Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
Кібербезпеки та захисту
інформації
_____Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційна робота
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 «Кібербезпека»
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Система багатофакторної автентифікації та об’єктового контролю на малому підприємстві»

Виконавець: студентка IV курсу, групи КБ-41

_____ **Марія ПАНАСЄЙКО**
(підпис) (прізвище ім’я по-батькові)

	Підпис	**Ім’я ПРІЗВИЩЕ**
Керівник		Микола БРАІЛОВСЬКИЙ
Нормоконтроль		Олександр ЛУКАШОВ

Київ 2025

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
Кібербезпеки та захисту
інформації
_____Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої-професійної програми)

студентці **КБ-41** **Панасєйко Марії Олександровні**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Система багатофакторної автентифікації та об'єктового контролю на малому підприємстві

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Детальний огляд поточної IT-інфраструктури об'єкта, включаючи апаратне забезпечення турнікетів і камер, існуючі мережеві протоколи та сервіси автентифікації, а також набір алгоритмів хешування, шифрування та біометричної верифікації, які вже застосовуються в системі.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту фізичного доступу, аналіз методів та
засобів багатофакторної автентифікації, архітектурні підходи до побудови

системи контролю доступу, технічні протоколи взаємодії периферійних пристроїв і центральних сервісів, основні вразливості турнікетів та зчитувачів, ризики обходу біометричних модулів і відеоаналітики, масштабування та моніторингу системи контролю доступу.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Можливість впровадження розроблених рішень на невеликих підприємствах.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: «29» листопада 2024 року

Завдання видав		Микола БРАІЛОВСЬКИЙ
	(підпис)	(ім’я, прізвище)
Завдання прийняв до виконання		Марія ПАНАСЄЙКО
	(підпис)	(ім’я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	23.01.2025 – 11.02.2025	*виконано*
3	Розгляд архітектури систем фізичного доступу та багатофакторної автентифікації	12.02.2025 – 24.02.2025	*виконано*
4	Дослідження основних вразливостей турнікетів, біометричних модулів і відеоаналітики	25.02.2025 – 24.03.2025	*виконано*
5	Вибір технологічного стеку для реалізації	25.03.2025 – 07.04.2025	*виконано*
6	Формування рекомендацій із інтеграції, масштабування та моніторингу системи	08.04.2025 – 20.05.2025	*виконано*
7	Оформлення пояснювальної записки	21.05.2025 – 08.06.2025	*виконано*
8	Підготовка до захисту	09.06.2025 – 19.06.2025	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім’я, прізвище)

Завдання прийняв до виконання _____ Марія ПАНАСЄЙКО
(підпис) (ім’я, прізвище)

Термін подання кваліфікаційної роботи до ЕК « 13» червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 60 сторінок, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. Крім того, робота містить 1 додаток із загальною кількістю сторінок 2. У пояснювальній записці кваліфікаційної роботи міститься 9 рисунків і 10 таблиць.

Метою роботи є формування комплексного підходу до побудови системи фізичного доступу з використанням сучасних методів ідентифікації, біометричних технологій та засобів відеоспостереження.

Для досягнення зазначеної мети поставлено наступні завдання:

- проаналізувати існуючі технології та підходи до автентифікації осіб при доступі до контрольованих об’єктів;
- визначити функціональні та нефункціональні вимоги до системи;
- сформувати архітектуру системи багатофакторної автентифікації з використанням камер відеоспостереження та алгоритмів розпізнавання обличчя;
- розробити структуру бази даних та алгоритми підтримки прийняття рішень у випадках спірних або нестандартних ситуацій.

Об’єктом дослідження є процес організації системи контролю доступу на об’єктах підприємницької діяльності.

Предметом дослідження є технічні та алгоритмічні засоби автентифікації ідентичності особи під час проходження через систему фізичного контролю доступу.

Практичною цінністю отриманих результатів є можливість впровадження розроблених рішень на невеликих підприємствах.

Ключові слова: ідентифікація, автентифікація, багатофакторна система, контроль доступу, розпізнавання обличчя, відеоспостереження, база даних, охоронна система, безпека підприємства.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

MTBF − Mean time between failures – середній наробіток між відмовами;

UPS − Uninterruptible Power Supply – джерело безперебійного живлення;

FAR − False Acceptance Rate – частота помилкового прийняття;

FRR − False Rejection Rate – частота помилкових відмов;

GPS − Global Positioning System - система глобального позиціювання;

SSO − Single Sign-On – технологія єдиного входу;

RFID − Radio Frequency Identification – радіочастотна ідентифікація;

OSDP − Open Supervised Device Protocol – відкритий протокол контрольованих пристроїв OSDP;

NFC − Near field communication – технологія бездротового зв’язку;

ONVIF − Open Network Video Interface Forum – галузева міжнародна організація;

RTSP − Real time streaming protocol – потоковий протокол реального часу;

NTP − Network Time Protocol – протокол мережевого часу;

PTP − Precision Time Protocol – протокол точного часу;

PoE − Power over Ethernet – технологія, яка передає віддаленому пристрою електричну енергію разом із даними;

VPN − Virtual private network – віртуальна приватна мережа;

GDPR − General Data Protection Regulation – загальний регламент із захисту даних;

PTZ-камера − Pan-tilt-zoom – камера, яка підтримує віддалене керування напрямком і збільшенням;

TCP − Transmission Control Protocol – протокол управління передачею;

IP − Internet Protocol – унікальний числовий ідентифікатор мережевого рівня;

TLS − Transport layer security – протокол захисту транспортного рівня;

LCD-панель − Liquid-crystal display – рідкокристалічний дисплей;

VMS − Video management system – система управління відео;

TCO − Total cost of ownership – сукупна вартість володіння;

API − Application programming interface – інтерфейс програмування застосунків;

DR-план − Disaster Recovery Plan – план аварійного відновлення;

SOA − Service-oriented architecture – сервісно-орієнтована архітектура;

HSM − Hierarchical Storage Management – ієрархічне керування носіями;

PKI − Public key infrastructure – інфраструктура відкритих ключів;

LDAP − Lightweight Directory Access Protocol – полегшений протокол доступу до директорій, каталогів;

SIEM − Security information and event management – аналіз у реальному часі подій (тривог) безпеки;

SNMP − Simple Network Management Protocol – простий протокол керування мережею;

GPU − Graphics processing unit – графічний процесор;

REST − Representational State Transfer – передача репрезентативного стану;

DMZ − Demilitarized Zone – демілітаризована зона мережі;

BLOB − Binary Large Object – бінарний великий об’єкт.

ВСТУП

Актуальність. У сучасних умовах стрімкого розвитку інформаційних технологій та зростання загроз несанкціонованого доступу до захищених об’єктів проблема забезпечення надійної ідентифікації користувачів стає особливо актуальною. В умовах, коли з одного боку зростає складність використовуваних засобів обходу безпеки, а з іншого – підвищуються вимоги до оперативності й зручності проходження на підприємствах різних профілів, багатофакторна автентифікація виступає одним із найефективніших механізмів захисту фізичного доступу.

Метою кваліфікаційної роботи є формування підходу до побудови системи фізичного доступу з використанням сучасних методів ідентифікації, біометричних технологій та засобів відеоспостереження.

Досягнення мети потребує розв’язання таких **задач**:

- аналіз існуючих технологій та підходів до автентифікації осіб при доступі до контрольованих об’єктів;
- визначення функціональних та нефункціональних вимог до системи;
- сформувати архітектуру системи багатофакторної автентифікації з використанням турнікетів, камер відеоспостереження, алгоритмів розпізнавання обличчя тощо.

Об’єкт дослідження: процес організації системи контролю доступу на об’єктах підприємницької діяльності.

Предмет дослідження: технічні та алгоритмічні засоби автентифікації ідентичності особи під час проходження через систему фізичного контролю доступу.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Оцінка сучасного стану проблеми проведена на основі вітчизняних

публікацій, які аналізують організаційні аспекти впровадження систем контролю доступу, а також зарубіжних досліджень у галузі комп’ютерного зору і криптографії для біометрії. Виявлено, що попри значні досягнення в обробці біометричних даних і масштабованих клієнт-серверних архітектурах, існує потреба в уніфікації протоколів взаємодії між периферійними пристроями та центральними сервісами, а також у гнучких механізмах адаптації продуктивності під різні сценарії навантажень.

Галузь застосування. Галузь охоплює корпоративні системи безпеки та автоматизації пропускного режиму на великих виробничих підприємствах, торгових центрах, аеропортах і інших об’єктах із підвищеними вимогами до безпеки. Запропоноване рішення може бути інтегроване як у нові інсталяції, так і в існуючі інфраструктури завдяки модульній архітектурі та відкритим API.

Новизна. Новизна роботи полягає у поєднанні інноваційних алгоритмів розпізнавання облич і відбитків пальців, адаптивного керування режимами продуктивності системи та автоматизованого журналювання з історизацією політик доступу. Запропоновано механізм контекстної зміни порогів біометричної верифікації залежно від інтенсивності потоку користувачів та рівня оцінки ризику, що дозволяє утримувати баланс між швидкістю обслуговування та точністю перевірки особи.

Практична цінність полягає в тому, що реалізована система може зменшити кількість невдалих спроб доступу та час простою користувачів у пікові періоди, підвищити стійкість до відмов обладнання за рахунок гарячого резервування модулів і забезпечити прозорість аудитів завдяки докладній історії транзакцій. Використання запропонованого підходу сприяє зниженню загальної вартості володіння (ТСО) та підвищенню рівня довіри до механізмів безпеки на об’єктах будь-якого масштабу.

РОЗДІЛ 1
АНАЛІЗ ПРОЦЕСІВ КОНТРОЛЮ ДОСТУПУ НА ПІДПРИЄМСТВІ

1.1 Огляд пропускної системи підприємства

Пропускна система є головним елементом інфраструктури фізичного доступу на підприємстві, яка забезпечує контрольний відбір та фільтрацію персоналу, що входить до приміщень виробничих або адміністративних корпусів. В контексті досліджуваної системи багатофакторної автентифікації й об’єктового контролю, пропускна система повинна задовольняти низку вимог до продуктивності, визначених робочим навантаженням підприємства. Зокрема, основним критерієм є здатність обробляти не менше 20-30 осіб за хвилину без зниження рівня зручності та безпеки.

Продуктивність пропускної системи вимірюється через кількість осіб, які мають можливість пройти механізм контролю доступу за одиницю часу. У реальних умовах промислового підприємства пікові навантаження спостерігаються під час початку та завершення робочих змін, що породжує кластери потоків працівників. Тому розрахункова пропускна здатність повинна враховувати як середню інтенсивність руху, так і пікові значення, які можуть перевищувати заплановані 20-30 осіб на хвилину.

Фактори, які впливають на пропускну здатність, доцільно сформувати наступним чином:

1) тип турнікетів і швидкість механізмів. Турнікети мають бути оснащені швидкодіючими роторними або шліцьовими елементами, здатними змінювати положення під дією електроприводів за час не більше 1,5-2 секунд на одного користувача;

2) швидкість взаємодії користувача із зчитувачем. Оптичні або радіочастотні зчитувачі повинні ідентифікувати електронні перепустки або

брелоки за час не більше 200-300 мс. Біометричні модулі (зокрема, сканери обличчя) вимагають додаткового часу на обробку зображень (до 0,5-1 секунд), що має бути враховано при плануванні інтервалу безперервної роботи;

3) інтеграція з відеоаналітикою. При багатофакторній авторизації система повинна одночасно зчитувати фото з перепустки, знімок з камери та, за потреби, додатковий факт участі охоронця. Затримка передачі відеоданих і їх обробка ШІ-алгоритмом розпізнавання облич не повинні перевищувати 1,5-2 секунд, щоб загальний час проходження не перевищував 3-4 секунд;

4) програмна оптимізація. Серверні компоненти повинні підтримувати асинхронне оброблення запитів, кешування результатів розпізнавання та багатопоточність, що дозволить уникнути вузьких місць у роботі системи при одночасному надходженні сотень запитів;

5) мережеві характеристики. Затримка при передачі даних між контролерами турнікетів і центральним сервером не повинна перевищувати 50-100 мс, а пропускна здатність локальної мережі має бути достатньою для передачі відеопотоку в реальному часі (щонайменше 10 Мбіт/с на камеру).

Для досягнення цільового рівня 20-30 осіб на хвилину необхідно передбачити конфігурацію з кількома каналами та резервними шляхами проходу. Рекомендовано застосування щонайменше двох стрімких турнікетів із пріоритетом для працівників із найбільшим інтенсивним потоком у пік. У разі перевищення запланованої інтенсивності (понад 30 осіб на хвилину) система може переключитися в режим високої продуктивності:

– збільшення затримки відповіді зчитувачів на налаштування мінімального часу читання;

– автоматичне підвищення пріоритету обробки розпізнаних зображень біометрії;

– тимчасове зниження суворості контролю (наприклад, відключення додаткового візуального підтвердження охоронцем).

Висока продуктивність повинна поєднуватися з гарантованим часом безвідмовної роботи (наприклад, середній час між відмовами – MTBF не менше

5×10^4 годин для обладнання та 99,9 % доступності серверних компонентів). Система резервного живлення (UPS) та дублювання мережевих карт контролерів створюють умови для безперервного функціонування навіть у разі відключення електроживлення або відмови окремих компонентів.

Для перевірки відповідності продуктивності заявленим вимогам слід застосувати такі методи:

1) стрес-тестування з емульованими потоками 50-60 користувачів на хвилину із фіксацією часу обробки одиничного запиту та середнього часу проходження;

2) моніторинг у реальному часі із накопиченням статистики про інтервали проходження та кількість одночасно оброблюваних транзакцій;

3) аналіз вузьких місць із використанням профайлерів програмного коду, мережевого моніторингу та тестування продуктивності дискових підсистем серверів;

4) випробування у реальних умовах підприємства протягом не менше тижня у пікові години змін.

На рис. 1.1 наведено базову схему контролю доступу підприємства, яка включає використання серверу, камер відеоспостереження різних типів тощо [1].

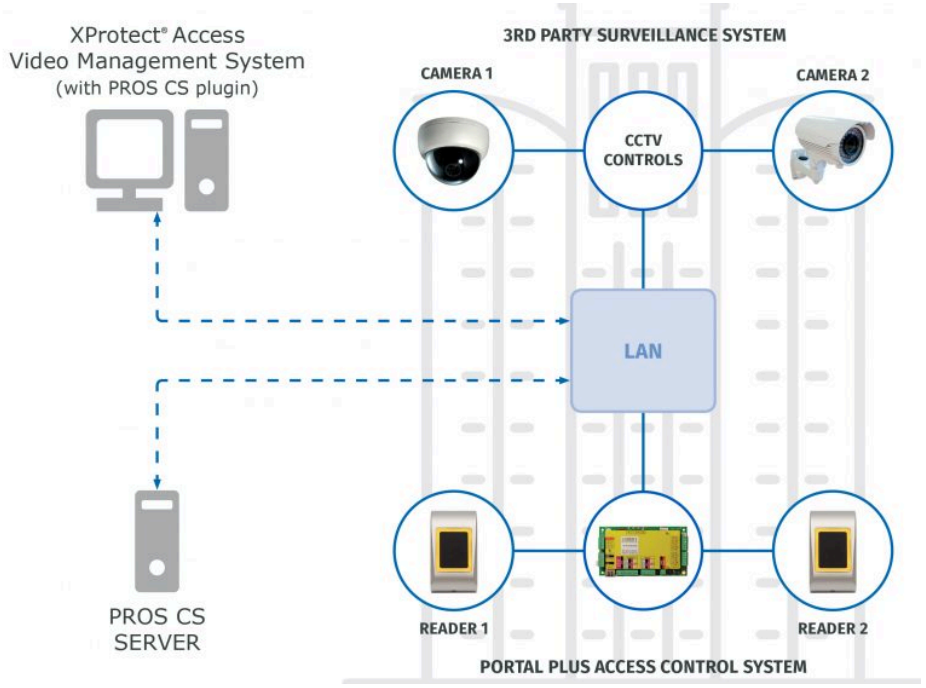

Рисунок 1.1 – Базова схема контролю доступу підприємства

Враховуючи всі зазначені фактори, пропускна система повинна бути спроєктована з врахуванням багатоканальної архітектури, високошвидкісних компонентів зчитування, оптимізованого програмного забезпечення та відмовостійких рішень.

Забезпечення продуктивності від 20 до 30 осіб за хвилину відповідає вимогам безперервності виробничих процесів, що необхідно для промислових і адміністративних об’єктів малого та середнього бізнесу.

1.2 Механізми ідентифікації та автентифікації

В сучасних інформаційних системах та засобах фізичного доступу поняття ідентифікації та автентифікації є фундаментальними для забезпечення безпеки ресурсів і контролю доступу [2]. Ідентифікація розглядається як початковий етап встановлення особи користувача або суб’єкта доступу до системи шляхом зіставлення наданих ним засобів ідентифікації з записами в опорній базі даних [3]. При цьому ідентифікаційним атрибутом може виступати будь-який унікальний маркер від логіна та номеру перепустки до біометричних ознак, що гарантовано відрізняють одну людину від іншої. Так, для підтвердження того, що зазначений суб’єкт дійсно є тим, за кого він себе видає, здійснюється автентифікація – процес підтвердження відповідності отриманих облікових даних справжньому власнику [4, 5]. Відмінність між цими двома етапами полягає в тому, що ідентифікація відповідає на питання «хто ви?», а автентифікація – «чи справді ви той, за кого себе видаєте?» [6].

В контексті побудови систем контролю доступу та відеоспостереження термін «ідентифікаційні дані» часто охоплює набір метричних і неметричних параметрів, що характеризують особу суб’єкта. Метричні дані включають кількісні показники, у той час як неметричні – якісні характеристики, такі як малюнок візерунка на відбитку пальця або геометрія обличчя. Для обробки та

порівняння цих даних застосовуються методи комп’ютерного зору, машинного навчання та штучного інтелекту, які здійснюють класифікацію та верифікацію заздалегідь навчених моделей.

Ключовим показником вбудованих біометричних модулів є точність, яку визначають через такі характеристики, як коефіцієнт хибного прийняття (False Acceptance Rate – FAR) та коефіцієнт хибного відхилення (False Rejection Rate – FRR) [7]. Перший показник відображає відсоток неавторизованих спроб, які були помилково визнані успішними, а другий – частку вірних користувачів, яким було відмовлено в доступі. Баланс між FAR і FRR є важливим: зниження FAR призводить до збільшення FRR, і навпаки. У багатофакторних системах застосування кількох незалежних факторів дозволяє оптимізувати цей баланс, знижуючи загальний ризик проникнення зловмисника при збереженні прийнятної зручності для легітимних користувачів [8].

Разом із цим у системах фізичного доступу використовують додатковий термін «нейтральний третій фактор» або «контекстний фактор», який охоплює характеристики оточення чи поведінки користувача. Це може бути час доби, місцезнаходження за GPS-координатами або аналіз шаблонів руху протягом робочого дня. Аналізуючи такі дані в реальному часі, система підтримки прийняття рішень може у разі невідповідностей або підозрілих аномалій блокувати спробу доступу або ініціювати додаткову перевірку [9].

У межах систем контролю відвідуваності підприємства важливим є розмежування понять «ідентифікація» та «автентифікація» від «авторизації». Якщо перші два процеси зосереджені на підтвердженні особи, то авторизація визначає, які саме права та привілеї належать цій особі після успішного входу в систему. У фізичних системах це може проявлятися у вигляді налаштування прав доступу до окремих зон підприємства: від адміністративних кабінетів до виробничих ділянок зі спеціальними умовами безпеки [10].

Єдині облікові дані (Single Sign-On, SSO) дозволяють користувачеві виконувати автентифікацію лише одного разу для отримання доступу до кількох систем без повторного введення пароля чи даних біометрії. Водночас така

архітектура вимагає підвищеного рівня захисту центрального механізму автентифікації, оскільки його компрометація відкриває доступ до всіх інтегрованих ресурсів. Наступним кроком важливо розуміти відмінності між «верифікацією» і «встановленням особи». Верифікація полягає в порівнянні наданих даних із заздалегідь збереженими шаблонами для підтвердження відповідності, тоді як встановлення особи може включати пошук за базою даних – наприклад, у разі розпізнавання обличчя серед великої кількості можливих зразків. Такий підхід працює за принципом «один до багатьох, 1:N», тоді як верифікація – за принципом «один до одного, 1:1» [11].

Отже, системи багатофакторної автентифікації на малих підприємствах поєднують у собі різноманітні технології та процедури, спрямовані на ефективне та безпечне підтвердження особи. Глибоке розуміння основних понять і термінів у цій сфері дозволяє правильно спроєктувати архітектуру, обрати оптимальне поєднання засобів і методів, а також забезпечити відповідність сучасним стандартам безпеки та нормативним вимогам.

1.3 Огляд загальних принципів побудови систем захисту фізичного доступу

Принципи побудови систем захисту фізичного доступу базуються на фундаментальній ідеї розподілу відповідальності між різними рівнями компонентів, які постачають комплекси засобів від запобігання незаконному проникненню до своєчасного виявлення та реагування на інциденти [12]. Перший і водночас найважливіший аспект полягає в ретельному аналізі об’єкта захисту та оцінці ризиків, адже лише після всебічного вивчення особливостей інфраструктури, взаємодії з навколишнім середовищем і потенційних загроз можна вибудовувати ефективну стратегію. Цей підхід передбачає системне застосування принципу багаторівневості, коли жоден окремий засіб не несе на собі всю відповідальність за безпеку, а кожен з рівнів доповнює інший,

створюючи оборонний простір із декількох захисних рубежів. На рівні периметра захисту реалізуються фізичні бар’єри та технологічні засоби стримування, що створюють перший рубіж проти несанкціонованого доступу [13]. В цьому контексті з метою попередження спроб злому чи обходу системи встановлюються різноманітні типи огорож, воріт, шлагбаумів та контрольно-пропускних пунктів, які оснащуються електромеханічними або електронними замками. Проте перше враження про безпеку має поєднуватися з удосконаленою внутрішньою організацією потоків людей та транспорту, тому простір периметра повинен бути чітко зонований відповідно до ступеня ризику та пріоритетності захисту. У поєднанні з механічними перешкодами, технологічні засоби контролю периметра доповнюються обладнанням відеоспостереження, що дає змогу фіксувати інциденти та проводити попередню аналітику руху завдяки алгоритмам штучного інтелекту.

Другий рівень захисту формується на внутрішніх контурах приміщень і включає контрольні точки у вигляді турнікетів, пропускних пунктів або дверей з електромагнітною фіксацією. Застосування біометричних модулів, RFID-зчитувачів [14, 15] та смарт-карт забезпечує точну ідентифікацію та автентифікацію користувачів та формування детальних журналів проходу. Особливу увагу приділяють часам відгуку засобів ідентифікації, аби зберегти пропускну спроможність підприємства та мінімізувати черги у пікові періоди. Центральні контролери керують відкриттям механізмів та синхронізують інформацію з серверною частиною, де відбувається зберігання та обробка даних [16, 17].

Третій рівень можна охарактеризувати як аналітично-реактивний: це сукупність систем, які здійснюють моніторинг подій у реальному часі, аналіз патернів поведінки та своєчасне оповіщення персоналу служби безпеки. До таких компонентів належать системи відеоаналітики, що за допомогою алгоритмів розпізнавання облич та виявлення аномалій в потоці осіб автоматично фільтрують підозрілі дії, а також датчики руху, відкриття та закриття дверей, розбиття скла і навіть сенсори температури або шуму.

Результати обробки надходять до консолі охоронця або центру керування, де працює система підтримки прийняття рішень. Інтелектуальні алгоритми розрізняють повідомлення за пріоритетністю та рівнем критичності, надаючи можливість миттєво зорієнтуватися в ситуації та прийняти оптимальне рішення – заблокувати доступ, викликати групу швидкого реагування чи відправити попереджувальне повідомлення відповідальним особам.

Забезпечення безперервності та надійності роботи системи захисту досягається шляхом впровадження резервування найважливіших елементів: резервних каналів зв’язку, дублювання серверів, автономних джерел живлення та аварійного проходу в разі виходу з ладу центральних контролерів або мережевого обладнання. Архітектура повинна підтримувати модульність, що дозволяє масштабувати систему з урахуванням зростання потреб підприємства чи зміни рівня загроз. Не менш важливою є сумісність з уже встановленими засобами та відкритими протоколами обміну даними, що забезпечує легку інтеграцію нових блоків системи без необхідності повноцінної заміни існуючої інфраструктури.

Будь-яка система захисту фізичного доступу повинна враховувати баланс між рівнем безпеки та комфортом користувачів. Перебільшена кількість перевірок або надто повільні процедури ідентифікації можуть призвести до зниження ефективності роботи підприємства та викликати незадоволення персоналу. Тому проєктувальники обирають оптимальні технологічні рішення з урахуванням специфіки діяльності, пропускної спроможності та психологічних аспектів взаємодії з користувачами. Усе це забезпечує створення системи, що поєднує високий рівень захисту, гнучкість налаштувань та зручність експлуатації, що в комплексі гарантує безперебійний та безпечний доступ уповноважених осіб до об’єктів малого підприємства.

1.4 Постановка завдання

У межах кваліфікаційної роботи основним завданням є розробка концепції та практичної реалізації системи багатофакторного контролю фізичного доступу, орієнтованої на потреби малого підприємства. Проблематика дослідження полягає в необхідності забезпечення надійного, швидкого та зручного механізму авторизованого проходу співробітників і відвідувачів до контрольованих зон із врахуванням обмежених фінансових і технічних ресурсів організації.

Система має відповідати сучасним вимогам інформаційної безпеки, а також бути адаптованою до змін навколишнього середовища, інфраструктурних особливостей об’єкта та людського фактору. Завданням є побудова рішення, яке поєднує в собі засоби ідентифікації та автентифікації за кількома незалежними ознаками (RFID, біометрія, PIN-код тощо), з можливістю централізованого управління правами доступу, збору та аналізу даних проходу, а також інтеграції з існуючими або новими системами безпеки.

Передбачається також розгляд архітектурних аспектів побудови системи, включаючи вибір програмно-апаратної платформи, способи зберігання та захисту персональних і біометричних даних, механізми реагування на аномальні події й забезпечення безперервності функціонування.

Постановка завдання охоплює як теоретичне обґрунтування вибору методів і засобів реалізації системи контролю доступу, так і створення прототипу з можливістю практичного застосування, що відповідатиме встановленим критеріям ефективності, надійності, масштабованості та відповідності нормативним вимогам у сфері захисту інформації та персональних даних.

1.5 Висновки за розділом 1

Перший розділ кваліфікаційної роботи висвітлює актуальність проблеми побудови надійних систем багатофакторної автентифікації в умовах зростання загроз інформаційній безпеці, окреслює мету й завдання дослідження, а також аналізує сучасні підходи до організації контролю доступу. У результаті було визначено, що поєднання декількох незалежних факторів і використання автоматизованих механізмів збору та обробки даних здатні значно підвищити рівень захисту об’єктів різного рівня важливості, що формує основу для подальших проєктних рішень.

РОЗДІЛ 2
МЕТОДИ ТА ТЕХНОЛОГІЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

2.1 Однофакторні та багатофакторні системи доступу

Однофакторні системи контролю доступу базуються на застосуванні єдиного критерію перевірки особи, який зазвичай полягає у пред'явленні та зчитуванні одного виду облікових даних. Традиційним прикладом є використання статичних паролів або пін-кодів, введення яких здійснюється користувачем за допомогою клавіатури або сенсорної панелі. На рис. 2.1 наведено порівняння різних видів автентифікації. [9, 11, 18].

Рисунок 2.1 – Порівняння різних видів автентифікації

У фізичних системах доступу цей підхід реалізується через магнітні або радіочастотні картки, що зберігають у чипі унікальні ідентифікаційні ключі, опрацьовувані контролерами турнікетів чи електромагнітних замків. Хоча однофакторні системи відрізняються простотою впровадження та відносно низькими витратами на обладнання й обслуговування, їхня безпека обмежується вразливістю до крадіжки чи копіювання єдиного секрету [18]. Під час порушення конфіденційності облікового носія зловмисник отримує

миттєвий доступ до всіх зон, які відкриває цей фактор, що створює критичні загрози для цілісності об’єкта.

Натомість багатофакторні системи доступу передбачають одночасну перевірку кількох незалежних факторів, які різняться за своєю природою й методами отримання. У рамках такої архітектури ідентифікація користувача здійснюється за наступною комбінацією [9, 11]:

1) те, що знає користувач;

2) те, що є у користувача;

3) те, чим є користувач.

У фізичних системах контролю доступу означає перевірку поєднання електронної перепустки та сканування відбитків пальців або розпізнавання обличчя за допомогою відеокамер. Поєднання різнорідних чинників ускладнює задачу компрометації системи, адже зловмисник має заволодіти фізичним носієм й подолати біометричні механізми або розкрити секретну інформацію.

У практичних реалізаціях багатофакторних систем ключове значення має послідовність і логіка обробки даних, оскільки кожен етап перевірки генерує власні затримки та ризики помилок. Початковий фактор дозволяє здійснити швидкий попередній відбір користувачів, одночасно вносячи мінімальні тимчасові витрати. Далі слідує біометричний етап або запит на введення секретного коду, що потребує більшої складності обробки й ресурсів системи. Останній крок за участі охоронця чи системи підтримки прийняття рішень гарантує додатковий рівень контролю, знижуючи рівень невідповідності навіть у випадках, коли попередні фактори дали суперечливі результати. Модульний підхід дозволяє додавати або вилучати фактори залежно від рівня загроз чи вимог нормативної бази. Зокрема, можна ввести додаткові шари аналізу поведінкової біометрії або контекстної інформації, такої як географічне розташування. При цьому необхідно передбачити протоколи взаємодії між локальними контролерами та центральною аналітичною платформою з обов’язковим застосуванням шифрування даних та захищених каналів зв’язку, щоб запобігти інтерцепції інформації й модифікації запитів.

В умовах малого або середнього підприємства вибір на користь одного з підходів визначається співвідношенням ризиків і ресурсів. Однофакторні системи можуть забезпечувати достатню безпеку там, де ймовірність цілеспрямованих атак є низькою, а основною задачею є контроль великих потоків персоналу зі швидким проходом через турнікети. У той же час багатофакторні системи доцільні в об’єктах, де необхідно убезпечити критичні зони з цінними активами або конфіденційною інформацією, незважаючи на зростання капітальних витрат та складність обслуговування.

2.2 Контроль доступу з використанням турнікетів

Засоби контролю доступу з використанням турнікетів формують фундаментальний елемент систем фізичного доступу, оскільки вони поєднують механічну перешкоду з електронним контролем і слугують безпосереднім інтерфейсом між середовищем охоронюваного об’єкта та користувачем. У сучасних рішеннях турнікети виконують роль бар’єру, що фізично обмежує проникнення, а також модуля активації взаємодії різних компонентів системи – від зчитувачів безконтактних карток до біометричних сенсорів, в тому числі інформування центрального контролера про факт і час проходження [19]. Схему роботи турнікету наведено на рис. 2.2. За конструкцією турнікети можуть відрізнятися за висотою, типом рухомих стрижнів чи шторок та характером приводу, проте в усіх випадках їх призначення полягає в забезпеченні одночасного поєднання механічної надійності, електронної точності й оперативного зворотного зв’язку з охоронною системою.

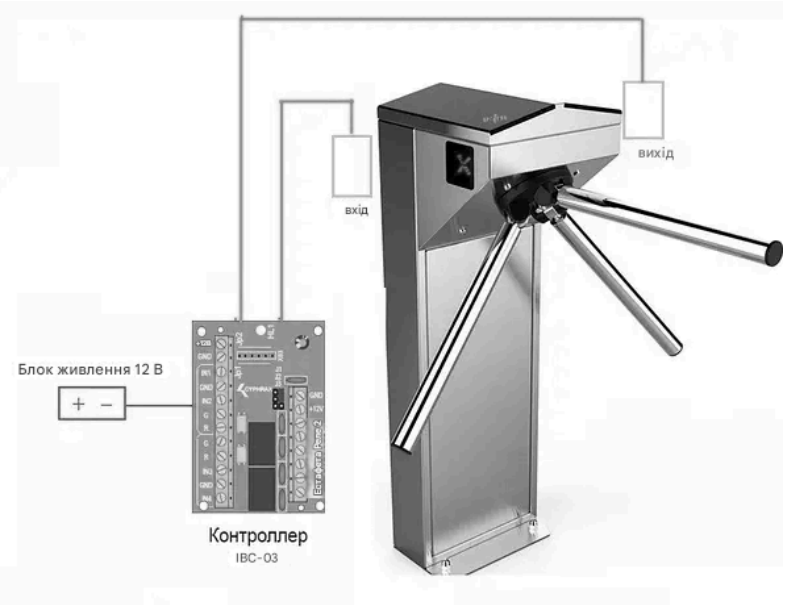

Рисунок 2.2 – Схема роботи турнікету

Головним параметром турнікетів є швидкість активації та періоду відкриття проходу, оскільки від цього залежить пропускна спроможність зони контролю доступу. Високошвидкісні турнікети забезпечують розкриття стрижнів або шторок протягом однієї секунди після отримання сигналу дозволу, що мінімізує час очікування працівників у години пік та запобігає формуванню заторів у контрольних пунктах. Цей показник досягається за рахунок використання потужних електродвигунів з високим крутним моментом та оптимізованих механізмів блокування, які гарантують одночасно швидкий рух і стійкість до навмисних спроб зриву або вандалізму [19]. Необхідним елементом є також регулювання моменту інерції рухомих елементів, що дозволяє досягти плавності пересування без різких ривків, які б могли призвести до травматизації користувачів або пошкодження обладнання.

Сучасні турнікети інтегруються в єдину мережеву інфраструктуру, де кожна спроба проходження супроводжується передачею цифрового сигналу на центральний контролер, а у випадку невдалого або несанкціонованого доступу – негайним оповіщенням служби безпеки. Така взаємодія здійснюється за допомогою стандартизованих протоколів обміну, серед яких найпоширенішими є Wiegand, OSDP та Ethernet TCP/IP, що забезпечують захищену передачу даних

із можливістю криптографічного шифрування. Водночас апаратна архітектура турнікетів передбачає наявність вбудованих реле для керування приводом, підсилювачів сигналу зчитувачів і модулів діагностики стану, що в режимі реального часу відслідковують напругу живлення, температуру двигуна та ступінь зносу механічних деталей [19]. Система датчиків безпеки гарантує зупинку або відкриття рухомих елементів у разі зустрічного руху або надмірного тиску. Імпульсні акустомагнітні або інфрачервоні сенсори фіксують присутність людини в зоні проходження й автоматично запобігають спрацьовуванню механізмів до повного звільнення простору.

Сучасні турнікети підтримують багатофакторну автентифікацію, інтегруючи в себе різні зчитувачі від безконтактних карток та NFC-пристроїв до сканерів відбитків пальців і камер для розпізнавання обличчя. Синхронізація даних від різнорідних сенсорів відбувається завдяки високопродуктивним процесорам реального часу, які аналізують вхідні сигнали та виносять рішення про надання або відмову в доступі. Комплексний підхід дозволяє підвищити рівень безпеки без значного зниження пропускної здатності, адже кожен етап обробки даних оптимізований і часто відбувається паралельно.

Дані про проходження, фото- або відеознімки, журнали подій та аналітичні звіти передаються в єдину базу даних, де зберігаються з можливістю подальшого пошуку і генерації статистичних звітів. Так, описані процеси створюють основу для систем підтримки прийняття рішень, які на основі накопичених даних здатні прогнозувати пікові навантаження, виявляти нетипову поведінку або потенційні загрози, а також планувати модернізацію інфраструктури для забезпечення належного рівня безпеки та зручності роботи персоналу. В цілому ж турнікети як засіб контролю фізичного доступу поєднують у собі механічну міцність, електронну інтелектуальність та гнучку інтеграцію в єдину систему безпеки.

2.3 Камери відеоспостереження та їх інтеграція в систему

Основним завданням камер відеоспостережень є забезпечення безперервного моніторингу зон впливу пропускних пунктів, фіксація й ідентифікація осіб, а також своєчасне передавання сигналів тривоги у разі виявлення небезпечних чи аномальних ситуацій [20]. Якість відеопотоку визначається технічними характеристиками камер: роздільною здатністю сенсорів, частотою кадрів, динамічним діапазоном та здатністю працювати в умовах змінного освітлення. У проєктуванні систем необхідно враховувати, що оптимальна роздільна здатність повинна забезпечувати можливість розпізнавання облич на відстані, достатній для коректної роботи алгоритмів аналізу, але в той же час не створювати надлишкового навантаження на мережу та сховища даних [21]. Інтеграція камер до єдиної платформи здійснюється за допомогою програмного забезпечення відеоменеджменту, яке відповідає за збір, архівацію й обробку відеоданих, а також за керування доступом до потоків через багаторівневі права користувачів.

На рис. 2.3 наведено різновиди камер відеоспостереження. На рис. 2.4 наведено приклад встановлення камери відеоспостереження біля турнікетів для контролю доступу. Приклад зображення, яке надає камера відеоспостереження, наведено на рис. 2.5.

Рисунок 2.3 – Камери відеоспостереження

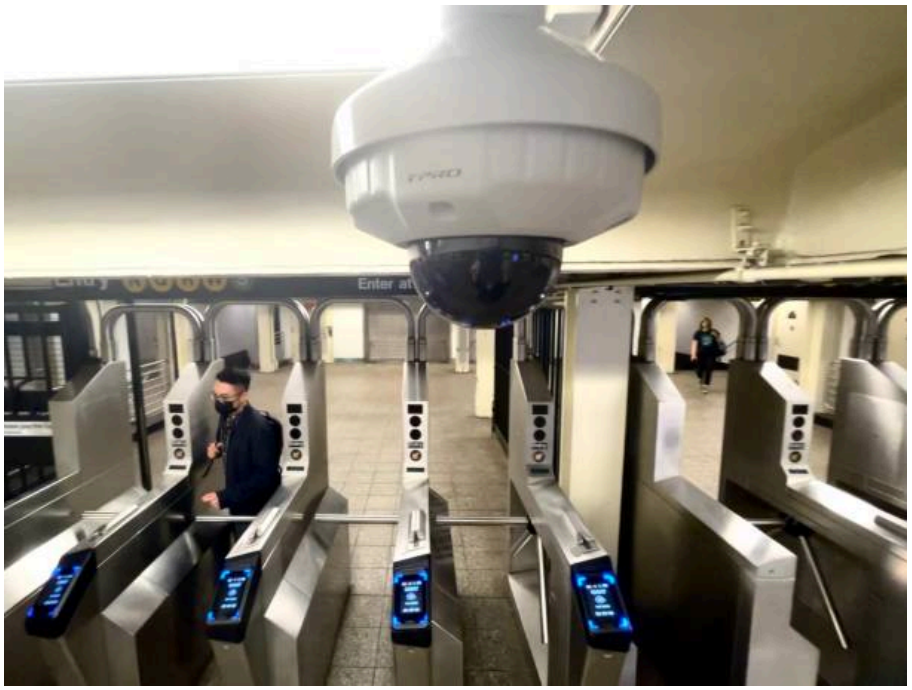

Рисунок 2.4 – Встановлена камера відеоспостереження

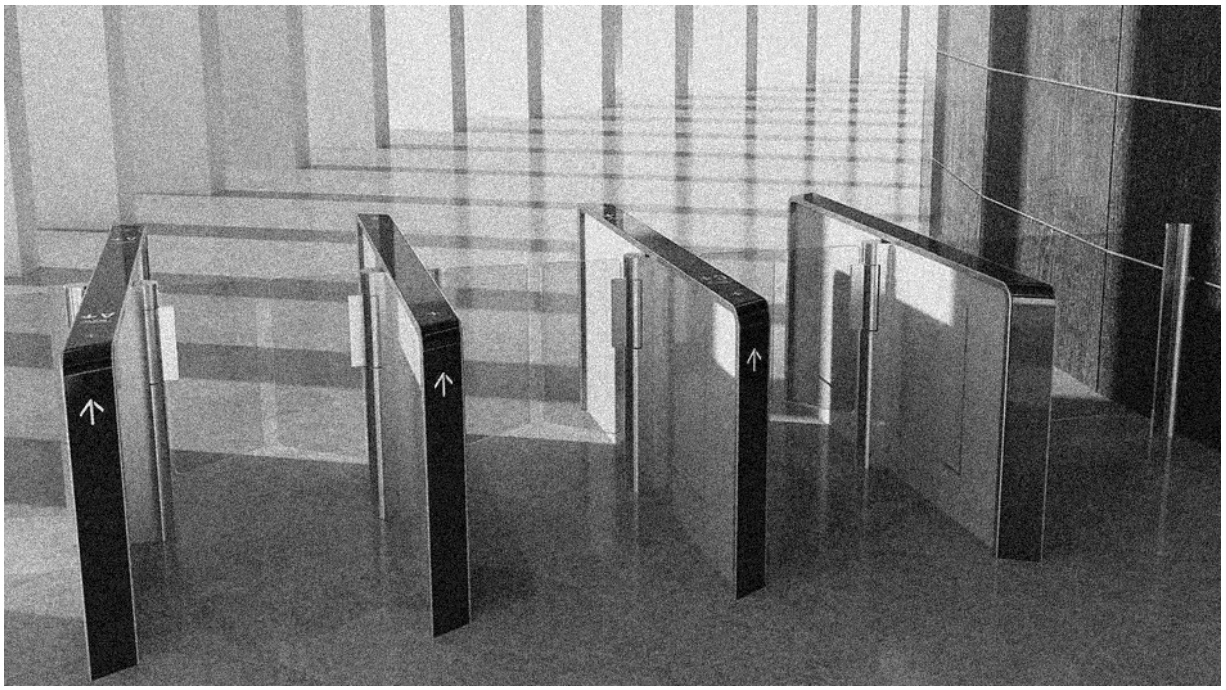

Рис. 2.5 – Зображення з камери відеоспостереження

Наступним етапом є налаштування архітектури передачі даних: для цього застосовуються протоколи ONVIF та RTSP, які стандартизують обмін командами та відеопотоком між камерами різних виробників і серверними компонентами системи. За сучасними вимогами до захищеності інформації передача й збереження кадрів відбуваються з використанням шифрування на рівні транспортного шару, що перешкоджає несанкціонованому доступу до архіву та унеможливлює підслуховування мережевого трафіку [22].

Для підвищення інтелектуальних можливостей системи все ширше впроваджуються алгоритми відеоаналітики на базі штучного інтелекту. Вони дозволяють автоматично виявляти та класифікувати рухомі об’єкти, розпізнавати обличчя та порівнювати їх із шаблонами в базі даних, визначати чисельність людей у кадрі, а також виявляти підозрілі дії, наприклад спроби прискореного проходу біля турнікету або присутність невпізнаних осіб у контрольованій зоні. Така аналітика, інтегрована з підсистемою контролю доступу, сприяє прискоренню обробки звернень: у разі успішного розпізнавання право на вхід надається миттєво, а в разі невідповідності – формуються

тривожні повідомлення, які передаються охоронцям або в ситуаційний центр для подальшого реагування.

Для синхронізація відеопотоку з іншими подієвими записами системи, зокрема з журналами проходження на турнікетах, кожному запису з камери привласнюється часовий штамп із високою точністю синхронізації через протоколи NTP або PTP. Це дозволяє у разі необхідності відтворити хронологію подій, встановити послідовність спрацьовувань декількох сенсорів та зіставити їх із відео, що істотно полегшує розслідування інцидентів і підтверджує правомірність дій персоналу.

Часто відеокамери встановлюються в мережеві архітектури із застосуванням протоколу Power over Ethernet (PoE), що одночасно забезпечує їх електроживленням і передачею даних. У цьому випадку важливо передбачити резервні канали живлення, стійкі до коливань напруги, а для критичних зон – дублювання камер із перекриттям полів огляду. Зберігання відео організовано на мережевих відеореєстраторах та системах з розподіленим сховищем, обладнаних механізмами реплікації даних. При цьому стратегія зберігання може передбачати прецедентне видалення найстаріших файлів лише після того, як на них не було жодних звернень протягом певного періоду, що дозволяє гарантувати доступ до архівів на випадок спливу термінів звичайних політик зберігання [23].

Оператори та адміністративний персонал повинні мати доступ до відеопотоку в реальному часі та архівних матеріалів з будь-якої точки у межах корпоративної мережі або через захищені VPN-з’єднання з віддалених локацій. Інтерфейс відеоменеджменту часто доповнюється мобільними додатками, які спрощують отримання тривожних сповіщень та оперативний перегляд фрагментів запису. Враховуючи сучасні вимоги до кібербезпеки, такі програми використовують багатофакторну автентифікацію та шифрування даних від початку до кінця, зберігаючи конфіденційність інформації навіть у разі втрати пристрою користувача [20, 21]. Оскільки відеоспостереження включає обробку чутливої інформації про осіб, необхідно додатково передбачити механізми

анонімізації, коли для щоденного моніторингу використовується спрощене зображення з розмиттям облич, а детальний матеріал доступний лише у разі підтверджених інцидентів або за запитом уповноважених осіб. Управління правами доступу до відеоканалів, аудит операцій із запитами на відтворення та зберігання логів забезпечують прозорість і контроль за дотриманням норм GDPR або інших регуляцій.

Конфігурація камер та їх оптимальне розташування в просторі реалізується на основі попередньої оцінки характеристик охоронюваного об’єкта та моделювання полів огляду. Використання 3D-моделей та спеціалізованого програмного забезпечення дозволяє імітувати розміщення пристроїв, оцінити покриття зони та визначити оптимальні кути нахилу та положення, щоб уникнути «сліпих зон» та мінімізувати імовірність перекривання секторів огляду. Під час монтажу слід враховувати зовнішні чинники: рівень освітленості, інтенсивність трафіку, погодні умови, а також необхідність захисту корпусів камер від пилу та вологи відповідно до рейтингів IP. На стадії введення в експлуатацію відбувається фінальне тестування системи на стабільність роботи під піковими навантаженнями, а також перевірка взаємодії камер із турнікетами та іншими сенсорами. У ході цього тестування відстежуються показники затримок обробки відеоаналітики, швидкість реагування на тривожні події та коректність запису подій із точністю до мілісекунд. Результати тестування надалі використовуються для коригування налаштувань: наприклад, підвищення частоти кадрів у ключових зонах під час змін пік-годин або збільшення інтенсивності освітлення там, де алгоритми розпізнавання облич показали найнижчу точність [22, 23].

В умовах малого підприємства зі стриманим бюджетом необхідно досягти балансу між функціональністю та вартістю обладнання. Виробники пропонують широкий спектр камер із різною глибокою інтеграцією до систем доступу: від базових моделей з підтримкою PoE до високошвидкісних PTZ-пристроїв із програмними модулями аналітики. За оптимальної стратегії вибору можна сконцентрувати більш потужні й інтелектуальні модулі у найбільш вразливих

чи критичних точках, а для зон із середніми вимогами використовувати бюджетніші рішення з базовим набором функцій реєстрації.

Отже, камери відеоспостереження стають невід'ємним компонентом комплексних систем контролю фізичного доступу, де їх роль полягає в постійному моніторингу, аналітичній обробці даних та взаємодії з іншими засобами безпеки. Інтеграція відеопотоку зі зчитувачами перепусток, турнікетами і центральними серверними компонентами забезпечує єдиний механізм прийняття рішень у режимі реального часу, що гарантує як швидкість проходу легітимних користувачів, так і своєчасне виявлення та попередження спроб несанкціонованого доступу. Належне проєктування, монтаж і налаштування системи відеоспостереження сприяють створенню ефективного, масштабованого та безпечного середовища для роботи персоналу малого підприємства.

2.4 Технології розпізнавання обличчя

Технології розпізнавання обличчя в складових сучасних систем фізичного доступу поєднують у собі досягнення галузі штучного інтелекту, обчислювальної техніки та прикладної статистики й служать ключовим механізмом верифікації особи на підставі аналізу візуального образу [24]. У центрі цих технологій лежить ідея зіставлення двох наборів даних: довідкового зображення, зафіксованого під час видачі перепустки чи створення профілю користувача, та фрагментів відеопотоку, який надходить з камер спостереження в режимі реального часу. Процес розпізнавання обличчя складається з послідовних етапів, кожен з яких вимагає узгодженої роботи апаратних засобів і програмних алгоритмів.

Первинний етап включає отримання відеокадру та попередню обробку зображення з метою виявлення присутності людського обличчя. На цьому кроці застосовуються методи комп'ютерного зору, зокрема каскадні або згорткові

нейронні мережі, які здійснюють локалізацію зон інтересу та виділення координат ключових точок на обличчі. Альтернативою класичним підходам може виступати система на основі глибокого навчання, яка одночасно визначає місцерозташування об’єкта та створює первинний опис його просторово-геометричних характеристик. На цьому етапі визначається, чи відповідає кадр мінімальним технічним вимогам: достатній чіткості, освітленості та розмірності області з обличчям, адже некоректна сегментація призводить до зниження точності подальшого порівняння. Після успішного виявлення обличчя здійснюється нормалізація зображення: кадр вирівнюється за обертанням та масштабом згідно із заздалегідь визначеними еталонними точками [25, 26]. Цей крок дозволяє компенсувати варіативність положення голови та зменшити вплив незначної деформації при зйомці під різними кутами. Подальша корекція кольорових каналів і фільтрація шумів забезпечують стандартизованість вхідних даних для алгоритмів, які працюють з високорозмірними векторами ознак.

Наступним елементом при побудові моделей розпізнавання облич є формування дескрипторів – компактних чисельних векторів, які максимально стисло характеризують особливості обличчя людини. Архітектури глибоких згорткових мереж, наприклад на основі ResNet або MobileNet, часто використовують п’ять-дев’ять блоків згорток і пулінгу разом із шаром нормалізації, щоб досягти оптимального співвідношення між точністю та швидкістю обробки. Під час тренування такі моделі піддаються навчальному процесу на великих базах даних, де зображення пронумеровані належністю до конкретних осіб. Використання функції втрат типу triplet loss або ArcFace дозволяє створити таке параметричне відображення, у якому вектори ознак одного й того ж користувача лежать близько в просторі ембеддінгів, тоді як вектори різних осіб віддалені один від одного на відстань вище встановленого порогу.

Після отримання дескрипторів як з референтного зображення перепустки, так і з фрагменту відеопотоку, необхідно виконати процедуру порівняння в

просторі ознак. Алгоритмічний механізм зазвичай полягає у вимірюванні косинусної відстані або евклідової відстані між двома векторами [26, 27]. Якщо розрахована відстань не перевищує заздалегідь визначене значення, система вважає, що особа на відео відповідає тій, чия фотографія міститься в базі даних. Порогове значення формується з урахуванням компромісу між коефіцієнтом хибного прийняття та коефіцієнтом хибного відхилення, що критично впливає на експлуатаційні характеристики системи. Реалізація цієї функціональності в рамках системи контролю доступу передбачає інтеграцію модуля відеоаналітики з центральною платформою керування. Камери передають відеопотік на сервер або вбудований модуль, де відбувається попередня обробка та побудова дескрипторів. Оскільки обчислювальні ресурси на місці можуть бути обмежені, часто застосовують розподілену архітектуру: на периферії розгортаються легкі нейромережеві модулі, які здійснюють детекцію та нормалізацію кадрів, а важкі обчислення дескрипторів та порівняння відбуваються на центральному сервері або в хмарі. Такий поділ завдань забезпечує оперативну реакцію на події та знижує затримки в локальній мережі.

Системи, які використовують технології розпізнавання обличчя, повинні бути оптимізовані з урахуванням варіативності умов експлуатації: змін освітлення, різних положень користувача під час проходу через турнікет, носіння окулярів, головних уборів, масок або шарфів. Для підвищення стійкості системи до подібних викликів застосовуються стратегії навчання з аугментацією даних, які включають випадкову зміну яскравості, контрасту, повороти зображень та накладення штучних перешкод. У деяких рішеннях впроваджують багатокадрову агрегацію, коли алгоритм аналізує не один одиночний кадр, а серію кадрів протягом декількох часток секунди, створюючи середній дескриптор, який менш чутливий до раптових змін виразу обличчя або напрямку погляду [25-27].

Інтеграція модуля розпізнавання обличчя з компонентами контролю доступу передбачає взаємодію з базою даних користувачів, в якій зберігаються шаблони-дескриптори, а також додаткові атрибутивні дані: рівень доступу, роль

у системі, графік роботи та інші метадані, необхідні для прийняття рішення про надання дозволу чи відмову. Після успішної верифікації система передає сигнал на контролер турнікета, фіксує факт проходу з точним відміткою часу та, за необхідності, робить знімок або короткий запис події в архіві. Якщо ж верифікація не пройшла – на моніторі служби безпеки відображається кадр з невдалою спробою, а автоматизована система може сповіщати охоронців про потенційну загрозу. Напрямком розвитку технологій розпізнавання облич є застосування адаптивного машинного навчання, коли модель постійно оновлюється під впливом нових даних, отриманих в процесі експлуатації. Це дозволяє підвищити точність та стійкість системи до майбутніх змін зовнішніх умов, але при цьому вимагає жорсткого контролю за якістю даних, щоб уникнути непередбачуваних похибок або вразливостей через атаки на процес навчання.

Технології розпізнавання обличчя в сучасних системах фізичного доступу виступають як високотехнологічний компонент, що поєднує комп’ютерне бачення, розробки в галузі глибокого навчання та архітектурні рішення з відмовостійкості й безпеки даних. Їх впровадження дозволяє знизити ризики несанкціонованого проникнення, оптимізувати облік робочого часу, автоматизувати звітність та підвищити зручність використання системи для легітимних користувачів. За умови правильної інтеграції, налаштування та підтримки ці технології стають надійним інструментом забезпечення надійного, безпечного та комфортного доступу на малих підприємствах.

2.5 Попередження про відеоспостереження і інформаційні табло

У концептуальному сенсі попереджувальні системи можна розглядати як зв’язок між технологічною інфраструктурою і психологічним аспектом поведінки людей, адже наявність видимої індикації відеоспостереження або

інформаційних табло стимулює усвідомленість працівників і відвідувачів щодо необхідності дотримання встановлених процедур безпеки. У загальній архітектурі систем попередження передбачено використання як стаціонарних, так і динамічних інформаційних панелей, розташованих у ключових точках доступу та пересування. Стаціонарні елементи виконані у вигляді постійних табличок та наклейок на видимих поверхнях турнікетів, дверей і стін коридорів, і містять графічні та текстові повідомлення щодо того, що територія перебуває під відео- та аудіомоніторингом. Динамічні інформаційні табло, які мають можливість відображення змінюваних повідомлень у режимі реального часу, інтегруються безпосередньо з центральною системою контролю доступу та відеоменеджменту, що дозволяє демонструвати оперативну інформацію про стан контролю доступу, кількість поточних транзакцій проходу та навіть ідентифіковані обличчя або коди перепусток осіб, які наближаються до контрольного пункту.

Функціональна логіка роботи динамічних табло передбачає, що при фіксації події успішного розпізнавання особи або підтвердження дійсності перепустки система автоматично формує повідомлення, яке виводиться на екран відповідного інформаційного вузла. Ці повідомлення можуть бути стандартизованими, наприклад, відображенням часу та позначенням зони доступу, або контекстно залежними – наприклад, інформуванням про режим роботи турнікета (активний чи у технічному обслуговуванні).

Інтеграція табло з підсистемами відеоспостереження забезпечує ще один рівень інформування – у разі виявлення аномальних або небезпечних ситуацій динамічні екрани можуть негайно відобразити попереджувальні сигнали та інструкції з евакуації або додаткові оповіщення про необхідність втручання охорони. Це досягається за рахунок налаштування подієвої логіки центрального програмного забезпечення, яке аналізує відеопотік, події з детекторів руху та інформацію від контролерів турнікетів. У разі перевищення заданих порогів або фіксації спроби несанкціонованого доступу табло переключається у режим екстреного інформування, змінюючи фонове зображення, колірні акценти та

текстові повідомлення, що привертають увагу до ситуації. Для синхронізації часових міток та версій повідомлень між усіма компонентами системи з метою гарантування коректності відображення інформації застосовується єдина мережа часу з використанням протоколів NTP або PTP, а дані про події з контролерів пропуску й аналітичних модулів надходять до центрального сервера, де формуються пакети з повідомленнями для кожного інформаційного вузла. Передача здійснюється через захищені канали TCP/IP з використанням TLS-шарів, що унеможливлює підміни або зависання контенту.

В умовах малого підприємства, де ресурси для впровадження великих інформаційних мереж можуть бути обмежені, системи попередження й табло зазвичай реалізуються на базі недорогих, але надійних рішень із використанням стандартних медіаплеєрів і LCD-панелей малого формату. Програмна платформа, що керує контентом, може працювати на локальному сервері або віртуальній машині з невеликими апаратними вимогами. Для зручності експлуатації передбачається автоматичне оновлення контенту по мережі та можливість завантаження нових шаблонів простою заміною текстових та графічних файлів у певному каталозі.

У комплексній системі захисту фізичного доступу інформаційні табло виконують не лише функцію інформування, але і виступають елементом психологічного стримування. Видимість відеокамер у поєднанні з нагадуваннями про моніторинг створюють відчуття безперервного нагляду, що значно знижує ймовірність навмисних порушень. Одночасно динамічне відображення даних допомагає підвищити рівень залученості працівників до процедур безпеки, оскільки наочні показники спонукають їх дотримуватися вимог і оцінювати результати власної дисципліни.

Таким чином, системи попередження про відеоспостереження і інформаційні табло становлять невід’ємну складову сучасних комплексів контролю фізичного доступу. Вони забезпечують багаторівневе інформування користувачів, сприяють дотриманню законодавчих вимог, підвищують рівень безпеки та комфорту, а також виконують соціальну роль у формуванні культури

безпеки на підприємстві. Застосування таких систем на малих підприємствах дозволяє досягти ефективного балансу між інвестиціями в інфраструктуру та якістю контролю, що позитивно позначається на загальній економічній доцільності проєкту.

2.6 Аналіз та порівняння обладнання

Вибір обладнання для систем фізичного доступу обумовлений необхідністю поєднати високу продуктивність із гнучкістю масштабування та оптимальною вартістю володіння. В табл. 2.1 проведено аналіз обладнання [28-31].

Таблиця 2.1

Аналіз обладнання

Категорія обладнання	**Продуктивність**	**Вартість (€)**	**Споживана потужність**	**Примітки**
1	2	3	4	5
Турнікети (економ)	20-25 осіб/хв	300-600 €	–	Механічні з електромеханічним приводом; базова пропускна спроможність для малого бізнесу
Камери (базові)	–	100-150 €	5-20 Вт	2-4 Мп, PoE, ONVIF/RTSP; фіксують події, базова аналітика відео
Камери (середній рівень)	–	200-350 €	5-20 Вт	6-8 Мп, ШІ-аналітика на борту, розширений динамічний діапазон
Камери (преміум)	–	400-600 €	5-20 Вт	4K, вбудовані нейропроцесори для реального аналізу; найвища автономність

продовження таблиці 2.1

Біометричні модулі (економ)	–	150-200 €	–	Оптичні/ємнісні сканери відбитків; час розпізнавання 0,5-1 с, вищий рівень хибних відмов
Сервери (базові)	~50-100 камер або 20 турнікетів	600-800 €	сотні Вт	4-ядерний CPU, 8 ГБ RAM, SSD 256 ГБ; базова аналітика та обробка потоку відео
Сервери (середній рівень)	до 200 камер і 50 турнікетів	1 500-3 000 €	сотні Вт	Intel Xeon, 16-32 ГБ RAM, RAID-масив; підходить для середніх підприємств
Сервери (клас Enterprise)	тисячі одночасних підключень	десятки тисяч €	сотні Вт – кВт	Кластерні рішення, петабайтні системи зберігання, глибинна аналітика з ML

Ринок рішень для контролю проходу пропонує широкий спектр апаратних та програмних продуктів, які відрізняються швидкістю обробки транзакцій (кількість користувачів, яких система може обслужити за одиницю часу), можливістю нарощувати потужність без втрати якості роботи, а також загальною вартістю впровадження й експлуатації. Аналіз найпопулярніших рішень дозволяє виявити закономірності, які лежать в основі ухвалення ефективних інженерних та економічних рішень для підприємств малого та середнього бізнесу.

Починаючи з турнікетів, які виступають першою лінією фізичного бар’єру, на ринку представлена продукція від відомих виробників – від класичних механічних турнікетів із електромеханічним приводом до високошвидкісних моделей із вбудованими зчитувачами RFID та біометричними сканерами. Турнікети економкласу зазвичай забезпечують пропускну здатність близько 20-25 осіб на хвилину, при цьому вартість одиниці може коливатися в межах від 300 до 600 євро залежно від типу приводу та матеріалів корпусу. Моделі середнього рівня з оптимізованими

електроприводами та швидкими зчитувачами дозволяють обробляти до 30-35 осіб за хвилину та оснащені додатковими датчиками безпеки й аварійного розблокування – їхня ціна стартує від 700 євро і сягає 1200 євро за одиницю.

Найдорожчі високошвидкісні турнікети бізнес-класу з можливістю інтеграції в єдину IT-інфраструктуру та вбудованими модулями аналізу потоків можуть обслуговувати понад 50 осіб на хвилину, проте вартість таких рішень зазвичай перевищує 2000 євро за турнікет, що робить їх менш привабливими для малих підприємств, але доцільними в установах із високою інтенсивністю руху [28, 29].

Камери відеоспостереження, інтегровані в системи контролю доступу, також представлені в різних цінових сегментах. Базові мережеві камери з роздільною здатністю 2-4 Мп і підтримкою PoE забезпечують достатню якість зображення для загальної фіксації подій за ціною близько 100-150 євро за одиницю. Вони легко інтегруються з системами VMS (Video Management Software), працюють із відкритими протоколами ONVIF та RTSP, але їхні можливості відеоаналітики обмежені вбудованими або додатковими ліцензійними модулями. Камери середнього рівня з підтримкою аналітичних алгоритмів на базі ШІ, розширеним динамічним діапазоном і роздільною здатністю 6-8 Мп коштують приблизно 200-350 євро, але забезпечують покращене розпізнавання облич і виявлення руху з високою точністю. Пристрої преміум-класу, оснащені вбудованими нейропроцесорними модулями для аналізу відеопотоку в реальному часі й підтримкою 4K-запису, можуть коштувати від 400 до 600 євро за одиницю, проте вони забезпечують оптимальне поєднання продуктивності й автономності обробки даних, знижуючи навантаження на центральні сервери й мережеву інфраструктуру [30, 31].

Біометричні модулі, які є складовою багатофакторних систем, мають власну структуру цінових категорій. Економічні рішення на базі оптичних або ємнісних зчитувачів відбитків пальців початкового рівня продаються за ціною близько 150-200 євро і демонструють швидкість розпізнавання 0,5-1 секунди,

проте мають підвищений рівень хибних відмов у складних умовах експлуатації. Модулі середнього класу, що поєднують оптичні й ультрафіолетові технології сканування, забезпечують підвищену стійкість до підробки відбитків і швидкість на рівні 0,3-0,5 секунди, їхня ціна варіюється від 250 до 400 євро [30]. Найдорожчі біометричні системи, що працюють за принципом мультібіометрії (відбитки пальців плюс розпізнавання долоні або венозної сітки), а також оснащені високопродуктивними алгоритмами ШІ, можуть коштувати понад 600 євро за пристрій, але дозволяють обробляти сотні перевірок за хвилину з надзвичайно низькими показниками FAR і FRR, що робить їх незамінними для об’єктів із підвищеними вимогами до достовірності верифікації.

З точки зору інформаційної складової, центральні сервери для обробки даних систем контролю доступу та відеопотоку також поділяються на класи продуктивності й цінові категорії. Просте програмно-апаратне рішення на базі 4-ядерного процесора з 8 ГБ оперативної пам’яті та SSD-диском об’ємом 256 ГБ коштує в середньому 600-800 євро і може обслуговувати до 50-100 одночасних камер або 20 турнікетів із базовою аналітикою. Системи середнього рівня з процесорами Intel Xeon, 16-32 ГБ оперативної пам’яті та RAID-масивами дисків забезпечують можливість обробляти до 200 камер і 50 турнікетів з багатофакторною автентифікацією і можуть мати вартість від 1500 до 3000 євро [30]. Для великих підприємств із високим навантаженням випускаються потужні вузли з можливістю масштабування в кластері, оснащені десятками ядер, сотнями гігабайтів оперативної пам’яті та системами зберігання у петабайтному діапазоні; їхня вартість обчислюється десятками тисяч євро й більше, але вони здатні обслуговувати тисячі одночасних підключень і проводити глибинний аналіз за участю алгоритмів машинного навчання.

Серед характеристик, які впливають на остаточну вартість системи, слід врахувати не лише ціну обладнання, а й витрати на ліцензії програмного забезпечення, послуги з монтажу та налаштування, навчання персоналу і щорічну підтримку. Багато постачальників пропонують моделі ліцензування

«per device» або «per channel», де вартість одного турнікета чи однієї камери включена у вартість базової ліцензії, а додаткові функції аналітики або модулі ШІ купуються окремо. При цьому комбінування обладнання одного вендора часто дозволяє отримати знижки на об’єднану ліцензію та скоротити витрати на інтеграцію, а використання рішень із відкритим кодом може знизити витрати на ПЗ, але підвищити потребу в технічних навичках для підтримки системи.

При первинному аналізі часто акцент робиться на ціні закупівлі, проте надійність, тривалість служби та вартість технічного обслуговування можуть значно змінити кардинальні цифри протягом 5-10 років експлуатації. Економічні турнікети та камери зазвичай мають гарантію 12-24 місяці, тоді як професійні моделі – до 60 місяців. Вартість заміни вузлів або сервісних виїздів інженера може становити від 50 до 150 євро за прилад, що слід враховувати при плануванні загальних витрат на володіння (TCO). Крім того, важлива готовність виробника надавати оновлення прошивки та програмного забезпечення протягом усього періоду експлуатації, оскільки це суттєво впливає на безпеку й продуктивність системи.

Сучасні турнікети та камери споживають від 5 до 20 Вт у робочому режимі, а сервери можуть витрачати сотні ват. Витрати на електроенергію та охолодження можуть становити до 20-30% від загального TCO системи, тому вибір енергоефективних компонентів, підтримка режимів енергозбереження та використання PoE-комутаторів із стандартом IEEE 802.3az може знизити ці витрати з часом.

Огляд ринку обладнання для систем фізичного доступу демонструє, що оптимальне рішення для малого підприємства починається з чіткого визначення вимог до продуктивності – кількості користувачів на хвилину та одночасних підключень, – розуміння необхідної гнучкості для масштабування проєкту й адекватної оцінки всіх статей витрат, включно зі вартістю обладнання, ліцензій, монтажу, підтримки та енергоспоживання.

2.7 Інтеграція з IT-інфраструктурою та масштабування системи

Проблематика інтеграції охоплює як технічний, так і організаційний рівень, вимагаючи врахування апаратних, програмних і адміністративних аспектів взаємодії між різними компонентами IT-середовища. Особливої актуальності це питання набуває в умовах малого й середнього бізнесу, де ресурси для глибокої адаптації обмежені, а вимоги до простоти обслуговування й оперативного реагування залишаються високими. Практично кожне підприємство вже має певний набір інформаційних сервісів: доменну структуру на базі Active Directory або її аналоги, засоби електронної пошти, системи документообігу, програмні платформи для обліку робочого часу, CRM або ERP-рішення. Інтеграція системи автентифікації з цими сервісами дозволяє мінімізувати дублювання даних, уникнути конфліктів у керуванні обліковими записами та спростити впровадження політик безпеки на всіх рівнях.

Найбільш раціональний підхід полягає у створенні єдиного центру автентифікації з підтримкою протоколів LDAP, Kerberos або SAML, до якого буде прив’язана система контролю доступу. Важливою технічною вимогою до інтеграції є також уніфікація форматів зберігання та обміну даними між підсистемами. На практиці це означає використання стандартних структур JSON або XML, RESTful API для запитів і відповідей, а також дотримання принципів розділення доступу на рівні ролей та дозволів. Наприклад, API контролера доступу має дозволяти не тільки запити на відкриття турнікета чи зчитування подій, а й зміну параметрів конфігурації, додавання нових користувачів або оновлення політик у режимі реального часу. Підтримка таких функцій вимагає дотримання принципів транзакційності, зворотності операцій та журналювання будь-яких змін, що має відображатися у внутрішній структурі баз даних та сервісів, що обслуговують запити.

Інтеграція також неможлива без врахування питань безпеки – як на рівні протоколів, так і на рівні загальної архітектури. Необхідно забезпечити

шифрування всіх каналів зв’язку (TLS 1.3), автентифікацію клієнтів і серверів за допомогою цифрових сертифікатів (PKI), а також захист від несанкціонованого втручання в протоколи команд. Важливо, щоб кожен компонент – від камери до центрального сервера – міг проходити взаємну автентифікацію й отримувати доступ лише до дозволених функцій. На рівні архітектури це реалізується через політики Zero Trust, коли кожен запит перевіряється незалежно від того, звідки він надійшов, і кому належить.

2.8 Висновки за розділом 2

У другому розділі проведено детальний огляд і порівняльний аналіз доступного на ринку обладнання для реалізації систем контролю, зокрема турнікетів, біометричних сканерів, камер відеоспостереження та серверної інфраструктури. Встановлено, що вибір комбінації компонентів має базуватися на їхній пропускній здатності й вартості та енергоефективності, можливості масштабування й інтеграції з існуючими корпоративними сервісами, а також на супровідних витратах, які включають ліцензування, монтаж та технічну підтримку. Такий комплексний підхід забезпечує оптимальне співвідношення загальної вартості володіння й рівня безпеки системи.

РОЗДІЛ 3
ПРОЄКТУВАННЯ БАГАТОФАКТОРНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ

3.1 Функціональні та нефункціональні вимоги до системи

Процес формування вимог до системи багатофакторної автентифікації та контролю доступу починається з глибокого аналізу бізнес‑процесів підприємства, виявлення потреб користувачів та визначення критичних сценаріїв використання. На цьому етапі необхідно окреслити головні функціональні ролі майбутнього рішення в контексті забезпечення захищеності, ефективності організації пропускного режиму та зручності щоденного застосування. З одного боку, система повинна виконувати базову функцію контролю доступу: надавати або відмовляти у праві проходження на підставі перевірки одночасно кількох факторів, які поєднують фізичний носій, біометричні дані та за необхідності участь персоналу служби безпеки. З іншого боку, необхідно передбачити можливість ведення повного журналу подій із точними часовими відмітками, збереженням фотографій та супроводжуючих атрибутів транзакцій, а також формувати запити на звіти за фільтрами за різними ознаками, що сприятиме оперативному та ретроспективному аналізу поведінки персоналу.

У ході збору функціональних вимог необхідно врахувати сценарії як денного пікового навантаження, так і неробочого часу з мінімальними затримками або автоматичним переходом у режим карантину. Застосунок повинен реагувати на потік працівників зі швидкістю не менше ніж двадцять осіб на хвилину в базовому режимі та забезпечувати плавне розгортання високопродуктивного режиму при значно вищому навантаженні з мінімальною деградацією показників. Рішення має об’єднувати кілька апаратних компонентів: модулі керування турнікетами, біометричні сенсори або камери

розпізнавання облич, контролери, а також програмний рівень, що виконує зіставлення отриманих даних із базою авторизованих користувачів. При цьому система зобов’язана дотримуватися чіткої послідовності перевірки: спочатку зчитування електронної перепустки або запиту від мобільного додатка, потім – біометричної автентифікації та, за потреби, автоматичного оповіщення або ручної перевірки охоронцем.

В табл. 3.1 наведено усі функціональні вимоги до системи.

Таблиця 3.1

Функціональні вимоги системи

Категорія вимоги	**Опис**
1	2
Багатофакторна автентифікація	Забезпечення контролю доступу з одночасною перевіркою кількох факторів (фізичний носій, біометричні дані, за потреби участь персоналу служби безпеки)
Повний журнал подій	Реєстрація всіх транзакцій із точними часовими мітками, збереженням фотографій або відео невдалих/успішних спроб, а також додаткових атрибутів транзакцій
Генерація аналітичних звітів	Можливість формувати звіти за різними фільтрами (час, користувачі, тип події тощо) для оперативного та ретроспективного аналізу
Підтримка пікового та позаробочого режимів	Автоматичне перемикання між режимом мінімальних затримок у пікові години та карантинним режимом у неробочий час

Серед нефункціональних вимог, які наведено в табл. 3.2, ключове місце посідають показники продуктивності та відмовостійкості. Архітектура системи повинна гарантувати безперервний час відгуку на запит авторизації не більше ніж одну секунду в середньому для кожної транзакції в нормальних умовах, з максимальною затримкою в критичних періодах не більше трьох секунд.

Таблиця 3.2

Нефункціональні вимоги системи

Категорія вимоги	**Опис**
1	2
Мультиканальні оповіщення	Централізована конфігурація ланцюжка сповіщень: при відсутності реакції на перше повідомлення за певний час автоматично надсилається наступне повідомлення вищому рівню відповідальності
Збір телеметрії інтерфейсу оператора	Моніторинг часу відображення повідомлень, кількості одночасно відкритих вікон, частоти звернень до модулів аналітики тощо для оцінки ефективності роботи та швидкого коригування інтерфейсу
Захищеність каналів передачі	Використання шифрування TLS 1.3 та сертифікатів PKI для всіх комунікацій між периферійними пристроями, сервером автентифікації та модулями відеоаналітики
Висока доступність і відмовостійкість	Побудова кластеризованої СУБД із реплікацією та автоматичним відновленням вузлів, застосування HSM-модулів для зберігання ключів шифрування та дескрипторів
Інтуїтивний адміністративний інтерфейс	Консоль з простим управлінням користувачами, ролями, робочими зонами, шаблонами звітів та налаштуваннями обладнання з багаторівневою системою доступу до функцій адміністрування

Важливо передбачити горизонтальне та вертикальне масштабування компонентів, щоб підтримувати зростання кількості точок доступу та користувачів без необхідності повної переробки інфраструктури. Сервісні шари мають бути розгорнуті в контейнерах або віртуальних машинах із автоматичним балансуванням навантаження та механізмами гарячого резервування для усунення одиничних точок відмови.

Дані повинні зберігатися з використанням кластеризованих рішень для БД з реплікацією в режимі реального часу та автоматичним відновленням у разі пошкодження окремого вузла. Передача даних між периферійними пристроями та центральним сервером має здійснюватися через захищені канали з

використанням сучасних стандартів шифрування TLS 1.3 та симетричних алгоритмів з високим ступенем стійкості. Зберігання чутливих даних, зокрема біометричних дескрипторів, повинно реалізовуватися із застосуванням апаратних модулів безпеки (HSM) та односторонніх хеш-функцій із сольовими значеннями для виключення можливості їх відновлення. Цифрові сертифікати для довіреної взаємодії між сервісами необхідно реалізувати на основі PKI з періодичною ротацією ключів та централізованим аудитом їх використання.

Інтерфейс адміністратора має включати інструменти для простого керування користувачами, керування правами доступу, налаштування робочих зон та часових графіків, а також моніторинг стану обладнання в режимі реального часу. Для зниження витрат на навчання персоналу слід передбачити єдину консолілю з інтуїтивно зрозумілим інтерфейсом, можливістю налаштовувати шаблони звітів і автоматизовані сповіщення про аномалії або збої. Також необхідно забезпечити багаторівневу систему ролей і прав доступу до самих адміністративних функцій, щоб мінімізувати ризики випадкової або навмисної зміни налаштувань.

З точки зору надійності експлуатації, до нефункціональних вимог належить забезпечення сервісного обслуговування обладнання без необхідності зупинки роботи всієї системи. Це можна досягти завдяки модульній конструкції апаратних компонентів та можливості їх гарячої заміни або резервуванню з автоматичним переключенням. Базові системні компоненти мають підтримувати дистанційний моніторинг показників зносу та температурних режимів із використанням SNMP або подібних протоколів управління мережевими пристроями, що дозволить формувати завдання на профілактичне обслуговування до настання критичного стану. Також необхідно забезпечити підтримку LDAP/Active Directory для централізованого керування обліковими записами й інтеграцію з корпоративними SIEM‑системами для централізованого збору логів і кореляції подій безпеки. Зручність розгортання системи посилюється за рахунок контейнеризації сервісів, автоматичних

скриптів для налаштування середовищ та готових Docker/Kubernetes‑чартів для швидкої інтеграції в хмарні або гібридні середовища.

Система має відповідати вимогам GDPR щодо обробки персональних даних, забезпечувати можливість виконання запитів на видалення даних та оновлення записів відповідно до законодавства. Для об’єктів із підвищеними вимогами до безпеки слід врахувати стандарти ISO 27001 та 30107 для біометричних систем, а також національні нормативні документи із фізичного захисту об’єктів критичної інфраструктури.

Необхідним нефункціональним атрибутом є відмовостійкість і здатність системи оперативно відновлюватися після інцидентів. Для цього потрібно інтегрувати в архітектуру механізми бекапу та резервного копіювання даних, включно з чутливими та архівними записами, а також відпрацювати процедури аварійного відновлення в рамках DR-плану. Кожен ключовий компонент системи – контролер доступу, сервер автентифікації, модуль відеоаналітики – повинен мати штатні й аварійні сценарії, які передбачають автоматичне перемикання на резервні канали або сервери та повідомлення адміністраторів.

Поза цим, система повинна забезпечувати гнучкість для подальшого розширення функціональності. Інтерфейси API для інтеграції зі сторонніми додатками та службами дозволять у майбутньому додавати нові методи автентифікації або аналітики без зміни базових модулів. Забезпечення відповідності архітектурним патернам SOA або мікросервісів дає змогу швидко масштабувати окремі підсистеми та вмикати їх у загальне середовище автоматизації підприємства.

Отже, формування вимог до системи багатофакторної автентифікації та контролю фізичного доступу є комплексним завданням, що включає точне визначення функціональних сценаріїв, які гарантують своєчасну та надійну ідентифікацію користувачів, а також встановлення суворих нефункціональних критеріїв щодо продуктивності, безпеки, надійності, зручності експлуатації, сумісності з IT‑інфраструктурою і відповідності нормативам. Відтак рішення повинно поєднувати передові технології апаратної та програмної складових із

гнучкою архітектурою, що забезпечує високий рівень захисту, якісну аналітику, оперативність роботи та можливість подальшого росту й адаптації до нових викликів безпеки.

3.2 Архітектура системи багатофакторної автентифікації

Архітектура системи багатофакторної автентифікації представляє багаторівневу модульну структуру, спрямовану на забезпечення високої надійності, відмовостійкості та гнучкості в розгортанні і подальшій еволюції комплексу засобів захисту фізичного доступу. В табл. 3.3 розглядаються компоненти архітектури системи. У її основі лежить концепція розподілених сервісів, кожен з яких відповідає за окремий клас функціональних задач, при цьому логічна зв’язність компонентів досягається через стандартизовані інтерфейси й протоколи взаємодії. Ключовим елементом архітектури є виділення трьох базових шарів: периферійного, проміжного та центрального, а також підшару управління, який забезпечує координацію та оркестрацію всіх сервісів в єдиний інтегрований механізм перевірки особи і контролю проходу.

Таблиця 3.3

Компоненти архітектури системи

Шар	Компоненти	Функції
Периферійний	Турнікети з вбудованими контролерами, RFID-зчитувачі, біометричні сенсори, IP-камери	Початкова обробка сигналів і верифікація коректності зчитування; формування цифрових пакетів; передача даних по захищених каналах TLS
Проміжний	Кластер сервісів попередньої обробки (маршрутизація, балансування, кешування, фільтрація за політиками)	Фільтрація подій (за графіками, зонами), маршрутизація та балансування навантаження, кешування успішних результатів; масштабування кластера
Центральний	Сервери автентифікації, БД з реплікаціями, модулі	Виконання ресурсомістких алгоритмів (біометрія, політики доступу), прийняття рішень про

	обчислення дескрипторів, API для прийняття рішень	дозвіл/відмову, зберігання журналів подій

продовження таблиці 3.3

Шар управління	Адміністративна консоль, SNMP/REST-моніторинг, система CI/CD, Kubernetes, черги повідомлень (RabbitMQ/Kafka)	Оркестрація всіх сервісів, централізоване адміністрування політик, моніторинг стану компонентів, автоматичне реагування на інциденти

На периферії системи розташовані апаратні модулі, встановлені безпосередньо у точках доступу підприємства. До них належать турнікети з вбудованими контролерами, зчитувачі радіочастотних карток, біометричні сенсори та IP-камери розпізнавання обличчя. Кожен із цих пристроїв виконує початкові операції – зчитування чи фіксацію вхідних даних – й формує цифровий пакет, який надсилається до проміжного рівня. При цьому архітектурна модель передбачає тонке клієнтське розвантаження: на місці відбувається лише первинна обробка сигналів та верифікація коректності зчитування, тоді як всі ресурсоємні алгоритми обчислюються далі. Система використовує сучасні стандарти передачі даних, зокрема захищені канали на базі TLS, що гарантують цілісність і конфіденційність інформації під час транспортування від периферійних пристроїв до центральних серверів.

Проміжний шар відповідає за попередню обробку вхідних повідомлень, маршрутизацію запитів та балансування навантаження. У цьому підшарі розгортаються спеціалізовані сервіси, які приймають потоки подій від десятків чи сотень точок доступу, застосовують до них чергові правила, наприклад фільтрацію за часовими графіками або зонованими політиками контролю, та передають результати до серверів автентифікації. Тут же здійснюється кешування останніх успішних результатів верифікації, що істотно знижує затримки при повторних проходах протягом короткого періоду. Архітектурні

рішення проміжного рівня передбачають горизонтальне масштабування: за необхідності до кластеру сервісів можна додавати нові вузли, а балансувальник розподіляє запити згідно із заданими правилами продуктивності та доступності.

Центральний рівень включає ядро системи – сервери автентифікації, бази даних користувачів, модуль обробки відеоаналітики та сервіс звітності. Сервер автентифікації приймає дескриптори як з модулів біометрії, так і з модулів зчитування перепусток, виконує порівняння з шаблонами в базі даних і приймає остаточне рішення про дозвіл або відмову в доступі. Для розпізнавання обличчя застосовується модуль глибинного навчання, який базується на заздалегідь натренованих нейронних мережах. Ці мережі можуть бути реалізовані як у вигляді окремого сервісу на GPU‑прискорювачах, так і як сервіс у хмарі, залежно від вимог до продуктивності й бюджету. Центральний сервіс відеоаналітики синхронізується з системою контролю та формує додаткові метадані: рівень впевненості в розпізнаванні, час проходу й геоприв’язку з камер.

Компонент зберігання даних реалізований на основі кластеризованої СУБД з реплікацією у режимі реального часу, що гарантує 99,9% доступність і захищеність від втрати інформації при виході з ладу окремого вузла. База даних містить не тільки облікові записи користувачів з їх атрибутами, але й детальні журнали подій, архів відеофрагментів, фотографії невдалих спроб і логи змін конфігурації. Для захисту конфіденційних біометричних векторів передбачено їх шифрування на рівні рядка та використання HSM-модулів для зберігання ключів шифрування.

Шар управління в архітектурі виконує роль оркестратора, відповідального за централізоване адміністрування, моніторинг стану всіх компонентів та автоматичне реагування на інциденти. Інтерфейс адміністратора надає уніфіковану консоль, де можна керувати завантаженням нових політик доступу, оновленнями ПЗ периферійних пристроїв, налаштовувати правила відеоаналітики та переглядати статистику в реальному часі. Для дистанційного моніторингу застосовується система SNMP- та REST-запитів до кожного

сервера і контролера, що дозволяє оперативно виявляти відмови, заповнювати звіти про апаратну деградацію й відкривати автоматизовані тикети в системі технічної підтримки.

Комунікаційні шари між рівнями побудовані на основі мікросервісної архітектури з використанням контейнеризації та оркестрації через Kubernetes, що забезпечує легке розгортання, автоскейлінг і початкову конфігурацію в різних середовищах – від локальних дата-центрів до публічних чи приватних хмар. Сервіси спілкуються між собою за допомогою асинхронних черг повідомлень (RabbitMQ або Apache Kafka), що надає можливість відокремити відлік транзакцій від безпосередньої обробки, знижує ризик втрати даних при тимчасових піках навантаження та дозволяє легко додавати нові споживачі повідомлень (наприклад, модулі аналітики або BI-системи).

Для забезпечення безпеки міжсервісної взаємодії використовується mTLS із взаємною автентифікацією, що виключає можливість підміни або несанкціонованого підключення. Кожний мікросервіс володіє власним сертифікатом, що керується централізованим PKI-центром, – це дозволяє швидко відкликати або оновлювати сертифікати без зупинки всієї платформи. Внутрішня мережа поділена на зони безпеки (DMZ, внутрішній сегмент), причому кожна зона має самостійні балансувальники й шлюзи безпеки, які фільтрують трафік за контекстними правилами доступу.

Архітектурна модель передбачає повне резервування критичних компонентів, від дублювання контролерів турнікетів до багаторазового кластера серверів автентифікації та георепліkованих баз даних. У випадку виходу з ладу одного з вузлів кластера система автоматично переключає користувачів на доступні ресурси, зберігаючи безперервність роботи без помітних для кінцевого користувача пауз. Резервне живлення через відокремлені UPS-модулі та аварійні генератори гарантує стабільність функціонування під час перебоїв з електроживленням.

На рівні інтеграції з корпоративною IT-інфраструктурою архітектура підтримує єдину точку входу через LDAP/Active Directory, що дає змогу

використовувати єдині облікові дані для адміністраторів та користувачів системи контролю доступу. Така інтеграція забезпечує зменшення операційних витрат на синхронізацію користувацьких записів, а також дозволяє централізовано реалізувати політику безпеки паролів і сертифікатів відповідно до внутрішніх стандартів.

Сучасні DevOps-практики лягли в основу процесів CI/CD, що дозволяє регулярно деплоїти оновлення компонентів без перерв в роботі. Тестування автоматизованих змін здійснюється через підсистему стейджингу, де відбувається відпрацювання змін у конфігурації, політик і версій алгоритмів розпізнавання облич із можливістю відкату до попередньої стабільної версії. Завдяки такому підходу архітектура системи залишається гнучкою й швидко адаптується до виникнення нових загроз чи появи інновацій в сфері біометрії та штучного інтелекту.

Архітектурна концепція багатофакторної системи автентифікації поєднує в собі модульність периферійних пристроїв, розподілену обробку та аналітику в проміжному шарі, потужні центральні сервіси з відмовостійкими базами даних, а також єдиний шар управління, який відповідає за оркестрацію, моніторинг і безпеку. Така архітектура забезпечує відповідність високим вимогам до продуктивності й надійності, а також гнучкість масштабування, швидкість інтеграції з IT-ландшафтом підприємства та готовність до швидкого впровадження новітніх технологічних рішень у сфері контролю доступу.

3.3 Блок-схема роботи підсистеми ідентифікації й автентифікації

Підсистема ідентифікації й автентифікації в комплексній системі контролю фізичного доступу побудована як послідовність взаємопов’язаних етапів обробки інформації, кожен із яких виконує свою роль у забезпеченні точності, оперативності та захищеності процедури допуску користувачів до охоронюваного простору. Усі внутрішні кроки об’єднані єдиним потоком даних

від фіксації початкового сигналу на периферії до остаточного рішення про надання доступу з одночасною реєстрацією результату в журналі подій. Блок-схема підсистеми зображена на рис. 3.1.

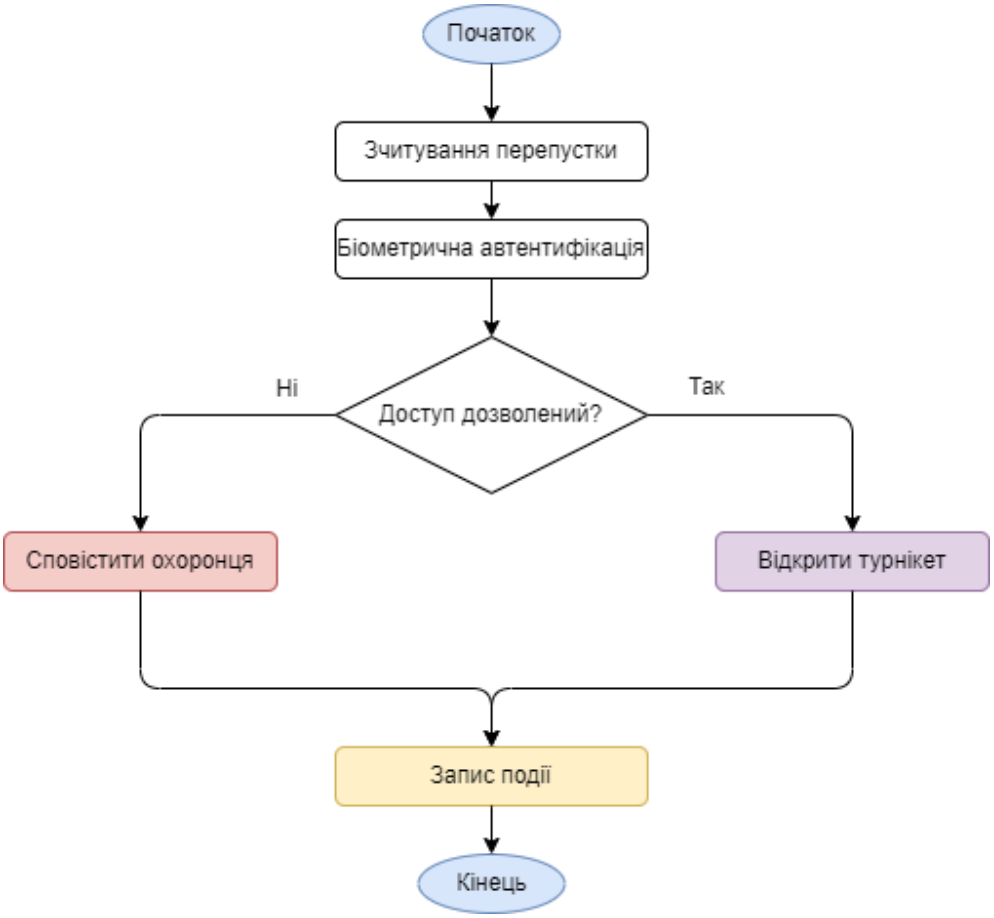

Рисунок 3.1 – Блок-схема підсистеми

Згідно з рис. 3.1:

1) перший етап підсистеми починається в точці входу, коли користувач підносить свою електронну перепустку, мобільний токен або інший апаратний носій до зчитувача. При цьому вбудований контролер турнікета або автономний модуль перетворює сигнал радіочастотного мітки чи QR-коду в цифровий запит, який містить унікальний ідентифікатор користувача й часовий штамп. Система миттєво перевіряє коректність формату даних та автентичність самої перепустки через криптографічний механізм: кожен запит підписаний електронним цифровим підписом, що дозволяє виключити можливість підміни

або відтворення чужої картки. Хибні чи некоректні формати запитів відсіюються вже на місці, а їхня інформація передається в логи контролера як успішна або невдала спроба, позначена кодом причини відмови;

2) далі починається другий етап – біометрична перевірка. Якщо користувач успішно пройшов початкову перевірку RFID, зчитувач активує камеру або сенсор відбитків пальців. У випадку розпізнавання обличчя відеопотік передається до локального модуля попередньої обробки, де із застосуванням каскадних фільтрів визначаються ділянки кадру, які відповідають області обличчя. Цей модуль виконує нормалізацію зображення, тобто кадри вирівнюються за орієнтацією і масштабу, а після цього будуються дескриптори – компактні вектори, які кодують унікальні ознаки обличчя. У випадку відбитків пальців сенсор здійснює оптичне сканування, створюючи біометричний шаблон. Усі шаблони підписуються локальним ключем контролера та додаються до того ж цифрового пакета, що надійшов від зчитувача перепустки;

3) третій етап характеризується відправленням єдиного пакета, в якому поєднані дані електронної перепустки та біометричного сенсора, через захищений канал до центрального сервісу автентифікації. Використання TLS із взаємною автентифікацією гарантує нерозголошення конфіденційної інформації в процесі передачі. На цьому ж етапі проміжний вузол може перевірити політику доступу: чи відповідає запит графіку роботи користувача, чи дозволено йому проходити через цю зону в поточний час, чи належить його роль до обслуговуваних рівнів приміщень;

4) четвертий етап полягає в основній перевірці на центральному сервері. Сервер автентифікації спочатку перевіряє цифровий підпис пакета, щоб упевнитися в його цілісності та справжності. Якщо підпис вірний, система звертається до бази даних авторизованих користувачів, шукаючи запис із відповідним ідентифікатором перепустки. У разі відсутності користувача в базі відбувається негайна відмова з кодом «не зареєстровано в системі». Якщо запис знайдено, сервер порівнює наданий біометричний шаблон із тим, що зберігається в базі. Виконання цього порівняння відбувається за допомогою

алгоритму обчислення косинусної або евклідової відстані між двома векторами. Якщо відстань перевищує встановлений поріг, система розцінює це як невідповідність і відмовляє в доступі, фіксуючи рівень довіри та оцінюючи ризики хибного спрацьовування;

5) п’ятий етап – це застосування додаткового контекстного фактору. У разі сумнівного результату або при виникненні внутрішніх політик безпеки система може автоматично ініціювати запит на ручну перевірку охоронцем. Цей сценарій передбачає відображення на консолі охоронця фото з камери та інформації про користувача з номерами змін та попередніми спробами доступу. Охоронець за допомогою довіреного інтерфейсу підтверджує або відхиляє запит. У разі підтвердження управління повертає сигнал дозволу на проміжний контролер, який у свою чергу активує механізми розблокування турнікета;

6) шостий етап – фінальне рішення та акт реєстрації. Після отримання рішення сервер відправляє пакет із відповіддю назад до точки доступу. Там контролер турнікета отримує сигнал і, у разі дозволу, подає команду на електропривід, який відкриває бар’єр. Одночасно з цим фіксується остаточний запис у журналі подій із точною міткою часу, ідентифікатором користувача, результатом перевірки кожного фактору, а також, за необхідності, знімком з камери, щоб забезпечити повний цифровий протокол дій. У разі відмови система сигналізує про це світловою та звуковою індикацією й утримує бар’єр закритим, очікуючи на наступну спробу або ручне втручання;

7) сьомий етап передбачає постобробку статистичних даних і аналітику. Всі зібрані журнали подій надходять у підсистему звітності та BI-аналізу, де формуються звіти про продуктивність пропускного пункту, рівень невдалих спроб доступу, час очікування користувачів та інші метрики. Це дозволяє адміністраторам коригувати налаштування порогів біометрії, змінювати правила зонування чи розширювати кількість каналів проходу для підвищення ефективності та безпеки.

Таким чином, блок-схема роботи підсистеми ідентифікації й автентифікації представляє собою суворо впорядкований ланцюжок етапів, який

вирізняється високим рівнем автоматизації, пошаровою обробкою даних і багатофакторним підходом до підтвердження особи. Кожен з кроків виконує свою роль в забезпеченні цілісності, надійності та гнучкості процесу автентифікації, що в сукупності гарантує оперативний пропуск уповноважених осіб і відхилення будь-яких спроб несанкціонованого доступу. Для забезпечення масштабованості та відмовостійкості всі вузли системи можуть бути розміщені у вигляді кластерів з автоматичним балансуванням навантаження і резервуванням, що дає змогу підтримувати безперервну роботу навіть за умов пікових навантажень або збою окремих компонентів.

3.4 Проєктування бази даних

При проєктуванні реляційної бази даних для обліку входу та виходу користувачів у системі багатофакторної автентифікації необхідно закласти узгоджену концепцію зберігання сутностей, які відображають учасників процесу, пристрої контролю, способи ідентифікації та власне події проходу через точки доступу. Ця концепція повинна забезпечувати цілісність даних, зручність запитів із побудови аналітики і масштабованість при розширенні кількості користувачів, біометричних шаблонів і точок доступу. Головна сутність, яка представляє подію входу чи виходу, – запис у журналі. До атрибутів цього запису належать унікальний ідентифікатор транзакції, часові мітки початкової ініціалізації запиту, результуючий час підтвердження доступу, результат перевірок кожного фактору автентифікації і посилання на контекстні дані про користувача, точку доступу та використані пристрої. Таблиця 3.4 журналу входів/виходів побудована таким чином, що кожен рядок цього журналу прямо пов’язаний із записом в таблиці 3.5 користувачів.

Таблиця 3.4

Журнал входів/виходів (events)

Поле	Тип	Обмеження	Опис
1	2	3	4
event_id	INTEGER	PRIMARY KEY AUTOINCREMENT	Унікальний ідентифікатор події

продовження таблиці 3.4

transaction_id	TEXT	NOT NULL, UNIQUE	Зовнішній ідентифікатор транзакції
user_id	INTEGER	NOT NULL, REFERENCES users(user_id) ON DELETE RESTRICT	Користувач, для якого зафіксовано подію
device_id	INTEGER	NOT NULL, REFERENCES devices(device_id) ON DELETE RESTRICT	Пристрій, через який проходив користувач
request_timestamp	DATETIME	NOT NULL	Час початку обробки
confirmation_timestamp	DATETIME		Час підтвердження (успіх/відмова)
access_result	TEXT	NOT NULL	Результат («granted»/»denied»)
factor_results	TEXT		JSON-серіалізований звіт із результатами кожного фактора автентифікації

Таблиця 3.5

Користувачі (users)

Поле	Тип	Обмеження	Опис
1	2	3	4
user_id	INTEGER	PRIMARY KEY AUTOINCREMENT	Унікальний ідентифікатор користувача
employee_code	TEXT	NOT NULL, UNIQUE	Код співробітника

last_name	TEXT	NOT NULL	Прізвище
first_name	TEXT	NOT NULL	Ім’я
patronymic	TEXT		По батькові
department	TEXT		Підрозділ
access_level	INTEGER	NOT NULL	Рівень доступу (наприклад, 1-5)
credential_ref	INTEGER	REFERENCES credentials(credential_id) ON DELETE SET NULL	Посилання на комплект біометричних шаблонів чи перепусток

Таблиця з користувачами (див. табл. 3.5) відповідає за зберігання ідентифікаційних даних: унікального коду співробітника, прізвища, імені та по батькові, структури підрозділу, рівня доступу, а також покажчика на сукупність біометричних шаблонів чи електронних перепусток, що наведені в табл. 3.6. Усі зв’язки реалізовані через зовнішні ключі, що гарантує недопущення висячих подій без прив’язки до конкретної особи. Центральна сутність журналу зберігає вказівку на таблицю пристроїв, через яку здійснювався вхід або вихід – і це може бути турнікет, камера розпізнавання обличчя або автономна точка сканування коду. У таблиці 3.7 пристроїв контролю доступу передбачено фіксацію типу пристрою, його унікального ідентифікатора, місця встановлення та його конфігураційних параметрів. Прив’язка запису з журналу до пристрою таким чином дозволяє відтворювати топологію системи контролю доступу: мапу точок входу й виходу, їх продуктивність, а також обчислювати надійність і відмовостійкість обладнання на рівні окремих пристроїв або їх кластерів. Оскільки кожен пристрій може мати власний цикл обслуговування, важливо також вести окремий журнал технічних подій пристроїв, описаний в табл. 3.8, який через відношення «один до багатьох» з’єднаний із сутністю пристроїв. Це дозволяє відстежувати, в який момент і на який час точка доступу була недоступною, і виключати такі відрізки при аналізі навантаження.

Таблиця 3.6

Біометричні шаблони. Перепустки (credentials)

Поле	**Тип**	**Обмеження**	**Опис**

1	2	3	4
credential_id	INTEGER	PRIMARY KEY AUTOINCREMENT	Унікальний ідентифікатор запису
user_id	INTEGER	NOT NULL, REFERENCES users(user_id) ON DELETE CASCADE	Користувач, якому належить
method_id	INTEGER	NOT NULL, REFERENCES authentication_methods(method_id)	Метод автентифікації

продовження таблиці 3.6

template_data	BLOB	NOT NULL	Закодовані дані шаблону (біометричні вектори або серіалізовані ключі)

Таблиця 3.7

Пристрої контролю доступу (devices)

Поле	**Тип**	**Обмеження**	**Опис**
1	2	3	4
device_id	INTEGER	PRIMARY KEY AUTOINCREMENT	Унікальний ідентифікатор пристрою
device_type	TEXT	NOT NULL	Тип пристрою (наприклад, «Turnstile», «Camera», «Scanner»)
unique_id	TEXT	NOT NULL, UNIQUE	Серійний номер або інший унікальний ідентифікатор
location	TEXT		Місце встановлення (точка доступу)
config_params	TEXT		JSON-серіалізовані параметри конфігурації

Таблиця 3.8

Журнал технічних подій пристроїв (device_logs)

Поле	**Тип**	**Обмеження**	**Опис**
1	2	3	4
log_id	INTEGER	PRIMARY KEY AUTOINCREMENT	Унікальний ідентифікатор запису

device_id	INTEGER	NOT NULL, REFERENCES devices(device_id) ON DELETE CASCADE	Пристрій, до якого належить подія
event_timestamp	DATETIME	NOT NULL	Час події
event_type	TEXT	NOT NULL	Тип події (наприклад, «Failure», «Maintenance», «Calibration»)
description	TEXT		Деталі події

Біометричні та електронні методи автентифікації зберігаються у супутній табл. 3.9, де для кожного користувача ведеться інформація про типи перепусток, їх унікальні ключі, криптографічні сертифікати і дати випуску чи відкликання. Ключовою вимогою є забезпечення цілісності та захисту цих даних, тому текстове зберігання шаблонів виключається – усі біометричні дескриптори заносяться в зашифрованому вигляді у BLOB-полях, а доступ до них контролюється на рівні транзакцій із використанням призначених для цього ролей бази. Кожен такий запис пов’язаний з користувачем через зовнішній ключ, а також містить посилання на журнал змін, де фіксуються операції створення, оновлення або видалення шаблону, що дозволяє відтворювати повну історію маніпуляцій з біометрією.

Таблиця 3.9

Методи автентифікації (authentication_methods)

Поле	**Тип**	**Обмеження**	**Опис**
1	2	3	4
method_id	INTEGER	PRIMARY KEY AUTOINCREMENT	Унікальний ідентифікатор методу
name	TEXT	NOT NULL, UNIQUE	Назва (наприклад, «RFID», «Fingerprint», «FaceRecognition»)
description	TEXT		Детальний опис

Окрім основного запису журналу, у базі створюється таблиця станів автентифікації, де для кожного журналу зберігаються проміжні результати

перевірок: успіх чи невдача фактору «щось, що у вас є», «щось, чим ви є», а також контекстний фактор, наприклад рішення охоронця. Ця таблиця пов’язана із сутністю журналу через зовнішній ключ і дає можливість проводити гнучкий аналіз випадків, коли один з факторів дав збій, але загальний результат був дозволом або відмовою. За рахунок такого розподілу даних вдається уникнути дублювання детальних показників у кожному рядку журналу та підтримувати нормалізовану структуру бази.

Для оптимізації запитів, пов’язаних із побудовою аналітичних звітів та статистикою, використовуються матеріалізовані уявлення, які агрегують дані журналу за часовими інтервалами, зонами доступу та результатами перевірок. Ці уявлення періодично оновлюються поза піковим навантаженням і дозволяють швидко отримувати показники продуктивності точок доступу. Оскільки база може обслуговувати сотні тисяч записів на день, індексація стовпців із часовими мітками, ідентифікаторами користувачів та результатами автентифікації є критичною для підтримки високої швидкості пошукових та аналітичних запитів.

Таблиці із політиками доступу, часом роботи зон і правилами реагування на події з’єднані з центральною сутністю журналу таким чином, щоб кожен запис події містив посилання на конфігурацію, яка діяла в момент транзакції. Це дає змогу відновити точний контекст прийняття рішення, навіть якщо політики налаштовані повторно чи змінені з часом. Архівування старих версій політик проводиться автоматично через механізм історичних таблиць, який самостійно переносить застарілі записи в окремий схов файл при досягненні певного терміну життя.

База даних розгортається у кластері з реплікацією та автоматичним відновленням вузлів у разі збоїв. При цьому використовуються механізми блокування рядків при записі, аби виключити стан гонки при одночасній реєстрації декількох проходів через одну точку доступу. В усіх таблицях передбачені необхідні log-trigger’и для миттєвого копіювання критичних змін у незалежний журнал аудиту, який захищений від модифікацій адміністративними

засобами СУБД. Це дозволяє у будь-який момент з’ясувати, хто і коли вносив правки в систему, а також швидко відновити її попередній стан у разі інциденту.

На рис. 3.2 представлено зв’язки між таблицями бази даних.

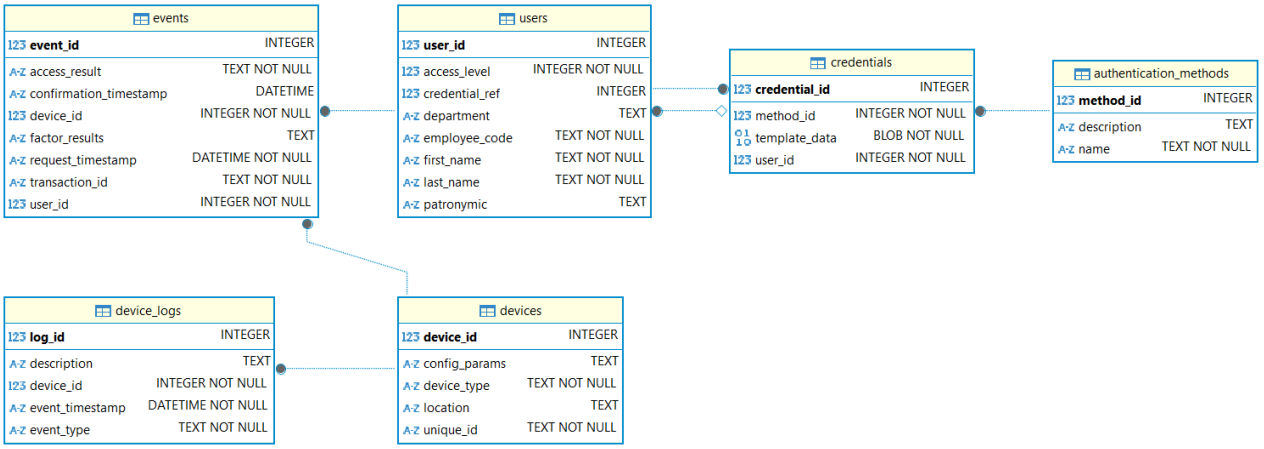

Рисунок 3.2 – Зв’язки між таблицями бази даних

Програмний код створення бази даних наведено в додатку А.

Доповнюючи модель, варто вирішити питання версифікації даних і контролю їхнього життєвого циклу. Для цього кожна основна таблиця отримує поля створення та оновлення записи, а також позначку видалення без фізичного усунення рядка. Такий підхід дозволяє зберігати історію колишніх користувачів, перепусток чи налаштувань, що особливо важливо для проведення аудиту та розслідування інцидентів. При цьому у запитах реалізується фільтрація за ознакою «активний запис», що забезпечує наскрізну прозорість системи для внутрішнього та зовнішнього контролю.

Архітектура бази даних для обліку входу та виходу поєднує сувору нормалізацію ключових сутностей з гнучкими механізмами зберігання історії конфігурацій, забезпечує цілісність даних через зовнішні ключі й транзакції, а також гарантує відмовостійкість за допомогою реплікації і розподілених блокувань. Використання матеріалізованих уявлень та індексів значно прискорює аналітичні запити, тоді як ретельно продумана система аудиту і версіонування надає максимальну прозорість і контроль за станом системи в будь-який момент часу. Застосування таких принципів проєктування дозволяє

створити надійну, безпечну та масштабовану базу даних, здатну обслуговувати високі навантаження й забезпечувати повний звіт про доступ користувачів на обладнанні малого чи середнього підприємства.

3.5 Алгоритм підтримки прийняття рішень

За замовчуванням система працює у нормальному, стандартному режимі. Але у разі перевищення запланованої інтенсивності (понад 30 осіб за хвилину), система може переключитися в режим високої продуктивності. На рис. 3.3 наведено блок-схему моніторингу інтенсивності роботи системи.

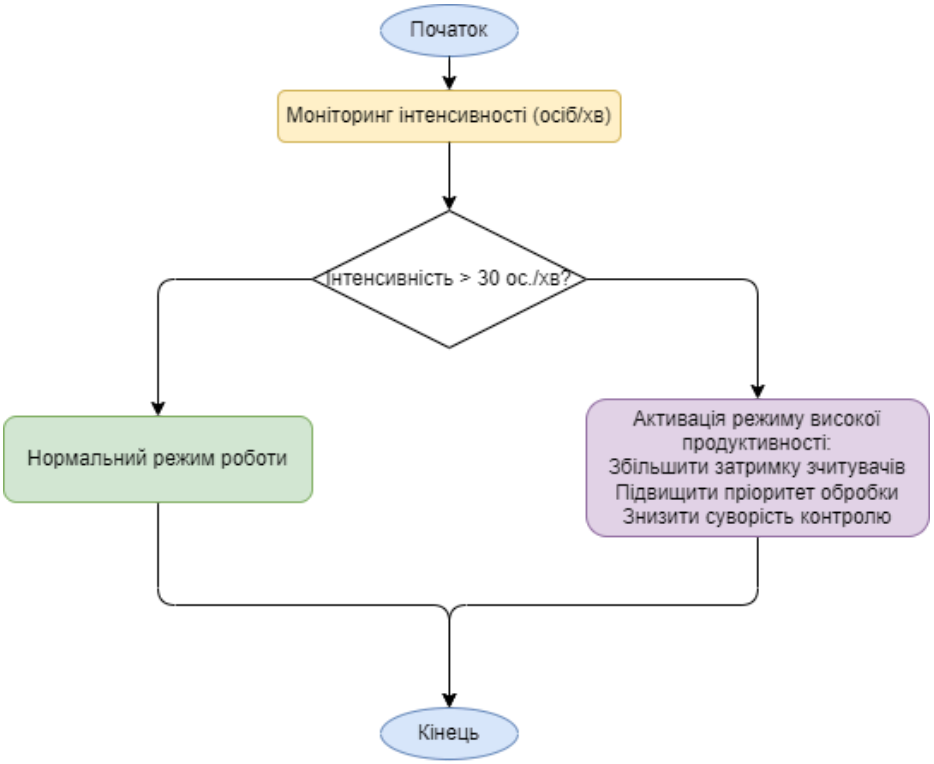

Рисунок 3.3 – Блок-схема моніторингу інтенсивності роботи системи

Участь охоронця як додаткового фактору автентифікації реалізується через спеціальний алгоритм підтримки прийняття рішень, який інтегрує дані автоматичних підсистем із суб’єктивною оцінкою людини-оператора. Відповідно до обраної методології, цей алгоритм запускається в тих випадках, коли автоматична перевірка першого та другого факторів не дає однозначної

відповіді, або коли система реєструє невідповідність із встановленими порогами довіри. Ідея полягає в тому, що охоронець отримує на свою консоль зведену картину поточної ситуації: відеозображення особи, результати сканування перепустки, показники якості біометричних даних і рекомендації автоматичної системи. У цій фазі алгоритм виступає в ролі «асистента», що надає охоронцеві інформаційний контекст і варіанти реагування, упорядковані за ступенем ризику та ймовірності успішної верифікації.

Включення людини у процес автентифікації починається з того, що в разі невпевненого результату автоматичного аналізу система генерує тривожний запит, який включає мультимедійну картку події. Ця картка містить серію ключових кадрів, знімок перепустки, часові мітки кожного з етапів перевірки та показники алгоритмічної впевненості. У правому полі екрану для охоронця відображається інформація про те, наскільки близька задана косинусна відстань дескрипторів до порогового значення, а також статистика попередніх звернень цього користувача у вигляді кількості успішних проходів, кількості невдалих спроб та часу останньої реєстрації. Додатково система може подавати сигнали про незвичну поведінку – наприклад, повторні невдалі спроби за короткий проміжок часу або спроби одночасного проходу двох осіб через одну перепустку.

На етапі прийому тривожного запиту охоронець має можливість, використовуючи інструменти інтерфейсу, здійснити телеекзаменацію – наблизити відео, зробити зупинку на ключовому кадрі, змінити кут огляду в разі наявності декількох камер, а також запросити додатковий відеопотік із сусідніх камер. Якщо особа проходить через турнікет із камерою розпізнавання обличчя, то поруч із зображенням з основної камери з’являються кадри з інших кутів, що дозволяє охоронцеві оцінити цілісність образу та виключити можливість використання підроблених масок чи фотографій. Важливо, що всі ці дії відбуваються в межах одного вікна програми, яка має зручний поділ на зони: велике зображення обличчя, мініатюрні кнопки з каналами спостереження та інформаційні панелі з текстовими вказівками.

Наступний крок алгоритму полягає в генерації рекомендацій на основі комбінованої оцінки ризиків. Система розраховує інтегральний бал для поточної ситуації, враховуючи вагові коефіцієнти трьох основних компонентів: віддаленості дескрипторів біометрії від контрольного порогу, частоти невдалих спроб протягом останньої доби та наявності попереджень про нетипову поведінку. Якщо інтегральний бал знаходиться в діапазоні низького ризику, то охоронець побачить на екрані м’яку підказку, мовляв, прохід цілком може бути дозволено після візуальної перевірки перепустки. У випадку середнього ризику система рекомендує уточнити додаткові дані або запросити допомогу іншого посту, а при високому рівні ризику – негайно заблокувати прохід і повідомити керівника служби охорони. Особливістю алгоритму є можливість активного самонавчання: система зберігає рішення охоронця разом із результатами подальшого підтвердження (наприклад, якщо після ручного дозволу виявилося, що користувач справді був легітимним, або навпаки – в результаті перевірки документів виявилося шахрайство). Ці дані надходять у модуль аналітики, який виконує корекцію вагових коефіцієнтів та порогів, покращуючи рекомендації у майбутньому. Таким чином, алгоритм підтримки не залишається жорстко закладеним: він еволюціонує, враховуючи особливості конкретного підприємства, профілі поведінки співробітників і частоту превентивних інцидентів.

У випадку, коли охоронець підтверджує прохід, система автоматично записує його дію в окремий журнал охоронця із зазначенням ідентифікатора користувача, ідентифікатора камери, часової мітки та коду рішення «дозвіл вручну». Якщо ж охоронець відхиляє спробу, активується механізм відправлення тривоги до центрального пульта, а також може бути ініційована процедура блокування дверей і оповіщення сусідніх секторів. У будь-якому випадку після ручного рішення алгоритм завершує обробку поточної події та повертає стан інтерфейсу в режим очікування наступного запиту.

Ключовим аспектом ефективної роботи даної підсистеми є мінімізація навантаження на охоронця та запобігання перенавантаженню інформацією. Для

цього інтерфейс адаптується під потік подій: якщо протягом однієї зміни на обробку надходить значна кількість тривожних запитів, відбувається динамічне регулювання порогів, коли система автоматично допускає до слуху низькоризикові випадки без звернення до людини. Натомість високоризикові сценарії залишаються пріоритетними для розгляду. Ця адаптивність дозволяє підтримувати прийнятний рівень завантаження операторів навіть у випадках пікових навантажень, не жертвуючи при цьому безпекою. У межах алгоритму передбачено також можливість колективного прийняття рішення у разі надзвичайних ситуацій. Коли рівень ризику піднімається вище максимальної межі, система може одночасно ініціювати запити до декількох охоронців на різних постах із відображенням однієї й тієї ж події. Кожен оператор приймає незалежне рішення, а фінальне рішення формується за принципом більшості голосів або з урахуванням ролей кожного охоронця (наприклад, рішення старшого змінного стежать).

3.6 Інтерфейс оператора

Інтерфейс оператора системи багатофакторної автентифікації та контролю фізичного доступу виступає єдиним вікном взаємодії людини з комплексом апаратно-програмних засобів, що забезпечують моніторинг подій, формування аналітичних звітів та своєчасне інформування про інциденти. З першого погляду на екран оператора він бачить панель поточного стану системи, де в центральній частині візуалізується жива схема розміщення точок доступу підприємства, а навколо неї розташовані віджети з основними показниками – кількістю одночасних спроб проходу, швидкістю обробки транзакцій та середнім часом реакції на подію. Оскільки кожен турнікет, камера чи біометричний сенсор має власний ідентифікатор і географічне розташування на плані, оператор у реальному часі бачить карту підприємства, де гарячі точки підсвічуються червоним кольором, що сигналізує про зростання кількості

невдалих спроб чи про підозрілі аномалії в потоці відвідувачів. Навігація по інтерфейсу дозволяє оператору одним кліком отримати детальний перегляд будь-якої точки доступу – будь то окремий турнікет біля головного входу або віддалений камерний модуль на складі. При виборі конкретного об’єкта на карті відкривається вкладка з інформацією про конфігурацію пристрою, статус його живлення, час останньої синхронізації даних з центральним сервером та рівень завантаженості процесора вбудованого контролера. Якщо на обраному турнікеті виникла помилка або відключилася камера, оператор одразу бачить повідомлення про природу збою та пропозицію викликати технічну службу або переключити трафік на резервну лінію.

У режимі моніторингу подій оператор має доступ до живих відеопотоків з усіх камер, інтегрованих в підсистему відеоспостереження, причому основне вікно відтворює зображення з камери, яка першою виявила рух або невдалу спробу проходу. Поряд із відео відображаються супровідні метадані: ідентифікатор користувача, дані зчитування перепустки, час та результат аудиту кожного з факторів автентифікації. Завдяки синхронізації часових міток оператор бачить точний момент активації турнікета та порівнює його з відеокадром, що дозволяє одразу відтворити ланцюжок подій та оцінити поведінку відвідувача. При потребі оператор може зробити зупинку потоку або крокування кадрів назад-вперед для детального вивчення ситуації, а також миттєво створити скріншот чи короткий відеокліп, який автоматично зберігається в архіві інцидентів. Формування звітності реалізоване через конструктор запитів, який дозволяє оператору без навичок програмування задавати критерії вибірки, наприклад, інтервали часу, типи пристроїв, категорії подій, і отримувати у вигляді таблиць або графіків інформацію про продуктивність точок контролю. Звіти можуть бути представлені у вигляді інтерактивних діаграм із часовими рядами, де позначено кількість транзакцій за кожну хвилину, середній час обробки факторів автентифікації та частку відмов. Оператор може експортувати результати у формати PDF або CSV для подальшої передачі керівництву підприємства чи аналітичному відділу. Кожен

сформований звіт зберігається в історії звітів із відміткою про автора запиту, параметри фільтрації та час генерації, що забезпечує прозорість і можливість відтворення будь-якого аналітичного висновку.

Система оповіщень попередньо класифікує всі події за рівнями важливості від інформаційних повідомлень про успішну транзакцію до тривожних сигналів про неодноразові невдалі спроби або про вторгнення. У випадку надходження тривожного повідомлення на екран миттєво виводиться спливаюче вікно з коротким описом ситуації та рекомендованими діями, а одночасно запускається звуковий сигнал і відсилається push-сповіщення на мобільний пристрій відповідального охоронця. Приглушена червона панель вздовж верхнього краю екрану нагадує оператору про пріоритет обробки таких повідомлень, і навіть якщо він знаходиться в іншому модулі інтерфейсу, достатньо одного кліку, щоб перейти до вікна докладного розгляду інциденту.

Усунення надмірного навантаження на операторів досягається за рахунок фільтрів і профілів сповіщень. Досвідчений охоронець може активувати тільки найкритичніші оповіщення, залишивши менш важливі для перегляду у вільний час, тоді як новачок може отримувати кожне повідомлення про невдалу спробу. Система також дозволяє групувати оповіщення за категоріями та відправляти їх різним групам користувачів: технічній підтримці, старшим охоронцям або адміністрації, що гарантує швидке реагування відповідних служб і запобігає хаосу при одночасному надходженні великої кількості повідомлень. Інтерфейс підтримує багатоваріантні сценарії оповіщення. Усі канали сповіщення налаштовуються централізовано з можливістю створення ланцюжка оповіщення, коли, наприклад, при відсутності реакції на перше повідомлення за п’ять хвилин автоматично повідомляється вища інстанція. Це гарантує, що навіть нічний черговий швидко отримує сигнал і може вжити необхідних заходів щодо забезпечення безпеки. Безперервний моніторинг роботи інтерфейсу оператора забезпечується вбудованими механізмами збору телеметрії. Час інтервалів між відкриттям повідомлень і початком реакції, кількість одночасно відкритих вікон, частота звернень до модулів аналітики. На

основі цих даних адміністратор може оцінити ефективність роботи операторів, виявити вузькі місця в інтерфейсі та оперативно коригувати його компонування або навчання персоналу, що сприяє безперервному покращенню взаємодії людини з системою і дозволяє адаптувати графічне оточення до реальних потреб служби безпеки підприємства.

3.7 Напрямки подальшої роботи та досліджень

Проведене дослідження виявило низку критичних аспектів, які потребують подальшої розробки та вдосконалення в майбутніх дослідницьких ініціативах. Одним із пріоритетних напрямків подальших досліджень є розробка адаптивних алгоритмів обробки біометричних даних у реальному часі, які можуть автоматично змінювати параметри верифікації залежно від умов середовища, типу користувача або навантаження на систему. Такий підхід дозволить вирішити одну з основних проблем сучасних рішень – зниження точності ідентифікації у разі поганої освітленості, змін зовнішності користувача або наявності перешкод (наприклад, захисних масок). Складність цього завдання полягає в необхідності балансування між рівнем хибних позитивних і негативних спрацьовувань, швидкістю обробки даних і ресурсною ємністю алгоритмів.

Наступним напрямком подальших досліджень є розробка концепції контекстуальної автентифікації, яка передбачає врахування поведінкових, просторових і часових факторів під час прийняття рішення про доступ. Система, окрім звичних факторів (що знає користувач, що має і ким є), повинна враховувати також місцезнаходження пристрою, попередні шаблони переміщення, час доби, історію входів, а також аналіз взаємозв’язків між подіями, що передували спробі автентифікації.

Під час дослідження було виявлено, що у випадку використання обладнання від різних виробників часто виникають складнощі з узгодженням

протоколів обміну даними, що призводить до додаткових витрат на адаптацію та зниження стабільності функціонування. Враховуючи це, перспективним напрямом є створення уніфікованих відкритих протоколів і фреймворків, які дозволятимуть забезпечити інтероперабельність компонентів системи без необхідності глибокої кастомізації. Також значного потенціалу набуває напрямок, пов’язаний із використанням технологій машинного навчання для автоматизованої класифікації інцидентів і прогнозування загроз. Перші спроби вбудовування елементів штучного інтелекту в системи відеоспостереження вже демонструють здатність автоматично виявляти підозрілу поведінку або нетипову активність у контрольованих зонах. Проте наразі бракує цілісних досліджень, присвячених синтезу подій із різних джерел – відеоаналітики, журналів доступу, сенсорних сигналів – у рамках єдиної моделі оцінювання ризиків. Майбутні дослідження повинні бути спрямовані на створення багаторівневих моделей оцінювання контексту з динамічним перерахунком порогових значень, що керують реакцією системи на вхідні події. Це дозволить мінімізувати кількість помилкових тривог, підвищити адаптивність і знизити навантаження на персонал служби безпеки.

З огляду на зростання значимості персональних даних та посилення нормативних вимог у сфері захисту інформації, подальшим стає напрям досліджень, пов’язаний з безпечним зберіганням та обробкою біометричних шаблонів. Зокрема, перспективним є використання механізмів гомоморфного шифрування, яке дозволяє здійснювати обчислення над зашифрованими даними без їх розшифрування, а також дослідження застосовності мультипартійних обчислень (MPC) для підвищення конфіденційності у розподілених архітектурах. Інтеграція таких технологій потребує переосмислення поточної моделі архітектури і вимагає значного перегляду вимог до обчислювальних ресурсів, проте у довгостроковій перспективі вона може стати основою для побудови дійсно надійних і законодавчо сумісних систем контролю доступу.

У реальних умовах малі підприємства також часто стикаються з обмеженнями енергетичної інфраструктури, а постійна робота камер, серверів і

турнікетів створює суттєве навантаження на електромережу. Це диктує необхідність пошуку нових рішень – від застосування енергоефективних процесорів ARM-архітектури до впровадження динамічного вимкнення та ввімкнення компонентів залежно від поточного навантаження або присутності персоналу.

Логічним кроком розвитку стане створення адаптивної хмарної платформи для керування системами доступу малого та середнього бізнесу. Такі платформи повинні забезпечити масштабованість, централізоване управління політиками доступу, автоматизований аудит і моніторинг інцидентів. Питанням для подальших досліджень тут виступає побудова безпечних каналів передачі даних між периферійними пристроями та хмарним середовищем, реалізація політик Zero Trust і забезпечення цілісності журналів подій. Також необхідно дослідити варіанти інтеграції із зовнішніми сервісами, такими як календарі, HR-системи або корпоративні платформи звітності, з метою підвищення автоматизації та зниження витрат на адміністрування.

3.8 Висновки за розділом 3

Третій розділ кваліфікаційної роботи було присвячено проєктуванню віртуально-апаратної архітектури системи, формулюванню функціональних та нефункціональних вимог, моделі даних і сценаріїв роботи під навантаженням. Запропонована багаторівнева архітектура з периферійним, проміжним і центральним шарами дозволяє ефективно розподіляти обчислювальні ресурси, гарантувати відмовостійкість та підтримувати гнучке масштабування.

Розроблена база даних забезпечує коректне зберігання інформації про користувачів, методи автентифікації, пристрої та журнали подій, а алгоритм перемикання режимів продуктивності гарантує безперервність роботи в пікові години. Загалом виконана робота створює цілісне й адаптивне рішення для

багатофакторної автентифікації, що відповідає сучасним вимогам безпеки та експлуатаційної ефективності.

ВИСНОВКИ

У ході проведеного дослідження виконано комплексний аналіз існуючих підходів і технологій контролю фізичного доступу та багатофакторної автентифікації, що дозволило виокремити низку ключових висновків.

По-перше, виявлено, що структура сучасної системи захисту фізичного доступу обов'язково повинна будуватися за багаторівневим принципом: перший рівень – це бар'єри і турнікети по периметру, оснащені електромеханічними приводами й базовими зчитувачами; другий рівень – це внутрішні контрольно-пропускні пункти з багатофакторною автентифікацією на основі смарт-карток, PIN-кодів або біометрії; третій рівень – аналітико-реактивні модулі, що включають відеоаналітику та моніторинг у режимі реального часу. По-друге, дослідження показало, що пропускна здатність системи, яка складається з турнікету, зчитувача та серверу, повинна становити не менше 20-30 осіб за хвилину на кожний канал у пікові години, що забезпечується високошвидкісними електроприводами, оптимізованою інтеграцією RFID-модулів та паралельною обробкою відеопотоку.

В процесі побудови рекомендацій було виявлено низку проблем, які потребують особливої уваги при практичній реалізації системи багатофакторної автентифікації:

– недостатня швидкість обробки біометричних даних у разі використання виключно периферійних модулів без залучення центрального сервера, що призводить до збільшення середнього часу проходу понад допустимі 3-4 секунди;

– відсутність у деяких бюджетних рішень механізмів гарячого резервування, що знижує відмовостійкість і підвищує ризик простоїв при виході з ладу одного з компонентів;

– недостатня масштабованість деяких монолітних платформ, які складно інтегрувати з існуючою інфраструктурою підприємства без повного переоснащення;

– відсутність або недостатня аналітична підтримка в реальному часу при виявленні аномальних подій, що знижує ефективність реагування служби безпеки;

– неузгодженість політик зберігання відеоданих та журналів проходу, що унеможливлює відновлення хронології інцидентів із точністю до мілісекунд при розслідуванні.

Результатом виконаної кваліфікаційної роботи стали конкретні напрацювання, що можуть бути використані під час проєктування й впровадження систем фізичного доступу на малих підприємствах:

– розроблено вимоги до багаторівневої архітектури, що поєднує периферійні контролери, проміжні вузли обробки та центральну серверну платформу з контейнеризацією мікросервісів;

– сформульовано набір функціональних і нефункціональних вимог з чіткими показниками продуктивності (20-30 осіб на хвилину у базовому режимі, ≤1 с середній час обробки), відмовостійкості (MTBF обладнання $\geq 5 \cdot 10^4$ год.) та безпеки (FAR ≤ 0,01 %, FRR ≤ 1 %, шифрування TLS 1.3, HSM);

– визначено оптимальний набір технологій для ідентифікації та автентифікації: RFID, біометрія (відбитки, розпізнавання обличчя), контекстні фактори (GPS-координати, часові політики), що дозволяє досягти високої точності при мінімальних затримках;

– проведено порівняльний аналіз комерційних пристроїв (турнікети, камери, біометричні модулі, сервери) за критеріями пропускної здатності, стійкості до несприятливих умов, вартості володіння (TCO) та вартості обслуговування;

– запропоновано механізми інтеграції відеоаналітики (ONVIF, RTSP, PoE, NTP/PTP) з контролем доступу та інформаційними табло для оперативного інформування користувачів і служби безпеки;

– розроблено рекомендації зі створення системи моніторингу та профілактичного обслуговування на основі SNMP, LDAP/AD, SIEM та audit-log для забезпечення прозорості й відповідності GDPR/

Отже, узагальнений результат роботи полягає у створенні цілісного методичного підходу до проєктування багатофакторних систем контролю фізичного доступу, який враховує як технічні, так і організаційні аспекти, забезпечує баланс між рівнем безпеки й оперативністю пропускного режиму, а також дає змогу малим підприємствам реалізувати рішення з урахуванням обмежених ресурсів без втрати якості й надійності. Застосування отриманих рекомендацій дозволить оптимізувати капітальні й операційні витрати, підвищити рівень довіри користувачів та створити стійку платформу для подальшого масштабування й вдосконалення системи у відповідь на зростаючі виклики безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Why integration and flexibility are key to access control management. URL: https://www.locksmithjournal.co.uk/integration-flexibility-key-access-control-management (дата звернення: 01.05.2025).

2. Ouvrard R., Poinot T., Trigeassou J.-C. Partial Moments in System Identification. Cham : Springer Nature Switzerland, 2024. URL: https://doi.org/10.1007/978-3-031-58156-4

3. Nita S. L., Mihailescu M. I. *Identification Schemes. Cryptography and Cryptanalysis in Java*. Berkeley, CA, 2024. С. 219–232. URL: https://doi.org/10.1007/979-8-8688-0441-0_13

4. Zhao G., Bao H., Wang J. A lightweight security authentication protocol for RFID. *Peer-to-Peer Networking and Applications*. 2025. Т. 18, № 3. URL: https://doi.org/10.1007/s12083-025-01965-2

5. Jøsang A. User Authentication. *Cybersecurity*. Cham, 2024. С. 165–189. URL: https://doi.org/10.1007/978-3-031-68483-8_8

6. Di Campi A. M., Luccio F. L. Accessible authentication methods for persons with diverse cognitive abilities. *Universal Access in the Information Society*. 2025. URL: https://doi.org/10.1007/s10209-025-01189-4

7. Shaik Riyaz N. B., Parthipan V. A Novel Prediction Analysing the False Acceptance Rate and False Rejection Rate using CNN Model to Improve the Accuracy for Iris Recognition System for Biometric Security in Clouds Comparing with Traditional Inception Model. *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, м. Greater Noida, India, 16–17 груд. 2022. С. 690–694. URL: https://doi.org/10.1109/icac3n56670.2022.10074026

8. Mahansaria D., Roy U. K. Contextual authentication of users and devices using machine learning. *Computing*. 2024. Т. 106, С. 4083–4107 URL: https://doi.org/10.1007/s00607-024-01333-7

9. Multi-factor authentication scheme based on custom attributes / D. Zhu та ін. *Cluster Computing*. 2024. Т. 27, С. 7741–7756 URL: https://doi.org/10.1007/s10586-024-04371-0

10. Anisimov A. V. Digital Friend-or-Foe Authentication. *Cybernetics and Systems Analysis*. 2024. Т. 60, С. 341–349 URL: https://doi.org/10.1007/s10559-024-00675-6

11. Boonkrong S. Multi-factor Authentication. *Authentication and Access Control. Berkeley*, CA, 2020. С. 133–162. URL: https://doi.org/10.1007/978-1-4842-6570-3_6

12. An Attribute-Based Access Control for Cloud-Enabled Industrial Smart Vehicles / M. Gupta та ін. *IEEE Transactions on Industrial Informatics*. 2020. С. 4288–4297. URL: https://doi.org/10.1109/tii.2020.3022759

13. Security Patterns for Physical Access Control Systems / E. B. Fernandez та ін. *Data and Applications Security XXI*. Berlin, Heidelberg, 2007. С. 259–274. URL: https://doi.org/10.1007/978-3-540-73538-0_19

14. Zhao G., Bao H., Wang J. A lightweight security authentication protocol for RFID. *Peer-to-Peer Networking and Applications*. 2025. Т. 18, № 3. URL: https://doi.org/10.1007/s12083-025-01965-2

15. An Ultra-Lightweight Secure RFID Authentication Protocol for Low-Cost Tags / S. Kumar та ін. *Journal of Computer Virology and Hacking Techniques*. 2024. Т. 18, № 158. URL: https://doi.org/10.1007/s11416-024-00533-1

16. Kumar S., Banka H., Kaushik B. Lightweight group authentication protocol for secure RFID system. *Multimedia Tools and Applications*. 2024. Т 83, С. 89249–89277 URL: https://doi.org/10.1007/s11042-024-19013-1

17. Akiirne Z., Sghir A., Bouzidi D. UDAP: ultra-lightweight dot product-based authentication protocol for RFID systems. *Cybersecurity*. 2024. Т. 7, № 1. URL: https://doi.org/10.1186/s42400-024-00252-6

18. Sharphathy M. N., Sumalatha V. SSS-EC: Cryptographic based Single-Factor Authentication for Fingerprint Data with Machine Learning Technique. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*,

м. Namakkal, India, 19–21 лип. 2023. С. 308–315. URL: https://doi.org/10.1109/icecaa58104.2023.10212308

19. Aliyeva S., Parsayan A. Turnstile Access based on Facial Recognition and Vaccine Passport Verification. *2022 IEEE 16th International Conference on Application of Information and Communication Technologies (AICT)*, м. Washington DC, DC, USA, 12–14 жовт. 2022. С. 1–5. URL: https://doi.org/10.1109/aict55583.2022.10013579

20. Multi-Camera Video Scene Graphs for Surveillance Videos Indexing and Retrieval / T. Patel та ін. *2021 IEEE International Conference on Image Processing (ICIP)*, м. Anchorage, AK, USA, 19–22 верес. 2021. URL: https://doi.org/10.1109/icip42928.2021.9506713

21. Intelligent Video Surveillance Systems / V. Chundi та ін. *2021 International Carnahan Conference on Security Technology (ICCST)*, м. Hatfield, United Kingdom, 11–15 жовт. 2021. URL: https://doi.org/10.1109/iccst49569.2021.9717400

22. Dhar P., Chowdhury D. P. Source camera identification for securing AI-enabled surveillance cameras. *2024 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC)*, м. Ghaziabad, India, 21–23 листоп. 2024. С. 1–6. URL: https://doi.org/10.1109/akgec62572.2024.10869166

23. Target-Aware Camera Placement for Large-Scale Video Surveillance / H. Wu та ін. *IEEE Transactions on Circuits and Systems for Video Technology*. 2024. Т. 34, № 12. URL: https://doi.org/10.1109/tcsvt.2024.3445151

24. Gaur S., Pandey M., Himanshu. Realization of Facial Recognition Technology for Attendance Monitoring Through Biometric Modalities Employing MTCNN Integration. *SN Computer Science*. 2024. Т. 5, № 7. URL: https://doi.org/10.1007/s42979-024-03225-1

25. Luo Y., Huang L. Research on the Application of Deep Learning Algorithm in Face Expression Recognition. *2023 Global Conference on Information Technologies*

and Communications (GCITC), м. Bangalore, India, 1–3 груд. 2023. С. 1–4. URL: https://doi.org/10.1109/gcitc60406.2023.10425903

26. A Machine Learning based Facial Expression and Emotion Recognition for Human Computer Interaction through Fuzzy Logic System / K. Vinutha та ін. *2023 International Conference on Inventive Computation Technologies (ICICT)*, м. Lalitpur, Nepal, 26–28 квіт. 2023. С. 166–173. URL: https://doi.org/10.1109/icict57646.2023.10134493

27. Design of Facial Expression Recognition Algorithm Based on CNN Model / Y. Luo та ін. *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, м. Shenyang, China, 29–31 січ. 2023. С. 580–583. URL: https://doi.org/10.1109/icpeca56706.2023.10075779

28. Tripod Turnstiles. URL: https://turnstile.com.ua/en/catalog/trypod-turnikety/ (дата звернення: 01.05.2025).

29. Turnstiles. URL: https://www.elvis.com.ua/en/kontrol-dostupu-en/turniketi-en/ (дата звернення: 01.05.2025).

30. Amazon. URL: https://www.amazon.com/ (дата звернення: 01.05.2025).

31. AJAX systems. URL: https://ajax.systems/ (дата звернення: 01.05.2025).

32. IEEE 802.3az Standard. URL: https://standards.ieee.org/ieee/802.3az/4270/ (дата звернення: 01.05.2025).

ДОДАТКИ

Додаток А

Лістинг програмного коду для створення бази даних

```
import sqlite3

def init_db(db_path: str = 'access_control.db'):
    conn = sqlite3.connect(db_path)
    conn.execute('PRAGMA foreign_keys = ON;')
    cursor = conn.cursor()

    cursor.executescript("""
    CREATE TABLE IF NOT EXISTS users (
        user_id          INTEGER PRIMARY KEY AUTOINCREMENT,
        employee_code    TEXT    NOT NULL UNIQUE,
        last_name        TEXT    NOT NULL,
        first_name       TEXT    NOT NULL,
        patronymic       TEXT,
        department       TEXT,
        access_level     INTEGER NOT NULL,
        credential_ref   INTEGER,
        FOREIGN KEY(credential_ref) REFERENCES credentials(credential_id)
            ON DELETE SET NULL
    );

    CREATE TABLE IF NOT EXISTS authentication_methods (
        method_id   INTEGER PRIMARY KEY AUTOINCREMENT,
        name        TEXT    NOT NULL UNIQUE,
        description TEXT
    );

    CREATE TABLE IF NOT EXISTS credentials (
        credential_id  INTEGER PRIMARY KEY AUTOINCREMENT,
        user_id        INTEGER NOT NULL,
        method_id      INTEGER NOT NULL,
        template_data  BLOB    NOT NULL,
            FOREIGN KEY(user_id)    REFERENCES users(user_id) ON DELETE
CASCADE,
                                    FOREIGN     KEY(method_id)     REFERENCES
authentication_methods(method_id)
    );
```

Продовження додатку А

```
CREATE TABLE IF NOT EXISTS devices (
      device_id    INTEGER PRIMARY KEY AUTOINCREMENT,
      device_type   TEXT    NOT NULL,
      unique_id    TEXT    NOT NULL UNIQUE,
      location     TEXT,
      config_params TEXT
   );

   CREATE TABLE IF NOT EXISTS device_logs (
      log_id         INTEGER PRIMARY KEY AUTOINCREMENT,
      device_id      INTEGER NOT NULL,
      event_timestamp DATETIME NOT NULL,
      event_type     TEXT    NOT NULL,
      description    TEXT,
        FOREIGN KEY(device_id) REFERENCES devices(device_id) ON DELETE
CASCADE
   );

   CREATE TABLE IF NOT EXISTS events (
      event_id             INTEGER PRIMARY KEY AUTOINCREMENT,
      transaction_id        TEXT    NOT NULL UNIQUE,
      user_id              INTEGER NOT NULL,
      device_id             INTEGER NOT NULL,
      request_timestamp     DATETIME NOT NULL,
      confirmation_timestamp DATETIME,
      access_result         TEXT    NOT NULL,
      factor_results        TEXT,
          FOREIGN KEY(user_id)    REFERENCES users(user_id)    ON DELETE
RESTRICT,
        FOREIGN KEY(device_id) REFERENCES devices(device_id) ON DELETE
RESTRICT
   );
   """)
   conn.commit()
   conn.close()

if __name__ == '__main__':
   init_db()
```