Хмельницький національний університет

Факультет інформаційних технологій

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Багрія Максима Олеговича

на здобуття ступеня вищої освіти Бакалавра

Система контролювання доступу «Укрексімбанк» м. Хмельницький з використання біометричної ідентифікації

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

Шифр КРБКБ. 2101108.21.01.01 ПЗ

Виконав: студент 4 курсу, група КБ-21-1 Максим БАГРІЙ

Керівник: канд. техн. наук, доцент Ігор МУЛЯР

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

11 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Багрію Максиму Олеговичу
(Прізвище,ім'я, по батькові студента)

1 Тема роботи Система контролювання доступу «Укрексімбанк» м. Хмельницький з використання біометричної ідентифікації

Керівник роботи Ігор Муляр

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи модель банківського приміщення з розташуванням елементів системи контролювання доступу, рекомендації щодо встановлення і налаштування системи

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз сфери безпеки. Загрози доступності Принципи захисту. Біометричні методи. Вибір обладнання. Аналіз компонентів. Інтеграція систем. Проєктування СКД. Моделювання приміщення. Рекомендації з впровадження. Загальна вартість

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схема банківського відділення, Модель банківського відділення, Алгоритм роботи компонентів системи контролювання доступу

6 Консультанти розділів кваліфікаційної роботи

		Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	виконав
Ознайомлення з предметною областю	Лютий	виконав
Дослідження існуючих рішень	Лютий	виконав
Постановка задачі	Березень	виконав
Визначення загальних принципів рішення задачі	Березень	виконав
Деталізація принципів рішення задачі	Квітень	виконав
Впровадження системи	Квітень	виконав
Апробація проєктних рішень	Травень	виконав
Оформлення пояснювальної записки згідно вимог	Травень	виконав
Оформлення графічної частини	Травень	виконав
Захист КР	Червень	виконав

Студент _____ Максим БАГРІЙ

Керівник кваліфікаційної роботи _____ Ігор МУЛЯР

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система контролювання доступу «Укрексімбанк» м. Хмельницький з використання біометричної ідентифікації.

Автор роботи: Багрій Максим Олегович.

Керівник роботи: Муляр Ігор Володимирович.

Пояснювальна записка: 68 с., 3 додатки, 10 рисунків, 1 таблиці, 32 джерел.

Графічна частина: 3 плакати.

СИСТЕМИ КОНТРОЛЮВАННЯ ДОСТУПУ, БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ, БІОМЕТРИЧНИЙ ТЕРМІНАЛ.

Кваліфікаційна робота бакалавра присвячена розробці системи контролювання доступу (СКД) для банківського відділення у м.Хмельницькому («Укрексімбанк»).

В роботі проведені дослідження у сфері систем контролювання доступу, а саме рішеня безпек з використанням біометричних методів індитифікації та порівнняня різних існуючих способів. В результаті обраного рішення, було складено модель примішення та розміщення систем контролювання доступу. Отримано детальні рекомендації щодо встановлення та впровадження їх налаштування данних систем для забезпечення безпеки та охорони приміщення.

09.06

ABSTRACT

Subject of qualification work:

Author: Bahrii Maksym Olehovych.

Head of work: Muliar Ihor Volodymyrovych.

Explanatory note: 68 p., 3 appendices, 10 figures, 1 tables, 32 sources

Graphic part: 3 posters.

ACCESS CONTROL SYSTEMS, BIOMETRIC AUTHENTICATION, BIOMETRIC TERMINAL.

The bachelor's qualification work is devoted to the development of an access control system (ACS) for a bank branch in c.Khmelnytskyi (Ukreximbank).

The work included research in the field of access control systems, namely security solutions using biometric identification solutions and a comparison of various existing methods. As a result of the chosen solution, a model of the room and placement of the systems was drawn up. Detailed recommendations on how to install and configure these systems to ensure the safety and security of the premises were obtained.

09.06

ЗМІСТ

Вступ 7
1 Дослідження сфери захисту інфраструктур 8
1.1 Загрози доступності та збереження безпеки 8
1.2 Принципи забезпечення захисту 11
1.3 Біометричні складові систем для контролювання доступу 16
1.4 Постановка задачі 23
2 Пошук сучасних рішень 25
2.1 Підбір апаратного забезпечення для систем 25
2.2 Переваги та недоліки наявних компонентів, вибір надійного рішення 35
2.3 Аналіз постачальників систем безпеки 47
2.4 Висновки 50
3 Проектування системи контролювання доступом 51
3.1 Підбір апаратного забезпечення для відділення 51
3.2 Моделлювання та впровадження 54
3.3 Розробка рекомендацій для реалізації системи 56
3.4 Оцінка собівартості системи 62
3.5 Висновки 63
Висновки 64
Перелік джерел посилання 65
Додаток А Копія графічної частини 69

ВСТУП

Забезпечення фізичної та інформаційної безпеки у фінансових та критичних установах є надзвичайно важливим рішенням у поточних і майбутніх умовах, коли зловмисники використовують як кіберзагрози, так і фізичні методи втручання. Банківські відділення, що оперують із критичними даними та матеріальними цінностями, стають об’єктами як внутрішніх, так і зовнішніх атак, що змушує їх задуматися над впровадженням ефективних, надійних, безперебійних засобів захисту. Тому я пропоную приділяти особливу увагу системам контролювання доступу, які відіграють ключову роль у захисті та доступності приміщень і персоналу. Сучасні технології біометричної ідентифікації дозволяють значно підвищити рівень безпеки завдяки використанню унікальних фізіологічних характеристик особи. Такі рішення набагато зменшують, а при комбінувані рішень, унеможливлюють підробку чи несанкціонований доступ.

Розробка системи контролювання доступу для таких приміщень потребує комплексного підходу, що включає вибір апаратного забезпечення, моделювання приміщення та інтеграцію засобів біометричної аутентифікації. З огляду на високі вимоги до цілістності, надійності та безпеки, необхідно враховувати як технічні характеристики компонентів, так і зручність їхнього використання. Крім того, інтеграція із різними системами, обліку часу та аналізу подій дозволяє створити ефективну та масштабовану інфраструктуру безпеки.

Основною задачою цієї роботи є аналіз і проєктування системи контролювання доступу для відділення банку із застосуванням нових та прогресуючих біометричних технологій. Протягом процесу дослідження буде розглянуто сучасні засоби ідентифікації, проаналізовані порівняння їхніх можливостей надання захисту та створенно рекомендації щодо оптимальної реалізації системи з урахуванням особливостей об'єкта та вимог до розташування.

1 ДОСЛІДЖЕННЯ СФЕРИ ЗАХИСТУ ІНФРАСТРУКТУР

1.1 Загрози доступності та збереження безпеки

Безпека банківських відділеннь є невідємною частиною забезпечення захисту як матеріальних цінностей, так і персональної інформації працівників та клієнтів. З постійним вдосконаленням технологій та нових векторів атак, потрібно постійно адаптуватися та підтримувати стабільність операцій у таких сферах щодо захисту та виявлення шкідливих дій що можуть завдати незворотних збитків. Тому постійний попит на забезпечення повноційної безпеки змушує появи надійних рішення що б надати якісний контроль доступу та зменшенню втрат.

Основні категорії загроз з якими банківські відділення можуть зіткнутися є фізичними зі сторони внутрішної і зовнішної, та кібератаки що також можуть бути гібридні, скомбіновані з фізичними. У цій сфері, спеціалісти по безпеці, перше на що звертають увагу, це фізичні спроби атак на банківських відділень, банкоматів та дата-центрів. Ризиками для них можуть бути фізичні атаки, несанкціонованне втручання, пограбування, крадіжки, вандалізм, негативні внутрішні дії співробітників, витік інформації. Ці всі елементи можуть повязати за собою чи мало яких подій що негативно вплияють на ці установи [1].

Найбільш поширеними наслідками можуть бути:

Розголошення банківської інформації — це протиправні умисні або необережні дії працівників чи інших осіб, які призводять до несанкціонованого розкриття відомостей, що підлягають захисту та нерозголошення відповідно до встановленого порядку. То для цього потрібно слідкувати всі дії пов’язані до активів власності банку.

Викрадення інформації що зумовлене вилучення, неповідомляючи або без наданоъ на те згоди, носіїв даних із метою їх подальшого використання або передачі третім особам для отримання матеріальної вигоди або для подальших кіберзлочинів.

Знищення інформації може бути як навмисне та ненавмисне приведення носіїв даних до стану, за якого неможливо відновити або використовувати інформацію, що на них зберігалась.

Модифікація інформації є процесом внесення змін у зміст даних або у самі носії інформації, що призводить до втрати первинної достовірності та цілісності цієї інформації. Внаслідок таких змін інформація може стати недоступною, спотвореною або вимагати додаткового, ретельного аналізу для її подальшого використання, наприклад, у випадках, коли вона була зашифрована або піддана іншим формам трансформації.

Такий процес може мати як випадковий, так і навмисний характер, і в обох випадках він створює значні ризики для організацій, особливо у фінансовому секторі, де точність і цілісність даних є критично важливими. Окрім цього, існує загроза незаконного використання інформації, знань, даних, комерційних таємниць або технологій, які є власністю або результатом розробки іншої особи чи організації [2].

Таке використання відбувається без згоди власника або з порушенням встановлених правил доступу, і найчастіше здійснюється тими, хто отримав доступ до цієї інформації у зв’язку з виконанням службових чи професійних обов’язків. Це може включати копіювання, розголошення, продаж або інші форми експлуатації інформації, що завдають шкоди власнику і порушують законодавчі норми. Особливу загрозу у цьому контексті становлять людські чинники, адже джерелами таких ризиків можуть бути не лише зовнішні зловмисники, а й власні співробітники банку чи організації. Мотивація таких дій може бути різною — від матеріальної вигоди, корисливих намірів, особистої неприязні або бажання помсти, до прагнення самоствердження, визнання або навіть необізнаності про наслідки своїх дій.

Найбільш небезпечними є внутрішні загрози, що походять від співробітників, які мають легальний доступ до систем і даних, але через недостатню обізнаність у сфері інформаційної безпеки, нехтування

встановленими політиками захисту, або навіть через зловмисні наміри можуть спричинити витік, модифікацію або знищення критично важливої інформації. Внутрішні загрози особливо небезпечні тим, що вони важче виявляються, оскільки такі працівники мають знання про системи безпеки, доступ до ресурсів і можуть діяти непомітно для зовнішніх контролюючих органів [3].

Тому ефективний захист інформації вимагає не лише технічних заходів, а й комплексного підходу, що включає навчання персоналу, регулярний аудит, впровадження суворих політик доступу та моніторинг поведінки користувачів. Лише поєднання цих заходів дозволяє мінімізувати ризики модифікації інформації та незаконного використання даних, забезпечуючи надійний захист активів і довіру клієнтів.

Інформаційні ресурси банківської установи можуть піддаватися загрозам за різними шляхами їх реалізації. Серед них варто виокремити підкуп співробітників, які мають доступ до банківської таємниці чи іншої конфіденційної інформації; недбале або необережне поводження з такими даними; а також порушення встановлених порядків збереження інформації під час взаємодії з системами чи активами, що часто є наслідком правової або психологічної неготовності відповідальних працівників. Важливу роль у витоку банківської інформації відіграють різні технічні канали, такі як візуально-оптичні, акустичні, акустично-перероблювальні, електромагнітні та матеріально-речові.

У такому разі одним з можливих варіантів, запропонованих сучасними технологіями, є системи контролювання доступу, які раніше використовувалися виключно для аутентифікації персоналу та захисту банківських приміщень, сьогодні можуть бути використані для виконання функцій, що виходять за рамки безпеки, з метою покращення обслуговування та забезпечення кращого досвіду як для співробітників, так і для клієнтів [4].

1.2 Принципи забезпечення захисту

Інтеграція систем контролювання доступу з іншими засобами безпеки, такими як відеоспостереження та системи виявлення вторгнень, буде запорукою створення чудового та надійного фізичного захисту що дозволяє створити комплексну та багаторівневу систему для контролювання доступу. Банківські відділення мають співпрацювати з надійними партнерами, здатними забезпечити повний цикл управління безпековими рішеннями, і обирати виробників, які спеціалізуються на впровадженні передових та надійних технологій із підвищеним рівнем захисту [5].

Ці засоби спрямовані на обмеження або контроль доступу до особливо важливих ресурсів та інформації в межах організації, що володіє ресурсами. З одного боку, системи контролювання доступу до банківської системи безпеки пристосовані для нагляду за фізичним доступом до приміщень. Це стосується таких приміщень, як банківські відділення, серверні або сховища, а також доступу до комп'ютерних структур і конфіденційних даних.

В залежності від вимог, системи банківської безпеки доступом можуть використовувати набір технологій, що варіюється від звичайних систем замків і ключів до сучасних розробок, таких як біометричні сканери та багатофакторна перевірка достовірності.

Що стосується практичності, то системи банківської безпеки регулюються заздалегідь визначеними правилами і поведінковими алгоритмами. Це або дозволяє, або забороняє доступ, залежно від певних обставин. При розширенні, контроль доступу в банках зазвичай передбачає спосіб підтвердження, який включає в себе реєстрацію спроб доступу та інших пов'язаних з ними дій. У разі виникнення інциденту цей рівень підтвердження безпеки виконує значну функцію в реагуванні на подію [6].

Здебільшого банки починають впроваджувати заходи безпеки після того, як мають доступ до потужних систем. При цьому ці системи можуть бути

попередньо протестовані та змодельовані за допомогою спеціалізованого програмного забезпечення, яке моделює як фізичні, так і цифрові сценарії. До найбільш актуальних типів систем безпеки відносяться:

– електронні СКД переважно оснащуються кнопковими панелями та інтелектуальними замками, що забезпечують кілька способів ідентифікації: введення персонального PIN-коду або автоматичне розпізнавання попередньо зареєстрованих ключ-карт чи електронних брелоків при наближенні користувача. Такий підхід забезпечує гнучкість, зручність і підвищений рівень безпеки доступу.;

– фізичні СКД використовують стандартні картки, RFID-картки, біометричні технології та інше обладнання для контролю доступу. Біометричні методи засновані на унікальних фізичних характеристиках, таких як відбитки пальців, риси обличчя або структура райдужної оболонки ока. Найбезпечніші системи поєднують кілька таких методів для підвищення рівня довіри та безпеки;

– системи мережевого контролю, захищають доступ до комп'ютеризованих ресурсів банку. Такі системи часто використовують паролі, двофакторну автентифікацію, цифрові сертифікати та інші засоби ідентифікації. Вони також можуть включати брандмауери, системи виявлення несправностей та інструменти моніторингу активності;

– рольові системи безпеки використовуються як у фізичному, так і в електронному виді. Доступ визначається відповідно до ролі користувача в системі. Наприклад, касир матиме інший рівень прав доступу, ніж менеджер або директор.

Будь-яка система контролю доступу має свої унікальні переваги у забезпеченні вимог щодо доступності, цілісності та конфіденційності даних і активів, що зумовлює необхідність індивідуального підходу до її конфігурації залежно від специфіки установи, особливостей об’єкта та рівня цінності ресурсів, які вона повинна захищати [7].

Сучасні системи контролювання доступом (СКД) представляють собою складні інтегровані комплекси технічних і програмних засобів, що функціонують у тісній взаємодії для забезпечення надійного контролю над фізичним доступом до приміщень, територій чи окремих зон. До складу таких систем входять фізичні бар'єри, як-от двері, турнікети, ворота, обладнані електромагнітними або електронними замками, які перешкоджають несанкціонованому проникненню. Важливою складовою є засоби ідентифікації особи, що можуть включати пластикові картки, електронні брелоки, біометричні дані або коди, які зчитуються спеціальними пристроями ідентифікації [8].

Ці зчитувачі отримують інформацію з носіїв ідентифікаторів та передають її на контролер, який є центральним елементом системи. Контролер аналізує отримані дані, порівнює їх із заздалегідь встановленими правилами доступу, сценаріями та політиками безпеки, після чого приймає рішення про надання або відмову у доступі. Для підвищення надійності та безпеки контролери рекомендується розміщувати у прихованих або захищених місцях, що унеможливлює несанкціонований доступ до елементів керування замками, а також передбачати резервні джерела живлення, які забезпечують безперебійну роботу системи у випадку аварійного відключення електроенергії, що є критично важливим для підтримки безпеки об'єкта без збоїв.

Крім базових компонентів, сучасні СКД часто оснащуються додатковими модулями, такими як камери відеоспостереження, датчики руху, пристрої для фото- та відеофіксації подій, що дозволяє не лише контролювати доступ, а й документувати всі інциденти, забезпечуючи можливість ретельного аналізу та швидкого реагування на загрози. Програмне забезпечення, яке керує системою, є ключовим фактором її ефективності, воно повинно бути інтуїтивно зрозумілим, мати розгорнуту документацію та забезпечувати гнучкі можливості для налаштування системи під конкретні потреби установи. Якісне ПЗ дозволяє створювати індивідуальні профілі доступу, визначати рівні прав для співробітників і відвідувачів, вести облік робочого часу, формувати звіти, а

також інтегруватися з іншими системами безпеки, такими як пожежна сигналізація, охоронна система чи відеоспостереження. Особливо важливою є інтеграція СКД із системами відеоспостереження, що дозволяє отримувати відеопідтвердження подій у реальному часі, автоматично переводити камери у потрібні положення при проході користувачів, здійснювати верифікацію осіб для запобігання використанню чужих перепусток, а також контролювати допуск транспортних засобів на територію [9].

Така інтеграція створює більш комплексний і функціональний захист, ніж використання кожної системи окремо, підвищуючи рівень безпеки і оперативність реагування. Важливо також враховувати сумісність обладнання та програмного забезпечення, оскільки навіть незначні відмінності в моделях пристроїв можуть призводити до проблем сумісності, що ускладнює експлуатацію системи. Проте існують відкриті фреймворки та стандарти, які дозволяють інтегрувати різнорідні компоненти, забезпечуючи масштабованість і гнучкість системи. Перед впровадженням СКД необхідно ретельно визначити завдання, які вона має виконувати, врахувати особливості об’єкта, потенційні загрози та вимоги до безпеки, щоб обрати оптимальне рішення. Загалом, сучасні системи контролювання доступу є невід’ємною частиною комплексних заходів безпеки, що дозволяють не лише контролювати фізичний доступ, а й забезпечувати цілісність інформації, зберігати конфіденційність даних, а також підвищувати ефективність управління безпекою в організації [10].

В доповнення до основних компонентів, система може бути оснащена додатковими модулями, такими як камери для фото та відеозйомки, датчики руху на важливих периметрах або пристрої, що фіксують процес потрапляння на територію .

Але ніщо з цього не буде працювати без відповідно розробленої програми, яка вирішує, наскільки надійно ця система забезпечить безпеку. Корисність системи контролю та адміністрування доступу значною мірою визначається її комп'ютерною програмою, яка повинна бути інтуїтивно зрозумілою, мати якісну

документацію, а також бути прийнятною і простою у використанні для будь-якого оператора. Якісна програма дозволяє адаптивно налаштовувати систему під конкретні потреби, підтримувати вибране обладнання, розширювати можливості, здійснювати організацію, створювати звіти та вести облік робочого часу. Головною перспективою є подальша робота з базами даних, що слід враховувати при підключенні системи до комп'ютера: обладнання повинно мати відповідне виконання, щоб гарантувати швидку підготовку запитів і оперативність інформації, що зберігається. Чим швидше контролер знаходить інформацію, тим швидше реагують користувачі та пристрої управління і не створюють навантаження на повсякденну роботу працівників та відвідувачів [11].

Як правило, перед вибором системи контролювання доступу необхідно чітко визначити завдання, які вона повинна виконувати, а також технічні характеристики, яким вона має відповідати. Особливу увагу слід приділити сумісності з обладнанням, адже більшість програмного забезпечення постачається разом із пристроями, і кожен виробник має власне ПЗ. Навіть невелика різниця в моделі пристрою може призвести до часткової або повної несумісності зі сторонніми програмними рішеннями, навіть якщо виробник той самий. Проте існують відкриті фреймворки, що дозволяють інтеграцію з програмами сторонніх розробників, особливо якщо вони виконують додаткові функції, як-от аналітика, контроль фізичного доступу чи відеоспостереження. Якщо стороннє ПЗ має вбудований модуль адміністрування самої системи, то обладнання виробника, який підтримує інтеграцію, зазвичай функціонує без проблем. Контролери в таких випадках часто надаються безкоштовно та доступні у відкритому доступі через інтернет [12].

Окремі виробники пропонують базові версії програмного забезпечення безкоштовно, а розширені функції через платні підписки. Це варто враховувати при плануванні бюджету, аби уникнути непередбачених витрат. Важливо також звернути увагу на якість ПЗ, технічну підтримку та надійність постачальника,

оскільки саме програмне забезпечення є ключовим елементом для ефективного контролю доступу, включно з веденням обліку робочого часу. Хоча ця функція реалізується в більшості систем схожим чином, якість її виконання залежить від конкретної реалізації [13].

1.3 Біометричні складові систем для контролювання доступу

Основою біометрії можна вважати набір методів і технологій, які дозволяють розпізнати людину на основі її унікальних фізіологічних або біологічних характеристик, таких як відбитки пальців, райдужна оболонка ока, риси обличчя або голос.

Основою біометрії можна вважати набір методів і технологій, які дозволяють розпізнати людину на основі її унікальних фізіологічних або біологічних характеристик, таких як відбитки пальців, райдужна оболонка ока, риси обличчя або голос. Це все працює за правилом збору та зберігання цієї біометричної інформації, яка перевіряється з існуючою базою даних кожного разу, коли здійснюється спроба входу в систему. Якщо дані збігаються, доступ дозволяється; якщо даних немає, доступ забороняється. Завдяки високому рівню незмінної якості та складності імітації біометричної інформації, такі системи широко використовуються для контролю доступу до приміщень або інформаційних активів, підвищуючи рівень безпеки та спокою клієнтів. Біометричний ідентифікатор дозволяє швидко і точно підтвердити вашу особу, мінімізуючи небезпеку втручання несанкціонованого доступу до об'єкту [14].

Біометричні системи контролювання доступу знайшли широке застосування у різних сферах, зокрема в корпоративному секторі, освітніх установах, банках, медичних закладах та державних органах. Вони забезпечують надійний доступ лише для уповноважених осіб до обмежених територій, конфіденційної інформації чи критично важливих систем. У контексті

банківських установ, впровадження біометричних технологій дозволяє ефективно регулювати вхід працівників до чітко визначених зон, мінімізуючи ризики несанкціонованого проникнення. Крім того, такі системи сприяють удосконаленню управління персоналом і оптимізації внутрішніх процесів.

Зі зростанням вимог до зручності та швидкості доступу підвищується і потреба в надійнішому захисті. Саме тому біометричні технології можуть стати основою як сучасний підхід до ідентифікації, оскільки вони пропонують високий рівень точності при автентифікації особи. Використання багатофакторної аутентифікації, наприклад, поєднання PIN-коду з розпізнаванням обличчя або відбитків пальців, значно знижує ймовірність обходу системи, зокрема випадків використання чужих документів.

Спеціалізоване програмне забезпечення виконує перевірку документів і автоматично порівнює біометричні дані, зокрема зображення обличчя, із фотографією у документі для підтвердження особи. Для клієнтів банків це відкриває нові можливості, підтвердження транзакцій чи ідентифікація особи за допомогою обличчя, а також підтвердження підпису або виконання операцій через сканування відбитка пальця [14].

Фізична безпека у банківських відділеннях нерідко виявляється вразливою через інтенсивний потік відвідувачів, підвищену ймовірність пограбувань і крадіжок, порушення внутрішніх процедур безпеки, а також використання застарілих систем відеоспостереження. Такі фактори створюють додаткові ризики як для самого банку, так і для його клієнтів. Зокрема, ризики втрати матеріальних та інформаційних ресурсів, несанкціонованого доступу до конфіденційної інформації, а також можливість шахрайських дій викликають серйозне занепокоєння серед клієнтів, що обумовлює необхідність впровадження сучасніших та ефективніших засобів контролю та захисту.

У сучасних умовах банки змушені постійно вдосконалювати свої системи безпеки, впроваджуючи інноваційні технології та автоматизовані рішення. Це дозволяє не лише мінімізувати ризики, а й підвищити довіру клієнтів до

фінансової установи. Важливу роль у цьому відіграє комплексний підхід, що поєднує фізичну, інформаційну та кібербезпеку.

Процедури перевірки особи, підтвердження достовірності даних та автентифікації є складовими частинами процесу KYC (Know Your Customer – Знай свого клієнта). Вони дозволяють банкам ідентифікувати кожного відвідувача, запобігати шахрайству, відмиванню грошей та іншим протиправним діям. Хоча банківські сервіси, що використовують відбитки пальців, і надалі користуються популярністю, цей метод має певні недоліки. Серед них – можливість підробки, потреба у фізичному контакті, енергоспоживання та питання гігієни, особливо в умовах пандемії чи підвищеного ризику поширення інфекцій [15].

Біометричні системи розпізнавання обличь допомагають подолати ці обмеження, забезпечуючи надійніший та зручніший механізм ідентифікації. Вони дозволяють здійснювати безконтактну перевірку особи, що значно пришвидшує обслуговування клієнтів та знижує ризики поширення захворювань. У періоди найбільшого навантаження, коли охоронці не встигають перевірити всіх відвідувачів, такі системи швидко й точно розпізнають особу кожного клієнта незалежно від кількості людей. Вони також підвищують ефективність керування доступом, дозволяють налаштовувати облікові профілі для співробітників і клієнтів, визначати рівні доступу, встановлювати обмеження та створювати контрольні списки, що значно підсилює загальну систему фізичної безпеки банку. Використання унікальних засобів ідентифікації за допомогою відбитків пальців, обличчя або райдужної оболонки ока у критичних інфраструктур, забезпечує швидке та надійне встановлення особи за допомогою біометричних даних, особливо в періоди підвищеної активності. Наприклад, банки використовують біометричні дані для контролю доступу до захищених скриньок, гарантуючи, що тільки уповноважені особи можуть їх відкривати. Коли клієнти відвідують відділення, вони можуть бути верифіковані в робочій зоні, порівнюючи свої відбитки пальців, особливості обличчя або

райдужної оболонки ока з біометричною інформацією, яка вже була зареєстрована і збережена в рамках управління свого рахунка.

Окрім підвищення рівня безпеки, біометричні технології сприяють покращенню клієнтського досвіду. У перспективі біометричні посвідчення можуть розпізнавати звичайних клієнтів на вході, дозволяючи персоналу надавати їм персоналізовані послуги на основі їхньої історії та схильностей. Це відкриває нові можливості для розвитку сервісу, підвищення лояльності клієнтів та оптимізації внутрішніх процесів банку. Більше того, використання сучасних біометричних рішень у поєднанні з аналітичними системами дозволяє банкам виявляти підозрілі дії в режимі реального часу, швидко реагувати на потенційні загрози та ефективно управляти ризиками. Таким чином, інтеграція біометричних технологій у банківську інфраструктуру є не лише вимогою часу, а й важливим кроком до створення безпечного, інноваційного та клієнтоорієнтованого середовища.

Біометрична верифікація також набула популярності на банкоматах у багатьох розвинених країнах. Кілька банків запровадили унікальну функцію розпізнавання відбитків пальців у своїх банкоматах, що дозволяє клієнтам прив'язувати відбитки пальців до своїх рахунків. У банкоматі клієнт по суті прикладає палець до біометричного датчика, який зчитує унікальний відбиток пальця і порівнює його з інформацією, щоб підтвердити особу. Після підтвердження особи клієнт може здійснювати такі операції, як зняття готівки або оплата чеків, без використання фізичної картки або ПІН-коду. Ця стратегія пропонує корисний, точний і компактний механізм підтвердження особи, який добре підходить для використання в таких середовищах [16].

Біометричні системи контролювання доступу підвищують рівень безпеки завдяки використанню унікальних фізичних або поведінкових ознак особи, зокрема відбитків пальців, зображення обличчя чи голосових характеристик. На відміну від традиційних способів ідентифікації, біометричні методи забезпечують швидку, точну та індивідуальну перевірку, яка не може бути

передана іншій особі. Завдяки цьому біометрія широко впроваджується у сферах бізнесу, освіти та фінансів для запобігання несанкціонованому доступу.

У порівнянні зі стандартними системами доступу, біометричні технології вважаються надійнішими та ефективнішими через унікальність біометричних параметрів кожної людини. Це дозволяє значно зменшити ймовірність стороннього проникнення, що робить такі рішення актуальними для сучасних систем безпеки. Основні переваги біометричних систем включають:

– підвищений рівень захисту – біометрична аутентифікація демонструє вищу ефективність порівняно з паролями, ПІН-кодами чи пластиковими картками, оскільки базується на неповторних характеристиках кожної особи, що знижує ризик несанкціонованого доступу;

– високий ступінь надійності – на відміну від даних, які легко загубити або вкрасти, біометричні ознаки важко відтворити або підробити, що робить їх потужним засобом захисту;

– зручність для користувачів – немає потреби запам’ятовувати складні паролі чи носити фізичні пристрої, доступ відбувається за допомогою простого сканування обличчя або пальців;

– швидкодія – процес ідентифікації займає лічені секунди, що особливо корисно в умовах великої прохідності;

– економічна вигода – у довгостроковій перспективі такі системи зменшують витрати на адміністративне обслуговування, як-от відновлення доступу чи заміна карток;

– прозорість і моніторинг – біометричні системи фіксують усі спроби доступу, що покращує контроль і дозволяє детально відстежувати дії користувачів;

– гнучкість і масштабування – біометричні рішення легко адаптуються до великої кількості користувачів і можуть бути інтегровані з іншими безпековими системами, такими як відеонагляд або сигналізація [17].

Біометричні рішення у системах контролювання доступу поділяються на три основні типи: динамічні, статичні та мультимодальні. Динамічні системи розпізнають особу за характером рухів або поведінковими ознаками, тоді як статичні використовують незмінні фізіологічні характеристики для підтвердження особистості. Мультимодальні системи поєднують обидва підходи, що дозволяє значно підвищити рівень безпеки завдяки використанню кількох методів ідентифікації. Окрім цього, існує кілька варіантів реалізації таких систем:

– технологія розпізнавання обличь ґрунтується на обробці індивідуальних рис, таких як відстань між очима, форма носа та контури підборіддя, із використанням фотографій або відеозображень;

– сканування райдужної оболонки та сітківки полягає у фіксації унікальних структур, як-от візерунків райдужної оболонки чи розміщення кровоносних судин на сітківці, що здійснюється за допомогою інфрачервоного випромінювання;

– ідентифікація за відбитками пальців передбачає зіставлення характерних елементів, зокрема ліній папілярного візерунка, їх перетинів та розгалужень;

– технологія виявлення венозного малюнка використовує індивідуальну схему вен на пальцях або зап’ясті як основу для автентифікації;

– визначення особи за геометрією руки базується на вимірюванні її форми, пропорцій та довжини окремих ділянок;

– динамічний аналіз підпису враховує не лише його візуальне зображення, але й силу натискання, темп написання та напрям руху руки під час підписування;

– система розпізнавання голосу проводить автентифікацію за тембром, тоном і мовними особливостями, пов’язаними з анатомічними характеристиками голосового апарату;

– та інші перспективні біометричні методи, зокрема ідентифікація за формою вушної раковини, аналіз ДНК або визначення за запахом тіла, наразі активно вивчаються з метою їх майбутнього впровадження в галузі безпеки [18].

Існують складнощі та проблемні моменти, які слід враховувати і вміти контролювати. Передусім, це питання забезпечення безпеки та захисту біометричної інформації, оскільки недобросовісне зберігання або використання може призвести до витоку інформації та зниження довіри або спроб шахрайства шляхом підробки біометричних даних. Крім того, зовнішні змінні, такі як освітлення, температура або перебування клієнтів, можуть впливати на роботу систем, що може знизити точність і стабільність якості розпізнавальних ознак. Вкрай важливо гарантувати доступність і зручність для всіх категорій осіб, беручи до уваги можливі фізичні перешкоди. Впровадження таких систем при розширенні зазвичай пов'язане з високими початковими витратами та складністю інтеграції в існуючий фундамент. Крім того, важливо забезпечити джерела живлення, оскільки біометричні гаджети залежать від електроенергії. Таким чином, ефективне використання біометричного доступу до контролю вимагає ретельної організації та продумування таких змінних, щоб гарантувати адекватність і безпеку системи [19].

Окрім переваг, існує низка важливих моментів. Попри стрімкий розвиток біометричних технологій, зловмисники продовжують знаходити способи використання їхніх слабких місць для отримання несанкціонованого доступу до персональних даних користувачів. Зокрема, технологія deepfake створює додаткові загрози, оскільки здатна обманювати системи біометричної ідентифікації, ускладнюючи відрізнення справжньої особи від її цифрової підробки. Окрему складність становлять правові аспекти – вимоги до збирання, зберігання та обробки біометричної інформації суттєво відрізняються в різних країнах, але зазвичай є суворими. Банківські установи повинні чітко дотримуватись цих регламентів і гарантувати відповідність нормам захисту

персональних даних, що часто потребує значних витрат часу, коштів і зусиль [20].

Питання інтеграції штучного інтелекту в системи біометричної автентифікації набуває дедалі більшої актуальності, адже завдяки розвитку ШІ та технологій машинного навчання ці системи стають більш розумними та ефективними. Серед ключових інновацій – розпізнавання обличчя в реальному часі за допомогою ШІ, безконтактні методи автентифікації, які сприяють підвищенню рівня гігієни та безпеки, а також впровадження хмарних платформ для дистанційної ідентифікації користувачів. Додатково набирає популярності багатофакторна автентифікація, яка поєднує біометричні дані з іншими способами перевірки для посилення рівня захисту.

Однак, попри очевидні переваги, використання штучного інтелекту в цих системах викликає занепокоєння щодо дотримання конфіденційності та етичного використання персональних даних. Для мінімізації ризиків організаціям необхідно впроваджувати відкриті та зрозумілі політики управління даними і суворо дотримуватися стандартів захисту інформації. Водночас ШІ відіграє ключову роль у виявленні загроз у режимі реального часу, автоматизації процесів спостереження та підвищенні загальної ефективності безпекових систем, що робить його важливим елементом сучасних біометричних рішень [21].

1.4 Постановка задачі

Суть цього проекту полягає у створенні надійної та захищеної системи контролювання доступу до приміщення фінансової установи, з використанням сучасних методів біометричної ідентифікації. Така система повинна гарантувати високий рівень безпеки як фізичних об'єктів, так і інформаційних активів компанії, а також враховувати небезпеки, пов'язані з людським фактором, постійно виникаючими кіберзагрозами та порушеннями внутрішнього порядку.

Основними задачами є:

– провести аналіз сучасних загроз інформаційній та фізичній безпеці банківських установ;

– дослідити існуючі рішення в галузі систем контролювання доступу, зокрема ті, що базуються на біометричних технологіях;

– сформувати вимоги до системи доступу з урахуванням особливостей об’єкта (відділення банку);

– здійснити вибір та обґрунтування найбільш доцільних біометричних пристроїв (відбитки пальців, розпізнавання обличчя тощо);

– спроектувати модель контролю доступу в середовищі банківського приміщення із зазначенням розміщення компонентів;

– розробити архітектуру та програмну конфігурацію системи, що включає апаратні засоби, програмне забезпечення та засоби моніторингу;

– провести моделювання й експериментальну перевірку системи у віртуальному або тестовому середовищі;

– здійснити оцінку ефективності роботи системи, її надійності та зручності в експлуатації;

– надати рекомендації щодо впровадження системи у практичних умовах банківської інфраструктури.

2 ПОШУК СУЧАСНИХ РІШЕНЬ

2.1 Підбір апаратного забезпечення для систем

Біометричні пристрої стрімко набирають популярності як засіб ідентифікації та автентифікації особи завдяки використанню унікальних фізіологічних та поведінкових характеристик. Серед основних методів, які застосовуються в таких пристроях, розпізнавання відбитків пальців, обличчя, сканування вен долоні, райдужної оболонки ока, а також ідентифікація за голосом. Залежно від способу зчитування інформації, біометричні пристрої поділяються на контактні, що потребують фізичного дотику, безконтактні, які працюють на відстані та гібридні або комбіновані, що поєднують кілька методів для підвищення точності й надійності автентифікації [22].

Інфрачервона термографія (розпізнавання обличчя, рук або вен на руках): Інфрачервоні камери можуть фіксувати теплові візерунки, що випромінюються людським тілом, наприклад, обличчям або руками. Вважається, що ці теплові візерунки є унікальними для кожної людини. Хоча цей метод є неінвазійним, отримання високоякісних зображень може бути складним, якщо поблизу є інші джерела тепла. Він особливо підходить для прихованої ідентифікації. Схожа техніка, що використовує зображення в діапазоні ближнього інфрачервоного випромінювання, аналізує теплові візерунки рук, особливо на тильній стороні кулака, які також вважаються унікальними. Як і розпізнавання обличчя, цей метод повинен враховувати тривимірну форму та орієнтацію руки. Однак одним із недоліків є висока вартість інфрачервоних датчиків.

Геометрія руки передбачає вимірювання відносних розмірів пальців, положення суглобів, а також форми і розміру долоні. Це була одна з перших біометричних технологій, яка була автоматизована, а системи, що з'явилися в кінці 1960-х років, використовувалися протягом майже двох десятиліть. Ця техніка проста, зручна у використанні та економічно ефективна. На відміну від деяких біометричних методів, на неї не впливають суха погода або стан шкіри.

Однак геометрія руки не є достатньо характерною для ідентифікації осіб у великих групах населення і краще підходить для цілей верифікації. Вона також може бути ненадійною для дітей через їхній ріст і може залежати від фізичних обмежень, протезів або аксесуарів, таких як кільця.

Розпізнавання відбитків пальців відбувається з використанням унікальних візерунків рельєфів і впадин, розташованих на кінчиках пальців, і використовуються для ідентифікації протягом століть завдяки своїй високій точності. Раніше ці візерунки збиралися за допомогою відбитків чорнилом, але сьогодні компактні датчики цифровим способом фіксують зображення відбитків пальців шляхом прямого контакту. Деякі датчики можуть перевіряти такі характеристики, як температура і пульс. З часом контактні датчики можуть забруднитися або зноситися, що впливає на їхню роботу. Твердотільні датчики відбитків пальців вирішують багато з цих проблем, використовуючи електричну ємність для виявлення візерунків рельєфів і створення точних цифрових зображень. Сучасні сканери відбитків пальців зараз широко доступні і недорогі. У системах перевірки в режимі реального часу витяг ознак ідентифікує ключові дрібні деталі конкретні закінчення рельєфів і розгалуження розташування і орієнтація яких використовуються для порівняння із збереженими шаблонами. Однак сучасні системи розпізнавання відбитків пальців часто вимагають значних обчислювальних ресурсів.

Розпізнавання обличчя використовує здатність людини ідентифікувати осіб за рисами обличчя, що робить його популярним та інтуїтивним біометричним методом. Він є неінтрузивним і добре підходить для прихованих застосувань. Його використання варіюється від статичних зображень до динамічного розпізнавання в реальному часі в складних середовищах, таких як аеропорти або метро. Процес включає вилучення ознак з двовимірного зображення та порівняння їх із збереженим шаблоном. Техніки зазвичай базуються або на аналізі орієнтирів обличчя, очі, ніс, рот тощо, та їх просторовому розташуванні, або на глобальному аналізі з використанням математичних моделей, які

представляють обличчя як комбінації стандартних шаблонів. Хоча комерційні системи пропонують прийнятну продуктивність, вони все ще стикаються з проблемами змінного освітлення, змін орієнтації обличчя та міміки. Сучасні системи часто демонструють рівень помилкового відхилення близько 10% та рівень помилкового прийняття близько 1%. Розпізнавання обличь з різних кутів або при нестабільному освітленні було технічною проблемою, як і досягнення високого рівня впевненості при ідентифікації осіб з великих груп населення та з прогресом цих технологій в додаток використовують інфрачервоні камери та другу камеру що зміщена в бік та дає отримати інформацію про глибину зображення. Динамічний та виразний характер людського обличчя або якась маска, додає ще більшої складності для розпізнавання.

Розпізнавання сітківки ока передбачає зчитування унікального судинного малюнка сітківки, створюючи «підпис оком», який є унікальним для кожної людини і для кожного ока. Оскільки сітківка знаходиться всередині ока і її неможливо легко змінити або відтворити, цей метод вважається однією з найбезпечніших біометричних технологій. Однак для зчитування зображення сітківки необхідно, щоб об'єкт дивився через лінзу на фіксовану точку, що вимагає безпомилковості в діях. Крім того, оскільки сканування сітківки може виявити певні медичні стани, можуть виникнути занепокоєння щодо конфіденційності користувачів та прийняття суспільством.

Розпізнавання райдужної оболонки ока є однією з найточніших і найнадійніших біометричних технологій, що базується на унікальній та складній текстурі райдужної оболонки, яка містить численні особливості, такі як стрічки, гребені, заглиблення, кільця, німб, плями та зигзагоподібні комірці. Ці деталі формують унікальний візерунок, який практично неможливо підробити або повторити, що робить розпізнавання райдужної оболонки надзвичайно ефективним засобом ідентифікації особи. На відміну від сканування сітківки ока, яке вимагає близького контакту та спеціального обладнання, розпізнавання райдужної оболонки є менш проблематичним, оскільки райдужна оболонка

знаходиться зовні ока і може бути сканована на відстані, що підвищує комфорт і швидкість процедури. Особливою перевагою цього методу є те, що реакція райдужної оболонки на світло може служити додатковою перевіркою на життєздатність, гарантуючи, що зображення належить живій людині, а не фотографії чи штучному об'єкту. Цікаво, що навіть близнюки мають унікальні, відмінні візерунки райдужної оболонки, що робить цю технологію винятково надійною для точного розпізнавання. Сучасні сканери райдужної оболонки стали значно доступнішими та зручнішими у використанні, проте для отримання високоякісного зображення все ще необхідний точний контроль освітлення, фокусування, роздільної здатності та контрасту, що є важливими факторами для забезпечення максимальної точності ідентифікації. Хоча візерунки райдужної оболонки залишаються стабільними протягом усього дорослого життя, вони можуть дещо змінюватися в дитячому віці, що слід враховувати при використанні цієї технології для ідентифікації дітей.

Відбитки долонь, так само як і відбитки пальців, складаються з унікальних візерунків ровів і долин на поверхні долоні, що формують індивідуальний біометричний код кожної людини. Завдяки значно більшій площі долоні порівняно з пальцями, розпізнавання відбитків долонь може бути навіть більш надійним і точним, оскільки охоплює більшу кількість унікальних деталей. Однак для цього потрібні більш досконалі та дорогі сканери, здатні знімати зображення з високою роздільною здатністю, що забезпечує точне відтворення всіх дрібних деталей рельєфу. Сучасні системи розпізнавання долонь часто поєднують кілька біометричних ознак, таких як геометрія руки, основні лінії, зморшки та інші деталі рельєфу, що значно підвищує точність і надійність ідентифікації. Такий комплексний підхід дозволяє зменшити ймовірність помилкових спрацьовувань і підвищити рівень безпеки, особливо в умовах, де потрібна висока точність ідентифікації.

Використання голосу людини як біометричного параметра базується на унікальних фізичних характеристиках голосового апарату, таких як форма

голосового тракту, рот, носові ходи та губи, які формують індивідуальний тембр і звучання голосу. Хоча анатомічні аспекти голосового апарату залишаються відносно стабільними протягом життя, поведінкові характеристики голосу, такі як висота, тон, темп мовлення, можуть змінюватися залежно від віку, стану здоров’я, емоційного стану або навіть зовнішніх факторів. Системи розпізнавання голосу зазвичай поділяються на два основні типи: автоматична верифікація мовця, яка служить для підтвердження особи, та автоматична ідентифікація мовця, що спрямована на визначення, хто саме говорить. Для ефективної роботи таких систем необхідно записати голос суб’єкта під час реєстрації, часто протягом кількох сеансів, щоб врахувати природні варіації голосу. Процес виділення ознак у голосі зосереджується на формантах — характерних частотах мовлення, які є унікальними для кожної людини, а алгоритми зіставлення цих ознак мають багато спільного з тими, що використовуються у системах розпізнавання обличчя, що дозволяє досягати високої точності ідентифікації. Використання голосу як біометричного параметра є особливо зручним для безконтактної ідентифікації та аутентифікації, що робить його популярним у системах дистанційного доступу, телефонного банкінгу та інших сферах, де важлива швидкість і простота використання. Водночас, через можливі коливання голосу, системи розпізнавання голосу часто доповнюють іншими біометричними методами для підвищення надійності та безпеки. Таким чином, розпізнавання райдужної оболонки ока, відбитків долонь і голосу є потужними інструментами сучасної біометрії, кожен з яких має свої унікальні переваги та особливості, що дозволяють ефективно застосовувати їх у різних сферах безпеки та ідентифікації.

Також як варіантом біометрії, можливо віднести підпис. Він відобразить характерний, індивідуальний спосіб, у який людина підписує своє ім'я, що робить його поведінковою біометричною характеристикою. Він формується під впливом геометрії руки та нейром'язових звичок. Розпізнавання підпису вимагає активної участі та письмового приладдя. Хоча зразки підписів можуть

змінюватися з часом через такі фактори, як старіння або емоційний та фізичний стан, біометричні системи можуть виходити за межі візуального вигляду підпису, аналізуючи тиск, швидкість руху та стиль підписання. Ці динамічні особливості можуть допомогти підвищити точність і зменшити ризик підробки [23].

У поєднанні з аналітичними алгоритмами та системами відеоспостереження такі рішення забезпечують комплексну, багаторівневу безпеку, здатну протистояти сучасним викликам у сфері фізичного та інформаційного захисту. Для обґрунтування вибору оптимальних біометричних технологій у роботі було проведено порівняльний аналіз основних методів ідентифікації, результати якого наведено в таблиці 2.1. У ній оцінюються ключові характеристики для методів. Це дозволяє візуально визначити переваги кожного підходу та зробити обґрунтований вибір відповідно до потреб банківської установи.

Таблиця 2.1 – Оцінка методів біометрії

Біометрична характеристика	Універсальність	Унікальність	Стабільність	Вимірюваність	Ефективність	Прийнятність	Підробка
Інфрачервона термографія	H	H	L	H	M	H	L
Форма руки	M	M	M	H	M	M	M
Відбиток пальця	M	H	H	M	H	M	M
Лице	H	L	M	H	L	H	H
Сітківка	H	H	M	L	H	L	L
Райдужна оболонка	H	H	H	M	H	L	L
Відбиток долоні	M	H	H	M	H	M	M
Голос	M	L	L	M	L	H	H
Підпис	L	L	L	H	L	H	H

Контактні біометричні пристрої, це засоби ідентифікації, які потребують фізичного дотику для зчитування біометричних характеристик. Найчастіше вони

використовуються для зняття відбитків пальців або долоні за допомогою спеціальних електронних сенсорів. На ринку можна виділити три основні типи таких пристроїв: сканери відбитків пальців, сканери долонь і пристрої для аналізу геометрії руки. Найбільш поширеними серед них є сканери відбитків пальців, які представлені у двох основних варіантах: оптичні та ємнісні. Оптичні сканери, що зображені на Рис. 2.1, працюють на основі світлової технології і вони освітлюють палець світлодіодами, а потім фіксують зміни у відбитому світлі, перетворюючи ці сигнали в цифрові дані для подальшої обробки.

Рисунок 2.1 – Оптичні сканери відбитків пальців

Ємнісні сканери відбитків пальців працюють за принципом вимірювання змін електричного струму, які виникають внаслідок різної електропровідності шкіри. У таких пристроях використовуються ємнісні датчики, що фіксують відмінності між гребенями та борознами на поверхні пальця, формуючи точну цифрову карту відбитка. На відміну від оптичних сканерів, які зчитують

візуальне зображення за допомогою світла, ємнісні пристрої забезпечують вищий рівень точності та безпеки, оскільки складніше підробити електричні характеристики шкіри [24].

Сканери відбитків пальців є одним із найбільш усталених типів біометричних пристроїв, які широко застосовуються для ідентифікації та верифікації особи в різних сферах — від оформлення посвідчень особи, участі у виборах, банківських операцій до реєстрації SIM-карт та захисту в кіберпросторі. Вони є ефективним засобом боротьби з шахрайством, оскільки сучасні системи здатні виявляти спроби використання підроблених відбитків за допомогою технологій розпізнавання «живої» тканини. У зв’язку з пандемією зросла потреба в безконтактних рішеннях, тому на ринку з’явилися сканери, які дозволяють проводити автентифікацію без фізичного контакту, забезпечуючи вищий рівень гігієни та безпеки [25].

Сканери долонь, у свою чергу, є різновидом контактних біометричних пристроїв. Вони зчитують зображення всієї поверхні долоні за допомогою оптичних сенсорів і використовують його для підтвердження особи. За принципом роботи вони подібні до сканерів відбитків пальців, але охоплюють більшу площу, що дозволяє збирати більше унікальних біометричних даних. Саме здійснює ідентифікацію особи шляхом зчитування унікальних біометричних характеристик, зокрема венозного малюнка на долоні, та зіставлення їх із заздалегідь збереженими шаблонами в базі даних. Такі технології з’явилися на початку 2000-х років і знайшли широке застосування в об’єктах з підвищеними вимогами до безпеки наприклад, у державних установах, критичних інфрукструктурах і на військових об’єктах [26].

Сканери геометрії рук використовуються для ідентифікації людей шляхом вимірювання розміру та форми їхніх рук. Ці пристрої мають пластину з вбудованими штифтами, які направляють положення людської руки для досягнення найкращих результатів. Після того, як розміщується рука, камери з зарядовим зв'язком роблять її зображення, яке потім порівнюється з шаблоном,

що зберігається в пам'яті пристрою. Якщо біометричні дані геометрії руки збігаються з шаблоном, пристрій розблокується. Пристрої геометрії руки використовуються в різноманітних системах біометричної автентифікації та додатках, включаючи, але не обмежуючись ними: перевірка ідентифікації, облік робочого часу та відвідування, а також контроль фізичного доступу [27].

Безконтактні біометричні пристрої можуть знімати біометричні дані без необхідності фізичного контакту. Ці пристрої можна розділити на три типи, які широко доступні на ринку [16]:

– термінали розпізнавання обличчя;

– сканери райдужної оболонки ока;

– сканери вен на долоні.

На теперішній час термінали розпізнавання обличчя можуть бути найбільш широко використовуваним безконтактним біометричним пристроєм [28].

Термінали для розпізнавання обличь є одними з найсучасніших і найефективніших засобів біометричної ідентифікації, які використовують спеціалізовані камери, зокрема високодинамічні або інфрачервоні, для точного зчитування зображення обличчя користувача. Ці пристрої здатні фіксувати ключові риси обличчя, такі як очі, ніс, рот, а також кольорові характеристики шкіри, що дозволяє створювати унікальний біометричний профіль кожної особи. Під час проходу людини повз термінал система в режимі реального часу автоматично сканує обличчя, використовуючи складні алгоритми для виявлення та аналізу цих рис [29]. Отримане зображення проходить обробку, під час якої алгоритми розпізнавання зіставляють виявлені риси з базою даних збережених шаблонів, що дозволяє оперативно ідентифікувати або верифікувати особу. Якщо система знаходить відповідність між сканованим обличчям і записаним шаблоном, користувачу надається доступ до контрольованої зони або ресурсу.

Сучасні моделі біометричних терміналів, такі як Aratek BA8300, пропонують розширені функції, поєднуючи розпізнавання облич з можливістю зчитування безконтактних RFID-карток. Така комбінація забезпечує додатковий

рівень безпеки завдяки двофакторній автентифікації, що значно ускладнює несанкціонований доступ і гарантує, що лише уповноважені користувачі можуть потрапити до захищених приміщень або зон. Цей підхід особливо ефективний у банках, офісних комплексах, промислових підприємствах та інших об'єктах, де необхідно суворо контролювати доступ і мінімізувати ризики проникнення сторонніх осіб. Поєднання двох незалежних методів ідентифікації значно підвищує надійність системи і знижує ймовірність помилкових спрацьовувань.

Пандемія COVID-19 сприяла значному зростанню популярності терміналів розпізнавання облич, оскільки вони дозволяють здійснювати ідентифікацію без фізичного контакту, що є важливим для запобігання поширенню інфекцій. У відповідь на нові виклики багато виробників додали до своїх пристроїв інфрачервоні сенсори для безконтактного вимірювання температури тіла, а також алгоритми, здатні визначати наявність захисних масок на обличчі користувача. Ці функції перетворили біометричні термінали на комплексні рішення для безпечного контролю доступу до приміщень, що дозволяють оперативно виявляти потенційно інфікованих осіб і знижувати ризики поширення захворювань у громадських і робочих просторах. Завдяки цьому такі системи стали незамінними в медичних установах, навчальних закладах, транспортних вузлах, торговельних центрах та інших місцях скупчення людей, де важливо швидко і точно контролювати стан здоров'я відвідувачів і співробітників. Крім того, сучасні термінали оснащені функціями антивандального захисту, підтримкою роботи в різних кліматичних умовах і можливістю інтеграції з іншими системами безпеки, такими як відеоспостереження, охоронна сигналізація та системи керування доступом. Це робить їх універсальними і ефективними інструментами для комплексного забезпечення безпеки в різних сферах діяльності. З огляду на постійний розвиток технологій штучного інтелекту та машинного навчання, алгоритми розпізнавання облич стають все більш точними, швидкими і стійкими до спроб обману, що відкриває нові перспективи для їх застосування у майбутньому. Таким чином, термінали

розпізнавання облич є не лише зручним і безпечним засобом ідентифікації, а й важливим елементом сучасних систем безпеки, що відповідають вимогам часу та забезпечують високий рівень захисту персональних даних і об’єктів.

2.2 Переваги та недоліки наявних компонентів, вибір надійного рішення

Переваги та недоліки наявних компонентів систем контролю доступу, а також вибір надійного рішення значною мірою залежать від типу системи, її складності, вартості, а також від специфіки об’єкта, де вона впроваджується. Сучасна система контролювання доступом складається з кількох ключових компонентів, кожен із яких має свої особливості, що впливають на загальну ефективність і надійність системи.

Запобіжний пристрій, такий як двері або турнікет з електромагнітним замком, є фізичним бар’єром, що безпосередньо обмежує доступ до контрольованої зони. Перевагою таких пристроїв є їхня надійність і відносна простота експлуатації, а також можливість інтеграції з різними системами безпеки. Водночас, недоліком може бути необхідність регулярного технічного обслуговування, а також вразливість до фізичних пошкоджень або спроб злому, якщо не передбачені додаткові заходи захисту.

Індивідуальні ідентифікатори, такі як картки або брелоки, забезпечують зручний і швидкий спосіб ідентифікації користувачів. Вони відрізняються простотою використання і можуть бути легко видані або анульовані у разі потреби. Однак такі носії інформації можуть бути втрачені, викрадені або скопійовані, що створює потенційні ризики для безпеки. Для зниження цих ризиків часто застосовують двофакторну автентифікацію, поєднуючи ідентифікатори з біометричними даними або PIN-кодами.

Зчитувачі, які отримують інформацію з ідентифікаторів і передають її на контролер, є важливим технічним елементом системи. Їхня точність, швидкість

роботи та здатність коректно зчитувати різні типи носіїв визначають зручність і ефективність контролю доступу. Перевагою сучасних зчитувачів є підтримка безконтактних технологій (RFID, NFC, BLE), що забезпечує швидке і гігієнічне зчитування даних. Недоліком може бути їхня чутливість до зовнішніх перешкод або спроб підробки сигналу, що вимагає використання додаткових засобів захисту.

Контролер системи, який є мозком СКД, відповідає за обробку отриманої інформації, зіставлення її з базою даних і прийняття рішення про надання або відмову у доступі. Надійність, швидкість роботи та можливість масштабування контролера визначають загальну продуктивність системи. Сучасні контролери підтримують інтеграцію з іншими системами безпеки, ведення журналів подій, а також дистанційне адміністрування. Саме контролер або панель управління обробляє інформацію, яку отримує від зчитувачів, порівнює її з базою даних дозволених користувачів, а у разі позитивного збігу активує виконавчий механізм, зокрема електрозамок. Залежно від масштабу об'єкта, вимог до безпеки, зручності обслуговування та бюджету обираються різні типи контролерів. У виборі варто враховувати не лише технічні характеристики, а й можливість майбутнього масштабування, простоту монтажу та підтримку сучасних технологій. Однак складність налаштувань і необхідність кваліфікованого обслуговування можуть стати викликом для невеликих організацій.

Одним із базових варіантів є компактні контролери-зчитувачі, які поєднують функції зчитування та обробки даних в одному пристрої. Вони відзначаються простотою інсталяції, підтримкою безконтактної ідентифікації через смартфони та живленням по технології PoE, що спрощує прокладку кабелів. Подібні рішення, що можна оглянути на рис. 2.2, добре підходять для невеликих об’єктів або віддалених точок доступу, де не потрібна підтримка розширених функцій. Однак варто врахувати, що такі пристрої зазвичай не підтримують біометричні зчитувачі, не інтегруються з ліфтами чи камерами

відеоспостереження та потребують ліцензованого хмарного ПЗ для повноцінного адміністрування.

Рисунок 2.2 – Система контролювання доступу з автономними контролерами

Наступним рівнем стають мережеві контролери-хаби, які можуть одночасно підтримувати декілька зчитувачів (зазвичай до чотирьох) та мають вбудоване програмне забезпечення для керування доступом. Їх перевагою є легка масштабованість, кілька таких пристроїв можуть бути з’єднані у мережу для управління десятками точок входу що зображено у рис. 2.3. Вони забезпечують базовий функціонал адміністрування, зручний веб-інтерфейс, а також можливість живлення по PoE і зв'язок через Wi-Fi. Утім, такі контролери все ще мають обмежену підтримку складних сценаріїв, не працюють з Active Directory,

не забезпечують інтеграцію з відеоспостереженням і не реалізують антипрохід чи багатоступеневу авторизацію.

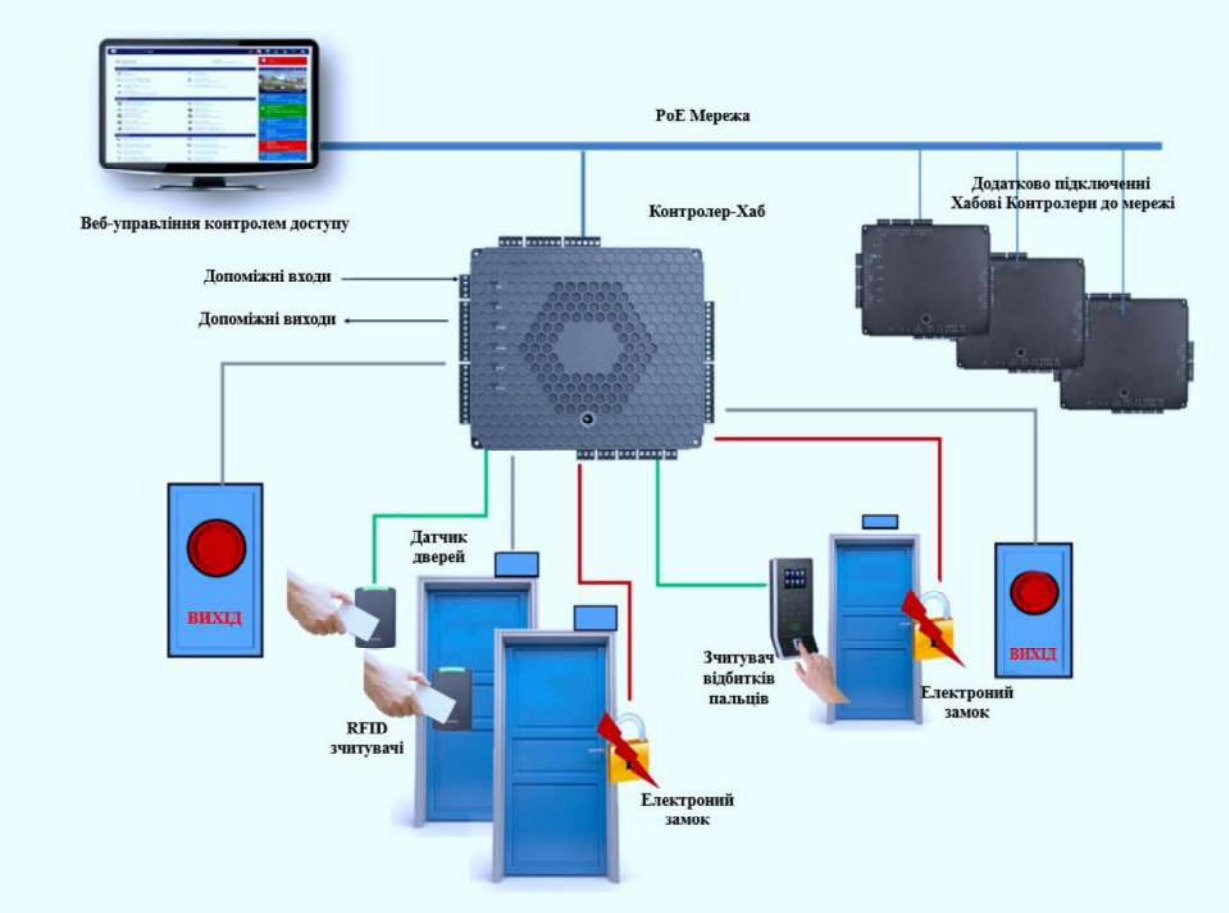


Рисунок 2.3 – Система контролювання доступу з хаб-контролерами

Для об'єктів з підвищеними вимогами до функціоналу варто розглядати контролери професійного-рівня. Це повнофункціональні пристрої, які підтримують широкий спектр зчитувачів: карткових, біометричних (відбиток пальця, розпізнавання обличчя, долоні), Bluetooth, QR-кодів. Вони дозволяють реалізувати складні логічні сценарії: обмеження доступу за часом, подвійна ідентифікація, створення шаблонів пропусків, індивідуальні права на користування ліфтом, PIN-коди для екстрених ситуацій. Такі контролери зазвичай вимагають окремого живлення, хоча існують адаптери для використання PoE. Вони інтегруються з професійними системами відеонагляду, підтримують централізоване програмне забезпечення, надають розширену

звітність та аудит. Варто враховувати, що для використання усіх можливостей таких рішень необхідно придбати окрему ліцензію на керуюче ПЗ.

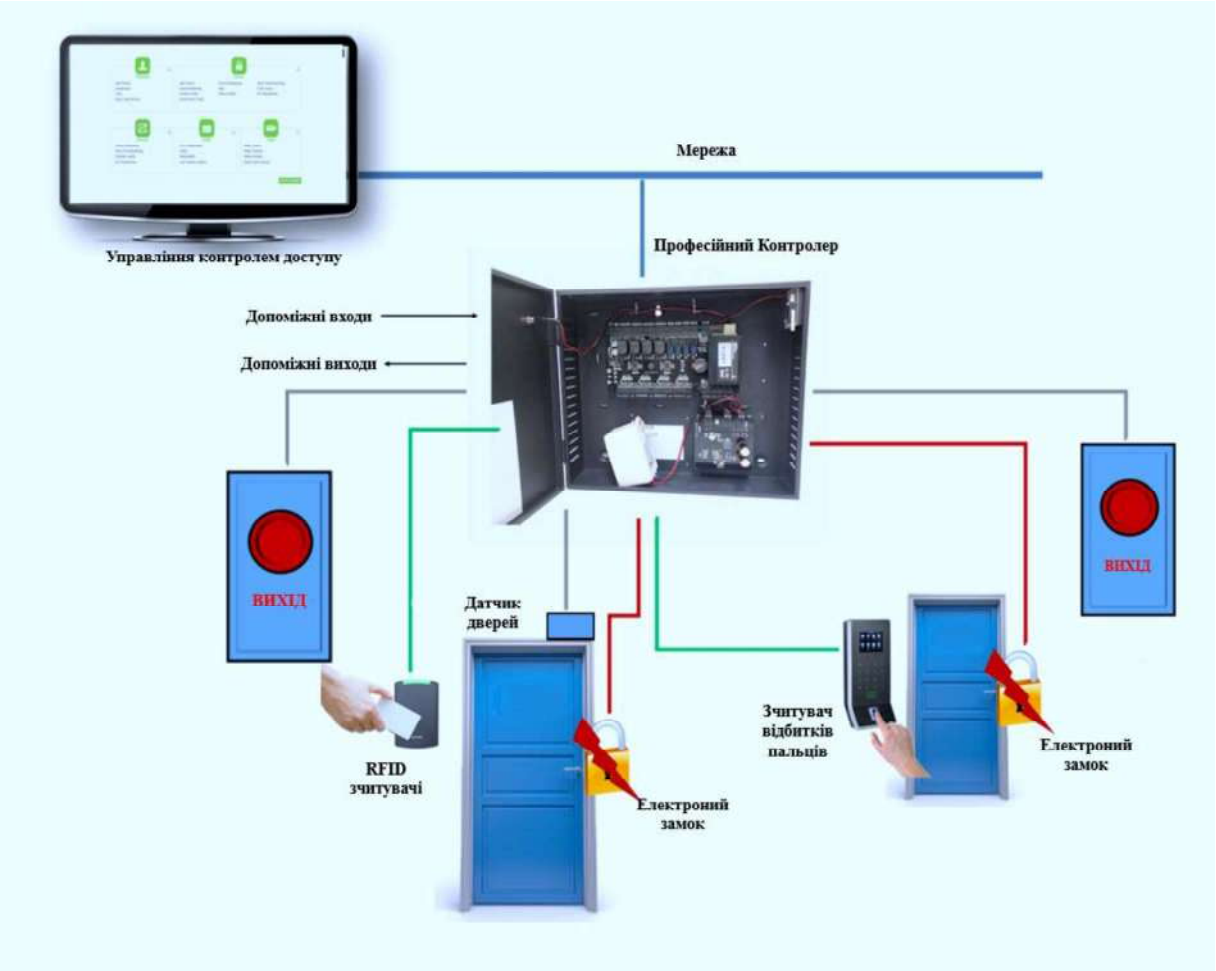


Рисунок 2.4 – Система контролювання доступу з про-контролером

Ще одним гнучким і сучасним варіантом є модульні підприємницький-контролери, які встановлюються безпосередньо біля дверей та об'єднуються у мережу. Завдяки своїй децентралізованій природі, кожен такий пристрій може зберігати локальну базу користувачів і працювати незалежно у разі втрати зв’язку з сервером. Вони підтримують смартфоні зчитувачі нового покоління, розпізнавання жестів, доступ без дотику або на відстані. Однією з переваг є можливість поступового розширення системи за потреби можна додати лише один новий пристрій без суттєвої перебудови всієї інфраструктури. Адміністрування здійснюється через будь-який браузер та більшість сучасних

пристроїв, що зручно для віддаленого доступу. Додатково підтримується інтеграція з Active Directory, управління ліфтами, сценарії дій з тригерами, розгалужені логіки реагування на події (наприклад, надсилання SMS або HTTP-запитів). Незважаючи на функціональну насиченість, такі контролери, як правило, не підтримують біометричні зчитувачі, а для використання повноцінного корпоративного ПЗ також потрібна ліцензія [30].

Додаткові опції, такі як камери для фотоверифікації, датчики положення дверей, пристрої для фіксації факту проходу та інші сенсори, значно підвищують функціональність і безпеку системи. Вони дозволяють не лише контролювати доступ, а й вести моніторинг подій у реальному часі, автоматично реагувати на спроби несанкціонованого проникнення, а також документувати інциденти для подальшого аналізу. Водночас додаткове обладнання збільшує вартість системи і складність її обслуговування, що слід враховувати при виборі рішення. Вибір надійного рішення для системи контролювання доступу повинен базуватися на комплексному аналізі потреб конкретного об’єкта, враховувати кількість точок доступу, рівень необхідної безпеки, бюджетні обмеження та можливості технічної підтримки.

Для великих підприємств з високими вимогами до безпеки оптимальними будуть мережеві системи з централізованим управлінням і широкими можливостями інтеграції. Для невеликих офісів або об’єктів з обмеженим бюджетом більш доцільними є автономні системи, які простіші у встановленні та експлуатації. Біометричні системи, хоча й дорогі, забезпечують найвищий рівень захисту і можуть бути рекомендовані для об’єктів із підвищеними вимогами до безпеки. Важливо також звертати увагу на сумісність компонентів, можливість масштабування системи в майбутньому, а також наявність якісної технічної підтримки від виробника чи інтегратора. Таким чином, правильний вибір системи контролювання доступу є ключовим фактором для забезпечення надійного захисту, ефективного управління доступом і зручності експлуатації.

Мережеві системи контролювання доступу є одними з найпотужніших і найгнучкіших рішень у сфері безпеки, особливо призначеними для великих підприємств, офісних комплексів, виробничих майданчиків та інших об’єктів із високими вимогами до контролю доступу. Основна перевага таких систем полягає в їхній здатності працювати через центральний сервер із відповідним програмним забезпеченням, що забезпечує централізоване управління всіма точками доступу в режимі реального часу. Це дозволяє не лише контролювати і регулювати доступ, а й вести детальний архів подій, який включає збереження фото- та відеоматеріалів, що є надзвичайно важливим для розслідування інцидентів, аудиту безпеки та звітності. Завдяки такій централізації адміністратори можуть оперативно реагувати на будь-які порушення, змінювати налаштування доступу, додавати або видаляти користувачів, а також інтегрувати систему з іншими підсистемами безпеки, такими як відеоспостереження, пожежна сигналізація, охоронна система або системи контролю робочого часу.

Сучасні мережеві СКД часто оснащені додатковими функціями, які значно підвищують їхню ефективність і зручність. Зокрема, підтримка технологій розпізнавання облич (Face ID) дозволяє здійснювати безконтактну та швидку ідентифікацію користувачів, що особливо актуально в умовах підвищених вимог до гігієни та безпеки. Крім того, системи можуть працювати з різними типами безконтактних ключів, такими як NFC (Near Field Communication) та BLE (Bluetooth Low Energy), що забезпечує гнучкість у виборі засобів ідентифікації та підвищує зручність для користувачів. Ці технології дозволяють легко інтегрувати доступ через смартфони або інші мобільні пристрої, що стає все більш популярним і відповідає сучасним тенденціям цифрової трансформації.

Однак, незважаючи на численні переваги, мережеві системи контролю доступу мають і певні недоліки. В першу чергу, це висока вартість їхнього впровадження, яка включає не лише закупівлю обладнання та ліцензійного програмного забезпечення, а й витрати на інсталяцію, налаштування, інтеграцію з існуючими системами та подальше технічне обслуговування.

Складність архітектури таких систем вимагає наявності кваліфікованого персоналу для їхнього адміністрування та підтримки, що може бути проблемою для організацій із обмеженими ресурсами або невеликим технічним відділом. Крім того, мережеві СКД можуть бути залежними від стабільності мережевого з'єднання та електроживлення, тому для забезпечення безперебійної роботи необхідно передбачати резервні джерела живлення і надійні канали зв'язку. Для невеликих підприємств або організацій із обмеженим бюджетом такі системи можуть виявитися надмірно складними та дорогими, а їхні можливості — зайвими, що робить більш доцільним використання автономних або простіших рішень.

Таким чином, при виборі мережевої системи контролю доступу важливо ретельно оцінити потреби об'єкта, масштаби і складність інфраструктури, а також фінансові можливості. Для великих і складних об'єктів з високими вимогами до безпеки мережеві СКД є оптимальним вибором, що забезпечує максимальний рівень контролю, гнучкість і масштабованість. Водночас для менших організацій варто розглянути альтернативні варіанти, які можуть бути більш економічними і простими у впровадженні, зберігаючи при цьому необхідний рівень безпеки.

Біометричні системи розпізнавання, які базуються на унікальних фізіологічних характеристиках людини, таких як відбитки пальців, розпізнавання райдужної оболонки ока, геометрія обличчя, голос або навіть структура вен, забезпечують найвищий рівень безпеки завдяки практично унікальності біометричних даних кожної особи. Ці системи значно ускладнюють можливість підробки або несанкціонованого доступу, оскільки біометричні характеристики є складними для копіювання чи підробки, а також важко передбачуваними. Наприклад, розпізнавання райдужної оболонки ока базується на складній та унікальній текстурі, яка містить стрічки, гребені, кільця та інші деталі, що робить її практично неповторною навіть у близнюків. Аналогічно,

відбитки пальців мають унікальні візерунки рів і долин, що дозволяє з високою точністю ідентифікувати особу.

Водночас, впровадження біометричних систем пов'язане з високими витратами на обладнання та програмне забезпечення. Спеціалізовані сканери, камери високої роздільної здатності, інфрачервоні сенсори та потужні алгоритми обробки даних вимагають значних інвестицій, що робить такі системи менш доступними для малих і середніх підприємств. Крім того, інтеграція біометричних систем у існуючу інфраструктуру може бути технічно складною, потребувати адаптації програмного забезпечення, налаштування мережевого обладнання та навчання персоналу, що також впливає на загальну вартість і терміни впровадження.

Ще одним важливим аспектом є питання конфіденційності та захисту персональних даних. Біометричні дані є особливо чутливою інформацією, і їхнє зберігання, передача та обробка повинні відповідати суворим стандартам безпеки і законодавчим вимогам, таким як GDPR чи інші локальні нормативи. Це вимагає впровадження додаткових заходів захисту, зокрема шифрування даних, багаторівневого доступу, аудитів безпеки та регулярного оновлення програмного забезпечення для запобігання кібератакам. Порушення безпеки біометричних даних може мати серйозні наслідки, оскільки на відміну від паролів чи карток, біометрію не можна просто змінити.

Крім того, біометричні системи повинні враховувати можливі зміни біометричних ознак у користувачів, що можуть виникати через фізіологічні зміни, травми, захворювання або вікові фактори. Наприклад, відбитки пальців можуть дещо змінюватися через пошкодження шкіри, а зовнішній вигляд обличчя через старіння або хвороби. Тому сучасні системи розпізнавання обладнані адаптивними алгоритмами, які здатні враховувати такі варіації, але це підвищує складність і вартість рішень.

З огляду на ці фактори, біометричні системи контролювання доступу найчастіше застосовуються на об'єктах із підвищеними вимогами до безпеки,

таких як державні установи, фінансові організації, наукові центри та критична інфраструктура. Водночас розвиток технологій, зниження вартості обладнання та покращення алгоритмів обробки даних поступово роблять біометричні рішення більш доступними і для бізнесу середнього рівня, що відкриває нові перспективи для широкого впровадження біометричної безпеки у найближчому майбутньому.

Автономні системи контролю доступу відзначаються своєю простотою конструкції та легкістю у використанні, що робить їх надзвичайно привабливими для невеликих офісів, приватних підприємств або об'єктів із обмеженою кількістю точок проходу, зазвичай 1-2. Основна архітектура таких систем базується на безпосередньому зв'язку між зчитувачем, який зчитує інформацію з ідентифікаторів користувачів (наприклад, карток, брелоків або біометричних даних), та електромагнітним замком, що контролює фізичний доступ. Відсутність необхідності у складній серверній інфраструктурі або централізованому управлінні суттєво спрощує їхнє встановлення, налаштування та подальше обслуговування. Це дозволяє швидко впроваджувати такі системи навіть у приміщеннях із обмеженим технічним персоналом або бюджетом.

Завдяки своїй простоті автономні СКД забезпечують базовий рівень контролю доступу, достатній для багатьох малих підприємств, де немає потреби у веденні детальних журналів подій або інтеграції з іншими системами безпеки. Вони дозволяють ефективно обмежити доступ до певних зон, зменшуючи ризики несанкціонованого проникнення, і при цьому не вимагають значних інвестицій у обладнання чи програмне забезпечення. Крім того, автономні системи часто мають компактні розміри і можуть бути встановлені у різних типах приміщень, включно з офісами, складами, невеликими виробничими цехами або приватними будинками.

Однак, незважаючи на свої переваги, автономні системи мають суттєві обмеження, які можуть стати критичними при масштабуванні або ускладненні вимог до безпеки. Відсутність централізованого управління означає, що кожна точка доступу працює незалежно, що ускладнює координацію і контроль за

всією системою в цілому. Це обмежує можливості швидкого реагування на інциденти, оновлення прав доступу або моніторингу подій у режимі реального часу. Крім того, автономні СКД зазвичай не ведуть детального журналу подій або обмежені у функціоналі журналювання, що ускладнює проведення аудиту безпеки або розслідування випадків порушень.

Ще одним недоліком є відсутність або обмежена можливість інтеграції з іншими системами безпеки, такими як відеоспостереження, сигналізація чи системи пожежної безпеки. Це знижує загальний рівень комплексного захисту об’єкта і робить автономні системи менш привабливими для великих підприємств або об’єктів із підвищеними вимогами до безпеки. У разі розширення об’єкта або збільшення кількості точок проходу автономна система може потребувати повної заміни або значної модернізації, що призводить до додаткових витрат і складнощів.

Таким чином, автономні системи контролювання доступу є оптимальним вибором для невеликих об’єктів із простими вимогами до безпеки, де важливі швидкість впровадження, низька вартість і простота експлуатації. Водночас для більш масштабних, складних або динамічних об’єктів варто розглядати більш функціональні мережеві або біометричні системи, які забезпечують централізоване управління, гнучке налаштування прав доступу, ведення детального журналу подій і інтеграцію з іншими системами безпеки, що значно підвищує рівень захисту та ефективність контролю.

Вибір надійного рішення для надійної системи контролювання доступу є складним і відповідальним процесом, який повинен базуватися на всебічному та детальному аналізі потреб конкретної організації, характеристик об’єкта, рівня складності інфраструктури, вимог до безпеки, наявного бюджету та можливостей технічного обслуговування.

Кожна організація має свої унікальні особливості, які впливають на вибір оптимальної системи: це можуть бути масштаб об’єкта, кількість точок доступу, кількість користувачів, специфіка діяльності, а також рівень загроз та ризиків,

що притаманні конкретній сфері. Для великих підприємств, офісних комплексів, виробничих майданчиків чи державних установ із високими вимогами до безпеки найбільш ефективним і перспективним варіантом є мережеві системи контролювання доступом.

Ці системи забезпечують централізоване управління, можливість інтеграції з іншими системами безпеки, такими як відеоспостереження, пожежна сигналізація, охоронна система, а також підтримують сучасні методи автентифікації, зокрема двофакторну ідентифікацію, що поєднує фізичні ідентифікатори з біометричними даними або PIN-кодами. Такий підхід значно підвищує рівень захисту, дозволяє гнучко налаштовувати права доступу, вести детальний аудит подій і оперативно реагувати на інциденти.

Для невеликих офісів, приватних підприємств або об’єктів із обмеженим бюджетом більш доцільними будуть автономні системи контролю доступу, які не потребують складної серверної інфраструктури і централізованого управління. Вони забезпечують базовий, але надійний контроль доступу, прості у встановленні та обслуговуванні, що робить їх оптимальним вибором для організацій із невеликою кількістю точок проходу і обмеженими ресурсами. Такі системи дозволяють швидко організувати контроль доступу без значних капіталовкладень, але мають обмежені можливості масштабування і інтеграції з іншими системами безпеки.

Біометричні системи контролю доступу, які використовують унікальні фізіологічні характеристики людини відбитки пальців, розпізнавання обличчя або райдужної оболонки ока, варто розглядати у випадках, коли потрібен найвищий рівень безпеки і є можливість інвестувати у сучасні технології. Такі системи забезпечують практично унікальну ідентифікацію користувачів, значно ускладнюючи можливість підробки або несанкціонованого доступу. Водночас вони вимагають суттєвих інвестицій у обладнання, програмне забезпечення, а також у заходи щодо захисту персональних даних і конфіденційності. Біометричні рішення особливо актуальні для об’єктів із підвищеними вимогами

до безпеки, таких як фінансові установи, державні органи, наукові центри чи критична інфраструктура.

При виборі системи контролювання доступу також надзвичайно важливо враховувати сумісність обладнання та програмного забезпечення, що забезпечить безперебійну роботу системи, можливість її масштабування та модернізації у майбутньому. Важливо, щоб обране рішення підтримувало інтеграцію з іншими системами безпеки та мало можливість оновлення, що дозволить адаптувати систему до змін у вимогах безпеки чи технологічному середовищі. Не менш важливою є наявність якісної технічної підтримки та сервісного обслуговування від виробника або інтегратора, що гарантує швидке усунення несправностей, оновлення програмного забезпечення та консультації з експлуатації.

Таким чином, правильний вибір системи контролювання доступу повинен бути збалансованим рішенням, яке враховує як технічні, так і організаційні аспекти, забезпечуючи надійний захист, гнучкість у налаштуванні, зручність експлуатації та економічну доцільність. Лише комплексний підхід до оцінки потреб і можливостей дозволить створити ефективну, масштабовану та безпечну систему, що відповідатиме сучасним стандартам і вимогам безпеки.

2.3 Аналіз постачальників систем безпеки

Серед провідних виробників систем контролювання доступу з біометрією в Україні варто виділити ZKTeco, Hikvision та Dahua. ZKTeco відома як глобальний постачальник біометричних рішень із широкою мережею сервісних центрів по всій Україні, а також офіційною технічною підтримкою. Компанія пропонує багатофункціональні контролери з підтримкою різних біометричних ідентифікаторів (відбитки пальців, розпізнавання обличчя, вени пальців, райдужка ока), гнучке програмне забезпечення, веб або автономне, та інтеграцію з хмарними сервісами. Продукція ZKTeco вважається доступною за ціною, з

гарантійною підтримкою та швидкою доставкою по Україні, а також має хорошу репутацію серед корпоративних клієнтів. Водночас конкуренція також дає про себе знати, Hikvision і Dahua — це китайські гіганти у сфері відеоспостереження та СКД, чиї рішення також широко використовуються в Україні. Обидві компанії пропонують широкий вибір контролерів і програмного забезпечення з підтримкою біометрії, мають розгалужену дистриб'юторську мережу та гарантійне обслуговування. За ціною їхні продукти часто знаходяться в середньому та бюджетному сегменті, що робить їх привабливими для масового ринку. Проте, згідно з розслідуваннями, пристрої Hikvision і Dahua можуть передавати дані на сервери виробників, що створює потенційні ризики для інформаційної безпеки, особливо з огляду на співпрацю Китаю з Росією. Камери відеоспостереження китайських компаній Hikvision і Dahua, заборонені в США через ризики безпеки, досі широко використовуються в Україні — на вулицях міст, у державних і приватних установах, а також у житлових будинках. Застарілі моделі цих камер особливо вразливі до злому без належних заходів захисту, чим, за повідомленнями, використовували російські спецслужби для коригування ударів по українських містах. У відповідь українські служби безпеки вже заблокували понад 10 000 таких пристроїв, які потенційно могли бути використані ворогом. Попри те, що Hikvision повністю контролюється китайською державою, а Dahua частково, обидві компанії внесені до українського списку міжнародних спонсорів війни, однак нажаль їхня техніка все ще використовується навіть в офіційних структурах України [31].

Порівнюючи контролери, ZKTeco вирізняється ширшим вибором біометричних ідентифікаторів і гнучким програмним забезпеченням, що підходить для інтеграції з різними системами обліку та аналітики. Hikvision і Dahua роблять акцент на суміщенні відеоспостереження та контролю доступу, пропонуючи комплексні рішення з інтегрованою аналітикою, але їхня біометрія часто поступається за функціональністю ZKTeco. За рівнем підтримки всі три бренди мають офіційних партнерів і сервісні центри в Україні, однак питання

кібербезпеки та політичних ризиків для Hikvision та Dahua залишаються актуальними, особливо у таких установах.

Тому для цієї задачі я обрав ZKTeco. Їх рішення охоплюють термінали доступу, контролери, зчитувачі, автономні електронні замки та інші пристрої, що забезпечують надійний контроль входу на об'єкти різного масштабу від невеликих офісів до великих підприємств із багатьма точками проходу, навіть у різних містах. Системи ZKTeco підтримують автентифікацію за допомогою безконтактних карт, відбитків пальців, кодів доступу, зображення обличчя або комбінованих методів. Рішення цієї компанії дозволяють гнучко та просто налаштовувати права доступу, інтегруються з системами відеоспостереження, охоронною та пожежною сигналізацією, а також підтримують різні інтерфейси зв’язку: RS485, Ethernet, Wi-Fi, GPRS [32]. За допомогою безкоштовного програмного забезпечення можна керувати всією системою, моніторити події в реальному часі, використовувати графічні плани приміщень і вести облік робочого часу. Програмне забезпечення ZKTeco пропонує комплексні рішення для ефективного управління системами контролю доступу та обліку робочого часу. Основним продуктом для малого та середнього бізнесу є ZKAccess 3.5, це професійне програмне забезпечення з сучасним інтерфейсом, що підтримує до 100 пристроїв і до 30 000 користувачів, дозволяючи одночасно керувати доступом та формувати звіти про відвідуваність. Окрім нього, компанія пропонує інші продукти: ZKBio Access IVS, веб-платформу для централізованого управління безпекою; мобільний додаток для дистанційного керування замками ZKSmartKey та мобільний застосунок для контролю одно та багатодверних пристроїв ZKBioGO; а також ZKBiolock Hotel Lock System, спеціалізоване рішення для готелів [33].

2.4 Висновки

У процесі дослідження сучасних рішень для систем контролювання доступу було встановлено, що біометричні технології значно підвищують рівень безпеки завдяки використанню унікальних фізіологічних і поведінкових характеристик користувачів. Серед основних методів ідентифікації виокремлено розпізнавання обличчя, відбитків пальців, геометрії руки, підпису та райдужної оболонки ока. Вибір того чи іншого рішення залежить від конкретних умов використання, зокрема вимог до швидкості, точності, зручності та рівня захисту. Значну увагу було приділено аналізу переваг і недоліків кожного методу, а також питанню сумісності із наявною інфраструктурою банківського відділення.

В додаток, особливо важливою є інтеграція біометричних систем із відеоспостереженням, охоронною сигналізацією, обліком часу та іншими додатками. Таке поєднання створює єдину багаторівневу інфраструктуру, здатну ефективно запобігати несанкціонованому доступу. Використання відкритих фреймворків і стандартизованих протоколів дозволяє досягти сумісності навіть між обладнанням різних виробників та використання уже готових рішень дозволить зекономити і швидше розгортнути систему з додатковою підтримкою від спеціалістів. Загалом, сучасні біометричні рішення є перспективними, зручними й масштабованими, що робить їх доцільними для впровадження у критичні інфраструктури із підвищеними вимогами до безпеки, зокрема у фінансових організаціях.

3 ПРОЕКТУВАННЯ СИСТЕМИ КОНТРОЛЮВАННЯ ДОСТУПОМ

3.1 Підбір апаратного забезпечення для відділення

Під час підбору апаратного забезпечення для підвищення безпеки та керованості доступу в межах відділення доцільним є використання біометричного контролера ZKTeco inBio460. Цей пристрій встановлюється у захищеному середовищі всередині приміщення, тоді як зовні розміщуються лише зчитувачі. Такий підхід дозволяє значно знизити ризики фізичного злому та несанкціонованого доступу до системи. Контролер підтримує як біометричні зчитувачі відбитків пальців, що підключаються через RS485, так і RFID-зчитувачі безконтактних карт через інтерфейс Wiegand. На базі inBio460 можна організувати доступ через чотири двері (або два турнікети), при цьому підтримуються до восьми біометричних зчитувачів і до 3000 шаблонів відбитків пальців із середньою швидкістю ідентифікації до 2 секунд.

Особливістю контролера є його здатність до гнучкої інтеграції з іншими системами безпеки, зокрема пожежною сигналізацією, відеоспостереженням та охоронними системами. Web-серверне програмне забезпечення забезпечує зручний інтерфейс для візуалізації подій у реальному часі на плані приміщення та дозволяє дистанційно керувати системними елементами. При наявності інтеграції з IP-камерами також забезпечується захоплення відео в момент події. Сам контролер має пластиковий корпус, оснащений світловими індикаторами, клемами для підключення периферії та слотом для SD-карти, яка може використовуватись як для розширення пам’яті, так і для резервного копіювання. У цьому виборі для захищення об’єкта, було важливим чудова репутація компанії, повноційне ПО і широкий спектр функцій у inBio460: доступ за відбитком або карткою, багатофакторна автентифікація, налаштування тимчасових зон і сценаріїв розблокування, ведення обліку робочого часу, заборона подвійного проходу, логіка шлюзових кабін, режим «вільного проходу» в зазначений час, а також функція примусового входу із сигналізацією тривоги.

Контролер також підтримує інтелектуальні реакції на події, як-от автоматичне збереження відео під час входу до приміщення. Технічно пристрій має розширені можливості: до 30 000 карт, 100 000 записів у внутрішньому журналі, підтримку PoE (через адаптер), інтерфейси RS485, TCP/IP, чотири порти Wiegand, вісім RS485-зчитувачів, чотири входи для герконів(магнітний датчик відкриття) і кнопок, чотири релейні виходи та чотири додаткові входи/виходи. Компактні розміри (185×106 мм) і живлення 9–14 Вольт постійного струму, дозволяють легко і непомітно впровадити систему в нашому середовищі з наданими вимогами до безпеки [34].

Для організації контролю доступу на вхід у приміщення передбачено встановлення триподного турнікета ZKTeco TS1022 Pro з електромеханічним механізмом, який обмежує прохід у двох напрямках і забезпечує перевірку права входу або виходу кожного відвідувача використовуючи біометричний метод ідентифікації. Турнікет виготовлений із нержавіючої сталі, що гарантує високу зносостійкість та тривалу безвідмовну експлуатацію. У стандартній комплектації передбачено використання контролера InBio260 та двох зчитувачів FR1200, що підтримують як зчитування відбитків пальців, так і RFID-міток стандарту Em-Marin. Система працює під керуванням програмного забезпечення ZKTeco Bioaccess IVS, що дозволяє централізовано керувати доступом та вести облік відвідувань до контролера та інших сумісних пристроїв.

Він забезпечує високу пропускну здатність аж до 30 осіб на хвилину при проході за RFID-карткою та до 25 осіб при використанні біометричного зчитування. Керування турнікетом можливе як автоматизовано через зчитувачі, так і дистанційно за допомогою пульта, радіобрелока чи ПК. Завдяки швидкому часу реакції система виключає утворення черг. У разі надзвичайної ситуації активується функція "антипаніка", яка дозволяє миттєво опустити штангу і забезпечити вільний прохід. Турнікет має захист від перенапруги, ширину проходу 520 мм та підтримує живлення від мережі та від безперебійних джерел живлення [35].

Для біометрії другим основним зчитувачем буде біометричний сканер ZKTeco MA300-BT/ID для відбитків пальців і ID-карток Em-Marine. Оснащений високоякісним оптичним сенсором і вдосконаленим алгоритмом ZK, він забезпечує точне та швидке розпізнавання за одну секунду. Пристрій підтримує до 1500 шаблонів відбитків пальців, 10000 карт і зберігає до 100000 транзакцій. Міцний металевий корпус зі ступенем захисту IP65 робить його ідеальним для зовнішнього встановлення, захищаючи від пилу, вологи й механічного впливу. MA300-BT працює як автономно, так і з будь-якими контролерами через Wiegand 26, а також має інтерфейси TCP/IP, RS485 та Bluetooth. Підтримка мобільного застосунку ZKBioBT дозволяє зручно керувати пристроєм, додавати користувачів, змінювати налаштування та керувати замком у режимі реального часу. Додаткові функції включають підключення кнопки виходу, сирени, захист від розтину, аудіовізуальну індикацію та можливість експорту даних через USB [36].

Та в додаток для нього, для покращення безпеки, встановимо біометричний зчитувач обличчя ZKTeco KF1000, який використовує сучасну технологію розпізнавання обличчя Visible Light і забезпечує високу точність, стабільність та швидкість ідентифікації з використанням інфрачервоної підсвітки. Пристрій працює в складі системи з контролерами серії InBio або іншими сумісними контролерами ZKTeco через інтерфейс Wiegand, забезпечуючи надійну автентифікацію користувачів. Завдяки підтримці інтерфейсів TCP/IP (100 Мб/с) і RS485, KF1000 дозволяє синхронізувати шаблони облич і дані в режимі реального часу. Незважаючи на відсутність прямого керування замком, пристрій може автономно виконувати функції обліку робочого часу. Додатково, серія KF1000 відповідає вимогам стандарту кібербезпеки ZKTeco, що гарантує захист персональних даних користувачів на високому рівні. Його дизайн дуже елегантно і непомітно вбудовується у більшість приміщенн, що не придає увагу потенційним зловмисникам і не дає просто знаяти зчитувач з місця встановлення. Також він є ідеальним запасним

варіантом ідентифікації у випадках, коли використання відбитка пальця неможливе , наприклад через пошкодження шкіри, вологі або забруднені пальці, або зайняті руки. Крім того, його можна використовувати в комбінації з дактилоскопічними зчитувачами для двофакторної автентифікації, що значно підвищує рівень безпеки та знижує ризик несанкціонованого доступу [37].

3.2 Моделлювання та впровадження

Моделювання внутрішнього простору банківського відділення було здійснено з метою оптимального розміщення елементів системи контролювання доступу, враховуючи як архітектурні особливості будівлі, так і функціональні зони з підвищеними вимогами до безпеки — серверні кімнати, касові вузли, сховища, кімнати з обмеженим доступом та зони взаємодії з клієнтами. Для побудови віртуальної моделі використовувалося спеціалізоване програмне забезпечення, яке дозволило створити детальний план-схему приміщення з точним розміщенням біометричних терміналів, електронних замків, кнопок аварійного відкривання, турнікетів та систем відеоспостереження. Візуалізація середовища дала змогу не лише визначити критичні точки входу та виходу, але й розробити та протестувати симуляційні сценарії руху персоналу, клієнтів, а також потенційних зловмисників.

Завдяки такому підходу стало можливим заздалегідь оцінити ефективність розміщення систем безпеки, змоделювати ситуації несанкціонованого доступу та виявити слабкі місця інфраструктури ще до початку фізичного монтажу. Це дозволило заощадити ресурси, уникнути непотрібних витрат на переробку обладнання в майбутньому та зменшити ризики, пов’язані з людським фактором або технічними недоліками. Крім того, модель легко піддається змінам, що дає змогу швидко ітеративно перевіряти нові конфігурації, адаптувати систему до змін в організації внутрішнього простору чи підвищення рівня загроз. Попереднє

тестування конфігурації у віртуальному середовищі допомагає переконатися в її надійності, оптимізувати маршрути руху та забезпечити максимальну ефективність системи контролювання доступу ще до її фактичного впровадження. Також після створення моделі було розроблено план впровадження, що передбачає поетапне правильне встановлення обладнання, вирішення минулих проблем, налаштування контролерів та інтеграцію з іншими інсуючими системами безпеки (відеоспостереження, пожежна сигналізація). Додатково увага приділена забезпеченню резервного живлення та прихованому прокладанню кабельних каналів для зменшення неконтрольованих випадків та навмисного і ненавмисного шкідливого втручання. Усі компоненти системи перевіряються на відповідність вимогам безперервної роботи та захищеності від фізичних пошкоджень або маніпуляці за Українськими стандартами. Такий підхід дозволяє забезпечити як технічну ефективність системи, так і її адаптацію до умов реального використання. Детальну модель такого приміщення можна оглянути на рис. 3.1.

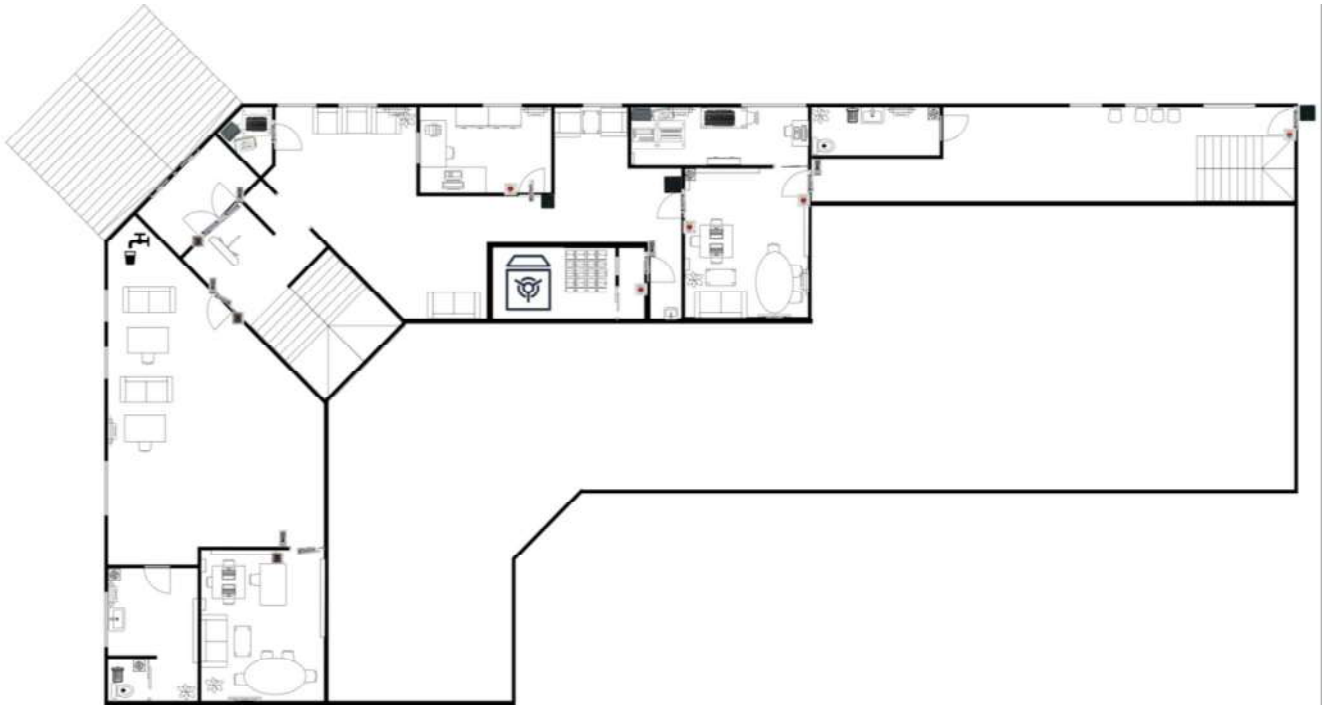


Рисунок 3.1 – Вигляд з верху на приміщення

3.3 Розробка рекомендацій для реалізації системи

Реалізація системи контролювання доступу у відділенні банку повинна відбуватися поетапно з урахуванням технічних, фізичних, організаційних та інформаційних вимог. Встановлення біометричних терміналів, контролерів, блоків живлення, а також підключення програмного забезпечення потребує ретельного проєктування, дотримання інструкцій виробника та врахування специфіки об’єкта. Насамперед слід визначити точки входу до захищених приміщень, і для цього можна використати раніше створену модель, маршрути руху персоналу, наявні технічні умови (електроживлення, мережеві порти), після чого можна переходити до монтажу обладнання.

Перед початком реалізації важливо чітко визначити потреби в системі контролю доступу та проаналізувати існуючі вразливості потенційні загрози. Це дозволить сформувати технічно обґрунтований план, який відповідатиме специфіці об’єкта та потребам організації. Такий підхід дає змогу уникнути помилок під час встановлення, запобігти зайвим витратам і забезпечити максимальну ефективність роботи системи. Багато підприємств і досі покладаються на традиційні механічні ключі, адже встановлення сучасної системи контролю доступу може здатися фінансово недосяжним. Навіть з огляду на довгострокову вигоду та підвищення рівня безпеки і довіри, деякі організації не готові інвестувати кошти у впровадження новітніх рішень, що значною мірою стримує перехід до більш ефективних технологій захисту [38].

Біометричні зчитувачі рекомендується встановлювати у місцях, де мінімізований вплив прямих сонячних променів або змін освітлення, адже це може спричинити зниження точності зчитування. Оптимальна висота встановлення термінала становить 130–150 см від підлоги, при цьому необхідно забезпечити зручний доступ для користувачів різного зросту. Зчитувачі повинні бути надійно закріплені, захищені від вандалізму та мати захист від потрапляння вологи чи пилу (рівень IP65 і вище). Контролери доцільно розміщувати у

спеціалізованих технічних приміщеннях або монтажних шафах, доступ до яких має бути суворо обмежений. Підключення обладнання слід виконувати відповідно до технічної документації виробника. Приклад працюючої підключеної системи можна побічити на рис. 3.2.

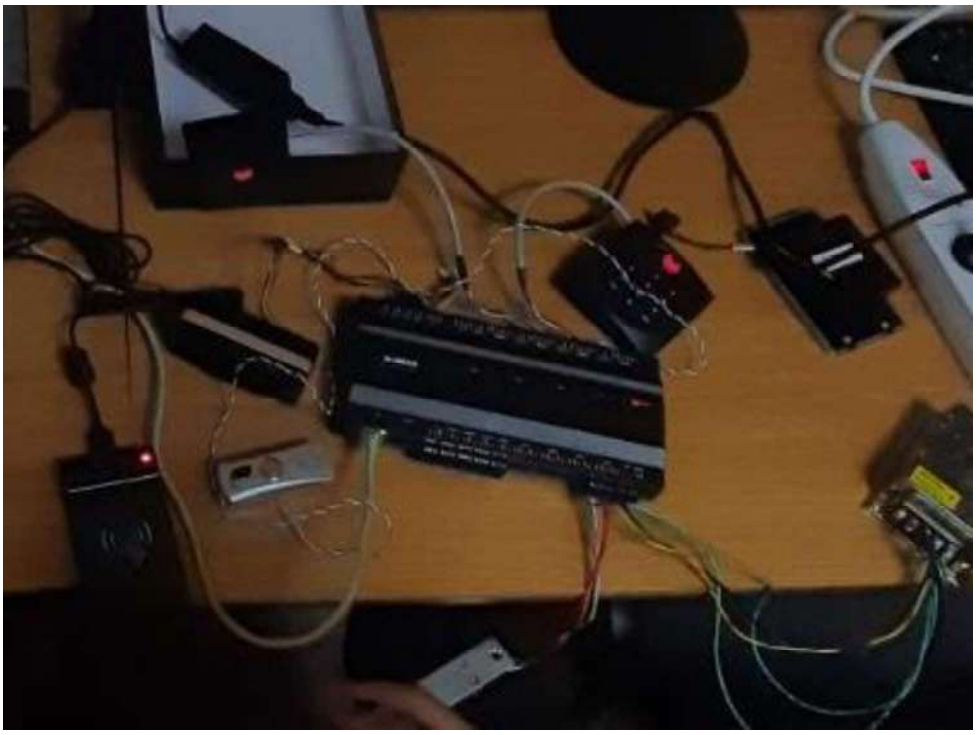


Рисунок 3.2 – Контролер системи контролювання доступу з приладами

Усі елементи повинні бути заземлені. Для забезпечення безперебійної роботи системи важливо передбачити резервне живлення на основі ДБЖ або акумуляторних модулів з автоматичним перемиканням та інверторів у разі зникнення основного джерела. Кабельну інфраструктуру слід проектувати з урахуванням захищених каналів передачі даних та відповідності стандартам електробезпеки. Всі мережеві з'єднання обладнання повинні бути виконані з використанням екранізованих кабелів категорії не нижче CAT5e, а фізичне розміщення слід проводити з дотриманням норм пожежної безпеки. Мережева інтеграція має передбачати виділення окремого сегменту VLAN із закритим зовнішнім доступом, а також використання статичних IP-адрес або DHCP із

прив’язкою MAC-адрес [39]. Потім прив’язуємо за цією адресою контролер та підключаємося, так як на рис 3.3, з пристроя з якого будемо налаштовувати

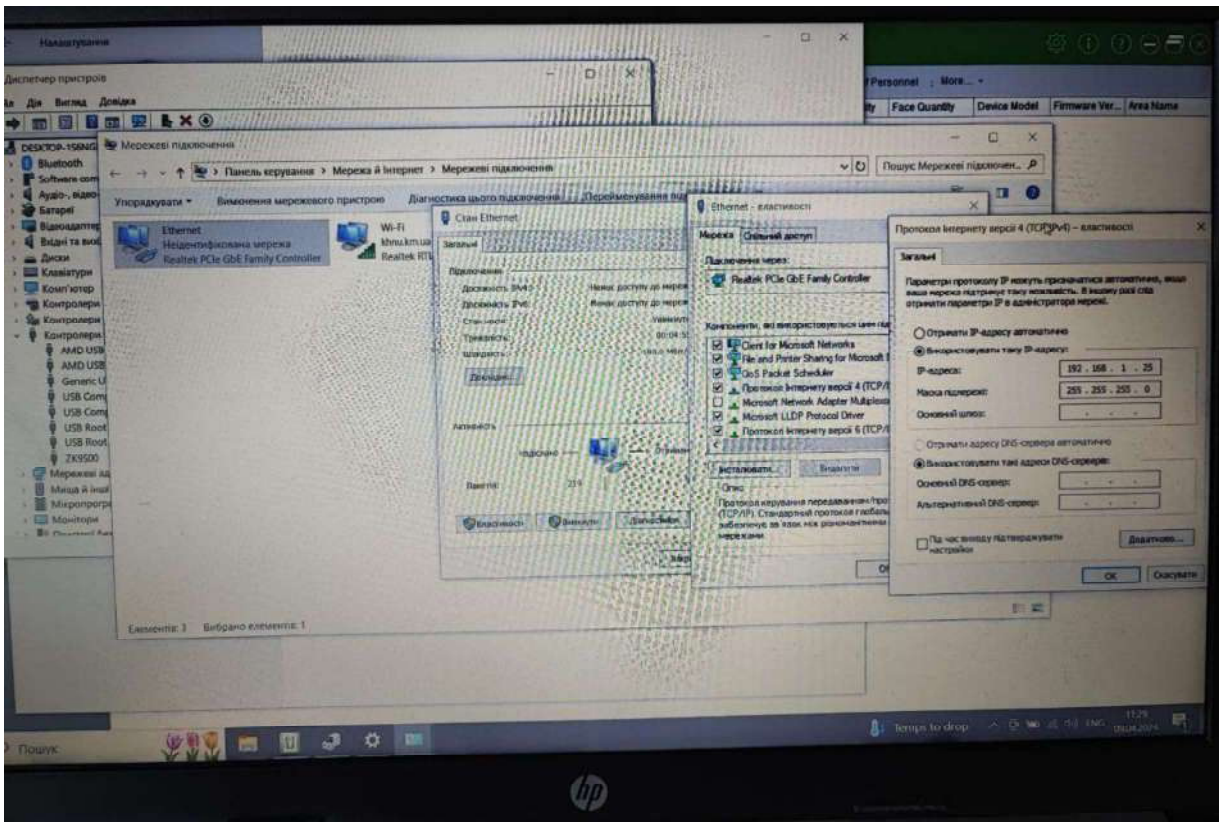


Рисунок 3.3 – Підключення до локальної мережі

Наступним кроком є встановлення та налаштування програмного забезпечення, що керує системою контролювання доступу. ПЗ слід інсталювати на захищеному сервері або спеціалізованій робочій станції адміністратора без прямого доступу до загальної локальної мережі. Запустивши програмне забезпечення, знаходимо систему та під'єднуємся, знайдену систему видно на рис. 3.4.

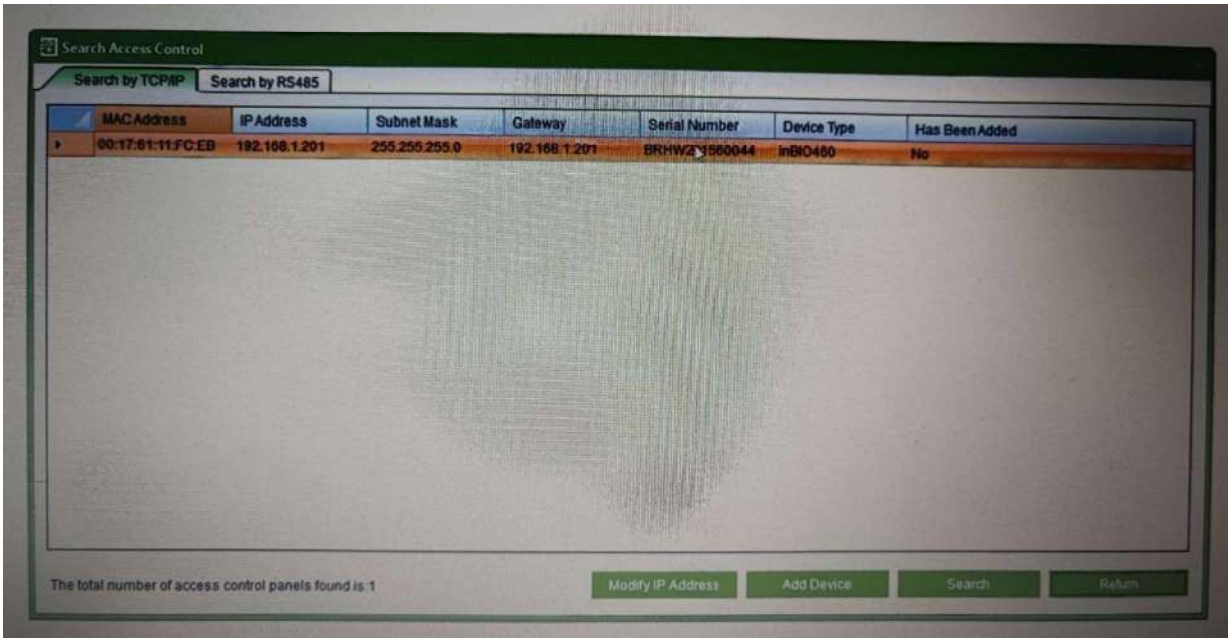


Рисунок 3.4 – Виявлено адресу контролера в локальній мережі

Після встановлення адміністратор має створити базову конфігурацію: внести структуру об'єкта, задати зони доступу, обмеження по часу та пріоритети проходів. Програмне забезпечення повинно підтримувати інтеграцію з відеоспостереженням, базами даних користувачів, а також мати модулі для ведення обліку робочого часу, якщо це передбачено політикою установи. Та при успішному налаштувані, обов'язково синхронізувати системні налаштування, для того що б зберегти, з пам'яттю контролера через мережу. Процес синхронізації зображено на рис. 3.5.

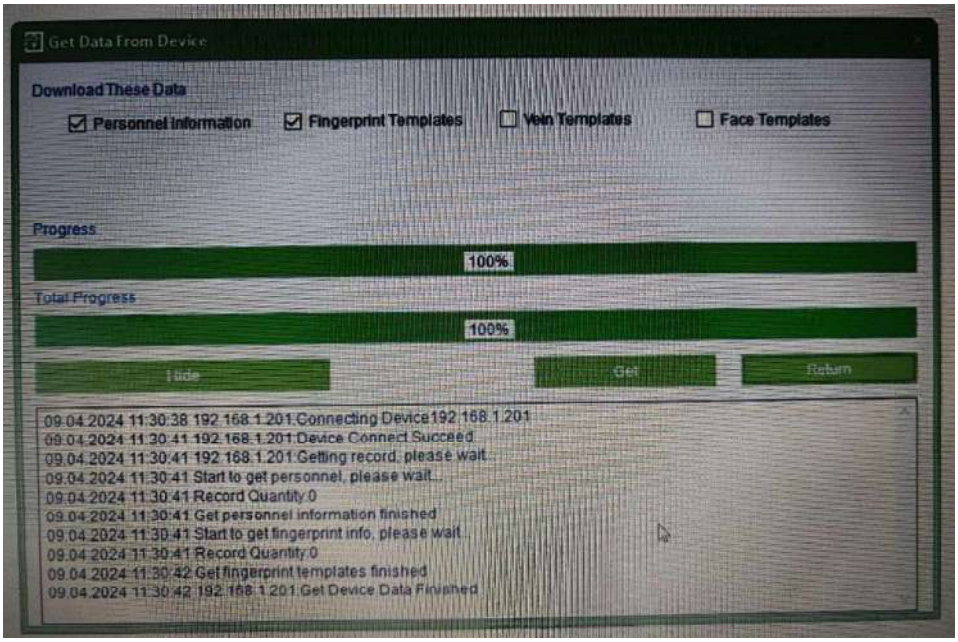


Рисунок 3.5 – Успішна синхронізація з присроєм

Реєстрація персоналу є обов'язковим етапом перед повноцінним запуском системи. Для кожного працівника створюється обліковий запис, до якого додаються його персональні дані, фото, біометричні шаблони (відбитки пальців, обличчя тощо) та права доступу. Під час первинного сканування біометрії необхідно дотримуватись інструкцій для досягнення максимальної точності і уникнення хибних відмов при подальшому розпізнаванні. Якщо система підтримує мультимодальну аутентифікацію, варто активувати додаткові способи підтвердження особи (наприклад, PIN-код або смарт-картку), особливо для доступу до зон з високим рівнем захисту [40].

Після завершення налаштування системи слід провести комплексне тестування. Випробування мають включати перевірку роботи кожного елементу: правильність зчитування біометрії, реакцію на спроби несанкціонованого доступу, працездатність резервного живлення, цілісність каналів зв'язку та коректність взаємодії з іншими системами безпеки (відеонагляд, сигналізація тощо). Крім того, необхідно налаштувати журналювання подій, яке дозволяє у разі інциденту відстежити всі спроби входу, порушення режиму або збої у

функціонуванні системи. Вот так на рис. 3.6, має виглядати активна система яка реагує та записує події щодо відкриття двері.

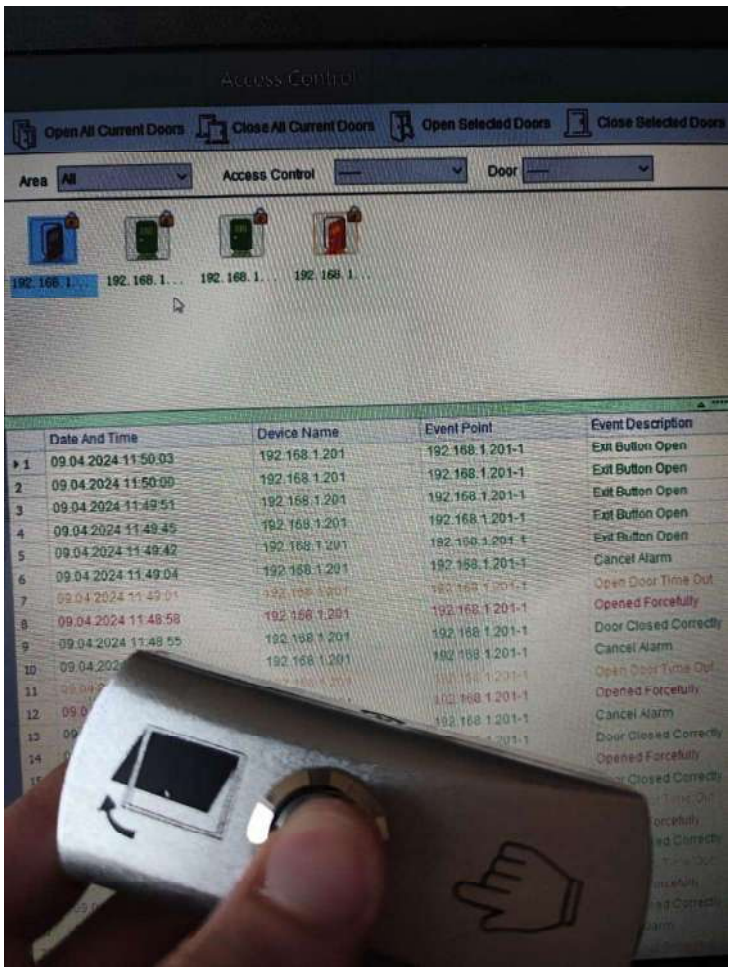


Рисунок 3.6 – Реакція системи на натиск кнопки відкриття двері

Для зручності моніторингу та аналізу подій система повинна підтримувати генерацію регулярних звітів про входи/виходи, спроби доступу з відмовами, перегляд історії доступу конкретних осіб або груп. Адміністратор має мати змогу формувати як стандартні, так і кастомізовані звіти за певними фільтрами (час, об’єкт, працівник, пристрій), а також експортувати ці звіти у формати CSV, PDF тощо. Ці звіти можуть бути корисними як для підвищення безпеки, так і для управління персоналом, наприклад, з метою контролю запізнень або понаднормових [41].

Таким чином, для ефективного впровадження системи контролювання доступу з біометричною ідентифікацією необхідно не лише грамотно обрати та встановити обладнання, а й забезпечити надійне мережеве середовище, якісне програмне забезпечення, коректну реєстрацію користувачів, а також регулярний моніторинг і супровід системи. Лише за умов дотримання всіх цих рекомендацій можна гарантувати надійну, безперебійну та безпечну роботу системи в умовах реального функціонування банківської відділення.

3.4 Оцінка собівартості системи

Що до забезпечення надійної та ефективної роботи системи контролювання доступу було обрано відповідні компоненти з урахуванням вимог до безпеки та сумісності обладнання:

- біометричний контролер доступу ZKTeco inBio460 - 14045₴ - 2шт;
- джерело живлення ZKTeco Power Supply TPM005B - 1677₴ - 2шт;
- електромагнітний замок для двойних дверей YM-280NTD - 3434₴ - 1шт;
- електромагнітний замок YM-280N - 1910₴ - 6шт
- кнопка виходу Yli Electronic PBK-817B-AL(R) - 525₴ - 4шт
- кнопка виходу безконтактна Yli Electronic ISK-840B - 672₴ - 3шт
- турнікет-трипод ZKTeco TS1022 Pro - 61043₴ - 1шт
- біометричний термінал ZKTeco MA300-BT - 4580₴ - 5шт
- Ббіометричний термінал розпізнавання облич зі зчитувачем Mifare ZKTeco KF1200 - 5040₴ - 3шт
- APC BE700G-RS Back-UPS ES 700VA Джерело безперебійного живлення - 5561₴ - 2шт
- блок живлення 12В/3А SEVEN PS-792SE - 289₴ - 10шт

Програмне забезпечення входить безкоштовно, та ще варто враховувати роботу спеціалістів. Повна сума всіх компоненті: 158949₴

3.5 Висновки

Здійсненили проєктування системи контролювання доступу з допомогою біометричної ідентифікації для відділення банку. Ретельно обрані апаратні компоненти, включно з біометричними терміналами та контролерами, враховували потреби банківського середовища в надійності, безпеці та зручності експлуатації. Підбору сумісних рішень є важливим моментом, який забезпечує ефективну роботу системи у режимі реального часу та мали можливість інтеграції з іншими елементами охоронної інфраструктури.

У процесі моделювання приміщення та розміщення апаратних засобів було сформовано оптимальний план інсталяції системи, що враховує логіку переміщення персоналу, контроль ключових зон доступу та безперебійність роботи в разі збоїв живлення. У рамках розробки також надано рекомендації з експлуатації системи, що охоплюють програмне налаштування, адміністрування користувачів та сценарії реагування на події.

Проведена оцінка собівартості проєктованої системи показала її економічну обґрунтованість у контексті довгострокової експлуатації. Порівняно із традиційними методами контролю доступу, запропоноване рішення забезпечує вищий рівень безпеки та потребує менших витрат на технічне обслуговування. Таким чином, реалізація системи біометричного контролю доступу в банківській установі є доцільним і ефективним рішенням, що сприяє покращенню фізичної безпеки, автоматизації внутрішніх процесів та підвищенню рівня захищеності від несанкціонованого проникнення.

ВИСНОВКИ

Системи контролювання доступу забезпечують комплексний захист приміщень, інформації та матеріальних активів, поєднуючи фізичні, електронні й мережеві компоненти. Ефективність таких систем значною мірою залежить від вибору надійного обладнання, якісного програмного забезпечення, інтеграції з іншими елементами безпеки, а також гнучкого налаштування під потреби конкретної установи. Додавання біометричних технологій до цих систем суттєво підсилює рівень безпеки та зміцнює довіру клієнтів, оскільки дозволяє точно ідентифікувати особу за унікальними фізіологічними характеристиками.

При впровадженні біометричних рішень важливо враховувати їхню сумісність з існуючою інфраструктурою, включно з системами відеоспостереження, сигналізації та іншими захисними модулями. Особливу увагу слід приділяти захисту біометричних даних застосовуючи шифрування, надійне зберігання та обмежений доступ. Багаторівнева система автентифікації допоможе ефективно запобігти несанкціонованому доступу та втручанню в мережу безпеки. Крім високої точності розпізнавання, біометрична система має бути зручною для користувача, з мінімальною кількістю хибних спрацьовувань і можливістю масштабування під потреби майбутнього.

Завдяки використанню природних ідентифікаційних ознак, таких як відбитки пальців, форма обличчя чи голос біометричні системи відкривають новий рівень захисту, водночас оптимізуючи робочі процеси та зменшуючи експлуатаційні витрати. У контексті сучасних викликів, біометричні технології не лише підвищують ефективність систем безпеки, а й стають ключовим інструментом захисту банківських установ, їхніх клієнтів та конфіденційної інформації. Успішне впровадження такої системи вимагає її відповідності чинним стандартам, інтеграції з наявною інфраструктурою та здатності адаптуватися до нових загроз і викликів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Bank Branch Security: Keeping Customers and Employees Safe. URL: https://www.americanalarm.com/blog/bank-branch-security-keeping-customers-and-employees-safe-024031 (дата звернення: 03.05.2025)

2. The Top 5 Security Concerns of Modern Financial Institutions. URL: https://www.garda.com/en-ca/articles/the-top-5-security-concerns-of-modern-financial-institutions (дата звернення: 03.05.2025)

3. Three Branch Security Threats to Consider. URL: https://stsgrp.com/3-branch-security-threats-to-consider-in-2020/ (дата звернення: 03.05.2025)

4. БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/29a2e041-c31e-44d9-b074-a26dfddfa97d/content (дата звернення: 03.05.2025)

5. Управління доступом в інформаційних системах : монографія / О. Г. Корченко, С. О. Гнатюк, В. М. Кінзерявий, Ю. Є. Яремчук. – Київ : ЦП «Компринт», 2023. – 298 с.

6. Федоренко, Н. В. Стандарти безпеки в системах контролю доступу / Н. В. Федоренко // Стандартизація, сертифікація, якість. – 2023. – № 2 (121). – С. 45–51.

7. Access control systems in banks: beyond security. URL: https://www.ventasdeseguridad.com/en/more-in-depth/technological-analysis/22915-access-control-systems-in-banks-beyond-security.html (дата звернення: 03.05.2025)

8. How Access Control Systems Benefit Regulatory Requirements in Banking URL: https://2krew.com/access-control-systems-benefit-regulatory-requirements-in-banking/ (дата звернення: 04.05.2025)

9. Шевченко, Л. П. Економічна ефективність впровадження систем контролю доступу на підприємствах / Л. П. Шевченко // Економіка та управління підприємствами. – 2022. – № 3. – С. 112–119.

10. Що таке СКД і як організувати систему контролю доступу в офісі чи іншому об'єкті? URL: https://bas-ip.kiev.ua/shcho-take-skud-i-yak-orhanizuvaty-systemu-kontroliu-dostupu-v-ofisi-chy-inshomu-obiekti/ (дата звернення: 04.05.2025)

11. Ящук, О. В. Системи контролю доступу для критичної інфраструктури : дис. ... д-ра техн. наук : 05.13.06 / О. В. Ящук ; Нац. техн. ун-т України «КПІ». – Київ, 2023. – 324 с.

12. Access Control Systems: Design and Implementation / J. Smith, R. Johnson, M. Williams. – 3rd ed. – Boston : Pearson, 2023. – 456 p.

13. Як вибрати систему контролю та керування доступом? URL: https://nadzor.ua/uk/blog/kontrol-dostupa/kak-vybrat-sistemu-kontrola-i-upravlenia-dostupom (дата звернення: 04.05.2025)

14. Контролери СКД: види, призначення, складові URL: https://nadzor.ua/uk/blog/kontrol-dostupa/kontrollery-skud-vidy-naznacenie-sostavlausie (дата звернення: 04.05.2025)

15. Біометричні технології ідентифікації URL: https://sib.com.ua/sib-1-135-2025/biometriya.html (дата звернення: 04.05.2025)

16. Access control systems in banks: beyond security URL: https://www.ventasdeseguridad.com/en/more-in-depth/technological-analysis/22915-access-control-systems-in-banks-beyond-security.html (дата звернення: 04.05.2025)

17. Використання потенціалу банківського сектору за допомогою технології розпізнавання облич URL: https://tvtdigital.com.ua/vykorystannia-potentsialu-bankivskoho-sektoru-za-dopomohoiu-tekhnolohii-rozpiznavannia-oblych/ (дата звернення: 04.05.2025)

18. Top 5 Use Cases of Biometrics in Banking URL: https://www.idenfy.com/blog/biometrics-in-banking/ (дата звернення: 04.05.2025)

19. What is a Biometric Access Control System? URL: https://www.creolestudios.com/what-is-biometric-access-control-system/ (дата звернення: 04.05.2025)

20. Biometrics in banking: What you should know before implementing URL: https://www.n-ix.com/biometrics-in-banking/ (дата звернення: 04.05.2025)

21. Biometrics in Banking: Unlocking Security and Efficiency URL: https://www.techmagic.co/blog/biometrics-in-banking (дата звернення: 04.05.2025)

22. Biometric Devices 101: Definition and Examples URL: https://www.aratek.co/news/biometric-devices-definition-and-examples (дата звернення: 04.05.2025)

23. BIOMETRIC RECOGNITION METHODS URL: http://old-eclass.uop.gr/modules/document/file.php/TST178/DiplomaPapers/SurveyOnBiometrics.pdf (дата звернення: 09.05.2025)

24. Fingerprint Scanner URL: https://www.aratek.co/product-category/fingerprint-scanner (дата звернення: 04.05.2025)

25. Хорошко, В. О. Методи криптографічного захисту в СКУД / В. О. Хорошко, А. О. Корченко // Безпека інформації. – 2022. – Т. 28, № 3. – С. 145–153.

26. Біометричні системи контролю доступу на основі відбитків пальців і малюнка судин - які відмінності? URL: https://worldvision.com.ua/articles/biometricheskie-sistemi-kontrolya-dostupa-na-osnove-otpechatkov-paltsev-i-risunka-sosudov-kakovi-razlichiya (дата звернення: 04.05.2025)

27. How a Biometric Attendance System Can Benefit Your Business URL: https://www.aratek.co/news/how-a-biometric-attendance-system-can-benefit-your-business (дата звернення: 04.05.2025)

28. Biometric Terminal URL: https://www.aratek.co/product-category/biometric-terminal#truface-terminal (дата звернення: 04.05.2025)

29. BA8300 URL: https://www.aratek.co/product/face-recognition-terminal-ba8300 (дата звернення: 04.05.2025)

30. Access Controller Comparison URL: https://kintronics.com/access-controller-comparison/ (дата звернення: 19.05.2025)

31. Ukrainian surveillance cameras send data to Chinese manufacturers URL: https://kyivindependent.com/media-chinese-cameras-widely-used-in-ukraine-pose-security-risks/ (дата звернення: 20.05.2025)

32. Системи контролю доступу URL: https://zktecoua.com/ua/solutions/skud/ (дата звернення: 20.05.2025)

33. Програмне забезпечення для контролю доступу URL: https://zkteco.systems/ua/prod-category/programmnoe-obespechenie/dlja-kontrolja-dostupa/ (дата звернення: 20.05.2025)

34. Біометричний контролер доступу ZKTeco inBio460 URL: https://secur.ua/biometrija/kontrolery-biometricheskie/biometricheskij-kontroller-dostupa-zkteco-inbio460 (дата звернення: 21.05.2025)

35. Турнікет-трипод ZKTeco TS1022 Pro ZKTeco 8896 URL: https://secur.ua/kk/turnikety/pripody/turniket-tripod-zkteco-ts1022-pro?sc_content=27521_r1816v2264 (дата звернення: 21.05.2025)

36. Біометричний термінал ZKTeco MA300-BT URL: https://elektron.kiev.ua/ua/p1021576734-biometricheskij-terminal-zkteco.html (дата звернення: 21.05.2025)

37. KF1100&KF1200 URL: https://zkteco.systems/ua/product/kf1100-kf1200/ (дата звернення: 21.05.2025)

38. Installing access control systems – A step by step guide URL: https://www.security101.com/blog/sanfrancisco/installing-access-control-systems-a-step-by-step-guide (дата звернення: 21.05.2025)

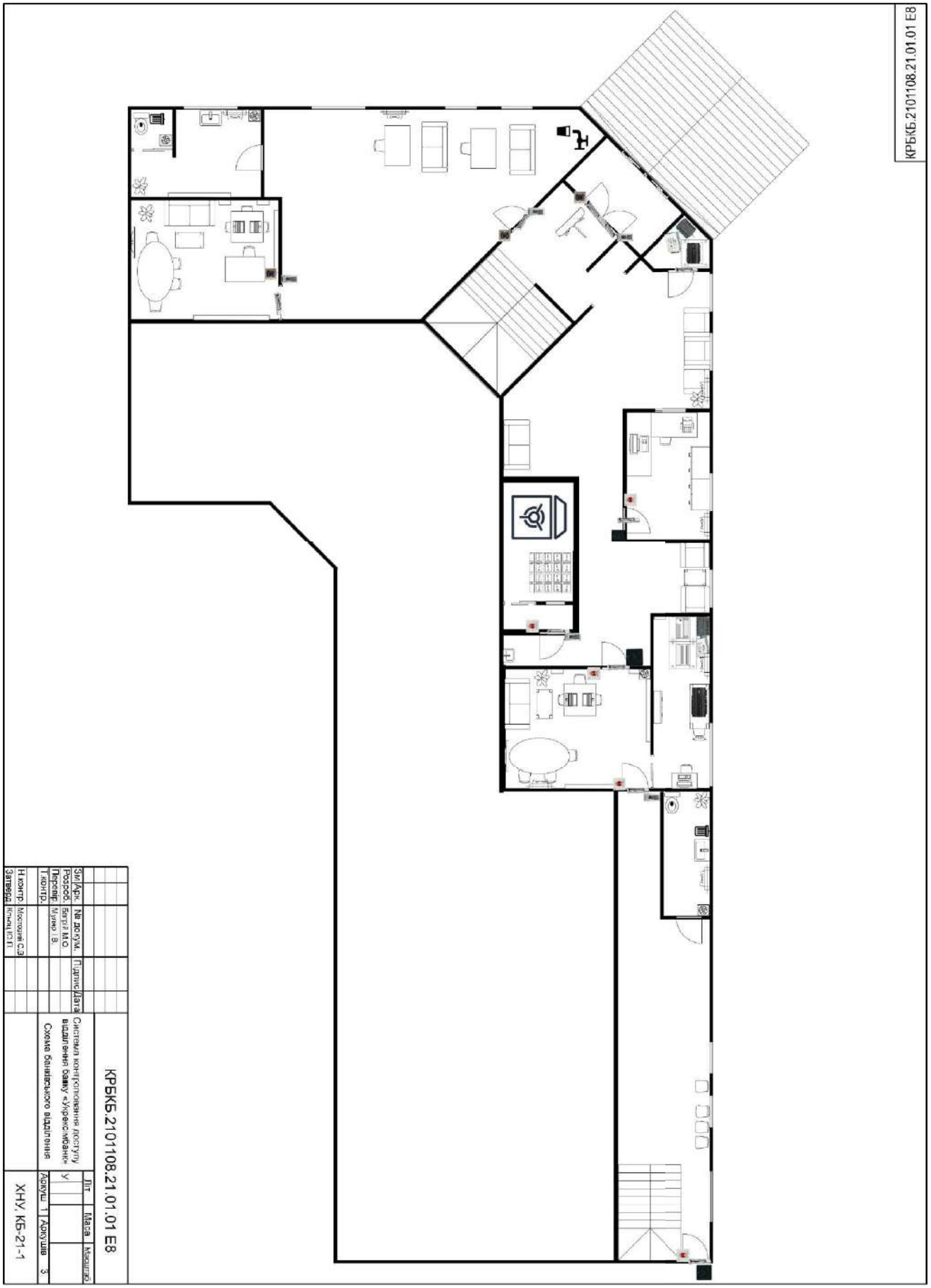
39. Biometric Access Control: Theory and Applications / edited by A. Brown, K. Davis. – London : Springer, 2022. – 387 p.

40. Modern Physical Access Control Systems / T. Anderson, P. Wilson. – California : O'Reilly Media, 2023. – 298 p.

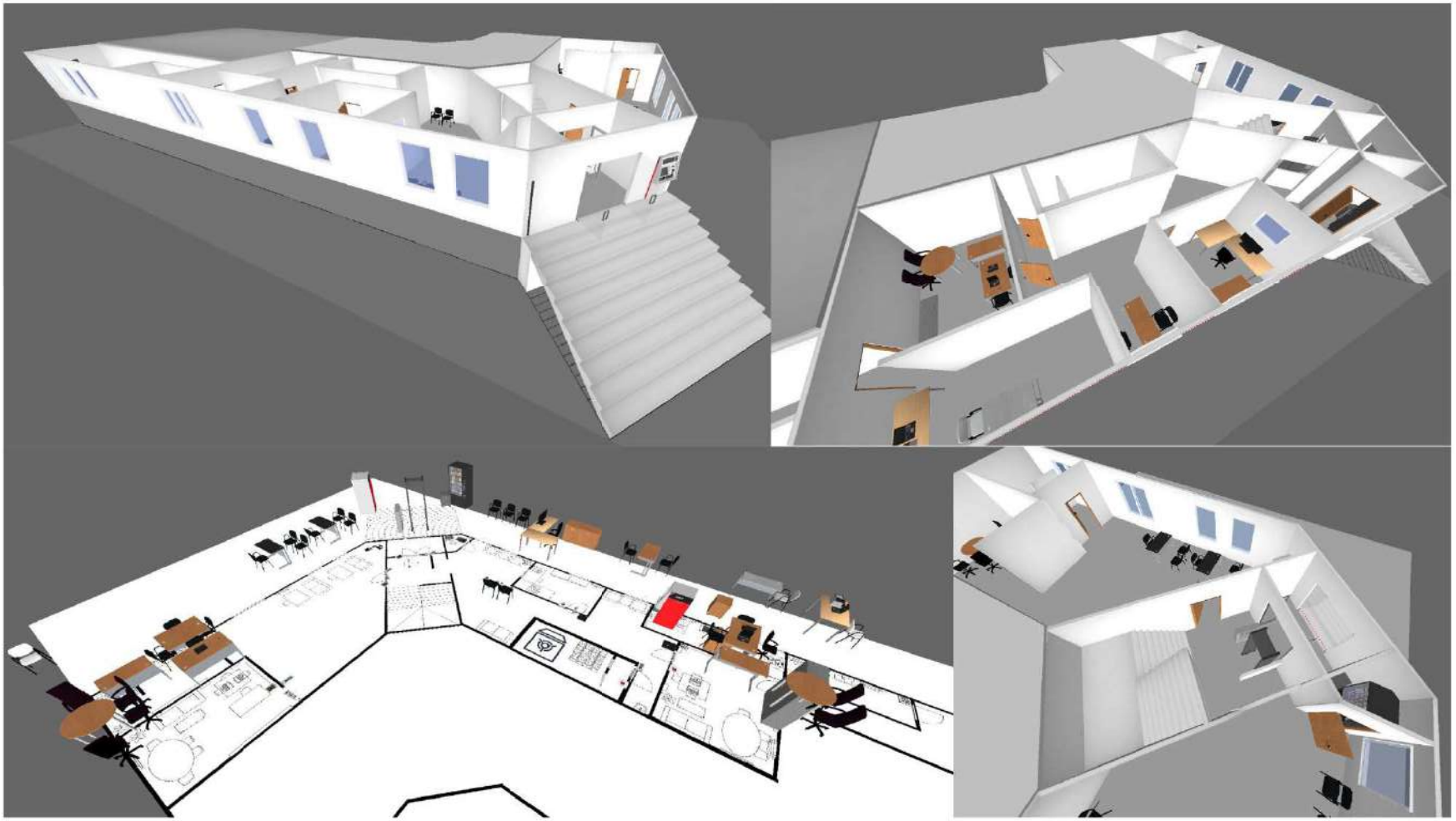
41. Security Engineering for Access Control Systems / edited by C. White, J. Taylor. – 2nd ed. – Cambridge : MIT Press, 2023. – 512 p.

ДОДАТОК А

Копія графічної частини

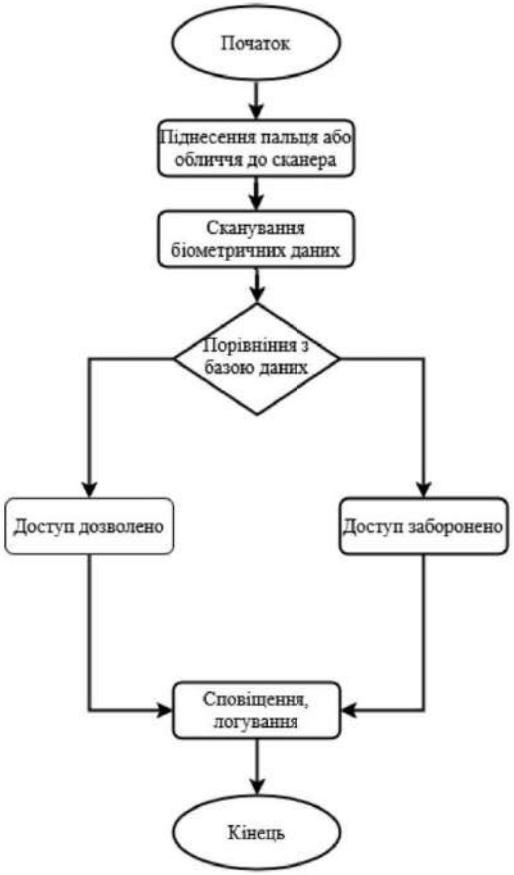


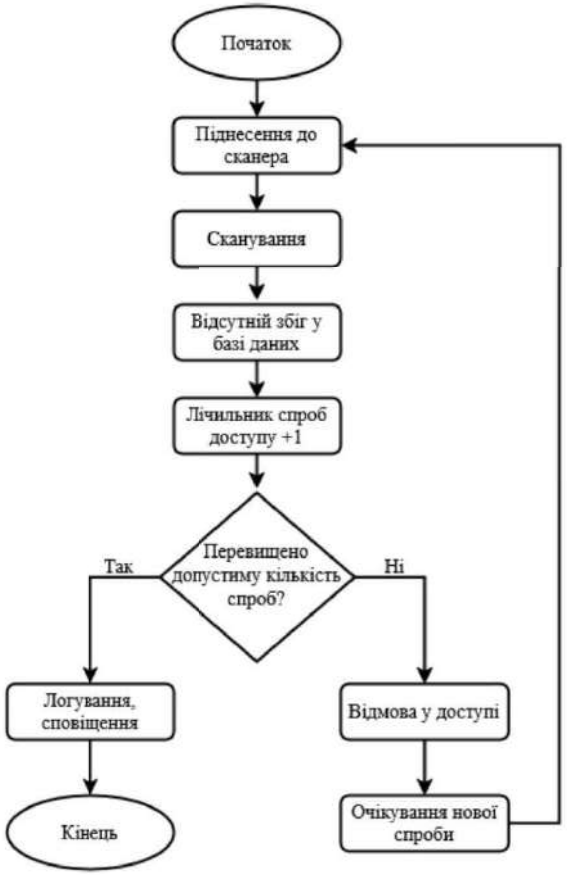
КРБКБ.2101108.21.01.01 Е8

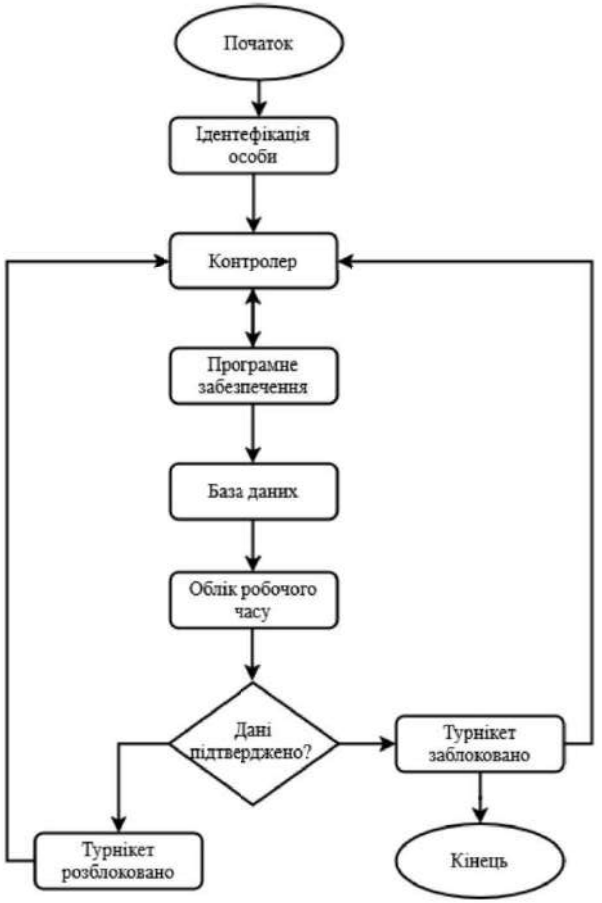


					КРБКБ.2101108.21.01.01 Е8			
Зм	Арк.	№ докум.	Підпис	Дата	Система контролювання доступу відділення банку «Укрексімбанк»	Літ	Маса	Масштаб
Розроб.		Бакрій М.О.				У		
Перевір.		Мупер І.В.			Модель банківського відділення	Аркуш 2	Аркушів 3	
Т.контр.								
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-1		
Затверд.		Кльоц Ю.П.						

КРБКБ.2101108.21.01.01 Е8







					КРБКБ.2101108.21.01.01 Е8			
Зм	Арк.	№ докум.	Підпис	Дата	Система контролювання доступу відділення банку «Укрексімбанк»	Літ	Маса	Масштаб
Розроб.		Багрій М.О.				У		
Перевір.		Мулар І.В.			Алгоритм роботи компонентів	Аркуш 3	Аркушів 3	
Т.контр.								
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-1		
Затверд.		Кльоц Ю.П.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Багрія Максима Олеговича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та зберження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

09.06
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Багрій Максим Олегович

Співавтор:

Назва: Система контролювання доступу «Укрексімбанк» м. Хмельницький з використання біометричної ідентифікації

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:2.1%

Коефіцієнт подібності 2:0.7%

Мікропробіли: 0

Заміна букв: 1

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-11 04:53:16.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

11.06.2025р.

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 7%**

ID: 244847 Title: Система контролювання доступу «Укрексімбанк» м. Хмельницький з використання біометричної ідентифікації Added in a DB: 2025-06-10 Authors: Багрій Максим Олегович Heads: Муляр І.В. Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	98675	603	509 (1%)	5 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система контролювання доступу «Укрексімбанк» м. Хмельницький з використання біометричної ідентифікації.

Автор: Багрій Максим Олегович.

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Ігор МУЛЯР, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 97,9%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Ігор МУЛЯР

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Багрій Максим Олегович

Тема Система виявлення атак на вузли в корпоративній мережі підприємства

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки .

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено систему контролювання доступу до банківського відділення та використали біометричну ідентифікацію. Проведено аналіз загроз фізичній та інформаційній безпеці, обґрунтовано вибір апаратного та програмного забезпечення, змодельована структура приміщення і системи доступу. В результаті сформовано рекомендації щодо впровадження СКД з використанням біометричних терміналів, що забезпечують захист від внутрішніх та зовнішніх загроз, створений план будівлі.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі повністю виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз загроз безпеки банківських інфраструктур та принципів їх захисту, з основним акцентом на сучасні біометричні методи ідентифікації. Другий розділ присвячено огляду існуючих рішень у сфері СКД, порівнянню біометричних пристроїв та обґрунтуванню вибору оптимального обладнання для банківського середовища. У третьому розділі реалізовано моделювання банківського приміщення з впровадженням обраних компонентів СКД, розроблено рекомендації з впровадження системи та оцінено її вартість.

4. Позитивні сторони роботи Робота має практичну цінність, оскільки розробляє ефективну систему контролювання доступу для банківського відділення на основі біометричної ідентифікації. Запропоновані рішення враховують сучасні загрози фізичній та інформаційній безпеці, забезпечуючи комплексний захист приміщення. Модель системи, апаратна частина та програмне забезпечення можуть бути впроваджені в реальних умовах банківської інфраструктури для підвищення рівня захищеності..

5. Негативні сторони роботи Встановлення біометричних СКД потребує значних фінансових ресурсів та технічної підготовки персоналу. У разі відсутності резервного живлення система може вийти з ладу. Чутливість до зовнішніх чинників.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень у проєктуванні та супроводі розробленої комплексної системи захисту інформації.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є "відмінно"

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Пивовар Олег Сергійович, к.т.н., доцент кафедри ТМІТ

« 12 » 06 2025. Пивовар О. С. (підпис)