Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи
магістра
(назва освітньо-кваліфікаційного рівня)

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: «Мультимодальна біометрична автентифікація користувачів в системах контролю доступу підприємства»

Виконавець: студент ІІ курсу, групи КБм-21

_____ ***Кубик Валентин Олександрович***
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Толюпа С.В.		
Рецензент	Степанов М.М.		
Нормоконтроль	Даков С.Ю.		

Київ 2022

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«__» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм-21* (група) *Кубику Валентину Олександровичу* (прізвище ім'я по-батькові)

Тема дипломної роботи *Мультимодальна біометрична автентифікація користувачів в системах контролю доступу підприємства*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процедура біометричного контролю доступу на підприємстві
Предмет досліджень	Методи біометрії в автоматизованих системах доступу на підприємстві
Мета	Реалізація методів біометрії в автоматизованих системах доступу на підприємстві на базі поєднання декількох підходів щодо автентифікації
Вихідні дані для Проведення роботи	Методи біометричної автентифікації в системах контролю доступу

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення систем контролю та керування доступом за рахунок поєднання методів біометричної автентифікації

Практична цінність покращення використання методів автентифікації в автоматизованих системах

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	29.10.2021 – 17.02.2022
Аналіз літературних джерел	18.02.2022 - 14.03.2022
Огляд сучасних систем контролю та керування доступом	15.03.2022 – 30.03.2022
Дослідження надійності технологій ідентифікації в СККД	31.03.2022 – 01.04.2022
Проектування архітектури та розробка алгоритму роботи системи контролю та керування доступом	02.04.2022 – 20.04.2022
Формування висновків і рекомендацій щодо подальшої розробки системи	21.04.2022 – 04.05.2022
Оформлення пояснювальної записки	05.05.2022 – 15.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Значне підвищення надійності систем контролю доступу при незначному підвищенні їх собівартості

Соціальний ефект Покращення технологій забезпечення захисту інформації в системах контролю доступу

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Мультимодальна біометрична автентифікація користувачів в системах контролю доступу підприємства» складається з вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 63 сторінки. Робота містить 11 рисунків, 8 таблиць. Список використаних джерел включає 30 джерел.

Об’єкт дослідження – процедура біометричного контролю доступу на підприємстві.

Мета роботи – реалізація методів біометрії в автоматизованих системах доступу на підприємстві на базі поєднання декількох підходів щодо автентифікації.

Методи дослідження:

- порівняння ступенів захищеності сучасних систем контролю доступу за методами автентифікації, що в них використовуються;
- системний підхід до огляду систем контролю та керування доступом;
- аналіз надійності технологій біометричної ідентифікації;
- моделювання розробленої системи.

Практичне значення роботи полягає в тому, що було запропоновано підхід щодо покращення використання методів автентифікації в автоматизованих системах, на базі поєднання автентифікації по відбитку пальця та по 3D-моделі обличчя, що дало можливість значно підвищити надійність системи контролю доступу при незначному збільшенні її вартості.

Результати здійснених у дипломній роботі досліджень можуть бути використані компаніями малого чи середнього розміру для підвищення рівня захищеності корпоративної інформації, спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Ключові слова: СККД, контроль доступу, біометрія, біометрична ідентифікація, мультимодальна біометрія.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

СККД	–	Система контролю та керування доступом
КПП	–	Контрольно-пропускний пункт
IBG	–	International Business Group
CCD	–	Charge-Coupled Device
CMOS	–	Complementary Metal-Oxide-Semiconductor
RFID	–	Radio frequency identification
FAR	–	False Acceptance Rate
FRR	–	False Rejection Rate
EER	–	Equal Error Rate
APB	–	Antipassback
ВП	–	Виконавчі пристрої
СУБД	–	Система управління базами даних
ОС	–	Операційна система

ЗМІСТ

ВСТУП

На даний час, у зв'язку з посиленням боротьби зі злочинністю та тероризмом, що сприяє зростанню галузі безпеки, ідентифікація осіб, з використанням біометричних технологій, є однією з найбільш перспективних областей, що швидко розвиваються. Серед сучасних методів та засобів ідентифікації особи провідні позиції займають саме біометричні системи.

Біометрія з'явилася в кінці 19 сторіччя в якості наукового розділу, що залучає статистичні методи для кількісних біологічних експериментів.

У класичному розумінні біометрія - це наука, яка вивчає методи ідентифікації (упізнання, просто кажучи) конкретної особистості на основі її особистих фізіологічних чи поведінкових особливостей [1]. До недавнього часу основними користувачами методів біометричної ідентифікації були різноманітні правоохоронні органи та спецслужби. Однак за останні півтора десятиріччя найбільш активно цікавитися методами біометричної ідентифікації почали власники різноманітних інформаційно-телекомунікаційних систем[2-3]. Це пов'язано, насамперед, з активним впровадженням комп'ютерних та телекомунікаційних технологій до комерційної сфери, як наслідок, швидким зростанням цінності інформації як такої. І, звичайно, з появою у світовій мережі величезного обсягу інформації, доступ до якої повинен бути обмежений. Розвиток комп'ютерних технологій, поява нових матеріалів та математичних алгоритмів дозволили створити спеціалізовані пристрої ідентифікації - біометричні сканери, які лежать в основі систем ідентифікації за біометричними характеристиками. Міжнародна біометрична група (IBG) відзначала збільшення доходів у галузі біометрії майже в 7 разів - з 0,6 (у 2002 році) до 4,04 (у 2007 році) мільярдів доларів.

Система контролю та управління доступом (СККД) - це сукупність технічних засобів та організаційних заходів, що дозволяють контролювати доступ до об'єктів СККД та відстежувати рух людей в зоні, яка охороняється. В даний час системи

контролю доступу визнані одним з найбільш ефективних методів вирішення складних завдань безпеки для об'єктів.

Забезпечення безпеки, запобігання витоку інформації та моніторинг ефективності персоналу є одними з найбільш значущих проблем на багатьох підприємствах у наш час. Для його забезпечення використовуються системи контролю та керування доступом. Ці системи являють собою поєднання апаратних та програмних засобів безпеки, спрямованих на обмеження та реєстрацію входу та виходу об’єктів (людей, транспортних засобів) на заданій території через «точки доступу»: двері, ворота, контрольно-пропускні пункти.

Актуальність дослідження полягає у тому, що на сьогоднішній день поширюється використання біометричних методів ідентифікації, як зручних і надійних у порівнянні з вартістю. Одна з головних переваг – відсутність використання паролю. Такий підхід ефективніший за використання смарт-карт, паролів, PIN-кодів.

Також варто відзначити, що на відміну від сучасної двофакторної автентифікації використання біометричних методів дозволяють ідентифікувати саме людину, а не конкретний пристрій, що є важливим при роботі з конфіденційною інформацією.

Захист інформації від несанкціонованого доступу має актуальне значення, оскільки зловмисником може бути як стороння особа, так і діючий працівник, тому головною метою щодо забезпечення режиму доступу є контроль суб’єктів, що знаходяться в межах території, яка охороняється.

Мета роботи – реалізація методів біометрії в автоматизованих системах доступу на підприємстві на базі поєднання декількох підходів щодо автентифікації.

Для досягнення зазначеної мети дипломної роботи було поставлено наступні **завдання:**

- провести аналітичний огляд сучасних біометричних систем та рівень їх надійності за допомогою математичної статистики;
- обгрунтувати використання біометричних методів;

- оцінити технології біометричної автентифікації користувачів з точки зору доцільності їх використання в СККД;
- проаналізувати мультимодальний метод;
- розробити модель системи автентифікації з використанням мультимодального методу.
- розробити функціональну схему системи, та описати функції і взаємодію її елементів;
- виконати обґрунтування доцільності використання системи.

Об'єкт дослідження – процедура біометричного контролю доступу на підприємстві.

Предмет дослідження – методи біометрії в автоматизованих системах доступу на підприємстві.

Для досягнення поставленої в роботі мети було застосовано наступні методи дослідження:

- порівняння ступенів захищеності сучасних систем контролю доступу за методами автентифікації, що в них використовуються;
- системний підхід до огляду систем контролю та керування доступом;
- аналіз надійності технологій біометричної ідентифікації;
- моделювання розробленої системи.

Практична цінність полягає в тому, що було запропоновано підхід щодо покращення використання методів автентифікації в автоматизованих системах, на базі поєднання автентифікації по відбитку пальця та по 3D-моделі обличчя, що дало можливість значно підвищити надійність системи контролю доступу при незначному збільшенні її вартості.

Апробація результатів роботи та публікації. Основні результати роботи доповідалися та обговорювалися на Міжнародній науково-практичній конференції "Прикладні системи та технології в інформаційному суспільстві" 2021р. Основні положення дипломної роботи викладені в матеріалі наукової конференції (додаток А).

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ГАЛУЗІ

1.1 Інформаційна безпека підприємств та організацій

Проблема інформаційної безпеки підприємств та організацій є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, інформаційних систем і мереж. Це можна пояснити зростаючими можливостями доступу до інформації: технічними та програмними, котрі не завжди є правомірними. Актуальністю проблеми інформаційної безпеки підприємств описується рядом взаємопов’язаних факторів, наслідком є процес інформатизації сучасного суспільства. З однієї сторони, формуються правові засади інформатизації, поширюються інформаційні технології у підприємницькій діяльності, а з іншого боку, висока уразливість інформаційних систем, та стрімкий прогрес розвитку «інформаційної зброї».

У інформаційній сфері історично сформувалися два напрями захисту від несанкціонованого доступу. У системах фізичного захисту вони називаються системами контролю та керування доступом (СККД), а в комп'ютерній сфері – системами ідентифікації і автентифікації.

Особливостями соціально-економічної ситуації, маємо відсутність реальних обмежень щодо доступу до засобів інформаційного нападу, які призводять до численних фактів їх застосування конкурентами, кримінальними елементами, іншими суб’єктами.

Окрім того, за умов жорстокої конкурентної боротьби, суб’єки економічних ринків проводять акт недобросовісної конкуренції, дії котрі пов’язані із промисловим шпигунством, тому виникла потреба в розмежуванні доступу до носіїв інформації безпосередньо та особливо на підприємствах, розділення та визначення

порядку отримання та використання інформації обмеженим та/або необмеженим доступом.

Підприємницька діяльність досить насичена не тільки діловими відносинами, їй значною мірою притаманні тісні інформаційні стосунки партнерів та конкурентів. Останні ж регулюються відповідними законодавчими та нормативними актами держави, а також нормативними документами підприємницьких структур.

Згідно зі ст. 60 Закону України «Про банки і банківську діяльність» до банківської таємниці належить інформація про діяльність і фінансовий стан клієнта, що стала відома банку у процесі його обслуговування і взаємовідносин із ним або з третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди.

Тлумачення поняття комерційної таємниці дається у ст. 30 Закону України «Про підприємства в Україні». Зокрема у статті вказується, що під комерційною таємницею підприємства розуміють відомості, пов’язані з виробництвом, технологічною інформацією, управлінням фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передання, витік) яких може завдати шкоди його інтересам.

Відповідно до ч. 3 ст. 30 Закону України «Про інформацію» власникам конфіденційної інформації надано право самим включати її до категорії конфіденційної, визначати режим доступу до неї та встановлювати систему (способи) її захисту.

Комерційна таємниця підприємства і проблеми її охорони і захисту.

Під комерційною цінністю інформації можна розуміти грошовий еквівалент, який в даному випадку може бути сплачений за право володіння відомостями. Конкуренти і інші суб'єкти, прямо або побічно пов'язані з підприємством, об'єктивно зацікавлені в зборі і отриманні інформації самого різного роду. Потенційна комерційна цінність відомостей має місце у разі, коли при певних обставинах, в певний час і у визначеному місці з'являється або може з'явитися інтерес третіх осіб до придбання інформації про підприємство [4].

Вільний доступ до відомостей означає відсутність заходів, направлених на охорону і захист інформації від спроб ознайомлення з нею третіх осіб. У вільному доступі, як правило, знаходяться загальні довідкові відомості про підприємство - реквізити, історія створення, основні напрями діяльності підприємства в тій частині, в якій вони не захищені положенням про комерційну таємницю. Деякі підприємства, які проводять політику інформаційної відвертості і організаційної прозорості для необмеженого кола осіб, можуть залежно від специфіки своєї діяльності розміщувати інформацію про своїх працівників, ціни на продукцію, що випускається, або послуги, що надаються. У ряді випадків у вільному доступі знаходяться повідомлення прес-служби або іншого підрозділу, адресовані засобам масової інформації, які можуть стосуватися різних питань діяльності підприємства.

Конфіденційність інформації охороняється підприємством, та здійснюється, на підставі виданих локальних нормативних актів, найважливішим з яких є «Положення про комерційну таємницю». Усі заходи безпеки, захисту інформації від несанкціонованого доступу ззовні і усередині підприємства з боку не уповноважених співробітників повинні базуватися саме на положеннях даного документа

Відомості, які доцільно відносити до предмету комерційної таємниці, по сферах і характеру діяльності підприємства можна виділити наступні групи відомостей:

- відомості про фінансову діяльність;
- інформація про ринок;
- відомості про виробництво, виконання робіт і надання послуг;
- відомості про наукові розробки;
- відомості про систему матеріально-технічного забезпечення;
- відомості про персонал підприємства;
- відомості про принципи управління підприємством;
- інші відомості.

З відомостями такого роду постійно працюють, і часто вони знаходяться не в електронному, а в фізичному (друкованому) вигляді. Тому виникає потреба в обмеженні доступу в приміщення, де вони обробляються та зберігаються.

1.2 Типи автентифікації в системах контролю та керування доступом

СККД – одне з найбільш ефективних рішень, що можуть запобігти проникненню зловмисників на територію, яка знаходиться під охороною. Системи контролю доступу можуть допомогти забезпечити цілісність та захист не лише матеріальних цінностей та важливої інформації, але й гарантувати безпеку персоналу та відвідувачів. Вони дозволяють захищати території від несанкціонованого доступу і в той же час не заважати робочій діяльності працівників. Окремі СККД здатні стежити за рухом усіх працівників в офісі, що дозволяє вести облік та фіксувати фактично відпрацьований час працівників та виявляти порушення трудової дисципліни(як от запізнення або прогул).

На сьогоднішній день в світі поширені різноманітні конфігурації систем контролю доступу: найпростіші з них розраховані лише на одні вхідні двері, а найскладніші призначені для контролю доступу на великих об'єктах - підприємствах, заводах і банках[5]. У цьому випадку найпростіший варіант СККД - звичайний домофон. Незалежно від конфігурації СККД, кожна така система складається з декількох обов’язкових вузлів, це контролери для управління, зчитувачі для ідентифікації, а також усі види виконавчих пристроїв для обмеження доступу: турнікети, електромагнітні замки та засови.

Автентифікація - це процес перевірки достовірності представленого ідентифікатора, та прийняття рішення про справжність користувача. Для підтвердження достовірності об’єкт повинен пред'явити щось, що може бути представлено тільки ним, і ніким більше.

Автентифікація в СККД використовується для встановлення автентичності і визначення повноважень об'єкта при спробі отриманні ним доступу, а також реєстрації його дій.

Розрізняють наступні типи автентифікації:

1. Користувач, який проходить перевірку справжності, знає певну унікальну інформацію. Приклад: автентифікація по паролю або парольній фразі.

2. Користувач володіє певною річчю з унікальними характеристиками або змістом. Приклад: магнітна картка, тощо.

3. Ідентифікатор є невід’ємною частиною користувача. Наприклад, відбитки пальців та інші типи біометричних ідентифікаторів(біометричну автентифікацію називають автентифікацією користувача за її біометричними ознаками).

В усіх трьох випадках процедура автентифікації виконується в наступні два етапи:

1. Еталонний зразок автентифікаційної інформації запитується у користувача один раз, наприклад, вводиться пароль чи парольна фраза(або такий пароль генерують випадковим чином та записують на ідентифікатор користувача). Цей зразок зберігає в собі суб'єкт системи, який перевіряє автентифікацію - контролера(в СККД цей суб'єкт може бути як окремим контролером, так і центральним сервером в залежності від конфігурації системи). Як правило, визначають певний термін дії цього еталону, після якого еталонний зразок запитується повторно.

2. Кожен раз при здійсненні аутентифікації в користувача запитують автентифікаційну інформацію, яка порівнюється з еталоном. На основі цього порівняння робиться висновок про справжність користувача.

Розглянемо переваги та недоліки основних систем автентифікації згідно з типами ідентифікаторів, які вони використовують.

1.2.1 Автентифікація на основі пароля

Перший тип ідентифікатора - секретна інформація, якою повинен володіти лише уповноважений суб'єкт. Такою інформацією може бути певна фраза або пароль, наприклад, у формі усного повідомлення, текстового представлення, комбінації жестів (дій) для розблокування або персонального ідентифікаційного номера (PIN).

Основна перевага автентифікації пароля - простота та звичність. Паролі вже давно стали невід’ємною частиною життя сучасної людини. При правильному використанні паролі можуть забезпечити прийнятний рівень безпеки для багатьох організацій[6]. Однак з точки зору сукупності характеристик їх слід визнати найслабшим засобом автентифікації оскільки автентифікація з допомогою пароля має багато недоліків:

1. На відміну від випадково згенерованих криптографічних ключів (які, наприклад, можуть містити унікальний елемент, що використовується для автентифікації), можна підібрати паролі користувачів через досить недбале ставлення більшості користувачів до генерування паролів. Часто трапляються випадки, коли користувачі вибирають легко передбачувані паролі, наприклад:

- пароль еквівалентний ідентифікатору (імені) користувача (або імені користувача, записаному у зворотному порядку, або легко формується з імені користувача тощо);
- пароль - слово або фраза, запозичена з якої-небуть мови; такі паролі можуть бути підібрані за невеликий проміжок часу за допомогою «словникової атаки» - перерахування всіх слів згідно словника, що містить усі слова та загальні фрази використовуваної мови;
- досить часто користувачі використовують нескладні паролі, які зламуються методом "грубої сили", тобто простого перерахування всіх можливих варіантів.

2. Існують і доступні та вільно доступні різні утиліти для відновлення паролів, у тому числі спеціалізовані для конкретних широко розповсюджених програмних засобів. Наприклад, на сайті www.lostpassword.com описана утиліта пошуку паролів для документа Microsoft Word 2000 (ключ відновлення пароля Word), призначеного для відновлення доступу до документа, якщо його власник забув пароль. Незважаючи на цю корисну мету, ніщо не заважає зловмисникам використовувати подібні утиліти для злому паролів інших людей.

3. Пароль можна отримати, застосовуючи насильство щодо його власника.

4. Під час введення пароля можна підгледіти або перехопити пароль.

Крім того працівники доволі часто повідомляють паролі колегам, щоб вони могли, наприклад, підмінити власника пароля на деякий час. Теоретично в таких випадках правильним рішенням буде використовувати засоби керування доступом, але на практиці цього ніхто не робить. Все вищевказане робить механізм парольної автентифікації слабо захищеним.

1.2.2 Автентифікація на основі унікального предмету

Другий тип ідентифікатора – унікальний фізичний об’єкт, яким повинен володіти лише уповноважений суб'єкт. Це може бути особиста печатка, ключ до замка, для комп’ютера - це файл даних, що містить ідентифікатор користувача. Такий ідентифікатор часто вбудовується в конкретний пристрій аутентифікації, наприклад, пластикова карта, смарт-карта. Зловмиснику стає важче отримати такий пристрій, ніж зламати пароль, і суб'єкт може негайно повідомити про викрадення пристрою. У більшості випадків автентифікація за допомогою унікального предмету забезпечує більш серйозний захист, ніж автентифікація пароля[7].

Елементи, що використовуються для даної автентифікації, можна розділити на дві групи:

1. "Пасивні" елементи, що містять інформацію про автентифікацію (наприклад, деякий випадково створений пароль) і передають її до модуля

аутентифікації на вимогу. У той же час інформація про автентифікацію може зберігатися в об'єкті як відкрито (приклади: магнітні картки, смарт-карти з відкритою пам’яттю, електронні планшети Touch Memory), так і в захищеній формі (смарт-карти із захищеною пам'яттю, USB-жетони). В останньому випадку потрібно ввести PIN-код для доступу до збережених даних, що автоматично перетворює елемент у двофакторний інструмент аутентифікації.

2. "Активні" елементи, які мають достатні обчислювальні ресурси та здатні брати активну участь у процесі аутентифікації (приклади: смарт-карти мікропроцесора та USB-жетони). Ця функція особливо цікава при віддаленій аутентифікації користувачів, оскільки на основі таких елементів може бути забезпечена сувора автентифікація. Цей термін означає тип автентифікації, під час якого секретна інформація, що дозволяє перевірити справжність користувача, не передається у відкритому вигляді.

При безконтактній радіочастотній ідентифікації інформація зчитується з ідентифікатора, розташованого на об'єкті, без фізичного чи оптичного контакту. Досить, щоб ідентифікатор і зчитувач знаходилися на відстані не більше заданої (зазвичай кілька сантиметрів), а між ними може бути будь-який неметалічний бар'єр (наприклад, корпус зчитувача).

Для здійснення безконтактної радіочастотної ідентифікації потрібні три компоненти:

- транспондер (ідентифікатор відповіді), розташований на об'єкті, який слід ідентифікувати;
- зчитувач інформації з ідентифікатора (він, якщо він надається, записує інформацію в транспондер);
- одержувач інформації - програма, комп'ютерна система обробки даних або оператор.

Зчитувач зазвичай містить радіочастотний модуль (передавач і приймач), блок керування, що включає мікропроцесор і пам'ять, і елемент зв'язку з транспондером. Крім того, багато зчитувачів оснащені додатковим інтерфейсом, щоб мати можливість передавати отримані дані в іншу систему (ПК, система обробки даних).

Транспондер - це пристрій, який фактично є носієм даних системи RFID, і, як правило, включає в себе приймач, передавальний ланцюг, антену та блок пам'яті для зберігання інформації. Приймач, передавальна схема і пам'ять структурно реалізовані як окрема інтегральна схема. Іноді в конструкцію RF-мітки також включається автономне джерело живлення. Транспондер активується лише тоді, коли він знаходиться в зоні опитування читача. Енергія, необхідна для активації транспондера, подається безконтактно через блок зв'язку разом з тактовими імпульсами та даними.

Процес ідентифікації радіочастоти виконується наступним чином:

1. Передавач зчитувача через антену постійно (або у визначений час) випромінює радіосигнал з частотою, прийнятою в цій системі;

2. Транспондер, розташований у зоні покриття зчитувача, приймає радіосигнал через антену і використовує цю енергію для живлення (це пасивність ідентифікатора - йому не потрібно джерело живлення). Транспондер зчитує код зі свого запам'ятовуючого пристрою (пам'яті) та імітує радіосигнал відповіді;

3. Зчитувач отримує сигнал відповіді, вибирає код, що міститься в ньому, проводить операції криптографічного захисту та анти колізійні процедури (послідовна робота з декількома ідентифікаторами, одночасно розташованими в зоні дії зчитувача), при необхідності і передає інформацію за призначенням: до контролера, системи обробки даних або оператору.

Робоча частота системи RFID визначає її робочу відстань. Низькочастотні RFID системи застосовуються там, де невелика відстань між об'єктом і зчитувачем допустима. Звичайна відстань зчитування - 0,5 м, а для мініатюрних тегів - зазвичай навіть менша, приблизно 0,1 м. Більшість систем контролю доступу, складських та виробничих систем використовують низькі частоти. Системи з проміжними значеннями робочої частоти використовуються там, де необхідно передавати значний об’єм даних, наприклад, в системах контролю доступу, в смарт-картках.

Високочастотні RFID-системи застосовуються там, де потрібні значна відстань та висока швидкість зчитування, наприклад, під час моніторингу

залізничних вагонів, контейнерів, вагонів та систем збору відходів. Висока відстань зчитування дозволяє безпечно встановлювати зчитувачі поза досяжністю людей.

Проте, автентифікація з використанням унікальних предметів має ряд суттєвих недоліків:

1. Ідентифікатор може бути викрадений у користувача.

2. У більшості випадків потрібне спеціальне обладнання для роботи з предметами.

3. Можливо зробити копію або емулятор об'єкта.

4. Працівник може забути або втратити ідентифікатор.

5. Час, необхідний читачеві для правильної передачі всіх своїх бітів даних за допомогою тегу з великою кількістю пам'яті, може у багато разів перевищувати час передачі лише унікального ідентифікатора.

6. Крім того, збільшення кількості переданих даних призводить до збільшення частоти помилок передачі.

1.2.3 Автентифікація на основі біометричної характеристики

Другий тип ідентифікатора – щось, що є невід’ємною частиною уповноваженого суб'єкта (біометрична характеристика). Ідентифікатором в даному випадку виступає певна фізична характеристика користувача. Це може бути зображення, відбиток пальця, сітківка чи райдужна оболонка очей. З точки зору користувачів, цей спосіб є найпростішим: не потрібно запам’ятовувати пароль або носити при собі автентифікаційний пристрій[7].

Для біометричної автентифікації можна використовувати багато різних аспектів фізіології, хімії чи поведінки людини. Вибір конкретного біометричного методу для використання в конкретному застосуванні включає зважування кількох факторів. Джейн та ін. (1999) визначив сім таких факторів, які слід використовувати при оцінці придатності будь-якої ознаки для використання в біометричній автентифікації:

1) Універсальність означає, що кожна людина, яка використовує систему, повинна володіти цією рисою.

2) Унікальність означає, що ознака повинна бути достатньо різною для особин відповідної популяції, щоб їх можна було відрізняти один від одного.

3) Постійність пов’язана зі способом зміни ознаки з часом. Більш конкретно, ознака з «гарною» стійкістю з часом буде досить незмінною щодо конкретного алгоритму узгодження.

4) Вимірність стосується простоти набуття або вимірювання ознаки. Крім того, отримані дані повинні мати форму, яка дозволяє подальшу обробку та вилучення відповідних наборів ознак.

5) Продуктивність пов’язана з точністю, швидкістю та надійністю використовуваної технології.

6) Прийнятність пов’язана з тим, наскільки добре люди у відповідній популяції сприймають технологію таким чином, що вони готові довірити системі свої певні біометричні ознаки.

7) Обхід стосується легкості імітації ознаки за допомогою артефакту або замінника.Біометрична система повинна бути високочутливою для підтвердження авторизованого користувача, але відхиляти зловмисника з подібними біометричними параметрами. Для цього в процесі біометричної аутентифікації еталонні та подані користувачем зразки порівнюють, допускаючи певну похибку, яка визначається та встановлюється заздалегідь. Похибка обрана для встановлення оптимального співвідношення двох основних характеристик використовуваних засобів біометричної аутентифікації:

1. FAR (False Acceptance Rate) – ймовірність помилкового допуску.

2. FRR (False Rejection Rate) – ймовірність помилкової відмови в доступі.

Обидва значення вимірюються у відсотках і повинні бути мінімальними. Слід зазначити, що значення зворотні, тому модуль аутентифікації при використанні біометричної автентифікації налаштовується індивідуально – в залежності від використовуваних біометричних характеристик та вимог до якості захисту, досягається деяка «золота середина» між значеннями вищезгаданих ймовірностей.

Серйозний засіб біометричної аутентифікації повинен дозволяти коригувати коефіцієнт FAR до значень порядку 0,01 - 0,001% з коефіцієнтом FRR до 1-3%.

Залежно від використовуваних біометричних характеристик засоби біометричної аутентифікації мають різні переваги та недоліки. Поширеним загальним недоліком біометричної аутентифікації є необхідність обладнання для зчитування біометричних характеристик, що може коштувати досить дорого.

З точки зору доцільності застосування в системах контролю та керування доступом, біометрична автентифікація має найвищий рівень надійності з представлених, оскільки використання біометричного ідентифікатора забезпечує набагато більший рівень захисту порівняно з традиційними засобами контролю доступу – паролями, безконтактними картками, брелоками та ін. Власник може забути пароль, втратити звичну карту доступу або брелок, їх можна скопіювати, викрасти, передати добровільно. На противагу цьому біометричні параметри людини набагато складніше, а в деяких випадках і неможливо підробити. Тому біометричні системи контролю доступу є одними з найнадійніших, до того ж вони постійно оновлюються та вдосконалюються.

1.3 Багатофакторна автентифікація

1.3.1 Поняття та суть багатофакторної автентифікації

Багатофакторна автентифікація - розширена автентифікація, метод контролю доступу до системи, в якій користувачеві для отримання доступу до інформації необхідно пред'явити більш одного «доказу механізму аутентифікації» [8].

Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності та вартості впровадження.

Відома організація NIST у своїй публікації розглядає порівняльну таблицю по використанню тих чи інших методів автентифікації (табл. 1.1).

Таблиця 1.1 - Порівняння рівня ризику та вимог до системи

Рівень ризику	**Вимоги до системи**	**Технологія автентифікації**	**Приклади використання**
Низький	У випадку крадіжки, зламу, розголошення конфіденційних відомостей не станеться значних наслідків	Рекомендована вимога – використовувати багаторазові паролі (довгий термін дії)	Реєстрація на сайті в мережі інтернет
Середній	У випадку крадіжки, зламу, розголошення конфіденційних відомостей буде заподіяно невеликих збитків	Рекомендована вимога – використовувати одноразові паролі (короткий, або незначний термін дії)	Реєстрація в банківській систем або застосунку
Високий	У випадку крадіжки, зламу, розголошення конфіденційних відомостей буде заподіяно значної шкоди	Рекомендована вимога – використовувати багатофакторну ідентифікацію	Проведення значних фінансових операцій або робота з ІзОД

1.3.2 Двофакторна автентифікація

Двофакторна автентифікація(у подальшому ДФА) є типом багатофакторної автентифікації. ДФА — представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів [9].

Хорошим прикладом двофакторної автентифікації є авторизація Google і Microsoft. Коли користувач заходить з нового пристрою, крім аутентифікації по імені та паролю, його просять ввести шестизначний (Google) або восьмизначний

(Microsoft) код підтвердження. Ви можете отримати його за допомогою SMS, або голосового дзвінка на ваш телефон, він може бути взятий з заздалегідь складеного реєстру разових кодів або ви можете використовувати додаток-автентифікатор, генеруючий новий одноразовий пароль за короткі проміжки часу. Вибрати один з методів можна в налаштуваннях вашого Google або Microsoft-акаунта.

1.3.3 Багатокрокова автентифікація

Багатокрокова автентифікація не завжди означає присутність багатьох факторів. Використання двох чи трьох етапів проходження автентифікації може здійснюватись багаторазовим введенням паролю, використанням декількох комбінованих методів одного фактору та інше.

PCI DSS вимагає, щоб всі фактори в багатофакторній аутентифікації були перевірені до механізму автентифікації, що надає запитаний доступ. Причому без попередніх знань про успіх або невдачу будь-який фактор повинен бути наданий індивідууму, доки не будуть представлені всі фактори. Якщо неавторизований користувач може вивести дійсність будь-якого індивідуального фактора аутентифікації, загальний процес автентифікації стає колекцією наступних однофакторних етапів аутентифікації, навіть якщо для кожного кроку використовується інший коефіцієнт[8].

Наприклад, якщо окрема особа подає облікові дані (наприклад, ім'я користувача / пароль), які після успішної перевірки, призводять до подання другого чинника для перевірки (наприклад, біометричного), це буде розглянуто, як "Багатосту" автентифікація. У середовищі можуть бути присутніми як багатоступенева, так і багатофакторна автентифікація. Наприклад, людина може виконати крок аутентифікації для входу в комп'ютер перед ініціюванням окремого процесу багатофакторної автентифікації для отримання доступу до CDE. Прикладом цього сценарію може стати вхідні дані віддаленого користувача для входу до свого корпоративного ноутбука. Після цього користувач може ініціювати VPN-

підключення до мережі організації за допомогою комбінації облікових даних і фізичної смарт-карти або апаратного маркера.

1.4 Нормативно-правова документація

При дослідженні та проектуванню системи контролю доступу буде використано наступну нормативно правову документацію:

- Закон України «Про інформацію» від 02.10.1992 № 2657-XII;
- Загальні критерії оцінки безпеки IT (The Common Criteria for Information Technology Security Evaluation / ISO 15408);
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР;
- ISO15408: Common Criteria for Information Technology Security Evaluation;
- Практичні правила управління інформаційної безпекою (Code of practice for Information Security Management / ISO 17799);
- Положення про технічний захист інформації в Україні;
- ISO 27001 – Управління інформаційною безпекою.

Висновки за розділом 1

В даному розділі були розглянуті теоретичні відомості про системи контролю та керування доступом та методи автентифікації користувачів, що сприяло формуванню основних методів та принципів проведення даного дослідження.

Розробка ефективної системи контролю доступу - необхідна умова ведення бізнесу в сьогоденні. При цьому особлива увага надається захисту від несанкціонованого доступу як до паперових носіїв інформації, так і до інформаційно-телекомунікаційної системи підприємства.

Залежно від особливостей структури та умов діяльності організації можливе використання різних типів СККД, проте, в будь-якому випадку, для успішного забезпечення контролю та керування доступом до ІТС(або приміщень з обмеженим доступом), СККД, що розробляється, повинна відповідати наступним вимогам:

- високий рівень надійності;
- задовільняти потреби організації;
- відповідати нормативно-правовій документації;
- бути доступною для різних сфер бізнесу;
- мати можливість масштабування;
- підтримувати інтеграцію з протипожежними та охоронними системами.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ В СККД

2.1 Методи біометричної автентифікації

2.1.1 Автентифікація за відбитком пальця

Незважаючи на довгу історію використання відбитків пальців у криміналістиці, детальні принципи формування папілярного малюнка стали відомі не так давно[10]. Якщо спростити, то на формування папілярного малюнка впливає ДНК та умови формування плоду. Саме тому навіть однакові близнюки мають різні, хоч і схожі відбитки пальців. Формування відбитків пальців відбувається протягом перших трьох місяців вагітності[11].

На сьогоднішній день дактилоскопія є найбільш поширеним методом автентифікації користувачів. Ідентифікація відбувається за допомогою відбитків пальців, які є унікальними для кожної людини, не змінюються з віком, проте глибокі пошкодження епідермісу можуть частково затерти папілярні лінії.

На даний момент на ринку представлено декілька типів дактилоскопічних сканерів, що мають суттєві технологічні відмінності. Характеристика та особливості їх будови наведено далі:

1. Ємнісні сканери

Ємність - це здатність провідника накопичувати електричний заряд. Ємнісний датчик відбитків пальців генерує зображення відбитків пальців за допомогою масиву, що містить тисячі дрібних пластин конденсатора. Матричні пластини утворюють "пікселі" зображення: кожна з них виступає як одна пластина конденсатора з паралельними пластинами, внаслідок чого дермальний шар шкіри, що здатний проводити струм діє як друга пластина конденсатора. Епідермальний шар в даному випадку виступає діелектриком[12].

Коли палець розміщений на датчику, утворюються слабкі електричні заряди, утворюючи малюнок між виступами або поглибленнями пальця і пластинами датчика. Використовуючи ці заряди, датчик отримує відомості про ємності на вимірюваній поверхні. Далі значення оцифровуються логікою датчика та надсилаються до сусіднього мікропроцесору для аналізу.

Технологія ємнісного сканування дозволяє отримати зображення відбитка пальця за рахунок різниці електричних потенціалів на окремих ділянках шкіри. Ці пристрої дещо дешевші, але вразливіші за оптичні: простої поломки (спричиненої, наприклад, розрядом статичного струму) достатньо, щоб елементи матриці сканування вийшли з ладу і якість розпізнавання погіршилася. Є два типи ємнісних датчиків: пасивні (у кожній осередку датчика є лише одна з пластин конденсатора) і активні (сенсорний елемент містить обидві пластини конденсатора).

Пасивні ємнісні сканери

Саме пасивні ємнісні датчики відбитків пальців найбільш чутливі до статичного струму, а також до сухої або пошкодженої шкіри пальця. Але вони досить добре працюють в різних умовах освітлення.

Основним обмеженням пасивних ємнісних датчиків є вимоги до мінімальної товщини захисного покриття, оскільки вони засновані на аналізі статичних зарядів між пальцем і датчиком(рис. 2.1).

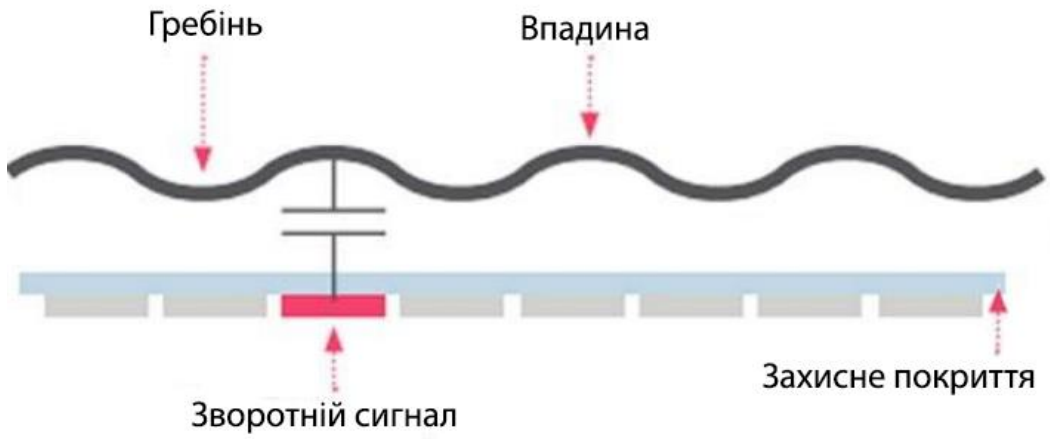

Рисунок 2.1 - Схема пасивного ємнісного сканера

Ємнісні датчики не можна обдурити, просто роздрукувавши зображення папіломи на папері. Більш важливою перевагою ємнісних сканерів є те, що вони більш компактні і тому легко інтегруються в портативні пристрої. Саме завдяки цій їх особливості вони отримали на даний момент найбільш широке використання в смартфонах.

Проте, незважаючи на складність, зламати ємнісний сканер цілком можливо, достатньо роздрукувати відбиток пальця з високою роздільною здатністю на електропровідному папері за допомогою спеціального принтеру і струмопровідної фарби.

Активні ємнісні сканери

Активний метод має такі переваги: він дозволяє використовувати додаткові функції для обробки зображення відбитків пальців, більш високий опір зовнішнім впливам, має більш високе співвідношення сигнал-шум(рис. 2.2).

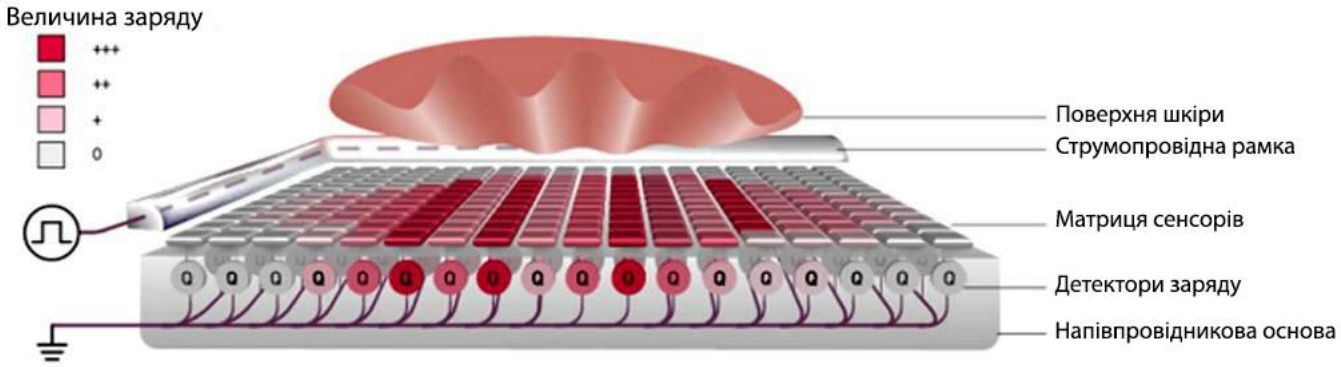

Рисунок 2.2 - Схема активного ємнісного сканера

Активні ємнісні сканери менш вимогливі до чистої шкіри, пошкодження епідермісу та бруду на поверхні датчика. Незважаючи на це, активні сканери забезпечують відмінну якість зображення, що дозволяє робити 3D-рендеринг відбитка пальця.

Ще одна істотна перевага активних ємнісних датчиків полягає в тому, що посилена передача сигналу між поверхнею відбитка пальця та датчиком дозволяє розміщувати датчик за товстим шаром захисного покриття або навіть за склом з мінімальним зниженням продуктивності.

Крім того, активні датчики дозволяють реєструвати електричні імпульси, які виникають під час скорочення серцевого м’яза, що значно знижує ризик використання муляжу. Активні ємнісні датчики - одна з найпоширеніших технологій зчитування відбитків пальців на даний момент.

2. Оптичні сканери

Ідеальне, надійне та зручне рішення - оптичне сканування. Саме оптичні сканери формують високоякісне, повномасштабне та повне зображення друку; Крім того, ці інструменти зручні у використанні: єдине, що потрібно від користувача, - торкнутися поверхні сканера.

В даний час оптичні сканери відбитків пальців використовують матриці CCD або CMOS, такі ж, як і IP камери(рис. 2.3). Історично матриці CCD були набагато кращими, ніж CMOS, але оскільки за останні десять років технологія CMOS зазнала значних змін, можливості технології CMOS наздогнали CCD. Тому в комерційних рішеннях зараз найбільш використовуваними матрицями є саме CMOS.

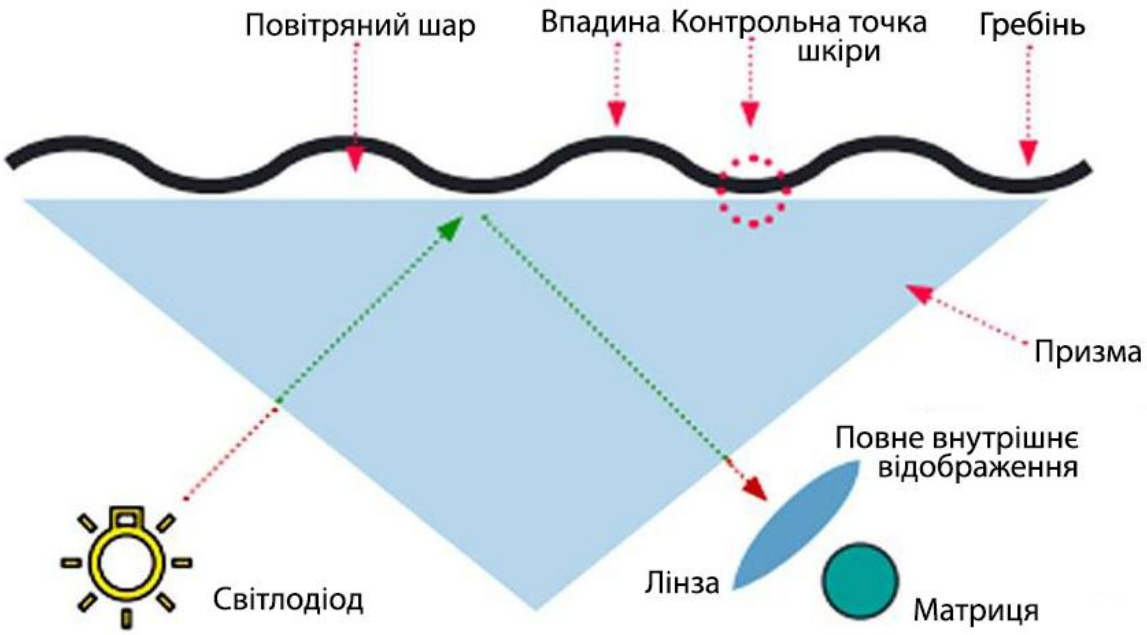

Рисунок 2.3 - Схема оптичного сканера

Сучасні оптичні сканери стійкі до спроб шахрайства за рахунок того, що вони можуть ефективно розпізнавати моделі на основі аналізу біометричного

ідентифікатора як живого біологічного об’єкта. Виділяються, зокрема, показники, що характеризують температуру пальця, його вологість, колір відбитка пальця тощо.

До переваг оптичних датчиків можна віднести низьку ціну. В першу чергу це стосується оптичних датчиків, що використовують CMOS.

До недоліків можна віднести:

• Розмір. Оптичні датчики, що використовують звичайну конструкцію, включаючи об'єктив та призму, є об'ємними та непридатними для використання в мобільних пристроях.

• Чутливість до забруднення поверхні призми. Оптичні датчики чутливі до великої кількості забруднень, які зазвичай зустрічаються в навколишньому середовищі, включаючи масло, бруд, конденсат, лід і навіть відбитки пальців, залишені попередніми користувачами. Крім того, різні умови освітлення можуть впливати на точність сканування.

• Зношення покриття призми. Зовнішнє покриття призми може зношуватися з часом, знижуючи точність сканування.

• Можливість підробки. Класичні оптичні сканери відбитків пальців можна відносно легко обманути за допомогою фальшивого пальця. Більш вдосконалені оптичні сканери менш схильні до підробки.

3. Ультразвукові сканери

Ультразвукові датчики відбитків пальців використовують для створення візуального зображення відбитка пальця ті ж принципи, що і медичне ультразвукове дослідження. Звукові хвилі генеруються за допомогою п'єзоелектричних перетворювачів, а відбита енергія фіксується за допомогою п'єзоелектричних матеріалів.

На відміну від оптичних сканерів, що фотографують поверхню пальця, ультразвукові датчики використовують високочастотні звукові хвилі. Це дозволяє ультразвуковим датчикам отримувати високоякісні зображення під час зчитування вологих і пошкоджених пальців, і цей метод сканування дозволяє отримати, крім відбитка, ще деякі додаткові характеристики (наприклад, пульс всередині пальця), що ускладнює використання муляжів.

Ультразвукові сканери відбитків пальців мають перевагу в тому, що вони надають більше біометричної інформації, ніж більшість інших. Проблеми з ультразвуковою технологією все ще заключаються значною мірою в тому, що вона повільна, коштовна, вимагає багато енергії та часу для обробки результатів сканування. Все це призводить до того, що цей тип датчиків не має широкого поширення.

4. Термосканери

Термосканери використовують датчики, що складаються з піроелектричних елементів того ж типу, що і в тепловізорах, вони фіксують різницю температур і перетворюють її на напругу.

Коли палець прикладають до термосенсора, датчик пасивного типу використовується для побудови температурної карти поверхні пальця, яка перетворюється на цифрове зображення, за температурою хребтів папілярного малюнка, що торкаються піроелектронних елементів і температурою повітря в западинах[12].

Проте є кілька серйозних проблем із тепловими сканерами:

• Зміна температури динамічна, тому зображення відбитків пальців короткочасне і стирається приблизно через одну десяту частину секунди, коли поверхня датчика досягає тієї ж температури, що і пальця.

• Вони чутливі до зносу поверхні датчика та забруднень.

• Коли температура навколишнього середовища близька до температури поверхні пальця, датчик потребує нагрівання, щоб різниця температур становила щонайменше один градус Цельсія.

Деякі з перерахованих вище проблем можна вирішити за допомогою активного термосканера. Однак активні термосканери також мають свої недоліки:

• Висока потреба в потужності.

• Неможливо розпізнати дрібні деталі, такі як потові пори.

• Немає можливості створити 3D-зображення.

5. Чутливі до тиску сканери

Ці пристрої використовують датчики, що складаються з матриці п’єзоелектричних елементів. Коли палець прикладається до скануючої поверхні, хребти папілярного малюнка чинять тиск на певну підмножину поверхневих елементів; відповідно, поглиблення не створюють ніякого тиску. Матриця напруг, отримана від п’єзоелектричних елементів, перетворюється на зображення поверхні пальця. Сканери, що чутливі до тиску, практично не використовуються в реальних комерційних продуктах через свою вартість.

6. Мультиспектральні сканери

Зчитувачі відбитків пальців, засновані на мультиспектральній технології, здатні отримувати інформацію не тільки про поверхню, але і про підповерхневий шар шкіри. Датчики MSI (Multispectral Imaging) дають серію знімків пальців при різних умовах освітлення, включаючи різні довжини хвиль, положення джерела світла та умови поляризації. Різні довжини хвиль видимого світла взаємодіють зі шкірою по-різному, що дозволяє значно збільшити обсяг даних. В результаті отримані зображення містять інформацію не тільки про поверхню, але й про внутрішні (підповерхневі) особливості шкіри.

Гребені папілярних ліній відбитка, які можна бачити на поверхні шкіри, мають приховану основу, у вигляді судин та інших підшкірних структур. Насправді видимі папілярні лінії пальців є просто «відлунням» фундаментального «внутрішнього відбитка».

На відміну від поверхневих особливостей відбитків пальців, які можуть бути змінені вологою, брудом або частково стерти, "внутрішній відбиток" є більш стійким і незмінним. Поєднання цих двох характеристик забезпечує новий метод високою надійністю та стійкістю до підробок.

2.1.2 Автентифікація за рисунком вен

Автентифікація за допомогою рисунку венозної сітки (Vein Recognition - англійською мовою) пальця або долоні заснована на отриманні шаблону при фотографуванні зовнішньої або внутрішньої сторони руки або пальця за допомогою інфрачервоної камери. Для сканування використовується інфрачервона камера. Картина вен стає помітною завдяки тому, що гемоглобін (забарвлюючий склад крові) поглинає інфрачервоне випромінювання і вени стають видимими в камері[13]. Програмне забезпечення на основі отриманих даних створює цифрову згортку.

Високий рівень безпеки та безконтактне розпізнавання роблять розпізнавання вен підходящим для багатьох застосувань, що вимагають дуже високої безпеки.

Що обмежує область застосування - це розмір та вартість сканерів. Сканери просто занадто громіздкі, щоб їх можна було вбудувати в більшість мобільних пристроїв, але вони чудово підходять для використання в системах контролю доступу. І навіть висловлюється думка, що з часом саме сканери венозного малюнка замінять зчитувачі відбитків пальців.

Крім того, автентифікація, що включає узгодження шаблону 1: N, може зайняти значний час, особливо якщо база даних містить велику кількість біометричних шаблонів. Це пов’язано з високими вимогами до обробки шаблонів, оскільки венозні візерунки дуже складні.

Однією з вирішальних переваг аутентифікації за допомогою венозного малюнка є складність отримання несанкціонованого шаблону. Оскільки вени знаходяться під шкірою, підробити їх розташування практично неможливо, що дозволяє отримати надійну автентифікацію зі низькою ймовірністю помилкової ідентифікації користувача, який не знаходиться в базі даних[14]. До того ж точність розпізнавання порівняна з автентифікацією за допомогою райдужної оболонки, хоча обладнання є значно дешевшим. Зараз цей тип сканування активно досліджується та впроваджується в СККД.

2.1.3 Розпізнавання обличчя

При розпізнаванні облич (face recognition - англійською мовою) використовуються різні візуальні маркери розташовані на обличчі людини, за допомогою яких будується унікальний цифровий шаблон[15]. Прикладами таких маркерів є форма носа або відстань між очима. Всього використовується більше 80 різних ознак.

Для аналізу отриманих маркерів використовуються різноманітні алгоритми та технології, які оцифровують та співставляють отриманий шаблон з базою даних.

3D-розпізнавання доволі нещодавно з’явилось на ринку систем контролю та керування доступом, проте за рахунок використання нейронних мереж та величезної бази даних з вуличних камер відеоспостереження с кожним роком точність ідентифікації особи підвищується. На сьогоднішній день припускають, що статистичну надійність розпізнавання обличь можна прирівняти до надійності методу розпізнавання відбитків пальців.

2.1.4 Автентифікація за сітківкою ока

Першими біометричними системами сканування очей (Retinal scan - англійською мовою) були саме сканери сітківки, що з'явилися ще в 1985 році. Сітківка залишається незмінною від народження до смерті, лише деякі хронічні захворювання можуть її змінити.

Сканування сітківки проводиться за допомогою інфрачервоного світла, яке виявляє капілярний малюнок і використовує його для аутентифікації[16].

Сканери сітківки використовують подібний до сканерів райдужки принцип роботи, але в той же час користувач повинна бути на невеликій відстані від об'єктиву камери. Ця камера проводить серію знімків крихітних судин що містяться

в оці, освітлених слабким лазером. Вважається, що такі сканери неможливо обійти за допомогою муляжів, тому вони встановлюються в зонах, де необхідний високий рівень безпеки. Проте їх широкому використанню заважає висока вартість та неприємні відчуття у користувачів під час, та деякий період після сканування.

Сканування сітківки використовували для ідентифікації (1: N) користувача в умовах високих вимог безпеки такі організації, як ФБР, НАСА та ЦРУ.

2.1.5 Автентифікація за допомогою райдужної оболонки

Процес аутентифікації за допомогою райдужної оболонки (Iris Recognition - англійською мовою) починається з детального зображення людського ока. Зображення для подальшого аналізу намагаються зробити в високій якості, але це не критично. Радужна оболонка ока настільки унікальна, що навіть нечітка картина дасть надійний результат[17]. Для цього використовують монохромну CCD-камеру з тьмяним освітленням, чутливу до інфрачервоного випромінювання(рис. 2.4). Зазвичай робиться серія з декількох фотографій через те, що зіниця ока чутлива до світла і постійно змінює свої розміри. Підсвічування ненав'язливе, а серія знімків робиться всього за кілька секунд.

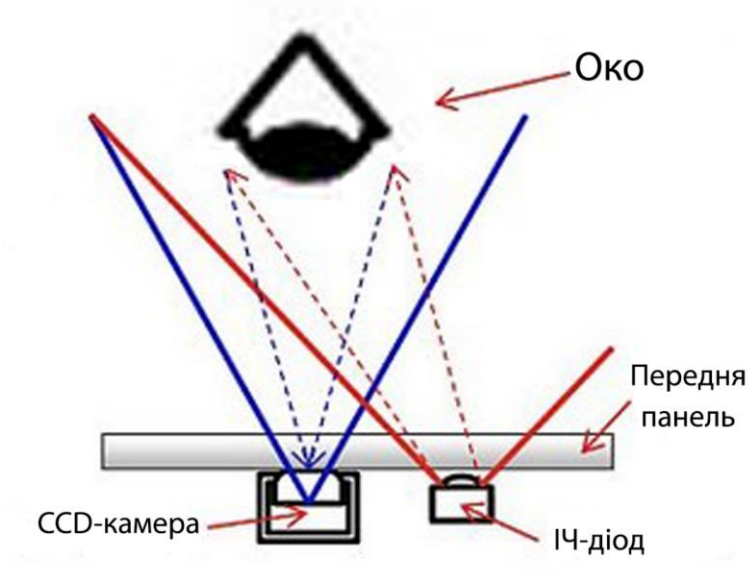

Рисунок 2.4 - Схема сканера райдужної оболонки ока

Потім з отриманих фотографій вибирається одна або кілька і починається сегментація, та проводиться співставлення з зображеннями, які містяться в базі на основі порівняння сегментів.

Метод розпізнавання за райдужною оболонкою і одним з найбільш надійних за рахунок того, що візерунок райдужки залишається практично незмінним протягом життя. Крім того, даний метод доволі важко обдурити, оскільки зловмиснику досить складно отримати скан райдужки непомітно навіть за допомогою спеціальних технічних засобів. До недоліків можна віднести високу ціну та майже цілковиту неможливість ідентифікації, після вживання користувачем алкоголю або ЛСД.

2.1.6 Автентифікація за допомогою ДНК

Аналіз ДНК (англ. DNA Biometrics) стає більш поширеною технологією біометричної аутентифікації і все частіше використовується в криміналістиці та охороні здоров'я[18].

Переваги автентифікації за допомогою ДНК:

• ДНК - єдина біометрична технологія, яка дозволяє ідентифікувати родичів за невстановленим зразком ДНК.

• Як і відбитки пальців, ДНК - одна з небагатьох біометричних характеристик людини, яку злочинці залишають на місці злочину.

• ДНК-тестування - це відносно зріла та динамічна технологія, яка широко використовується та знайома широкій публіці.

• Можна легко зберігати велику кількість результатів аналізу ДНК у базах даних, це дозволяє накопичувати дані та швидко виконувати автоматизований пошук.

Сучасні технології швидкої ідентифікації за допомогою ДНК скоротили процес секвентування до 90 хвилин. А використання портативних пристроїв з

автоматичною обробкою дозволяє провести аналіз навіть в умовах непідготовленого персоналу, достатньо попередньої годинної підготовки.

Проте в системах СККД автентифікація користувачів майже не використовується через високу вартість пристроїв та значний час очікування результатів.

2.1.7Автентифікація за допомогою голосу

Метод розпізнавання голосу визначає особистість людини за допомогою поєднання унікальних голосових характеристик. Алгоритми аналізують основні ознаки, за якими приймається рішення про особу мовця: джерело голосу, резонансні частоти мовного шляху та їх ослаблення, а також динаміку контролю артикуляції[19].

Перший міжнародний патент на систему розпізнавання голосу був поданий у 1983 р. Науково-дослідним центром телекомунікацій CSELT (Італія), авторами якого є Мікеле Каваца та Альберто Ціарамелла.

У травні 2013 року банківський відділ Barclays почав використовувати систему ідентифікації клієнтів по телефону протягом перших 30 секунд звичайної розмови. Система була розроблена фірмою Nuance.

Однак, оскільки голос людини може змінюватись залежно від віку, емоційного стану, здоров'я, гормонального рівня та ряду інших факторів, метод не є абсолютно точним. Крім того, системи розпізнавання голосу можуть мати проблеми з ідентифікацією близнюків[20].

Голосова автентифікація - одна з найпривабливіших технологій для ідентифікації людини, але проблеми, які існують на даний момент, слід враховувати принаймні при впровадженні в існуючий бізнес. Наприклад, розпізнавання голосу може ефективно використовуватися як додатковий метод, наприклад, для розпізнавання обличчя[21]. Основною відмінністю голосових систем автентифікації є практично повна відсутність необхідності використання спеціалізованого

обладнання для отримання біометрії. В більшості випадків, в таких системах можуть використовуватися стандартні мікрофони, які використовуються в смартфонах, гарнітурах для ПК, ноутбуках або планшетах. Проте, в даний час технологія потребує суттєвого вдосконалення, оскільки підробити мовні характеристики людини доволі просто, використовуючи спеціалізовані нейронні мережі. Крім того, голосова автентифікація може бути легко скомпрометована використанням пристроїв аудіофіксації для запису ключ-фрази при проходженні автентифікації авторизованим користувачем з подальшим використанням такого запису зловмисниками.

2.2 Переваги та недоліки методів біометричної автентифікації

Для оцінки якості роботи будь-якої біометричної системи існують характеристики, за допомогою яких можна отримати кількісні показники, що визначають надійність даних систем.

Основними характеристиками при оцінці надійності біометричних системи прийнято вважати ймовірність помилок першого та другого роду. Вони позначаються як FRR (False Rejection Rate) та FAR (False Acceptance Rate) відповідно[22]. Зауважимо, що помилки першого роду (FRR) мають менш тяжкі наслідки (вимагають повторної автентифікації користувача) ніж помилки другого роду (FAR), які спричиняють отримання порушником доступу до зони, що охороняється.

При порівнянні біометричних систем, більш надійною вважають ту, що має менше значення FRR при ідентичних значеннях FAR. В деяких випадках також використовують значення характеристики EER (Equal Error Rate), при якому графіки ймовірностей FRR та FAR мають однакове значення (Рис.2.5).

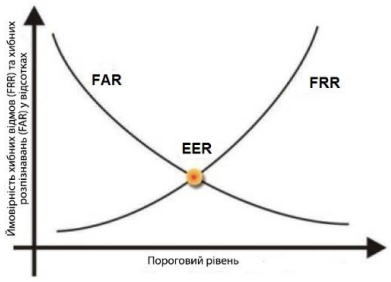

Рисунок 2.5 - Знаходження Equal Error Rate

Виходячи з цього, більш надійною вважають таку біометричну систему, в якій значення FRR менше при ідентичних значеннях FAR. В даній роботі розглядаються лише методи автентифікації за такими біометричними характеристиками людини, які доцільно використовувати в сучасних СККД (як правило, це статичні характеристики)[23]. Для прикладу, сканування ДНК людини, незважаючи на високі показники надійності, має досить низьку швидкодію(близько 90 хвилин на автентифікацію одного користувача), що унеможливлює використання цього методу в системах контролю та керування доступом в системах, де є значний обсяг користувачів.

Порівняння методів біометричної автентифікації за наступними характеристиками:

- ймовірність хибного допуску (FAR);
- ймовірність хибної відмови (FRR);
- швидкість автентифікації;
- можливість використання суворої автентифікації;
- сталість ідентифікатора (зміна характеристики залежно від часу або хвороб);
- стійкість до фальсифікації (підроблення) характеристики;
- складність автентифікації (необхідність спеціалізованих умов або обладнання для успішного отримання ідентифікатора під час сканування)
- вартість реалізації,

наведено в таблиці 2.1.

Виходячи з проведеного аналізу, найкращим рішенням для мультимодальної автентифікації за двома факторами є методи автентифікації за відбитком пальця та за 3D-моделлю обличчя. Таке поєднання значно зменшує ймовірність помилок другого роду при незначному збільшенні помилок першого роду при проходженні автентифікації одразу за двома характеристиками. Вартість системи при цьому зростає в незначному розмірі порівняно з використанням більш громіздких та вартісних методів автентифікації (наприклад, райдужна оболонка ока) при збереженні того ж рівня надійності.

$$FAR_{Мультимод} = FAR_{Відбитку} * FAR_{Обличчя} = 0{,}000001 \quad (2.1)$$

$$FRR_{Мультимод} = FRR_{Відбитку} + FRR_{Обличчя} = 0{,}156 \quad (2.2)$$

Таблиця 2.1 – Порівняльний аналіз характеристик методів біометричної автентифікації

Метод автентифікації	**FAR**	**FRR**	**Швидкість автентифікації**	**Сувора автентифікація**	**Сталість ідентифікатора**	**Стійкість до підробки**	**Складність автентифікації**	**Вартість реалізації**
За відбитком пальця	0.001	0.063	Висока	Так	Висока	Середня	Середня	Низька
За голосом	0.001	0.24	Висока	Ні	Низька	Низька	Низька	Низька
За сітківкою ока	0.001	0.04	Середня	Так	Висока	Дуже висока	Середня	Висока
За райдужною оболонкою	0.001	0.04	Середня	Так	Висока	Висока	Висока	Висока
За обличчям (3D)	0.001	0.093	Висока	Ні	Середня	Висока	Низька	Низька

За ДНК	0	0	Дуже низька	Так	Дуже висока	Низька	Висока	Дуже висока
За рисунком вен	0.001	0.008	Висока	Ні	Висока	Дуже висока	Висока	Середня

Висновки за розділом 2

Узагальнивши результати, отримані під час розгляду методів біометричної автентифікації користувача в СККД, можна підвести підсумок що поєднання методів автентифікації за відбитком пальця та 3D-моделлю обличчя дасть змогу суттєво підвищити надійність такої системи контролю доступу та не спричинить суттєвого підвищення її вартості чи швидкості проходження автентифікації користувача.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ

3.1. Розробка вимог та архітектури СККД

Система контролю та управління доступом призначена для забезпечення безпеки об'єкта, що охороняється, та запобігання несанкціонованого доступу.

СККД може бути як набором автономних елементів, призначених для вирішення простих завдань безпеки, так і інтегрованою системою, що відповідає конкретним вимогам[24].

У процесі проектування СККД необхідно:

- визначити тип завдань, які потрібно вирішити;
- вибирати склад системних елементів, що дозволяє найбільш ефективно вирішувати поставлені завдання;
- вибирати спеціалізоване програмне забезпечення, яке забезпечує можливість запису робочого часу тощо;
- для підвищення ефективності СККД можна поєднувати із системою відеоспостереження та пожежною сигналізацією[25].

В залежності від сфери діяльності, на підприємствах доступ до певних приміщень може бути дозволений лише уповноваженому персоналу. Наприклад, дослідницькі компанії обмежують доступ до лабораторій, щоб ніхто не порушував хід експериментів і не отримав дані про їх результати. Доступ до серверних кімнат та комунікаційних шаф надається лише відповідному IT-персоналу, щоб уникнути помилок та спроб саботажу. Фінансові установи обмежують доступ до цінностей та кас, тощо.

Для розмежування рівнів доступу персоналу, будівлю компанії слід розділити на зони залежно від критичності діяльності, що проводиться в кожній з них. Вестибюль можна розглядати як громадське місце, приміщення, в якому

здійснюється розробка програмного забезпечення, можна вважати повністю таємним, а офіси керівництва – таємним[26]. Використовувана класифікація не настільки важлива, важливо розуміти, що деякі приміщення можуть бути більш критичними, ніж інші, і що приміщення (зони) потребують різних механізмів контролю доступу, виходячи з вимог до рівня захисту. Окремі приміщення (зони) можуть вимагати використання спеціальних матеріалів та / або обладнання, що перешкоджають витоку інформації через технічні канали.

Виходячи з вищевказаного, був сформований набір вимог до СККД, що розробляється:

1. Контроль і управління доступом:
   - ідентифікація користувачів, що отримують доступ;
   - доступ тільки зареєстрованих співробітників і відвідувачів;
   - управління виконавчими пристроями (дверима, турнікетами, шлагбаумами);
   - формування сигналу тривоги при спробі несанкціонованого доступу;
   - ведення журналу подій;
   - розмежування доступу по часових зонах.
2. Облік робочого часу співробітників:
   - автоматизований облік часу приходу і відходу співробітників;
   - ведення табеля робочого часу;
   - створення звітів про наявність або відсутність співробітника на робочому місці, про запізнення і ранні відходи;
   - створення і ведення бази даних співробітників (електронна картотека);
   - імпорт даних в програму Microsoft Excel і ін.
3. Забезпечення безпеки приміщень - інтеграція з існуючими системами контролю доступу і охоронної сигналізації.

3.1.1 Архітектура комп'ютерної системи контролю доступу до захищених об'єктів

Розробка архітектури є невід’ємною частиною фази проектування системи. Усі дані розробленої СККД (дані про всі проходи через пропускні пункти - час, дата, повне ім’я та посаду користувача) повинні зберігатися в одному місці, тобто в одній базі даних, яка захищена від несанкціонованого доступу сторонніх осіб[27].

Виходячи з аналізу та порівняння сучасних методів автентифікації, в системі, що розробляється, було вирішено використовувати мультимодальну автентифікацію за відбитком пальця та геометрією обличчя, оскільки вартість побудови системи на основі цих методів значно нижча, ніж при використанні будь-якого іншого методу біометричної ідентифікації з аналогічними показниками надійності. Також визначені методи біометричної автентифікації не потребують особливих зовнішніх умов для роботи системи(наприклад, низький рівень освітлення тощо).

3.2 Аналіз елементної бази та розробка апаратної підсистеми

В якості апаратної підсистеми використовуються пристрої контролю та керування доступом. До них відносяться: зчитувачі (дактилоскопічний сканер, сканер обличчя), елемент управління (контролер) та виконавчі пристрої (електричні замки, дверні доводчики, датчики безпеки). Необхідно також вибрати найбільш підходящий інтерфейс передачі даних між зчитувачем і контролером[27]. Комбінована взаємодія цих апаратних засобів фактично забезпечує контроль доступу.

3.2.1 Вибір параметрів обладнання

Внаслідок проведеного аналізу існуючих рішень на світовому ринку, було обрано наступні елементи СККД для використання в розроблюваній системі:

1. Зчитувач відбитків пальців

Для використання в СККД серед наявних рішень було обрано сканер відбитків пальців фірми Zkteco RS-485 FR1500 (рис. 3.1).

Рис. 3.1 - Сканер відбитків пальців Zkteco FR1500

Застосування:

Призначений для роботи з мережевими та автономними системами безпеки для контролю та доступу, а також із системами оплати та лояльності. На офіційному сайті виробника розміщено посібник з використання та додаткове програмне забезпечення, що дозволяє швидко освоїти роботу з продуктом. Технічні характеристики зчитувача наведені в таблиці 3.1.

Табл. 3.1 - Технічні характеристики зчитувача

Напруга живлення	12 В
Споживана потужність (макс.)	0.72 Вт
Робоча температура	-10 °C ~ +45 °C
Розміри	121.3x77.3x38 мм
Максимальна довжина сполучного кабелю	10 м
Тип підключення до контролера	RS-485
Час сканування	0.3 с
Додатково	Можливість підключення

	зчитувача RFID-карт (в комплект не входить)

2. Турнікет

За результатами дослідження було прийнято рішення використовувати в системі контролю та керування доступом турнікет моделі T83M (рис. 3.2). Технічні характеристики даного контролера наведені в таблиці 3.2.

Рис. 3.2 - Турнікет T83M

Табл. 3.2 - Технічні характеристики турнікета

Напруга живлення	12 В
Пропускна спроможність	30 чол/хв
Робоча температура	-0°C ~ +50°C
Ресурс використання	2 000 000 проходів
Світлова індикація	Наявна (зелений, червоний)
Вид стопора	Електромагнітний замок
Макс. число подій	100 000

Макс. кількість контролерів доступу	6 шт
Тип підключення до комп’ютера	RS-485
Типи виконавчих пристроїв	Турнікети, електромагнітні замки

3. Пристрій блокування дверей

Для забезпечення блокування дверей за відсутності проходів через неї та можливості її автоматичного відмикання при дозволі проходу використовуються електричні керовані замки та засувки, які поділяються на дві основні категорії:

- електромеханічні;

- електромагнітні.

Основна відмінність цих інструментів полягає в тому, що в електромеханічних замках застосовуються в основному ті ж принципи, що і в звичайному механічному замку, тільки ригелем можна керувати або механічно (за допомогою ключа, як правило), або за допомогою електричного струму. В електромагнітному замку дверцята утримуються шляхом підтягування сталевої пластини (якоря), розміщеної на дверях, до електричного магніту (самого замка), встановленого на коробці, завдяки утвореному магнітному полю.

Для використання в системі контролю доступу було прийнято рішення використовувати електромеханічний замок EL480 (рис. 3.3). Технічні характеристики замка наведені в таблиці 3.3.

Рис. 3.3 - Електромеханічний замок EL480

Табл. 3.3 - Технічні характеристики турнікета

Індикація	- положення поперечини - положення ручки (натиснута - не натиснута)
Робоча напруга	12 або 24 В постійного струму (-10% - + 15%)
Робочий струм	- струм роботи 0,35 А - струм очікування 0,12 А (12 В) або 0,07 А (24 В)
Температурний діапазон	-20 ° С ... + 60 ° С
Вихід ригеля	14 мм
Шпиндель замка	8 мм
Покриття	хромування
Комплект поставки	електромеханічний замок, контактні муфти, кріпильні гвинти, інструкція по монтажу та підключення, схема електропроводки замка

Врізний електромеханічний замок моделі EL480 фінської компанії ABLOY відноситься до групи замків соленоїдного типу і призначений для установки на

вузькі профільні двері. На відміну від інших замків ABLOY, цей електромеханічний замок має незалежні зовнішні та внутрішні ручки, може працювати в режимах «нормально відкритий» та «нормально закритий», має світлу індикацію стану та встановлюється як на правобічні, так і на лівобічні двері[28]. При роботі під керуванням контролера СККД або кнопки виходу електромеханічний замок блокує / відмикає лише зовнішню ручку, а замок завжди можна відкрити або ключем, або внутрішньою ручкою.

Експерти ABLOY рекомендують використовувати електромеханічний замок EL480 як виконавчий пристрій для системи контролю та керування доступом для внутрішніх профільних дверей офісів, торгових приміщень, громадських або адміністративних будівель, складів, офісних приміщень банків тощо. Замок EL480 можна встановити на аварійні вихідні двері та на протипожежні двері. При необхідності електромеханічний замок можна налаштувати на відкривання в будь-який час за допомогою ключа або внутрішньої ручки.

При роботі EL480 в системах контролю та керування доступом, контролер СККД блокує або відмикає зовнішню ручку електромеханічного блокування, вимикаючи або подаючи живлення на замок. У режимі очікування електромеханічний замок знаходиться в заблокованому стані («нормально закритий»), його зовнішня ручка заблокована і напруга не подається на замок. Якщо на контролер з зчитувача поступає біометричний ідентифікатор співробітника, та він визнається таким, що має допуск до даної зони, контролер подає напругу в електромеханічний замок, зовнішня ручка блокування відмикається, і двері можна відкрити ззовні. В цьому випадку електромеханічний замок завжди можна відкрити зсередини за допомогою внутрішньої ручки.

Залежно від конфігурації системи контролю доступу, електромеханічним замком можна керувати не тільки контролером, але і зчитувачем, таймером, кнопкою виходу та іншими пристроями..

На відміну від інших замків електромагнітного типу ABLOY, електромеханічний замок EL480 має окремі шпинделі оригінальної конструкції, так що ручки замка можуть рухатись незалежно одна від одної. Крім того, EL480 є

універсальним: його можна налаштувати для роботи як правосторонніх, так і лівосторонніх дверей, перевести в режим «нормально відкритий» або «нормально закритий», змінюючи напрямок соленоїда, а також використовувати джерело постійної напруги 12 або 24 вольт для живлення.

4. Контролер

За результатами дослідження, оптимальним рішенням для використання в системі контролю та керування доступом було визначено контролер TSS-207-4W (рис. 3.4).

Контролери керування доступом серії TSS-207 можуть функціонувати у складі програмно-апаратного комплексу (під керуванням комп'ютера), в автономному (без зв'язку з комп'ютером) та напівавтономному режимі (при односторонній передачі даних від контролера до комп'ютера).

Рис. 3.4 - Контролер TSS-207-4W

Обмеження доступу, включаючи задані часові інтервали заборони доступу, враховуються при керуванні доступом як у комплексному, так і в автономному та напівавтономному режимі.

Обмеження доступу, включаючи тимчасові інтервали заборони доступу, враховуються при керуванні доступом як в комплексному, так і в автономному режимі.

У контролерів даної серії є вбудована Flash-пам'ять, в яку за допомогою комп'ютера можна завантажувати різні програми функціонування контролера в автономному режимі для реалізації на апаратному рівні необхідних алгоритмів керування доступом (наприклад, заборони повторного проходу, організації шлюзу тощо).

Крім цього, кожен із контролерів серії TSS-207 має:

• До 3 додаткових входів для підключення датчиків із виходом типу "сухий контакт".

• Індикатори режиму функціонування ("Режим"), стану електроживлення ("220 В", "12 В", "Розряд акумулятора") та рівня заповнення пам'яті подій (75% та 88%).

• Звуковий індикатор (біпер).

• Металевий корпус із блоком живлення від мережі ~220 В (50 Гц) та резервним акумулятором 7 А*год.

• Датчик відкриття кришки корпусу.

Детальні технічні характеристики даного контролера наведені в таблиці 3.4.

Таблиця 3.4 - Технічні характеристики контролера

Напруга живлення	220 В
Час роботи від акумулятора	12 год
Споживана потужність (макс.)	40 Вт
Робоча температура	-10°С ~ +55°С
Розміри	300x350x165 мм
Максимальна довжина сполучного кабелю	1000 м
Макс. кількість користувачів	65 000
Макс. число подій	100 000
Макс. кількість контролерів доступу	6 шт
Тип підключення до комп’ютера	RS-485
Типи виконавчих пристроїв	Турнікети, електромагнітні замки

5. Лицьова біометрія

В якості сканера біометрії обличчя користувачів було обрано термінал біометричного доступу Hikvision DS-K1T341AM (рис. 3.5).

Рис. 3.5 - Термінал біометричного доступу Hikvision DS-K1T341AM

Термінал Hikvision DS-K1T341AM працює на алгоритмі глибокого навчання, підтримує детекцію справжності біометричних даних особи. До терміналу можна підключити один зовнішній зчитувач карток через інтерфейс RS-485, а також додатковий контролер або зчитувач за протоколом Wiegand. Також можна підключити пристрій до контролера, який блокує двері при руйнуванні чи спробі зламутерміналу, обмежуючи доступ до приміщення, яке охороняється. Для зручного використання терміналу є голосові підказки. Передача даних здійснюється через підключення Ethernet. Для конфігурації використовується програма Hik-Connect, за його допомогою можна не тільки налаштовувати пристрій, але у віддаленому режимі відчиняти двері та переглядати відео. Технічні характеристики терміналу наведені в таблиці 3.5.

Таблиця 3.5 - Технічні характеристики біометричного терміналу

Напруга живлення	12 В (можливість живлення PoE)
Робоча температура	-30°C ~ +60°C
Час розпізнавання	0.2 с

Дистанція сканування	0.5 - 1.5 м
Розміри	172.5x83.2x22.7 мм
Максимальна довжина сполучного кабелю	100 м
Тип підключення до контролера, комп’ютера	Ethernet, RS-485, USB, Wiegand 34
Макс. кількість користувачів	1500
Макс. число подій	150 000
Додатково	Можливість підключення зчитувача RFID-карт

3.3 Система контролю та керування доступом

До складу СКУД входять точки контролю доступу (ТКД) двох типів:

1. Двері з одностороннім контролем - в приміщенні будівлі.
2. Турнікети на вході в будівлю.

Точка контролю доступу функціонально складається з контролера доступу виконавчого механізму (турнікет, електричний замок), зчитувачів, датчиків положення пристрою, що перегороджує, пультів (кнопок) управління виконавчим механізмом. До складу ТКД входить джерело резервованого живлення для підтримки працездатності пристроїв при тимчасовій пропажі напруги живлячої мережі. Прохід через точки з контролем доступу здійснюється при спів паданні шаблону з запропонованим відбитком. У разі успішної виконавчий пристрій розблоковується дозволяючи прохід.

Керування системою і моніторинг за її роботою здійснюється з сервера системи, контроль здійснює адміністратор. Він з допомогою настільного сканера заносить ілентифікатори співробітника чи відвідувача в базу системи доступу та назначає для кожного права доступу. Дані з шаблонами та правами призначеними для їх власників передаються в пам’ять контролера. Контролери доступу

підключаються до сервера за допомогою перетворювача інтерфейсів USB ~ Rs-485. Всі дані фіксуються в протоколі подій, який надалі дозволяє відновити картину що відбулася. Окрім подій системи на сервері розташовується база даних персоналу і конфігурації системи.

Живлення СКУД здійснюється від мережі змінної напруги 220 В. Захист кабелю здійснюється автоматичними вимикачами. Розрахунок струмів споживання системи контролю і управління доступом. При відключенні централізованого електропостачання вбудовані в контролери джерела безперебійного живлення забезпечують нормальну роботу системи.

3.3.1 Принципова схема системи

Система контролю та керування доступом - це комбінація апаратного та програмного забезпечення, призначеного для автоматизованого контролю доступу до окремих ділянок об’єкта[29]. Зазвичай СККД використовуються як один із компонентів інтегрованої системи безпеки. Найпоширеніша інтеграція - з охоронною сигналізацією.

Принцип роботи даної СККД простий: на вході на підприємство або в будь-яке інше приміщення, що підлягає контролю, встановлюються зчитувачі - спеціальні пристрої, які розпізнають відбитки пальців та обличчя користувача і передають їх в систему для перевірки за наступною схемою:

1. Контролер опитує периферійні пристрої та фіксує натискання кнопок виходу та активацію зчитувачів.

2. Якщо була натиснута кнопка виходу з приміщення, контролер подає сигнал на відкриття дверей до відповідного приміщення, супроводжуючи це світлодіодною індикацією зеленого кольору.

3. Якщо зчитувач був активований прикладанням пальця, він створює шаблон прикладеного відбитка, переводить його у вигляд хеш-функції та надсилає до контролеру, який порівнює представлений відбиток з наявними в базі даних.

Паралельно цим діям активується термінал розпізнавання обличчя, який сканує обличчя співробітника, порівнює з наявними у базі даних. На основі порівняння та перевірки чи належать модель обличчя та відбиток пальця одній і тій самій особі, контролер приймає рішення про допуск або відмову в допуску та зберігає відомості про спробу проходження через ПТ в СУБД. Якщо прийнято рішення про допуск користувача в захищену зону контролер подає сигнал на відкриття дверей до відповідного приміщення, супроводжуючи це світлодіодною індикацією зеленого кольору. В разі відмови в допуску контролер вмикає світлодіодну індикацію червоного кольору та залишає прохід закритим. Окрім того система контролю доступу запам'ятовує невдалі спроби входу та після третьої поспіль надсилає сигнал на пункт охорони. Структурна схема СККД зображена на рисунку 3.6.

Окрім того, зчитувач під’єднано до системи з вмонтованим в лінію живлення герконом, який розмикає електричний ланцюг живлення при відкриванні дверей, внаслідок чого зчитувач від’єднується від системи. Якщо двері біли відчинені без проходження біометричної автентифікації (злам) контролер надсилає сигнал на пункт охорони на вмикає сигналізацію. Окрім того, така схема підключення дозволяє фіксувати фактичний часовий період відкриття дверей для звітності.

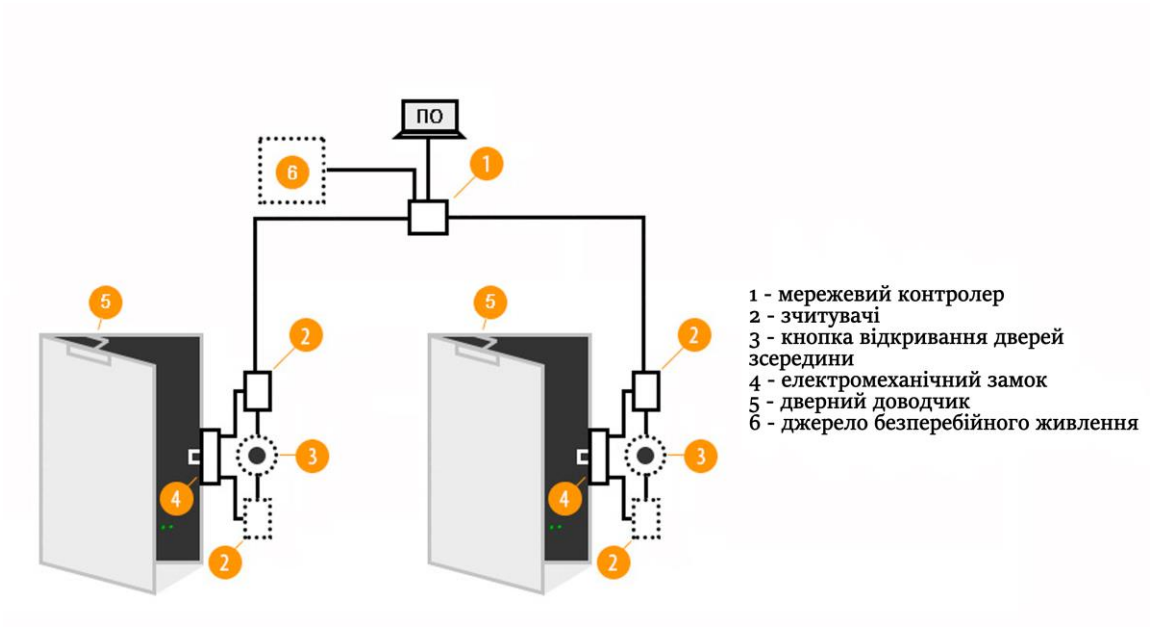

Рис. 3.6 - Структурна схема розробленої СККД

3.4 Порівняльний аналіз

Приведено порівняння окремо кожного з методів біометричної автентифікації та дослідженого мультимодального методу за основними критеріями[30]. Результати порівняння наведено в таблиці 3.6.

Таблиця 3.6 - Порівняльний аналіз

Критерій	**Відбиток пальця**	**Обличчя**	**Відбиток пальця + обличчя**
Швидкість автентифікації	Висока	Висока	Висока
Сувора автентифікація	Так	Ні	Так
Стійкість до підробки	Середня	Висока	Висока
Складність автентифікації	Середня	Низька	Низька
Вартість реалізації	Низька	Низька	Низька
FAR	0.001	0.001	0.000001
FRR	0.063	0.093	0,156

3.5 Висновки за розділом 3

Спроектована система вирізняється високою надійністю та доволі низькою вартістю, що випливає з наведеного вище порівняння. Також можна відзначити автономність та можливість зручного масштабування та інтеграції розробленої системи з існуючими протипожежними- та системами виявлення вторгнень (охоронними сигналізаціями).

ВИСНОВКИ

В результаті виконання дипломної роботи було спроектовано систему контролю та керування доступом на основі мультимодальної біометричної автентифікації, яка поєднує в собі методи автентифікації за відбитком пальця та моделлю обличчя особи.

При виконанні даної роботи було виконано ряд завдань, які є необхідними при проектуванні системи, а саме:

1) Проведено аналіз сучасного ринку контролю доступу.
2) Визначено критерії захищеності системи.
3) Досліджено технології створення біометричних систем контролю доступу.
4) Досліджено ефективність впровадження системи.
5) Досліджено біометричні методи.

Для досягнення мети роботи було проведено аналіз подібних існуючих комп'ютерних систем контролю доступу та методів біометричної ідентифікації. Здійснено розробку схеми структурного пристрою, алгоритму роботи СККД на основі автентифікації за відбитком пальця.

Результатом проектування є архітектура розробленої системи та структурна схема пристрою контролю та керування доступом.

Вищезгадана система володіє рядом переваг для встановлення на підприємстві, а саме:

- висока надійність;
- низька вартість компонентів системи;
- автономність – можливість роботи при відсутності зв’язку з центральним комп’ютером в режимі входу-виходу з фіксацією подій;
- легке та зручне масштабування та інтеграція з охоронними та протипожежними системами.

Підводячи підсумки можна сказати, що у системах, які вимагають особливих вимог до безпеки, треба використовувати мультимодальні методи біометричної

ідентифікації. Використання біометричних засобів спрощує процедуру ідентифікації особи, а також підвищує надійність систем безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болл Р.М. Руководство по биометрии: пер. с англ. Н.Е. Агаповой. – М.: Техносфера, 2007. – 368 с.

2. Распознавание личности по голосу: аналитический обзор / В.Н. Сорокин, В.В. Вьюгин, А.А. Тананыкин // Информационные процессы. – 2012. – Том 12, №1. – С. 1-30. Режим доступу: http://www.jip.ru/2012/1-30-2012.pdf.

3. Традиционные методы биометрической аутентификации и идентификации / В.М. Колешко, Е.А. Воробей, П.М. Азизов, А.А. Худницкий, С.А. Снигерев. – Минск: БНТУ, 2009. 107 с.

4. Швець В. А. Основні біометричні характеристики, січасні системи та технології біометричної аутентифікації / В. А. Швець, А. О. Фесенко. // Ukrainian Scientific Journal of Information Security. – 2013. – №19. – С. 99–110.

5. Лисенко А. М. Застосування біометричних систем для ідентифікації особи / А. М. Лисенко, О. С. Мельник. // Юридичні науки. Вісник Київського національного університету імені Тараса Шевченка. – 2004. – №60/62. – С. 87–91.

6. Лысак А.Б. Идентификация и аутентификация личности: обзор основных биометрических методов проверки подлинности пользователя компьютерных систем // Математические структуры и моделирование. – 2012. – № 26. – С. 124-134.

7. Кумченко Ю. О. Аналіз існуючих підходів біометричної ідентифікації та аутентифікації людини / Ю. О. Кумченко, А. І. Купін // Системні технології. Регіональний міжвузівський збірник наукових праць. – Дніпропетровськ, 2013. – Вип. 4 (87). – С. 129–134.

8. Das M. L. Two-factor user authentication in wireless sensor networks //IEEE transactions on wireless communications. – 2009. – Т. 8. – №. 3. – С. 1086-1090.

9. ISO/IEC JTC 1/SC 37 [Електронний ресурс]. – Режим доступу: https://www.iso.org/committee/313770.html

10. Задорожный В. В. Идентификация по отпечаткам пальцев / В. В. Задорожный. // PC Magazine. – 2004. – №1.

11. Задорожный В. В. Идентификация по отпечаткам пальцев / В. В. Задорожный. // PC Magazine. – 2004. – №2.

12. Гуреева О. Биометрическая идентификация по отпечаткам пальцев. Технология FingerChip / Ольга Гуреева. // Компоненты и технологии. – 2007. – №4. – С. 176–180.

13. Биометрическая идентификация по рисунку вен ладони [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://habrahabr.ru/post/149424/.

14. Тихонов І. А. Інформативні параметри біометричної аутентифікації користувачів інформаційних систем по інфрачервоному зображенню судинного русла / І. А. Тихонов. // Біомедична техніка і радіоелектроніка. – 2010. – №9. – С. 26–32.

15. P. Viola and M.J. Jones, «Robust real-time face detection», International Journal of Computer Vision, vol. 57, no. 2, 2004., pp.137–154.

16. Сабанов А. Г. Обзор технологий идентификации и аутентификации / А. Г. Сабанов. // Документальная электросвязь. – 2006. – №17. – С. 23–27.

17. Daugman J. Recognizing Persons by Their Iris Patterns / Daugman // Biometrics: Personal Identification in Networked Society / Daugman. – Amsterdam: Kluwer, 1998. – С. 103–121.

18. Перепечина И. О. Проблема категорического экспертного вывода в судебной ДНК-идентификации и разработка подхода к его решению [Електронний ресурс] / И. О. Перепечина – Режим доступу до ресурсу: http://www.k-press.ru/bh/2003/2/perepechina/ perepechina.asp.

19. Tran D. A Fuzzy approach to Statistical Models in Speech and Speaker Recognition / D. Tran, M. Wagner, T. Zheng. // IEEE International Fuzzy Systems Conference Proceedings, Korea. – 1999. – С. 1275–1280.

20. Сабанов А. Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии / А. Г. Сабанов. // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – №2. – С. 180–184.

21. Газин А. И. Особенности голосовой аутентификации личности [Електронний ресурс] / А. И. Газин. – 2010. – Режим доступу до ресурсу: cyberleninka.ru/article/n/osobennosti-golosovoy-autentifikatsii-lichnosti.pdf.

22. Системи контролю доступу [Електронний ресурс]. – Режим доступу до ресурсу: http://www.npblog.com.ua/.

23. Прудник А. М. Биометрические методы защиты информации / А. М. Прудник, Г. А. Власова, Я. В. Рощупкин, 2014. – 123 с.

24. Крахмалев А. К. Средства и системы контроля и управления доступом. Учебное пособие / А. К. Крахмалев., 2003.

25. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 2 / Д. В.Голев, О. Ю. Русляченко, Ю. В. Бєлова, Д. С. Гончарук // Комплекси технічного захисту інформації. Навчальний посібник / Д. В.Голев, О. Ю. Русляченко, Ю. В. Бєлова, Д. С. Гончарук. – Одеса, 2010. – С. 184.

26. Тарасов Ю. Контрольно-пропускной режим на предприятии. Защита информации / Ю. Тарасов. // Конфидент. – 2002. – №1.

27. ГОСТ 51241-2008 “Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний”.

28. Datasheet ABLOY EL480 EL482 [Електронний ресурс] – Режим доступу до ресурсу: https://aspirl.ie/pdf/EL480_EL482_manual.pdf.

29. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков, 2001.

30. Горлицин И. Контроль и управление доступом - просто и надежно / И. Горлицин., 2002.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Тези наукових доповідей

1. Кубик В. О. Розробка системи управління доступом на основі біометричних технологій / В. О. Кубик, Н. В. Лукова-Чуйко. // ІІІ Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS), збірник матеріалів доповідей та тез. – 2020. – №3. – С. 227–229.

2. Кубик В. О. Багатофакторна автентифікація з застосуванням біометрії як метод захисту об’єктів критичної інфраструктури / В. О. Кубик, С. В. Толюпа // Міжнародна науково-практична конференція "Прикладні системи та технології в інформаційному суспільстві" / В. О. Кубик, С. В. Толюпа. – Київ, 2021.