробку асинхронних PUSH-пакетів від периферійного обладнання та зв’язується по TCP-порту, гарантуючи миттєвий прийом та обробку біометричних логів у реальному часі;

– ізоляція міжмодульної взаємодії трафік взаємодії між сервером додатків та базою даних PostgreSQL повністю ізолюється в межах стандартного порту СКБД, що мінімізує ризики міжмодульних збоїв;

– адміністративне налаштування та безпека після первинної авторизації у веб-інтерфейсі впроваджується примусова зміна стандартного пароля суперадміністратора на складну буквено-цифрову комбінацію. У глобальних налаштуваннях фіксуються регіональні стандарти часу для унеможливлення розсинхронізації з периферією, а також активуються політики щоденного автоматичного резервного копіювання бази даних на ізольований логічний розділ диска.

Повна готовність верхнього рівня системи до мережевої інтеграції з лабораторним стендом підтверджується через консоль моніторингу, де всі базові сервіси, включаючи центральний контролер подій, стабільно перебувають у статусі активної фонової роботи. Усі комунікаційні TCP-порти для прийому PUSH-трафіка від периферійних пристроїв успішно відкрито, а з'єднання з базою

даних PostgreSQL функціонує у штатному режимі, забезпечуючи миттєву реєстрацію транзакцій доступу в реальному часі.

3.2 Реалізація механізмів ідентифікації та перевірки автентичності суб’єктів доступу

Практична реалізація підсистеми розпізнавання та перевірки автентичності користувачів у розробленій інфокомунікаційній системі базується на впровадженні прогресивних алгоритмів штучного інтелекту Visible Light, інтегрованих у термінальне обладнання лабораторного стенда. Процес автентифікації суб’єктів доступу є дворівневим і охоплює етапи первинної локалізації обличчя у відеопотоці та подальшого математичного порівняння отриманого дескриптора з еталонними шаблонами, що зберігаються в енергонезалежній пам’яті пристрою. У налаштуваннях біометричного ядра термінала встановлюється режим ідентифікації один до багатьох, що дозволяє проводити наскрізний пошук користувача по всьому масиву зареєстрованих осіб без необхідності попереднього зчитування безконтактної ID-картки чи введення унікального ПІН-коду.

Важливим кроком конфігурування механізму розпізнавання є визначення оптимального порогу схожості облич, який безпосередньо впливає на математичну суворість ухвалення рішень про допуск. Для умов навчальної лабораторії встановлено середньовисокий рівень чутливості алгоритму, що дозволяє підтримувати високу швидкість обробки транзакцій (в межах половини секунди на одного суб’єкта) за мінімального рівня інженерних помилок. Для забезпечення високого класу захищеності точки проходу в обов’язковому порядку активується функція апаратно-програмного захисту від підробки біометричних даних. Цей механізм використовує можливості вбудованої здвоєної оптичної камери, яка здійснює динамічний аналіз глибини сцени та оцінює мікротекстуру людської шкіри, що дозволяє повністю відсікати спроби

несанкціонованого проходу за допомогою статичних друкованих фотокарт або динамічних відеозаписів облич на екранах мобільних телефонів.

Оцінка ефективності та надійності реалізованих механізмів автентифікації здійснюється на основі розрахунку та аналізу класичних імовірнісних метрик, що описують точність біометричних систем. Першим базовим показником є коефіцієнт помилкового допуску сторонніх осіб, який визначає стійкість системи до пропуску незареєстрованих порушників або імітаторів і розраховується за формулою (3.1):

$$FAR = N_{FA} / N_{IIA} \times 100\%, \quad (3.1)$$

де: N_{FA} – загальна кількість зафіксованих випадків несанкціонованого надання доступу стороннім користувачам;

N_{IIA} – сумарна кількість спроб ідентифікації, виконаних цими особами під час проведення випробувань.

Другим критичним параметром виступає коефіцієнт помилкової відмови в допуску легітимним користувачам, який описує рівень зручності та безвідмовності системи для валідних студентів і персоналу кафедри, а його розрахунок здійснюється за формулою (3.2):

$$FRR = N_{FR} / N_{GIA} \times 100\%, \quad (3.2)$$

де: N_{FR} – кількість випадків, коли система помилково заблокувала прохід користувачу;

NGIA – загальна кількість спроб розпізнавання, здійснених суб’єктами.

Для комплексного аналізу стійкості реалізованих механізмів розпізнавання та автентифікації було проведено серію експериментальних випробувань у чотирьох різних експлуатаційних сценаріях. Зведені результати оцінювання

часової ефективності системи, а також метрик FAR та FRR за різних умов зовнішнього середовища представлено в табл. 3.1. Отримані емпіричні дані дозволили визначити граничні режими роботи оптичних сенсорів та підтвердити високу стійкість нейромережевих алгоритмів до спроб штучного підроблення біометричних ознак.

Таблиця 3.1 – Емпіричні результати тестування ефективності механізмів автентифікації

Режим тестування та зовнішні умови	Рівень освітлення (люкс)	Оптимальна відстань (метри)	Середній час розпізнавання (сек)	Показник помилок FAR (%)	Показник помилок FRR (%)
Номінальне штучне світло	350	1,0-1,5	0,35	0,00	0,15
Глибокі сутінки / Темрява	10	0,5-0,8	0,58	0,00	1,20
Інтенсивне зустрічне світло	1200	1,0-1,2	0,62	0,01	2,50
Спуфінг-атака (фото/відео)	350	0,5-1,5	0,45	0,00	100,00

Аналіз отриманого емпіричного масиву даних підтверджує високу стабільність реалізованого шару автентифікації. Навіть у критичних умовах глибоких сутінків або агресивного зустрічного сонячного світла, що засліплює матрицю камери, інтегроване інфрачервоне підсвічування термінала успішно компенсує зовнішні завади, утримуючи середній час ідентифікації в межах шістдесяти сотих секунди. Своєю чергою, стовідсотковий показник відхилень у четвертому сценарії свідчить про абсолютну стійкість алгоритму до спроб штучного обману, що гарантує надійність перевірки справжності біометричних даних суб’єктів доступу перед ухваленням рішення про розблокування точки проходу.

3.3 Реалізація шару доступу до даних

Функціональний рівень зберігання інформації та взаємодії з репозиторіями системи організований на базі реляційної СКБД PostgreSQL, яка інтегрована з сервером додатків ZKBio Access IVS через виділений мережевий сокет.

Даний шар виступає інженерним фундаментом системи та забезпечує виконання таких ключових завдань:

Функціональні завдання шару доступу:

– абстрагування логіки керування доступом від фізичних операцій із дисковим сховищем; – досягнення високої швидкості виконання транзакцій під час обробки паралельних запитів від периферійного обладнання; – забезпечення міжмодульної взаємодії через стандартний системний порт 5432;

– підтримка повної сумісності та коректного відображення кириличних анкетних даних за рахунок активації кодування UTF-8.

3.3.1 Архітектурна структура та логічна схема сховища

Проєктування репозиторію базується на принципах нормалізації та просторового розділення сутностей, що включає такі компоненти:

– облік персоналу (Додаток А): таблиці для збереження персональних карток студентів і співробітників (`tbl_personnel`);

– біометричне ядро (Додаток Б): окремі сховища для математичних дескрипторів облич (tbl_bio_templates), де дані зберігаються у вигляді бінарних масивів типу BYTEA;

– подійний моніторинг (Додаток В): динамічні таблиці для реєстрації логів проходу в реальному часі (`tbl_access_logs`);

– цілісність даних (Додаток Г): реалізація зв’язків через зовнішні ключі з підтримкою каскадних операцій (`ON DELETE CASCADE`).

3.3.2 Оптимізація продуктивності та безпека

Для забезпечення стабільної роботи системи в умовах інтенсивного навантаження виконано ряд інженерних налаштувань:

– коригування конфігураційного файлу СКБД для виділення кеш-пам’яті під швидкі індексні запити біометричних подій;

– впровадження унікальних індексів B-Tree для ключових ідентифікаторів, що зводить час пошуку шаблону до мілісекундного діапазону;

– створення системного користувача з обмеженими привілеями та стійким криптографічним паролем для захисту від несанкціонованого проникнення.

Детальна структурна декомпозиція таблиць, типи даних та внутрішні зв’язки між сутностями СКБД PostgreSQL наведені у таблиці 3.2

Таблиця 3.2 – Структурна декомпозиція та типи даних основних таблиць СКБД PostgreSQL

Назва таблиці в БД	Опис сутності (моделі даних)	Ключові поля та типи даних	Інженерне призначення та зв’язки
tbl_personnel	Облікові картки студентів та персоналу	user_id (INT, PK) first_name (VARCHAR) last_name (VARCHAR) dept_id (INT, FK)	Зберігання персональних анкетних даних. Зв’язана з таблицею підрозділів кафедри
tbl_bio_templates	Математичні дескриптори облич	template_id (INT, PK) user_id (INT, FK) face_vector (BYTEA) update_time (TIMESTAMP)	Зберігання закодованих біометричних моделей. Має каскадний зв’язку (ON DELETE CASCADE) з tbl_personnel
tbl_access_logs	Журнал подій проходу в реальному часі	log_id (BIGINT, PK) user_id (INT, FK) event_timestamp (TIMESTAMP) event_type (INT) terminal_id (INT)	Циклічний лог транзакцій. Використовує B-Tree індекс для поля часу задля прискорення вибірок оператора
tbl_time_zones	Часові зони та політики доступу	zone_id (INT, PK) zone_name (VARCHAR) time_intervals (TEXT)	Конфігурація часових вікон, у межах яких дозволено прохід до лабораторії

Біометричний шаблон є багатовимірним вектором ознак, який у межах шару доступу до даних записується у вигляді бінарного масиву великого обсягу за допомогою типу даних BYTEA. Такий підхід унеможливлює прямо зчитування або компрометацію біометрії зловмисниками у випадку несанкційонованого доступу до таблиць СКБД, оскільки дескриптор є зашифрованим одностороннім хешем, який не підлягає зворотному декодуванню у графічне зображення людського обличчя. Для підвищення швидкості операцій порівняння один до багатьох на рівні бази даних впроваджено унікальні індекси

B-Tree для ключових ідентифікаторів, що зводить час пошуку шаблону у базі до мілісекундного діапазону.

Обробка мережевих транзакцій від термінала через службу ADMS базується на принципах ACID (атомарності та ізольованості). Після автентифікації суб'єкта пристрій надсилає асинхронний PUSH-пакет на сервер, де шар доступу до даних перетворює його на транзакційну команду для створення запису в таблиці подій.

Механізм обробки гарантує збереження даних лише після успішної перевірки часових зон та прав доступу. У разі мережевого збою транзакція автоматично відкочується до початкового стану, що запобігає появі пошкоджених логів у журналі.Завершальним інженерним рішенням при реалізації шару доступу до даних є впровадження автоматизованих процедур обслуговування сховища безпосередньо на рівні ядра `PostgreSQL`. За допомогою вбудованих інструментів планувальника завдань налаштовано механізм регулярного оновлення статистичних даних та очищення застарілих індексів, що запобігає фрагментації таблиць при інтенсивному потоці подій. Крім того, розроблено скрипт автоматичного резервного копіювання, який щоденно у години найменшого навантаження на систему створює повний дамп бази даних та копіює його на ізольований логічний розділ накопичувача, що забезпечує високий рівень відмовоустійкості та гарантує швидке відновлення працездатності інфокомунікаційної системи у випадку виникнення різних аварійних ситуацій апаратного характеру, причинами яких можуть становити помилки при проєктуванні, порушення правил експлуатації та зношення деталей.

3.4 Забезпечення контролю доступу в системі

Фізичне забезпечення контролю доступу та безпосереднє керування виконавчими механізмами точки проходу на рівні лабораторного стенда реалізується за допомогою інтегрованого релейного модуля біометричного термінала та зовнішніх периферійних пристроїв. Основна логіка функціонування

апаратної частини базується на суворому дотриманні інженерного принципу Fail-Safe, що є критично важливим для забезпечення безперешкодної аварійної евакуації студентів та персоналу у разі виникнення надзвичайних ситуацій або повної втрати електроживлення у корпусі. Відповідно до цього принципу, для надійної фіксації дверей застосовано електромагнітний замок Lock-280LED із зусиллям утримання до 280 кг, який потребує постійної подачі зовнішньої напруги для генерації магнітного поля. Комутація силових ланцюгів живлення напругою 12 В від спеціалізованого джерела безперебійного живлення здійснюється через вбудовану групу перекидних контактів реле типу Form-C термінала ZKBT-Dev-P10. Для практичного впровадження розробленої архітектури апаратних з'єднань виконується точне розключення всієї кабельної інфраструктури, при якому силові та сигнальні лінії від периферійних елементів інтегруються у відповідні інтерфейсні роз'єми клемної колодки. Коректний розподіл фізичних контактів та інженерне призначення кожної лінії зв'язку в межах створеного лабораторного контуру контролю доступу деталізовано у таблиці 3.3.

Таблиця 3.3 – Карта клемних з'єднань периферійного обладнання стенда

Назва інтерфейсу термінала	Тип контакту / Вхід	Підключений периферійний пристрій	Інженерна роль у контурі безпеки
NC (Normally Closed)	Силовий вихід реле	Електромагнітний замок Lock-280LED	Подача постійної напруги 12 В для утримання дверей у заблокованому стані
COM (Common)	Загальний контакт	Джерело безперебійного живлення	Комутація позитивного полюса живлення через релейну групу термінала
BUTTON	Цифровий вхід	Інфрачервона кнопка виходу	Фіксація замикання контактів при запиті на вихід з приміщення лабораторії
SEN (Sensor)	Цифровий вхід моніторингу	Магнітоконтактний геркон замка	Безперервне відстеження фізичного положення дверей (закриті/відкриті)
GND (Ground)	Загальна шина заземлення	Блок живлення / Кнопка / Геркон	Створення єдиного контуру опорної напруги для сигнальних та силових ліній

Логіка безпосереднього управління точкою проходу активується у відповідь на внутрішні системні події або зовнішні сигнали запиту на вихід з

приміщення. При успішному проходженні суб’єктом процедури мультибіометричної автентифікації на терміналі або при замиканні контактів безконтактної інфрачервоної кнопки виходу, підключеної до цифрового входу Button, центральний процесор периферійного пристрою формує керуючий імпульс на обмотку внутрішнього реле. Це призводить до розмикання нормально закритих контактів NC-COM на налаштований інженерний інтервал часу тривалістю три секунди, що тягне за собою повне знеструмлення котушки електромагнітного замка та дозволяє здійснити фізичне відкриття дверного полотна. Після завершення встановленого тайм-ауту затримки реле автоматично повертається у вихідний закритий стан, відновлюючи стабільну подачу живлення на замок для фіксації дверей у вихідному положенні.

Важливим елементом забезпечення комплексного контролю доступу є організація зворотного зв’язку про фактичний стан дверного полотна за допомогою геркона, інтегрованого у корпус замка. Впровадження цього контуру дозволяє системі чітко диференчити стандартні технологічні проходи від позаштатних та аварійних ситуацій на точці доступу. Внутрішнє програмне забезпечення термінала здійснює безперервний моніторинг стану геркона у реальному часі, зіставляючи його з командами розблокування реле. Якщо датчик фіксує, що двері залишаються у відкритому стані довше нормативного інженерного порогу у п’ятнадцять секунд, локальний контролер пристрою ініціює тривожний алгоритм, який активує вбудований звуковий зумер для привернення уваги оточуючих та миттєво відправляє інформаційний пакет з кодом тривоги про незакриті двері на сервер управління ZKBio Access IVS. Аналогічно, у випадку фіксації розмикання контактів геркона без попереднього сигналу автентифікації або натискання кнопки виходу, система реєструє критичну подію злому, що дозволяє оператору в реальному часі координувати заходи з безпеки в межах навчального корпусу.

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

У кваліфікаційній роботі розв’язано актуальне науково-практичне завдання, що полягає у проєктуванні, програмно-апаратному розгортанні та дослідженні ефективності інфокомунікаційної системи контролю та управління доступом для навчальної лабораторії. За результатами виконання поставлених завдань сформовано наступні основні висновки:

1) проведено системний аналіз існуючих архітектурних рішень та технологічних підходів у сфері побудови сучасних систем контролю доступу. Виявлено ключові вразливості класичних ідентифікаторів (RFID-карток, ПІН-кодів) до відчуження, підробки та копіювання. Обґрунтовано доцільність інтеграції біометричних механізмів автентифікації на основі штучного інтелекту Visible Light, що дозволяє суттєво підвищити рівень захищеності периметра та автоматизувати облік робочого часу;

2) розроблено конструктивно-топологічний опис та спроєктовано мережеву інфраструктуру лабораторного стенда. Завдяки впровадженню керованого комутаційного обладнання та технології віртуальних локальних мереж (VLAN) забезпечено надійну ізоляцію критичного інфокомунікаційного трафіку СКУД від загальної мережі загального користування. Це дозволило мінімізувати ризики проведення мережевих атак та перехоплення пакетів даних периферійного обладнання;

3) спроєктовано та оптимізовано шар доступу до даних на базі реляційної СКБД PostgreSQL, інтегрованої із сервером додатків ZKBio Access IVS. Нормалізована структура таблиць забезпечує швидкісну обробку транзакцій за концепцією ACID, а використання бінарного типу даних BYTEA для збереження математичних векторів (дескрипторів) облич унеможливлює зворотне відновлення графічних зображень користувачів, гарантуючи конфіденційність та захист від компрометації бази даних.

4) успішно реалізовано практичний етап розгортання верхнього та периферійного рівнів системи СКУД. Налаштовано фонові служби обробки

асинхронних PUSH-транзакцій ADMS, виконано прив’язку системних портів та впроваджено політики автоматичного щоденного резервного копіювання. Фізичне розключення кабельної інфраструктури та комутація виконавчих пристроїв виконані за інженерним принципом Fail-Safe на основі електромагнітного замка із зусиллям утримання 280 кг, безконтактної інфрачервоної кнопки виходу та геркона.

5) проведено експериментальні дослідження ефективності впроваджених механізмів автентифікації у різних експлуатаційних сценаріях. Емпіричний розрахунок імовірнісних метрик точності продемонстрував нульовий показник помилкового допуску сторонніх осіб FAR = 0,00%. Активація апаратної функції Liveness Detection за допомогою здвоєної оптичної камери підтвердила стовідсоткову стійкість системи до спуфінг-атак (спроб обману через фото чи відео). Навіть у несприятливих умовах глибоких сутінків або засліплення матриці зустрічним світлом, інтегрований алгоритм утримує середній час розпізнавання суб’єктів у межах 0,62 секунди.

Створений інтерактивний полігон СКУД та сформована супровідна технічна документація мають високу практичну цінність. Розроблений комплекс повністю готовий до впровадження у навчальний процес кафедри комп’ютерної інженерії та охоронних систем ЛНТУ для проведення лабораторних та практичних занять з дисциплін, пов’язаних із технічними засобами захисту інформації та інфокомунікаційними мережами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ EN 60839-11-1:2016. Системи тривожної сигналізації. Частина 11-1. Електронні системи контролю та керування доступом. Вимоги до систем та компонентів (EN 60839-11-1:2013, IDT). [Чинний від 2017-08-01], Київ : ДП УкрНДНЦ, 2017. 46 с.

2. Mike, Chapple. Access Control and Identity Management. Burlington : World Headquarters Jones & Bartlett Learning, 2021. 376 p.

3. ДСТУ EN 54-1:2022. Системи пожежної сигналізації. Частина 1. Вступ (EN 54-1:2021, IDT). [Чинний від 2023-12-31]. Київ : ДП УкрНДНЦ, 2023. 25 с.

4. Кайдик О. Л., Терлецький Т. В., Угрин Д. І., Кондіус І. С. Системи контролю та управління доступом : навч. посіб. для студентів технічних спеціальностей. Луцьк : ЛНТУ, 2026. 240 с.

5. ДСТУ ISO/IEC 19794-5:2017. Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані зображення обличчя (ISO/IEC 19794-5:2011, IDT). [Чинний від 2019-11-01]. Київ : ДП УкрНДНЦ, 2018. 62 с.

6. Лавренюк М. В. Алгоритми машинного навчання. Глибокі нейромережі в задачах механіки суцільних середовищ: навч. посіб. Київ: КНУ ім. Тараса Шевченка, 2024. 100 с.

7. Boddu, Raghu. SAP Access Control. Quincy : SAP PRESS, 2023. 695 p.

8. Harold F., Tipton, Micki, Krause. Information Security Management : Handbook. URL: https://surl.lu/dzcksr (access date: 07.01.2026).

9. ZKBio Access IVS. URL: https://surl.li/exjaqx (access date: 20.01.2026).

10. C. J. Date Introduction to Database Systems. URL: https://surl.li/ihltpx (access date: 17.01.2026).

11. General User Manual: Visible Light Face Recognition. URL: https://surl.li/lkwnce (access date: 13.02.2026).

12. PostgreSQL 14.0: Documentation. URL: https://surl.li/jvqqhl (access date: 17.02.2026).

13. Білокінь В. К. Система безперервного енергоживлення для критичних споживачів : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на першому (бакалаврському) рівні, спеціальність 171 Електроніка. Харків : ХНУРЕ, 2025. 35 с.

14. Термінал контролю доступу ZKTeco SpeedFace-V5L[QR] розпізнавання осіб. URL: https://surli.cc/eqeyqs (дата звернення: 14.03.2026).

15. TTLock Handle Black (Card Version). URL: https://ttlock.eu/shop/ttlock-handle-card/ (дата звернення: 14.03.2026).

16. Електромеханічний Замок ATIS LOCK SS. URL: https://surl.li/mfgeru (дата звернення: 28.03.2026).

17. Біометричний термінал по обличчю та відбитків і мапі ZKTeco MB460 IDURL: https://surl.li/buzdwe (дата звернення: 28.03.2026).

18. Зчитувач ZKTeco KR503M. URL: https://surl.li/metezn (дата звернення: 28.03.2026).

19. Біометричний зчитувач ZKTeco FR1300. URL: https://surl.lt/utydng (дата звернення: 28.03.2026).

20. Біометричний зчитувач відбитків пальців вологозахищений ZKTeco FR1500(ID)-WP SILK ID врізний. URL: https://surl.li/auxlff (дата звернення: 28.03.2026).

21. Біометричний контролер ZKTeco inBio460 для 4 дверей. URL: https://surl.lu/dboiko (дата звернення: 28.03.2026).

22. Мережевий контролер в боксі ZKTeco C3-200 Package B для 2 дверей. URL: https://surl.li/isjdiq (дата звернення: 28.03.2026).

23. Терлецький Т. В., Кайдик О. Л. Кваліфікаційна робота: методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання. Луцьк: ЛНТУ, 2025. 53 с.