МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри ЗЗІ
_____ В.В. Козловський
«____»_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ
«БАКАЛАВР»

Тема: Біометричні методи аутентифікації та ідентифікації осіб

Автор: В.А. Панасюк

Науковий керівник: д.т.н., професор В.О. Темніков

Нормоконтролер: д.т.н., професор М.О. Шутко

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітнього ступеня: «Бакалавр»

Спеціальність: 125 Кібербезпека

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»

ЗАТВЕРДЖУЮ

Завідувач кафедри ЗЗІ

_____В.В. Козловський

«___»_____2022

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Панасюка Владислава Анатолійовича

1.Тема: Біометричні методи аутентифікації та ідентифікації осіб затверджена наказом ректора від 06.05.2022 р. № 483/ст.

2. Термін виконання: з 16 травня 2022 р. по 14 червня 2022р.

3. Вихідні дані: Розробити систему ідентифікації та доступу людини з урахуванням наявності сучасного обладнання.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):

1. Сучасні методи біометричної аутентифікації та ідентифікації
2. Аналіз сучасних методів біометричної аутентифікації та ідентифікації осіб
3. Порівняльний аналіз основних методів біометричної ідентифікації
4. Побудова системи контролю доступу

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Зміст	16.05.22	Виконано
2.	Вступ	18.05.22	Виконано
3.	1. Сучасні методи біометричної аутентифікації та ідентифікації	22.05.22	Виконано
4.	2. Аналіз сучасних методів біометричної аутентифікації та ідентифікації осіб	23.05.22	Виконано
5.	3. Порівняльний аналіз основних методів біометричної ідентифікації	26.05.22	Виконано
6.	4. Побудова системи контролю доступу	30.05.22	Виконано
7.	Висновки	2.06.22	Виконано
8.	Оформлення пояснювальної записки	4.06.22	Виконано

Дипломник _____ В.А. Панасюк

(підпис, дата)

Дипломний керівник _____ В.О. Темніков

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається з: вступу, чотирьох розділів, висновків та переліку використаних джерел. Обсяг роботи складає 68 сторінок. Список використаних джерел містить 38 джерел.

Метою роботи є аналіз сучасних методів біометричної аутентифікації та ідентифікації людини. В кваліфікаційній роботі було розглянуто методи біометричної аутентифікації та ідентифікації, та порівняльний аналіз основних методів біометричної ідентифікації.

Результатом роботи є розроблена система доступу з використанням системи біометричної ідентифікації, зроблено підбір оптимальної техніки для створення даної системи.

Ключові слова: БІОМЕТРІЯ, АУТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, СИСТЕМА КОНТРОЛЮ ДОСТУПОМ, ВІДБИТОК ПАЛЬЦЯ.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

СКД – система контролю доступом

СКУД – система контролю і управління доступом

FAR – коефіцієнт помилкового пропуску

FMR - можливість, що система неправильно порівнює вхідний зразок з невідповідним шаблоном у базі даних

FRR – коефіцієнт помилкової відмови

FNMR - ймовірність того, що система помилиться у визначенні збігів між вхідним зразком та відповідним шаблоном з бази даних

ВСТУП

Кожен має унікальні фізичні ознаки, деякі з них отримані від народження такі як ДНК, відбитки пальців, геометрія руки, малюнок вен, райдужна оболонка ока. Інші придбані з часом і можуть змінюватись протягом життя — хода, інтонація голосу, підпис. Всі ці параметри не повторюються ні в кого з людей, а значить, за ними можна ідентифікувати особистість.

На цьому і побудовані біометричні технології, які допомагають розпізнавати людей за однією або декількома фізичними та поведінковими ознаками.

За допомогою спеціальних сучасних пристроїв - сканерів, сенсорів та інших зчитувачів біометричні дані записуються в спеціальну базу даних. Система запам'ятовує цю інформацію (наприклад, відбиток пальця) і перетворює на цифровий код. Потім, коли ви знову прикладаєте палець до сканера, система порівнює новий код із тим, що записала раніше. Якщо коди співпадають, вона видасть відповідь, що це дійсно ви.

1. СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ

Слово "біометрія" перекладається з грецької мови як "вимір життя". Біометричні дані - це відомості, що характеризують фізіологічні особливості людини, на основі яких можна встановити її особистість: цифрова фотографія, відбитки пальців, зображення райдужної оболонки очей та інші біометричні персональні дані. Виділяють два типи біометричних параметрів: – статичні – ґрунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній характеристиці, даній їй від народження та невід'ємній від неї (відбитки пальців, геометрія руки, райдужна оболонка ока та інше); - динамічні - ґрунтуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі будь-якої дії (динаміка відтворення підпису, хода, динаміка набору тексту, голос та інше).

Біометричні технології сьогодні активно інтегруються у фінансову сферу. Для того, щоб визначити, що це саме та особа, а не інша збирається скористатися грошима, програма аналізує відбитки пальця, порівнюється з фотографією з паспорта. Одних паролів для захисту коштів сьогодні вже недостатньо. Адже ім'я користувача та пароль можна передати іншій особі, втратити і вони можуть бути скомпрометовані. Впровадження та використання біометричних технологій у фінансовій сфері спрощує фінансові операції: покупки, грошові перекази та оплата послуг стають легкими та швидкими. Біометрія також корисна в екстрених ситуаціях.

Біометричні технології працюють, ґрунтуючись на наступних операціях:

запис або знімок – фізичний чи поведінковий зразок знімається системою, у тому числі під час процесів ідентифікації та перевірки;

виділення чи вилучення біометричного зразка – унікальні дані витягуються, обробляються і перетворюються на математичний код, і створюється шаблон;

порівняння – шаблон порівнюється з представленим під час проведення аутентифікації/ідентифікації зразком;

збіг або розбіжність - результат про збіг біометричних зразків. [1]

Розпізнавання може виконуватися у вигляді **аутентифікації (верифікації) або ідентифікації**, визначаючи особу з бази даних про людей, відомих системі (визначення того, хто це, заздалегідь не знаючи імені людини).

Аутентифікація – перевірка приналежності особі ідентифікатора, який вона пред’явила.

Біометрична аутентифікація – процес доказу й перевірки істинності заявленого користувачем імені через пред'явлення користувачем свого біометричного образа.

У системі аутентифікації, коли отримані характеристики і збережений шаблон користувача, за якого себе видає людина, збігаються, система підтверджує ідентичність. **При проведенні аутентифікації виконується тільки одне порівняння** – параметрів людини, яка проходить процедуру аутентифікації, й того користувача, за якого ця людина себе видає, тобто **здійснюється порівняння 1:1.**

Ідентифікація – перевірка наявності запропонованого ідентифікатора у переліку зареєстрованих.

Біометрична ідентифікація – процес створення моделі, яка описує сукупність біометричних образів конкретної особи в рамках заданого способу вимірювання контрольованих біометричних параметрів.

У системі ідентифікації, коли отримані характеристики і один з збережених шаблонів виявляються **майже однаковими**, система ідентифікує людину з відповідним шаблоном з певною вірогідністю (**порівняння 1:n**).

1.1. Класифікація методів аутентифікації та ідентифікації осіб

Біометричні зчитувачі - пристрої для ідентифікації за особливими біологічними або анатомічними критеріями, упізнання та надання доступу відбувається за відбитком пальця, сітківки ока, райдужною оболонкою ока, формою долоні, формою особи та інші. Біометричні технології не мають збоїв і систему практично неможливо обдурити, це гарантує найвищий рівень безпеки. Біометричний захист є одним з кращих виборів у складі біометричної системи контролю керування доступом [1].

Біометричні системи контролю зручні тим, що носії інформації завжди знаходяться при користувачах, не можуть бути вкрадені або загублені. Біометричний контроль доступу вважається більш надійним, так як ідентифікатори не можуть бути передані третій стороні або скопійовані.

Технології біометричної ідентифікації

Методи біометричної ідентифікації:

1. Статичні, засновані на фізіологічних признаках людини, присутніх з нею протягом всього життя:

Ідентифікація за відбитком пальця;

Ідентифікація за геометрією руки;

Ідентифікація за обличчям;

Ідентифікація за термограмою особи;

Ідентифікація за сітківкою ока;

Ідентифікація за райдужною оболонкою ока;

Ідентифікація за малюнком вен;

Ідентифікація на основі акустичних характеристик вуха;

2. Динамічні беруть за основу поведінку людини, а саме підсвідомих рухах в процесі повторення будь-якого звичайної дії: почерк, голос, хода.

Ідентифікація за голосом;

Ідентифікація за рукописним почерком;

Ідентифікація за клавіатурним почерком та інші.

Одним із пріоритетних видів поведінкової біометрії є манера друку на клавіатурі. При її визначенні фіксуються швидкість набору тексту, натискання на клавіші, тривалість натискання клавіші, інтервали часу між натисканнями клавіш.

Окремим біометричним фактором може бути спосіб використання миші. Крім того, поведінкова біометрія охоплює велику кількість факторів, які не пов’язані з комп’ютером – хода, особливості того, як людина піднімається по сходах.

Існують також комбіновані системи ідентифікації, які використовують декілька біометричних характеристик, щоб відповідати найсуворішим вимогам до надійності та безпеки систем контролю доступу.

2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ ОСІБ

2.1. Статичні методи біометричної аутентифікації та ідентифікації осіб

Статичні методи ідентифікації засновані на аналізі постійних фізіологічних показників людини. До цих характеристик входять:

2.1.1. Ідентифікація за відбитком пальця

Відбитки пальців — це рельєфні лінії, так звані папілярні візерунки, структура яких обумовлена рядами гребенеподібних виступів шкіри, розділених борозенками. Ці лінії утворюють складні візерунки шкіри (дуги, петлі, завитки), які мають такі властивості:

індивідуальність (різний набір папілярних ліній, що утворюють візерунок за своїм розташуванням, конфігурацією, взаємним розташуванням, унікальний в іншому малюнку);

відносна стійкість (незмінність зовнішньої структури візерунка, що виникає в період внутрішньоутробного розвитку людини і зберігається протягом усього її життя);

пружність (при поверхневому порушенні шкірного покриву папілярні лінії відновлюються в попередньому вигляді).

Існує кілька алгоритмів розпізнавання відбитків пальців. Найпоширенішим є алгоритм, заснований на підборі деталей. Як правило, в принті від 30 до 40 дрібних деталей (рис. 2.1). Кожен з них характеризується своїм положенням – координатами, типом [2].

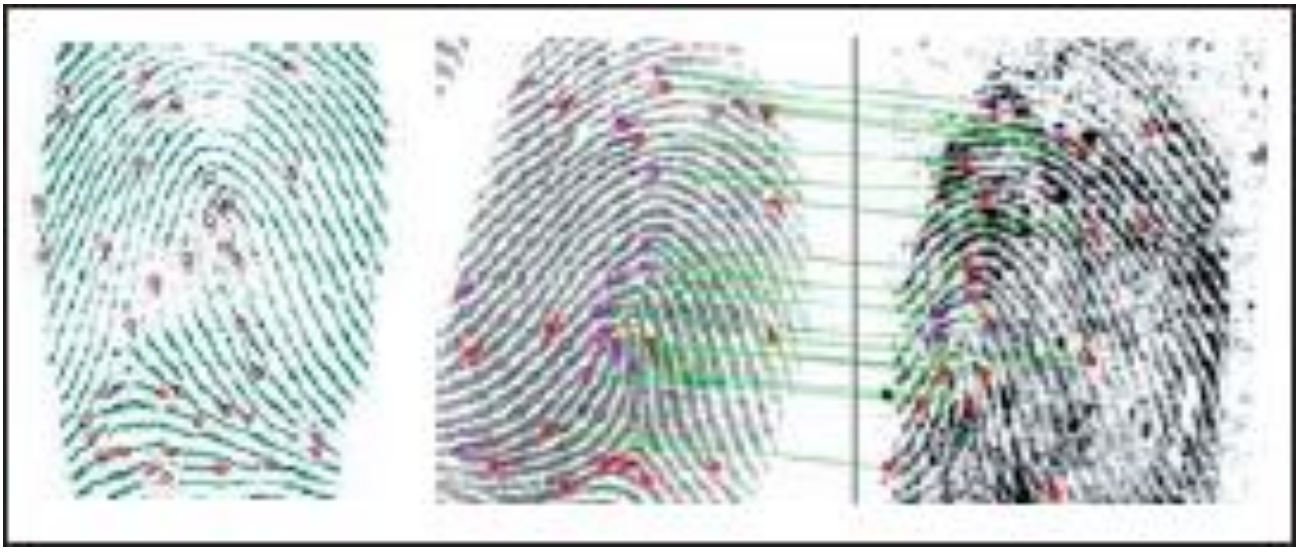

Рис.2.1. Розпізнавання відбитків пальців за виділеними деталями

З набору даних параметрів формується стандарт відбитка.

Кровоносні судини розташовані безпосередньо під епідермісом. Морфологія відбитка пальця тісно пов’язана з електричними та тепловими характеристиками шкіри. Це означає, що для отримання зображення відбитків пальців можна використовувати не тільки фарбу, а й електромагнітну енергію в різних її проявах. Зауважте, що сканування відбитків пальців з чітко окресленими папілярними лініями – завдання не з легких. Оскільки відбитки занадто дрібні, для отримання якісного зображення доводиться використовувати досить складні методи [2].

Усі існуючі електронні методи отримання відбитків пальців, залежно від фізичних принципів, що використовуються, діляться на наступні види:

оптичні;

ємнісні;

радіочастотні;

тиску;

ультразвукові;

температурні.

1) **Оптичний метод**

В даний час існує кілька різновидів сканерів, призначених для отримання відбитків пальців оптичним методом:

FTIR-сканери - це пристрої, в яких використовується ефект повного внутрішнього відображення (Frusted Total Internal Reflection). Ефект полягає в тому, що при падінні світла на межу розділу двох середовищ світлова енергія ділиться на дві частини - одна відбивається від призми, інша проникає через призму до другого середовища (рис. 2.2) [2].

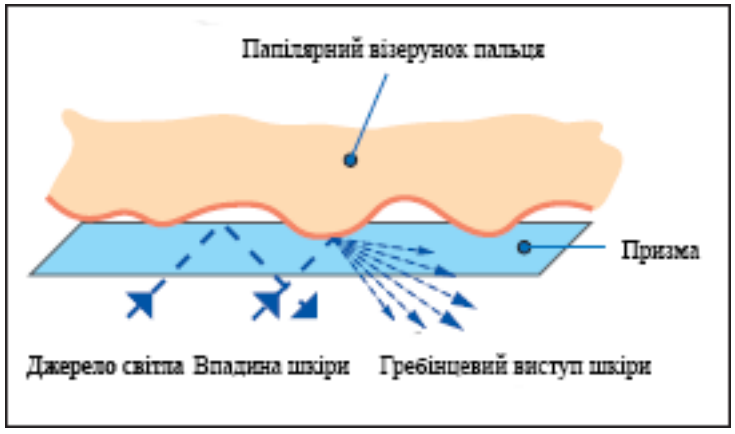

Рис. 2.2. Принцип роботи FTIR-сканерів

Оптоволоконні сканери (Fiber Optic Scanners) є оптоволоконною матрицею, в якій всі хвилеводи на виході з'єднані з фотодатчиками. Чутливість кожного датчика дозволяє фіксувати залишкове світло, що проходить через палець, у точці дотику пальця з поверхнею матриці (рис 2.3).

Зображення всього відбитка формується за даними, що зчитуються з кожного фотодатчика

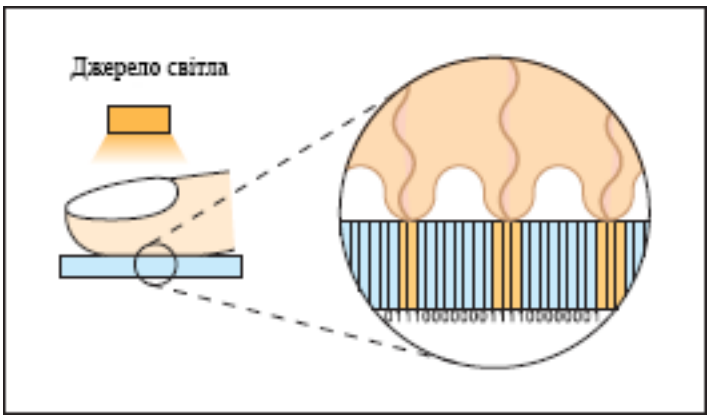

Рис. 2.3. Принцип роботи оптоволоконних сканерів

Електрооптичні сканери (Electro-Optical Scanners) - технологія заснована на використанні спеціального електрооптичного полімеру, до складу якого входить світловипромінюючий шар. Коли палець прикладається до сканера, неоднорідність електричного поля біля його поверхні (різниця потенціалів між горбками і западинами шкіри) відбивається на світінні шару. Таким чином, формується зображення відбитка пальця. Надалі датчик зображення перетворює отриману картинку на цифровий вигляд. Цей тип сканерів випускається компанією Security First Corp. [2]

Оптичні протяжні сканери (Sweep Optical Scanners) - багато в чому аналогічні FTIR-пристроям, за винятком того, що для отримання зображення відбитка палець не просто прикладається до сканера, а проводиться по тонкій смужці-зчитувачу (рис 2.4). У міру руху пальця робиться серія миттєвих фотографій. При цьому сусідні кадри знімаються з деяким накладенням, що дозволяє значно зменшити розміри призми, що використовується, і самого сканера. Для отримання результуючого зображення відбитка пальця використовується спеціалізоване програмне забезпечення. Провідним виробником сканерів цього типу є компанія Cogent Systems [2].

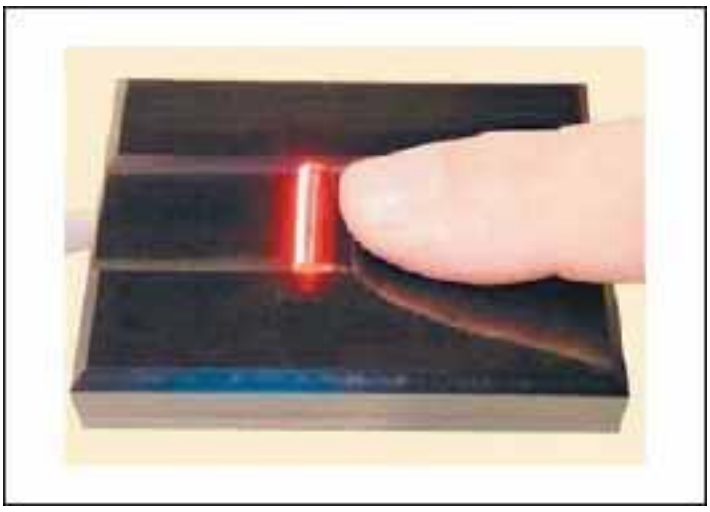

Рис. 2.4. Практична реалізація оптичного протяжного сканера

Роликові сканери (Roller Style Scanners) - дані пристрої є мініатюрними сканерами. Відбиток захоплюється при прокочуванні пальцем прозорого тонкостінного ролика (рис 2.5). Аналогічно протяжному сканеру, у міру руху пальця робляться миттєві знімки фрагментів папілярного візерунка з деяким накладанням зображення. При скануванні використовується найпростіша оптична технологія: усередині прозорого циліндра знаходяться статичне джерело світла, лінза та датчик зображення. Після повного прокручування пальця програмно збирається результуюче зображення його відбитка [2].

Рис.2.5. Принцип роботи роликового сканера

Безконтактні сканери (Touchless Scanners) – у цих пристроях палець не контактує безпосередньо з поверхнею сканера. Палець лише прикладається до отвору сканера і підсвічується знизу з різних боків декількома джерелами світла. По центру отвору розташована лінза, за допомогою якої зображення відбитка пальця проектується на КМОП-камеру (рис 2.6) [2].

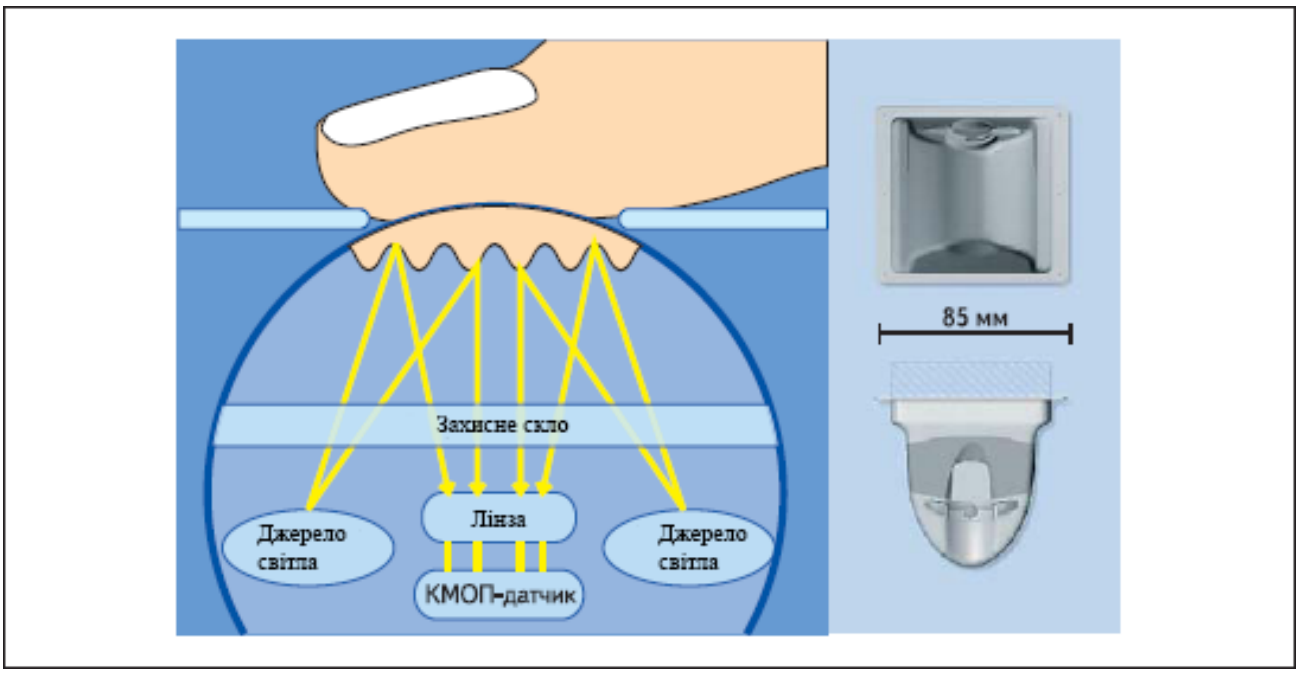

Рис. 2.6. Схема роботи безконтактного сканера та його реалізація

2) Ємнісний метод

Ємнісні сканери (Capacitive Scanners) є найбільш поширеними напівпровідниковими пристроями для отримання зображення відбитка пальця.

Їхня робота заснована на ефекті зміни ємності p-n-переходу напівпровідника при дотику гребінця папілярного візерунка з елементом напівпровідникової матриці. Існують модифікації ємнісних сканерів, у яких кожен напівпровідниковий елемент у матриці виступає у ролі однієї пластини конденсатора, а палець – у ролі іншої. При додатку пальця до датчика між кожним чутливим елементом та виступом-впадиною папілярного візерунка утворюється ємність, величина якої визначається відстанню між рельєфною поверхнею пальця та елементом. Матриця цих ємностей перетворюється на зображення відбитка пальця. Провідними виробниками сканерів цього типу є компанії Infineon, STMicroelectronics, Veridicom [2].

Нестача ємнісного методу — той самий неефективний захист від муляжів.

3) Радіочастотний метод

Радіочастотні сканери (RF-Field Scanners) — у таких сканерах використовується матриця елементів, кожен із яких працює як мініатюрна антена.

Радіочастотний модуль генерує сигнал низької інтенсивності та спрямовує його на скановану поверхню пальця. Кожен із чутливих елементів матриці приймає відбитий від папілярного візерунка сигнал. Величина наведеної в кожній мініатюрній антені EPC залежить від наявності або відсутності поблизу неї гребня папілярного візерунка. Отримана таким чином матриця напруги перетворюється на цифрове зображення відбитка пальця. Оскільки метод ґрунтується на фізіологічних властивостях шкіри, його важко обдурити імітацією пальця. До недоліків методу належить необхідність якісного контакту пальця та передавача, який може бути дуже гарячим. Відомим виробником радіочастотних сканерів є компанія Authentec [2].

4) Натискний метод (тиск)

Чутливі до тиску сканери (Pressure Scanners) у своїй конструкції використовують матрицю п'єзоелектричних елементів, чутливих до натискання.

При прикладанні пальця до скануючої поверхні гребінцеві виступи папілярного візерунка чинять тиск на деяку підмножину елементів матриці.

Впадини шкірного візерунка ніякого тиску не надають. Таким чином, сукупність отриманих з п'єзоелектричних елементів напруг перетворюється на зображення відбитка пальця. Цей метод має ряд недоліків:

• низька чутливість;

• неефективний захист від муляжів;

• схильність до пошкоджень при надмірно докладених зусиллях.

Чутливі до тиску сканери випускає компанія BMF. [2]

5) Ультразвуковий метод

Ультразвукові сканери (Ultrasonic Scanners) сканують поверхню пальця ультразвуковими хвилями. Відстані між джерелом хвиль і гребінцевими виступами та западинами папілярного візерунка вимірюються по відбитому від них відлуння (рис 2.7). Якість одержуваного зображення в десятки разів краще, ніж будь-якого іншого представленого на біометричному ринку методу. Крім того, даний спосіб практично повністю захищений від муляжів, оскільки дозволяє окрім відбитка папілярного візерунка пальця отримувати інформацію про деякі інші характеристики (наприклад, про пульс) [2].

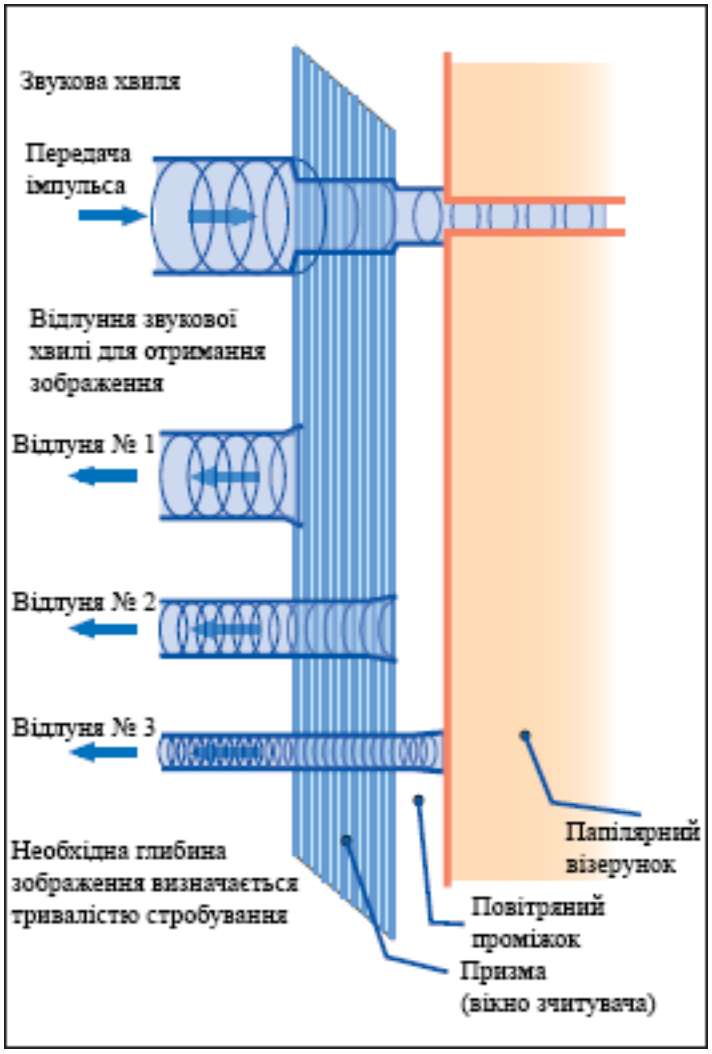

Рис. 2.7. Принцип роботи ультразвукового сканера

6) Температурний метод

Термосканери (Thermal Scanners) - у таких пристроях використовуються датчики, які складаються з піроелектричних елементів, що дозволяють фіксувати різницю температури та перетворювати її на напругу.

При прикладанні пальця до сканера за температурою торкаються до піроелектричних елементів виступів папілярного візерунка і температурі повітря, що знаходиться у западинах, будується температурна карта поверхні пальця, яка надалі перетворюється на цифрове зображення.

Температурний метод має безліч переваг. До них відносяться:

висока стійкість до електростатичного розряду;

стійка робота у широкому температурному діапазоні;

ефективний захист від муляжів.

До недоліків цього методу можна віднести те, що зображення швидко зникає.

При прикладанні пальця перший момент різниця температур значна і рівень сигналу, відповідно, високий. Після короткого часу (менше однієї десятої частки секунди) зображення зникає, оскільки палець і датчик приходять до температурної рівноваги [2].

2.1.2. Ідентифікація за геометрією руки

Даний метод біометричної аутентифікації передбачає вимірювання певних параметрів людської долоні, наприклад: довжина, товщина та вигини пальців, загальна структура кисті, відстань між суглобами, ширина та товщина долоні.

Руки людини є унікальними, тому для надійності даного виду аутентифікації необхідно комбінувати розпізнавання відразу за декількома параметрами.

Імовірність помилок при розпізнаванні геометрії становить близько 0,1%, а це означає, що при забитому місці, артриті та інших захворюваннях і пошкодженнях кисті, швидше за все, пройти автентифікацію не вдасться. Отже, цей метод біометричної автентифікації не підходить для забезпечення безпеки об'єктів високого ступеня секретності.

Однак, цей метод знайшов широке поширення, завдяки тому, що він зручний для користувачів з цілого ряду причин. Однією з таких причин є те, що пристрій для розпізнавання параметрів руки не завдає дискомфорту і не забирає багато часу (весь процес аутентифікації здійснюється за кілька секунд). Наступною причиною популярності аутентифікації за геометрією руки можна назвати той факт, що ні температура, ні забрудненість, ні вологість не впливають на процедуру автентифікації. Також зручний цей метод і тим, що для розпізнавання кисті можна використовувати зображення низької якості - розмір шаблону, що зберігається в базі всього 9 байт. Процедура порівняння користувача із встановленим шаблоном дуже проста та легко може бути автоматизована.

Пристрої даного виду біометричної автентифікації можуть мати різний зовнішній вигляд і функціонал - одні сканують лише два пальці (рис 2.8), інші роблять знімок усієї руки, а деякі сучасні пристрої за допомогою інфрачервоної камери сканують вени і зображують автентифікацію.

Рис. 2.8. Сканер геометрії руки

Цей метод вперше був використаний на початку 70-х років минулого століття. Сьогодні подібні пристрої можна зустріти в аеропортах та різних підприємствах, де необхідно формувати достовірні відомості про присутність тієї чи іншої людини, обліку робочого часу та інших процедур контролю.

2.1.3. Ідентифікація за обличчям

Кожна людина має унікальну будову обличчя. Спеціальне програмне забезпечення здатне аналізувати його, зіставляючи з інформацією в базі даних для подальшої ідентифікації того, хто ви такий (рис. 2.9).

Рис. 2.9. Сканер обличчя

Головний недолік технології розпізнавання обличчя - це погіршення якості розпізнавання при погіршення освітленості та зміні положення голови чи ракурсу [3].

Існує кілька підходів до створення алгоритму розпізнавання осіб.

Емпіричний підхід використовувався на початку розвитку комп'ютерного зору. Він базується на деяких правилах, які використовує людина для визначення

особи. Наприклад, лоб зазвичай яскравіший, ніж центральна частина особи, яка, у свою чергу, однорідна за яскравістю та кольором. Ще однією важливою ознакою є наявність частин особи на зображенні - носа, рота, очей. Для визначення осіб проводиться значне зменшення ділянки зображення, де передбачається наявність особи, або будуються перпендикулярні гістограми. Ці методи легко реалізувати, але вони практично непридатні за наявності великої кількості сторонніх об'єктів на фоні, кількох осіб у кадрі або зміни ракурсу.

Наступний підхід використовує інваріантні ознаки, характерні зображення особи. У його основі, як і попередньому методі, лежить емпірика, тобто спроба системи «думати» як людина. Метод виявляє характерні частини особи, її межу, зміну форми, контрастності тощо, об'єднує всі ці ознаки та верифікує. Даний метод може використовуватися навіть при повороті голови, але за наявності інших осіб або неоднорідному тлі розпізнавання стає неможливим [3].

Наступний алгоритм – це детектування осіб за допомогою шаблонів, які задає розробник. Особа представляється якимось шаблоном чи стандартом, і мета алгоритму – провести перевірку кожного сегмента наявність цього шаблону, причому перевірка може проводитися до різних ракурсів і масштабів. Така система потребує безліч трудомістких обчислень.

Усі сучасні технології розпізнавання обличчя використовують системи, які навчаються за допомогою тестових зображень. Для навчання використовуються бази із зображеннями, що містять особи, та не містять особи. Кожен фрагмент досліджуваного зображення характеризується як вектор ознак, з допомогою якого класифікатори (алгоритми визначення об'єкта у кадрі) визначають, є ця частина зображення обличчям чи ні.

Технологічно системи іноді можуть сильно відрізнятися щодо розпізнавання осіб, але вони мають приблизно загальні принципи роботи [3].

Крок 1: Виявлення обличчя

Для початку камера виявить обличчя людини, чи вона одна або перебуває в натовпі. Особа найкраще виявляється в той момент, коли людина дивиться прямо в камеру, проте сучасні технологічні досягнення дозволяють також виявляти обличчя і в тих ситуаціях, коли людина не дивиться прямо в камеру (звичайно, у певних межах).

Крок 2: Аналіз обличчя

Потім знімається фотографія обличчя та починається його аналіз. Більшість рішень для розпізнавання обличчя використовує 2D-зображення замість об'ємних 3D-зображень, оскільки вони можуть більш просто зіставляти 2D-фото із загальнодоступними фотографіями або фотографіями, що є в базі даних. Кожна особа складається з помітних орієнтирів або вузлових точок. Кожна людина має 80 вузлових точок. Програми для розпізнавання обличчя аналізують вузлові точки, такі як відстань між вашими очима або форма ваших вилиць [3].

Крок 3: Конвертація зображення в дані

Після цього аналіз вашого обличчя перетворюється на математичну формулу. Ваші риси обличчя стають числовим кодом. Такий числовий код називається відбитком обличчя (faceprint). Подібно до унікальної структури відбитка великого пальця, кожна людина має свій власний відбиток обличчя.

Крок 4: Пошук збігів

Далі код порівнюється з базою даних відбитків обличчя. У цій базі даних є фотографії з ідентифікаторами, які можна порівняти.

Потім технологія визначає відповідність ваших точних даних тому, що представлено в базі даних. Результатом цього стає ідентифікація людини з наданням додаткової інформації (ПІБ, адреса тощо) [3].

2.1.4. Ідентифікація за термограмою особи

Цей біометричний метод ідентифікації виявляється встановленням людини за її кровоносними судинами.

Більш надійним різновидом систем розпізнавання обличчя є аутентифікація та ідентифікація за «тепловим портретом» особи (рис. 2.9) в інфрачервоному діапазоні.

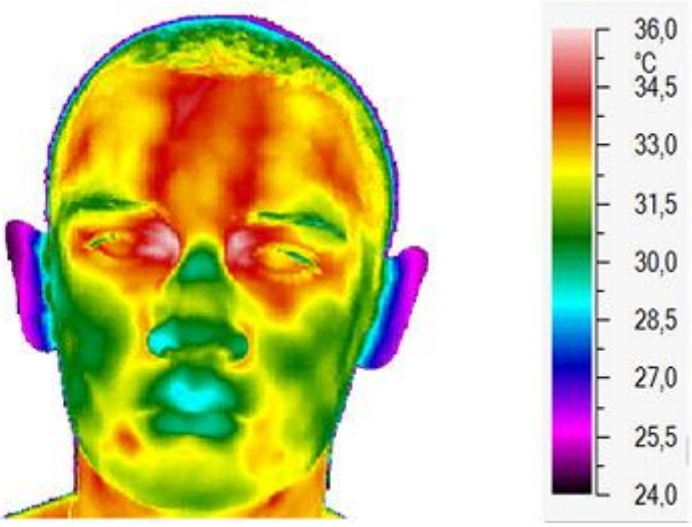

Рис. 2.10. Термограма обличчя

Цей метод, на відміну від звичайного, оптичного,
не залежить від змін обличчя людини (наприклад, появи бороди), тому що теплова картина обличчя змінюється дуже рідко. Дана технологія заснована на тому, що термограми обличчя людини (теплова картинка, створена випромінюванням тепла кровоносними судинами обличчя) унікальна для кожної людини і, отже, може бути використана в якості біокоду для систем

контролю допуску. Дана термограма є більш стабільним кодом, ніж геометрія обличчя, оскільки не залежить від часу і змін зовнішності людини. У процесі термографічної ідентифікації обличчя індивідуальний малюнок розподілу теплових областей на обличчі людини вводиться в комп'ютер за допомогою інфрачервоної камери та плати захоплення зображення [4].

Монохромне зображення, що надходить від інфрачервоної відеокамери, вводиться в комп'ютер за допомогою спеціального кабелю. В цей же час до зображення додається спеціально створена переглядова таблиця (lookuptable). Зображення піддається обробці спеціальною утилітою. Проблеми ідентифікації людини за «тепловим портретом» обличчя істотно спрощуються при переході спостережень у дальній інфрачервоний діапазон світлових хвиль. Запропоновано здійснювати термографію ідентифікуючого обличчя, яка виявляє унікальність розподілу артерій на обличчі, що забезпечують шкіру теплою кров'ю. Проблема підсвічування для цього класу біометричних пристроїв не існує, бо вони сприймають лише температурні перепади обличчя і можуть працювати в повній темноті. На результати ідентифікації не впливають перегрів особи, переохолодження, природне старіння обличчя, пластичні операції, тому що вони не змінюють внутрішнє розташування судин.

Дистанційне зчитування з будь-якої відстані незалежно від освітленості забезпечує високу пропускну здатність. Метод розрахований на

використання спеціалізованої відеокамери далекого інфрачервоного

діапазону, що й визначає його високу вартість [4].

2.1.5. Ідентифікація за сітківкою ока

Аутентифікація сітківки ока - це одна з біометричних технологій, що використовується для перевірки справжності особистості. Тип біометричної технології, що розглядається в цій статті, використовує фізіологічний параметр – унікальність сітківки ока. Цей метод часто плутають з автентифікацією по райдужній оболонці ока, однак це зовсім інший спосіб автентифікації.

На відміну від інших біометричних способів для розпізнавання сітківки потрібна велика кількість вимог від користувача для збору високоякісних даних. Необхідно, щоб користувач знаходився в безпосередній близькості від сканування сітківки. У цьому полягає велика різниця з розпізнаванням райдужної оболонки, коли дані можна збирати з великої відстані.

Процес можна розбити в такий спосіб.

Збір та обробка даних

На цьому, першому, етапі людина має зафіксувати своє око перед невеликим приймачем. Звідси інфрачервоний світловий промінь потім випромінюється в око, щоб повністю висвітлити сітківку. Щоб зменшити ймовірність помилки, це світло випромінюється на 360 градусів. Цей процес може тривати кілька хвилин. Щоб забезпечити збір якісних зображень, людина повинна залишатися абсолютно нерухомою, окулярів або лінз не повинно бути з метою усунення перешкод. На цій стадії можна зібрати та проаналізувати до п'яти необроблених зображень, щоб створити комплексне зображення, з якого потім будуть вилучені унікальні ознаки.

Створення шаблону реєстрації та підтвердження

На цьому, другому, етапі виходять унікальні ознаки. Генетичні чинники мало визначають склад структури кровоносних судин, у тому числі складається сітківка. Інакше кажучи, це вписується у структуру ДНК людини і передається потомству. Через це із сітківки може бути отримано до 400 унікальних ознак (для відбитка пальця – приблизно 30-40). Після цього створюється шаблон реєстрації. Розмір шаблону реєстрації сітківки становить лише 96 байт і вважається найменшим біометричним шаблоном із усіх. Це, мабуть, має численні переваги. По-перше, під час перевірки статистичної схожості між шаблонами перевірки та реєстрації значно знижуються витрати на обчислення.

По-друге, цей невеликий розмір означає, що більше шаблонів може зберігатися в одній базі даних. Цей процес також використовується для створення шаблону підтвердження [5].

Оскільки для розпізнавання сітківки потрібна висока точність при зборі даних, існує низка факторів, які можуть завадити процесу розпізнавання:

Неакуратність користувача при зчитуванні даних:

Як було описано, людина повинна залишатися абсолютно нерухомою протягом усього процесу. Будь-який раптовий або ненавмисний рух може негативно вплинути на відносне розташування лінзи, яка використовується для передачі променю інфрачервоного світла сітківки.

Велика відстань між оком та об'єктивом:

Для виконання високоякісного сканування між приймачем і сітківкою має бути відстань трохи більше 3 дюймів. Якщо відстань перевищує вищезазначене, процес сканування повинен повторюватися знову, доки ця вимога не буде дотримана. У цьому відношенні, в порівнянні з іншими біометричними методами, точність має першорядне значення при розпізнаванні сітківки [5].

Розмір зіниці людини:

Маленька зіниця може значно зменшити кількість зовнішнього світла, яке передається на сітківку. Також, ця проблема може погіршитися при стисканні зіниці через неправильні умови освітлення.

Переваги

Сітківка вважається дуже стабільною та практично не змінюється протягом життя людини. Таким чином, у цьому відношенні вона вважається найнадійнішою біометричною технологією, яка є доступною на ринку сьогодні.

Враховуючи невеликий розмір даних, що зчитуються і розпізнавання сітківки, система здатна швидко підтверджувати особистість людини.

Через велику кількість унікальних ознак, якими володіє сітківка, ймовірність помилкового спрацьовування вкрай низька [5].

Оскільки сітківка розташована всередині самої структури ока, вона не схильна до впливу зовнішнього середовища, на відміну від геометрії рук та відбитків пальців.

Недоліки

Багато людей побоюються, що ця процедура негативно впливає на зір (хоча науково цей факт не доведено).

У порівнянні з іншими біометричними методами, розпізнавання сітківки вимагає від користувача найбільше зусиль.

Через високі вимоги до користувача може знадобитися кілька спроб автентифікації та тривалий час для отримання результатів. Таким чином, якщо процес не буде виконаний правильно, це може призвести до дуже великої частоти помилкових відмов [5].

2.1.6. Ідентифікація за райдужною оболонкою ока

Це нова технологія біометричної ідентифікації, де як ідентифікатор виступає райдужна оболонка ока. У кожної людини вона унікальна, тож помилок не буде. Підробити райдужну оболонку не можна, тому СКУД, що базуються на розпізнаванні райдужної оболонки ока, дуже надійні [6].

Рис. 2.11. Сканер радужної оболонки ока

Щоб усе працювало, потрібно вбудувати в класичну СКУД зчитувач райдужної оболонки ока (рис. 2.10). Залежно від умов експлуатації, ми використовуємо один із таких варіантів:

• зчитувач райдужної оболонки ока;

• вуличний зчитувач райдужної оболонки ока.

Перший використовується для розміщення у приміщеннях. Другий призначений для вуличних умов. Він не боїться морозів, опадів та вітру.

Особливості ідентифікації по райдужній оболонці ока

Зчитувачі райдужки ока характеризуються:

• пропускною здатністю до 20 осіб на хвилину;

• можливістю реєстрації по одному або двох очах;

• можливістю поєднувати ідентифікацію по райдужці ока з іншим видом ідентифікації (наприклад, картою);

• надійний стандарт шифрування AES256, який використовують для захисту даних під грифом «Цілком таємно». Це означає, що біометричні дані не можна дістати і скопіювати;

• коректним розпізнаванням особистості, навіть коли людина в окулярах чи лінзах [6].

Сценарії використання ідентифікації по райдужці ока

Все, що потрібно для ідентифікації, - це затримати на мить погляд на зчитувачі. Прилад відсканує райдужку ока, порівняє її зі збереженими в базі шаблонами і знайде такий самий зразок. Так він встановить вашу особу. Якщо система не знайшла такий самий стандарт в базі, вона заборонить доступ чужинцю - не відкриє турнікет/двері.

Всі шаблони зберігаються в зашифрованому вигляді, тому ніякий зловмисник не зможе скористатися зразками біометрії.

Райдужна оболонка ока – це унікальний параметр кожної людини. Райдужка майже не змінюється з віком. Зчитувач, зберігаючи шаблон вашої райдужної оболонки, аналізує велику кількість параметрів – у рази більше, ніж зчитувач відбитків пальців. Завдяки цьому точність розпізнавання гранично висока, і це дозволяє використовувати ідентифікацію по райдужному оку в компаніях, де працюють тисячі людей [6].

А ще - це абсолютно безконтактний спосіб - не потрібно робити абсолютно ніяких рухів тіла, крім як звернути погляд на зчитувач. Зчитувачеві потрібно не більше трьох секунд, щоб завершити процес ідентифікації. Завдяки високій

швидкості роботи ви уникнете черг на вході, зберігши високу точність ідентифікації.

Переваги розпізнавання по райдужній оболонці ока

Розпізнавання райдужної оболонки є надзвичайно точним засобом.

Висока швидкість розпізнавання 0,3с.

Безконтактний метод використання підвищує надійність пристрою, при цьому не потрібно турбуватися через забруднення, сухість або інші проблеми шкіри, як при використанні відбитків пальця [6].

2.1.7. Ідентифікація за малюнком вен

Так само як райдужка, візерунки вен долоні є унікальними для кожної людини, навіть для ідентичних близнюків. Біометричні технології створюють зображення малюнка вен під шкірою і використовують це зображення в якості основи для індивідуальної ідентифікації. Щоб отримати зразок малюнка вен долоні, біометрична технологія використовує інфрачервоне світло (така ж технологія використовується в ТВ пультах) (рис 2.11) [7].

Рис. 2.12. Сканер малюнка вен

Цей метод вважається надзвичайно безпечним і надійним. На відміну від біометричної технології на основі зчитування відбитків пальців, яка для точної ідентифікації спирається на малюнок шкіри на кінчиках пальців і може бути

схильна до неточності через вплив віку, навколишнього середовища, наявності порізів, подряпин, синців, шрамів, бруду, цілісності шкіри, для розпізнавання малюнка вен - це не є проблемою.

Через надійність, простоту використання і швидкість - ця біометрична технологія може використовуватися в різних сферах, таких як ідентифікація студентів або прикордонний контроль.

Незважаючи на те що малюнок вен долоні дуже складно або навіть неможливо підробити, існує чимало обмежень для використання цієї біометрії. По-перше, ця методика вимагає фізичного контакту з біометричним пристроєм, що не дуже гігієнічно, а також необхідно здійснювати дезінфекцію обладнання після кожного використання, особливо при використанні в медичних установах. По-друге, обмеження полягає в тому, що дана технологія підходить лише для невеликих баз даних [7].

2.1.8. Ідентифікація на основі акустичних характеристик вуха

NEC Corporation представила нову біометричну технологію ідентифікації, яка ґрунтується на резонуванні звуку в порожнині людського вуха(рис 2.12). За даними компанії, нова технологія біометричної аутентифікації миттєво вимірює акустичні характеристики вуха (яка є унікальною для кожної людини) і працює за допомогою навушників із вбудованим мікрофоном для збору даних про те, як звуки резонують порожнини вуха [8].

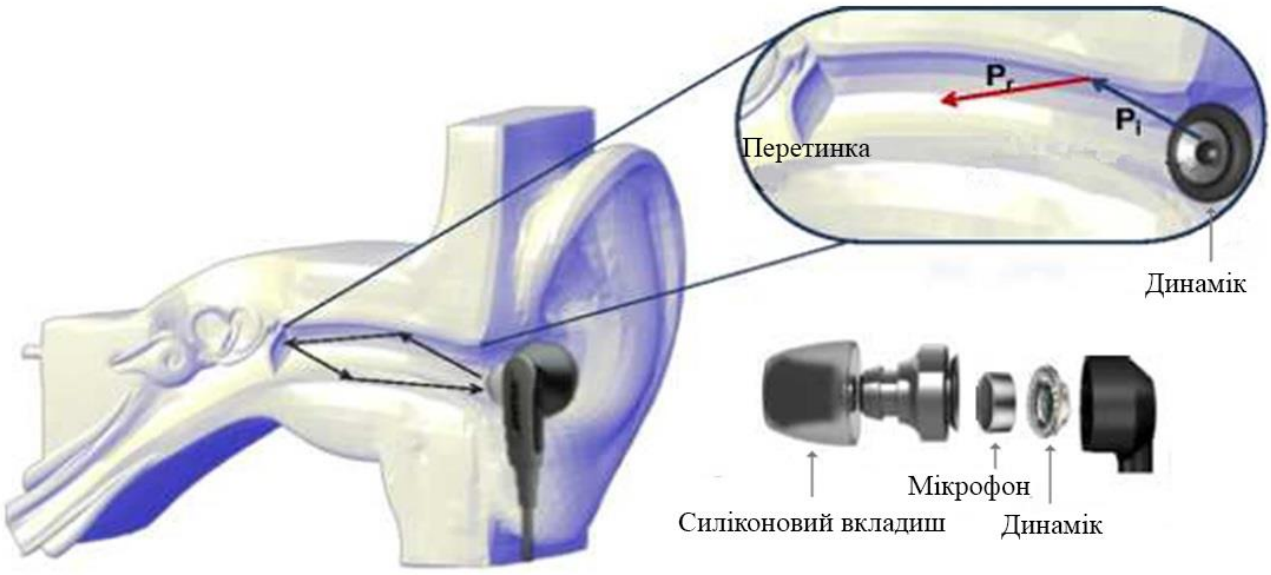

Рис. 2.13. Принцип роботи ідентифікації на основі акустичних характеристик вуха

Цей метод біометричної аутентифікації на основі акустичних характеристик вуха людини має високу швидкість та точність розпізнавання; може бути ефективно використаний для захисту телефонних дзвінків, персональних голосових повідомлень, бездротового радіозв'язку та іншої звукової інформації.

Відкриті біометричні образи (відбиток пальця, райдужка, обличчя, голос, автограф) перебувають «на виду» і тому компрометуються у природному середовищі навіть за дотримання всіх вимог щодо захисту. Зловмисник може зняти біометричні характеристики безконтактно або приховано від власника (наприклад, ручки дверей, фотографії).

Проект присвячений розробці методу та технології біометричної ідентифікації та аутентифікації з використанням даних про внутрішню будову зовнішнього вуха, які отримують за допомогою ехографії.

Індивідуальні особливості вушного каналу суб'єктів приховані від безпосереднього спостереження і можуть бути скопійовані шляхом

фотографування. "Плоске" зображення вуха недостатньо інформативно для виготовлення "муляжу" [8].

2.2 Динамічні методи біометричної автентифікації

Динамічні методи ідентифікації ґрунтуються на аналізі поведінкових характеристик особистості – особливостей, властивих кожній людині у процесі відтворення будь-якої дії. Динамічні методи суттєво поступаються статичним у точності та ефективності і, як правило, використовуються як допоміжні. До цих характеристик входять:

2.2.1. Ідентифікація за голосом

Цей метод дозволяє ідентифікувати та аутентифікувати людину за допомогою лише одного мікрофона, підключеного до пристрою запису. Використання цього методу корисно в судових справах, коли єдиним доказом проти підозрюваного є запис телефонної розмови. Спосіб розпізнавання мовлення дуже зручний - користувачеві потрібно лише вимовити слово, не виконуючи жодних додаткових дій. Нарешті, величезною перевагою такого підходу є право виконувати приховану аутентифікацію. Користувачам не завжди вказують включити додаткову аутентифікацію, тому зловмисникам важче отримати доступ. Формування особистісних закономірностей ґрунтується на багатьох характеристиках звуку. Це може бути інтонація, інтонація, модуляція, вимова певних голосів тощо. Якщо система аутентифікації правильно проаналізувала всі характеристики мовлення, можливість сторонньої аутентифікації є незначною.

Однак у 1-3% випадків система може відхилити справжнього власника голосу. Насправді голос людини може змінюватися під час хвороби (наприклад, застуди), залежно від психічного стану, віку тощо. Тому біометричні методи голосової аутентифікації непридатні для використання в об’єктах високої

безпеки. Його можна використовувати для доступу до комп’ютерних класів, бізнес-центрів, лабораторій та подібних об’єктів безпеки. Технологію розпізнавання голосу можна використовувати не тільки як аутентифікацію та ідентифікацію, а й як незамінний помічник для введення голосових даних [9].

2.2.2. Ідентифікація за почерком

У зв'язку з популярністю та масовим використанням різних пристроїв із сенсорним екраном, біометричний метод аутентифікації за підписом стає дуже затребуваним.

Верифікація підпису

Максимально точну верифікацію підпису забезпечує використання спеціального пристрою - світлового пір'я (рис 2.13).

Рис. 2.14. Різновиди світлового пір’я

У багатьох країнах електронні документи, підписані біометричним підписом, мають таку саму юридичну силу, як і паперові носії. Це дозволяє здійснювати документообіг значно швидше та безперешкодно [10].

Біометричний метод аутентифікації за підписом має два способи:

На основі аналізу візуальних параметрів підпису. Даним способом передбачається порівняння двох зображень підпису на відповідність ідентичності це може здійснюватися як системою, так і людиною.

Метод комп'ютерного аналізу динамічних параметрів написання підпису. Аутентифікація у такий спосіб відбувається після ретельного дослідження відомостей про сам підпис, а також про статистичні та періодичні характеристики його написання.

Формування шаблону підпису здійснюється залежно від рівня захисту. Усього, один підпис аналізує 100-200 характерних точок. Якщо ж, підпис ставиться з допомогою світлового пера, крім координат пера, враховується і кут його нахилу, натискання пера. Кут нахилу пера обчислюється щодо планшета та за годинниковою стрілкою.

Цей метод біометричної аутентифікації, як і розпізнавання клавіатурного почерку, мають спільну проблему - залежність від психофізичного стану людини [10].

2.2.3. Ідентифікація за клавіатурним почерком

Метод розпізнавання клавіатурного почерку є одним з перспективних методів біометричної аутентифікації сьогодення. Клавіатурний почерк є

біометричною характеристикою поведінки кожного користувача, а саме - швидкість введення, час утримання клавіш, інтервали між натисканнями на них, частота утворення помилок при введенні, число перекриттів між клавішами, використання функціональних клавіш і комбінацій, рівень аритмічності при наборі та ін.

Ця технологія є універсальною, проте, найкраще, розпізнавання клавіатурного почерку підходить для автентифікації віддалених користувачів. Розробкою алгоритмів розпізнавання клавіатурного почерку активно займаються IT-компанії [11].

Аутентифікація за клавіатурним почерком користувача має два способи:

уведення відомої фрази (паролю);

введення невідомої фрази (генерується випадковим чином).

Обидва способи аутентифікації передбачають два режими: режим навчання та режим самої аутентифікації. Режим навчання полягає у багаторазовому введенні користувачем кодового слова (фрази, пароля). У процесі повторного набору система визначає характерні особливості введення тексту і формує шаблон показників користувача. Надійність такого виду автентифікації залежить від довжини фрази, що вводиться користувачем.

Серед переваг даного методу аутентифікації слід зазначити зручність користування, можливість здійснення процедури аутентифікації без спеціального обладнання, а також прихованої аутентифікації. Мінусом даного методу, як і у разі розпізнавання голосу, можна назвати залежність відмови системи від вікових факторів та стану здоров'я користувача. Адже, моторика, куди сильніша за голос, залежить від стану людини. Навіть проста втома людини може вплинути на

проходження аутентифікації. Зміна клавіатури також може бути причиною відмови системи - користувач здатний не відразу адаптуватися до нового пристрою введення і тому, при введенні перевірочної фрази, клавіатурний почерк може не відповідати шаблону. Зокрема, це впливає на темп введення. Хоча, дослідники пропонують підвищити ефективність цього за рахунок використання ритму. Штучне додавання ритму (наприклад, введення користувачем слова під якусь знайому мелодію) забезпечує стійкість клавіатурного почерку та надійніший захист від зловмисників [11].

3. ПОРІВНЯЛЬНИЙ АНАЛІЗ ОСНОВНИХ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

3.1. Критерії біометричної ідентифікації

Для визначення ефективності СКУД на основі біометричної ідентифікації використовують такі показники:

FAR – коефіцієнт помилкового пропуску;

FMR - можливість, що система неправильно порівнює вхідний зразок з невідповідним шаблоном у базі даних;

FRR – коефіцієнт помилкової відмови;

FNMR - ймовірність того, що система помилиться у визначенні збігів між вхідним зразком та відповідним шаблоном з бази даних;

Графік ROC – візуалізація компромісу між характеристиками FAR та FRR;

Коефіцієнт відмови в реєстрації (FTE або FER) – коефіцієнт безуспішних спроб створити шаблон із вхідних даних (при низькій якості останніх);

Коефіцієнт помилкового утримання (FTC) - можливість, що автоматизована система неспроможна визначити біометричні вхідні дані, що вони представлені коректно;

Місткість шаблону - максимальна кількість наборів даних, які можуть зберігатися в системі.

3.2. Порівняння біометричних методів аутентифікації

Основними параметрами для оцінки будь-якої біометричної системи є два параметри:

FAR (False Acceptance Rate) - хибний показник проходження, тобто відсоток ситуацій, коли система дозволяє отримати доступ до користувача, який не зареєстрований в системі.

FRR (False Rejection Rate) - коефіцієнт помилкових відхилень, тобто відмови у доступі реальному користувачеві системи.

Обидві характеристики отримані розрахунком на основі методів математичної статистики. Чим нижче ці показники, тим точніше буде розпізнавання об'єкта [12].

Для найпопулярніших на сьогодні біометричних методів ідентифікації середні значення FAR і FRR є такими:

Таблиця 3.1

Порівняння методів біометричної аутентифікації з використанням математичної статистики (FAR та FRR)

Біометрична СКУД використовує:	**FAR**	**FRR**
Відбиток пальця	0,001%	0,6%
Розпізнавання обличчя 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,1%
Райдужна оболонка ока	0,00001%	0,016%

Сітківка ока	0,0001%	0,4%
Малюнок вен	0,0008%	0,01%

Але для побудови ефективної системи контролю доступу недостатньо відмінних показників FAR та FRR. Наприклад, складно уявити СКУД на основі аналізу ДНК, хоча за такого методу аутентифікації зазначені коефіцієнти прагнуть нуля. Натомість зростає час ідентифікації, зростає вплив людського фактору, невиправдано зростає вартість системи.

Таким чином, для якісного аналізу біометричної системи контролю доступу необхідно використовувати інші дані, які іноді можна отримати лише експериментальним шляхом.

Насамперед, до таких даних слід віднести можливість підробки біометричних даних для ідентифікації в системі та способи підвищення рівня безпеки.

По-друге, стабільність біометричних факторів: їхня незмінність з часом та незалежність від умов навколишнього середовища.

Як наслідок - швидкість аутентифікації, можливість швидкого безконтактного зняття біометричних даних для ідентифікації.

І, звичайно, вартість реалізації біометричної СКУД на основі аналізованого методу аутентифікації та доступність складових [12].

У будь-якому випадку **фальсифікація біометричних даних** є досить складним процесом, який часто вимагає спеціальної підготовки та технічної підтримки. Але якщо можна підробити відбиток пальця в домашніх умовах, то про успішну фальсифікацію райдужної оболонки поки не відомо. А для

біометричних систем автентифікації сітківки ока створити підробку просто неможливо.

Таблиця 3.2

Порівняння біометричних методів стійкості до фальсифікації даних

Біометрична СКУД використовує:	**Фальсифікація**
Відбиток пальця	Можлива
Розпізнавання обличчя 2D	Можлива
Розпізнавання обличчя 3D	Проблематична
Райдужна оболонка ока	Безуспішна
Сітківка ока	Неможлива
Малюнок вен	Неможлива

Підвищення рівня безпеки біометричної системи контролю доступу, як правило, досягається програмно-апаратними методами. Наприклад, технології «живого пальця» для відбитків, аналіз мимовільних посмикувань – для очей. Для підвищення рівня безпеки біометричний метод може бути одним із компонентів багатофакторної системи автентифікації.

Включення додаткових засобів безпеки в програмно-апаратний комплекс зазвичай досить значно збільшує його вартість. Однак для деяких методів можлива надійна автентифікація на основі стандартних компонентів: використання кількох шаблонів для ідентифікації користувача (наприклад, кілька відбитків пальців) [12].

Таблиця 3.3

Порівняння біометричних методів за можливістю суворої аутентифікації

Біометрична СКУД використовує:	**Сувора аутентифікація (один фактор)**
Відбиток пальця	Можлива
Розпізнавання обличчя 2D	Ні
Розпізнавання обличчя 3D	Ні
Райдужна оболонка ока	Можлива
Сітківка ока	Можлива
Малюнок вен	Можлива

Незмінність біометричної характеристики в часі також є умовним поняттям: всі біометричні параметри можуть змінитися в результаті медичної операції або травми. Але якщо звичайний домашній зріз, який може ускладнити верифікацію користувача за відбитком пальця, є поширеною ситуацією, то операція, яка змінює малюнок райдужної оболонки, — рідкість [12].

Таблиця 3.4

Порівняння методів аутентифікації за незмінністю біометричних характеристик

Біометрична СКУД використовує:	**Незмінність характеристики**
Відбиток пальця	Низька
Розпізнавання обличчя 2D	Низька
Розпізнавання обличчя 3D	Висока

Райдужна оболонка ока	Висока
Сітківка ока	Середня
Малюнок вен	Середня

Вплив параметрів навколишнього середовища на ефективність роботи СКУД залежить від алгоритмів і технологій роботи, які реалізує виробник обладнання, і може суттєво відрізнятися навіть у рамках одного біометричного методу. Яскравим прикладом таких відмінностей можуть служити сканери відбитків пальців, які в цілому досить чутливі до впливу зовнішніх факторів.

Якщо порівнювати інші методи біометричної ідентифікації, то найбільш чутливим буде 2D-розпізнавання обличчя: критичним тут може стати наявність окулярів, капелюха, нової зачіски чи зарослої бороди.

Системи, що використовують метод автентифікації сітківки ока, вимагають досить жорсткого положення ока відносно сканера, нерухомості користувача та фокусування самого ока [12].

Методи ідентифікації користувача за малюнком вен та райдужною оболонкою ока порівняно стабільні в роботі, якщо не намагатися використовувати їх в екстремальних умовах роботи (наприклад, безконтактна автентифікація на великій відстані під час дощу).

Найменш чутливим до впливу зовнішніх факторів є тривимірна ідентифікація по обличчю. Єдиний параметр, який може вплинути на роботу такої СКУД – надмірна освітленість.

Таблиця 3.5

Вплив параметрів довкілля на ефективність роботи СКУД

Біометрична СКУД використовує:	**Чутливість до впливу зовнішніх факторів**
Відбиток пальця	Висока
Розпізнавання обличчя 2D	Висока
Розпізнавання обличчя 3D	Низька
Райдужна оболонка ока	Середня
Сітківка ока	Висока
Малюнок вен	Середня

Швидкість автентифікації залежить від часу збору даних, розміру шаблону та обсягу ресурсів, виділених на його обробку, а також основних програмних алгоритмів, які використовуються для реалізації того чи іншого біометричного методу [12].

Таблиця 3.6

Порівняння за швидкістю аутентифікації

Біометрична СКУД використовує:	**Швидкість аутентифікації**
Відбиток пальця	Висока
Розпізнавання обличчя 2D	Середня
Розпізнавання обличчя 3D	Низька
Райдужна оболонка ока	Висока
Сітківка ока	Низька
Малюнок вен	Висока

Безконтактна автентифікація дає багато переваг використання біометричних методів у системах фізичної безпеки на об’єктах з високими санітарно-гігієнічними вимогами (медицина, харчова промисловість, науково-дослідні інститути та лабораторії). Крім того, можливість ідентифікувати віддалений об’єкт прискорює процедуру верифікації, що важливо для великих систем контролю доступу з великим потоком. А також безконтактну ідентифікацію правоохоронні органи можуть використовувати в службових цілях. Саме тому вчені прагнуть розробити системи безконтактної автентифікації відбитків пальців, але поки не досягли стійких результатів. Особливо ефективними є методи, що дозволяють фіксувати біометричні характеристики об'єкта на великій відстані і під час руху. З поширенням мегапіксельних камер відеоспостереження реалізація цього принципу роботи стає все легше [12].

Таблиця 3.7

Порівняння по можливості безконтактної аутентифікації

Біометрична СКУД використовує:	**Безконтактна аутентифікація під час руху**
Відбиток пальця	Безуспішна
Розпізнавання обличчя 2D	На великій відстані
Розпізнавання обличчя 3D	На середній відстані
Райдужна оболонка ока	На великій відстані
Сітківка ока	Неможлива
Малюнок вен	На маленькій відстані

Психологічний комфорт користувачів також є досить актуальним показником при виборі системи безпеки. Якщо у випадку двовимірного розпізнавання обличчя або райдужної оболонки – це відбувається непомітно, то сканування сітківки ока досить неприємний процес. А ідентифікація відбитків пальців, хоча і не приносить неприємного відчуття, може викликати негативні асоціації з методами судово-медичної експертизи [12].

Таблиця 3.8

Порівняння біометричних методів психологічного комфорту користувача

Біометрична СКУД використовує:	**Комфорт користувача**
Відбиток пальця	Середній
Розпізнавання обличчя 2D	Високий
Розпізнавання обличчя 3D	Середній
Райдужна оболонка ока	Високий
Сітківка ока	Низький
Малюнок вен	Середній

Вартість систем контролю доступу та обліку, залежно від використовуваних методів біометричної ідентифікації, сильно різниться між собою. Однак різниця може бути помітна навіть у межах одного способу, залежно від призначення системи (функціональності), технологій виробництва, способів підвищення захисту від несанкціонованого доступу тощо [12].

Таблиця 3.9

Порівняння за вартістю реалізації біометричних методів у СКУД

Біометрична СКУД використовує:	**Вартість**
Відбиток пальця	Низька
Розпізнавання обличчя 2D	Середня

Розпізнавання обличчя 3D	Висока
Райдужна оболонка ока	Висока
Сітківка ока	Висока
Малюнок вен	Середня

Наявність систем контролю доступу з використанням того чи іншого методу біометричної автентифікації залежить від їх поширеності в цілому. І, звичайно, специфіка ринку накладає свої обмеження.

При врахуванні складних економічних умов на перший план виходить ціна. Перш за все, наявність власних виробників на порядок знижує вартість обладнання. Крім того, наявність обладнання дозволяє розраховувати на швидку заміну або ремонт комплектуючих при необхідності [12].

Таблиця 3.10

Порівняння доступності методів біометричної ідентифікації в Україні

Біометрична СКУД використовує:	**Доступність на українському ринку**
Відбиток пальця	Висока
Розпізнавання обличчя 2D	Середня
Розпізнавання обличчя 3D	Середня
Райдужна оболонка ока	Низька
Сітківка ока	Низька

Малюнок вен	Висока

Проблем з розпізнаванням відбитків пальців та методом розпізнавання вен немає: споживачеві доступний широкий асортимент обладнання.

Двовимірна ідентифікація обличчя недостатньо ефективна, щоб на її основі побудувати систему безпеки. Швидше цей метод використовується для завдань відеоаналітики або як один із компонентів багатофакторних систем аутентифікації.

3D-аутентифікація є дорогою, навіть якщо порівняти біометричні методи ідентифікації.

Метод аутентифікації за сітківкою ока настільки вузькоспеціалізований, а об'єкти для яких він призначений настільки секретні, що краще про його доступність навіть не думати і не говорити вголос.

Метод ідентифікації райдужної оболонки ока вже багато років вважається одним з найбільш перспективних та ефективних і його частка на світовому ринку, безумовно, зростає. Водночас висока вартість і складна ситуація з технологічними патентами також обмежують на світовій арені.

Отже, найкращим методом біометричної аутентифікації являється розпізнавання відбитків пальців.

4. ПОБУДОВА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

Найбільш оптимальний вид біометричної ідентифікації це – ідентифікація по відбитку пальця.

Тож ми побудуємо систему аутентифікації на основі сканеру відбитків пальців.

4.1. Підбір обладнання

Для цього нам потрібно:

Біометричний сканер відбитка пальця.

Одна з головних частин схеми це сканер відбитків пальців. За допомогою нього і буде виконуватися ідентифікація та відкриття дверей.

Існує багато різних сканерів, які відрізняються характеристиками.

В таблиці 4.1 наведені результати **проведеного порівняльного аналізу** різних типів сканерів, на основі яких вибраний **DS-K1200EF** (рис. 4.1).

Рис.4.1. Біометричні сканери відбитків пальців

Таблиця 4.1

Характеристики біометричних сканерів відбитків пальців, що використовувались для порівняння

Характеристика	FPV10R	ZKTeco FV350	DS-K1200EF	DS-K1F820-F	DHI-ASR1102A(V2)	ZKTeco MA300
Струм споживання, мА	500	500	430	200	100	500

Кількість відбитків	8000	1000	9000	1500	3000	1500
Робочий діапазон температур, °С	-20-+45	-10-+45	-40-+70	-30 -+70	-5-+55	-10-+60
Живлення, В		12	12	5	9-15	12
Ціна, грн	5467 грн	8563 грн	3500 грн	2321 грн	2587 грн	4374 грн

Після проведення аналізу **найкращим варіантом є сканер DS-K1200EF**.

Контролер.

Контролер – це головна частина системи, призначена для управління доступом до приміщень, обліку часу проходу та подій, обробляти інформацію, що надходить зі зчитувача та, за допомогою чотирьох реле, здійснювати комутацію виконавчих пристроїв.

Для нашої системи було обрано контролер Hikvision DS-K2801 (рис. 4.2).

Рис. 4.2. Контролер Hikvision DS-K2801

Серія DS-K2800 є потужними і стабільними контролерами доступу, з використанням логічної архітектури. Його сигнал обробляється спеціальним шифруванням та може працювати в автономному режимі. Підтримує функцію тривоги.

Налаштовується через ПК командами через CMS (Content management system).

Розмір: 285x237x69 мм.

Робоча температура: -20°C - +65°C.

Живлення: DC 12В/1А, 3.5Вт.

Ціна: 4317 грн

Сервер.

Серверне обладнання (рис 4.3) найчастіше призначене для забезпечення роботи сервісів у режимі 24/7, тому часто комплектується дублюючими елементами, що дозволяють забезпечити «п'ять дев'яток» (99,999%; час недоступності сервера або простої системи становить менше 6 хвилин на рік). І тому конструкторами під час створення серверів створюються спеціальні рішення, відмінні від створення звичайних комп'ютерів.

Рис.4.3. Сервер HP ProLiant DL80 Gen9 12 LFF 2U

Процесор: Intel Xeon E5 v3/v4

Тип пам’яті: DDR4 RDIMM

Кількість слотів пам'яті: 8

Потужність блока живлення: 960 Вт

Ціна: 8 990 грн.

Електромагнітний замок.

Електромагнітний замок (рис. 4.4.) встановлюється на дверну коробку, відповідна планка - на двері. При подачі живлення - замок примагнічує відповідну планку, надійно замикаючи двері. При відсутності живлення - замок відкривається, що відповідає вимогам протипожежної безпеки.

Рис. 4.4. Електромагнітний замок YM-280N

Електромагнітний замок зі світловою індикацією, накладний, сила утримання 280кг.

Живлення: DC12V/520mA, DC24V/260mA.

Розміри: 250x48, 8x27, 9 мм.

Підходить для дерев'яних, скляних, металевих та протипожежних дверей.

Ціна: 850 грн.

Кнопка виходу.

Tyto BM-11-NO (рис. 4.5) — накладна металева кнопка виходу, використовують для монтажу в системах контролю доступу.

Рис. 4.5. Кнопка виходу Tyto BM-11-NO

Робоча температура: -10°C ~ +50°C

Розміри: 80 x 30 x 20 мм

Ціна: 265 грн.

Доводчик дверей.

Призначений для установки на всі стандартні типи дверей масою до 110 кг, як усередині приміщення, так і на вулиці. Підходить для установки на двері лівого і правого відкривання. Застосування доводчика (рис. 4.6) дозволяє значно зменшити знос дверних петель і іншої дверної фурнітури й забезпечити надійне закриття дверей.

Рис. 4.6. Доводчик дверей GEZE TS 1000 C

Вибіркова сила закривання EN 2/3 за допомогою зміщеного монтажу.

Регульований гідравлічний кінцевий дохлоп та швидкість закривання.

Робоча температура - від -35 °C до +60 °C

Ціна: 942 грн

Датчик положення дверей.

Датчик положення дверей (рис. 4.7) - з'єднується з замком, повідомляючи про статус двері "відкрито / закрито", точний монтаж без виступання за торець дверей, контакти приховані і захищені, коли двері закриті, саморегульована відстань між контактами.

Рис. 4.7. Датчик положення дверей SATEL B-3 A

Складається з двох частин – магніту та блоку з герконом. Принцип роботи датчика відкриття дверей/вікна ґрунтується на властивостях геркона – елемента, що проводить струм під дією змінного магнітного поля. У нормальному стані магніт і блок із герконом зімкнуті. Як тільки двері, на яких встановлено датчик, відчиняються - магніт віддаляється від геркона, геркон розмикається і перестає проводити струм - датчик спрацьовує.

Ціна: 491грн

Сирена.

Сирена Covi Security SR-03 (рис.4.8) призначена для подачі світлозвукового сигналу у разі тривоги. За допомогою потужного звуку 110 дБ сирена відлякує та впливає на зловмисника, та привертає увагу оточуючих людей. Додаткову дію та привернення уваги надає вбудована у сирену світлова індикація.

Рис. 4.8. Сирена Covi Security SR-03

Розмір: 122×72×43 мм

Ціна: 304 грн.

Конвектор.

Перехідник USB-RS-485 (рис. 4.9) - адаптер, призначений для підключення контролерів різних електронних компонентів, що використовують для обміну даними порт.

Рис. 4.9. Перехідник USB - RS485

Ціна: 68 грн.

4.2. Побудова системи

На базі вибраного обладнання в процесі виконання бакалаврської роботи була побудована система контролю доступу за відбитком пальця , наведена на рис.4.10.

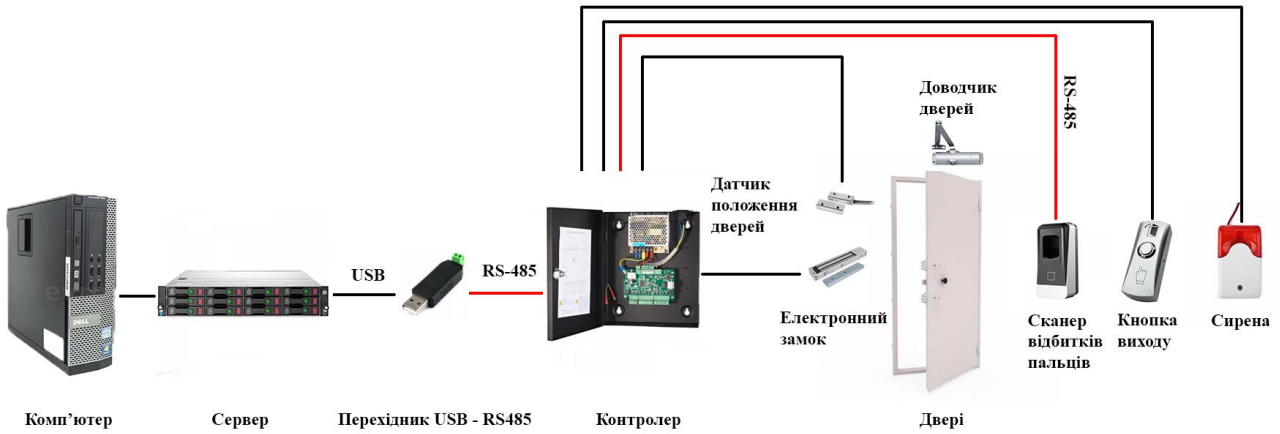

Рис 4.10. Схема роботи сканеру відбитків пальців

На початку контролеру через сервер дається шаблон відбитків пальців або карт.

При відскануванні відбитка (або карти) інформація передається контролеру та зрівнюється. Якщо в базі даних знайдено відбиток, то подається сигнал електронному замку і двері відчиняються. Якщо двері відкриті довше ніж запрограмоване в датчику положення дверей, то вмикається сирена.

Щоб вийти з кімнати присутня кнопка виходу. При активації кнопки йде сигнал контролеру а потім до електронного замка й двері відкриваються.

Розрахунок

Загальна вартість системи = 3 500 + 4 317 + 8 990 + 850 + 942 + 265 + 491 + 304 + 68 = **19 727 грн.**

Вартість системи склала – 19 727 грн.

ВИСНОВКИ

1) Було розглянуто методи біометричної аутентифікації та ідентифікації, та порівняльний аналіз основних методів біометричної ідентифікації.
2) Наведено порівняльний аналіз біометричних методів аутентифікації та знайдено найбільш оптимальний спосіб аутентифікації.
3) Розроблена система доступу з використанням системи біометричної ідентифікації та зроблено підбір оптимальної техніки для створення даної системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html
2. http://www.techportal.ru/glossary/biometricheskie-schityvateli-skud.html
3. https://www.aamsystems.ru/produkty/biometricheskie_schityvateli/
4. https://videogorod.ru/blog/sovremennye-biometricheskie-schityvateli/
5. https://txcom.ru/biometricheskiye-schityvateli
6. https://bio-smart.ru/biometricheskie-tekhnologii
7. http://new.groteck.ru/images/catalog/66267/e6b04eda0a972be4203942a39d51dfac.pdf
8. https://rep.bntu.by/bitstream/handle/data/44947/Identifikaciya_na_osnove_biometricheskih_dannyh_polzovatelej.pdf?sequence=1&isAllowed=y\
9. http://www.techportal.ru/glossary/biometriya_uha.html
10. https://worldvision.com.ua/articles/raspoznavanie-raduzhki-glaz-i-schitivanie-risunka-ven-chto-u-nih-obshchego
11. http://www.techportal.ru/glossary/kontrol-dostupa-po-risunku-ven.html
12. http://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf
13. https://thebell.io/paltsem-litsom-golosom-kak-tehnologii-identifikatsii-pomogayut-pokupat-brat-kredity-i-puteshestvovat-bez-parolej-pin-kodov-i-pasportov
14. http://www.techportal.ru/glossary/kontrol-dostupa-po-litsu.html
15. https://www.biolink.ru/technology/handwriting.php
16. https://ela.kpi.ua/bitstream/123456789/25537/1/Samoilenko_magistr.pdf
17. https://kit-e.ru/rfid/biometricheskaya-identifikacziya-po-otpechatkam-palczev-tehnologiya-fingerchip/
18. http://www.techportal.ru/glossary/kontrol-dostupa-po-raduzhnoi-obolochke-glaza.html
19. http://secuteck.ru/articles2/sys_ogr_dost/biometrich-sistema-identifikac-po-raduzhnoy-obolochke-glaza-panasonic-bm-et200-v-voprosah-i-otvetah
20. https://www.tadviser.ru/index.php/Статья:Системы_распознавания_лиц_(Facial_recognition)
21. https://www.azone-it.ru/sovremennye-metody-biometricheskoy-identifikacii#:~:text=Аутентификация%20по%20геометрии%20руки%20—%20данный,суставами%2C%20ширина%20и%20толщина%20ладони.
22. http://fingramota.by/ru/guide/practical/biometria
23. https://fincult.info/article/biometriya-chto-eto-i-kak-ona-menyaet-mir-finansov/

24. https://securitylab.com.ua/sistemy-kontrolya-dostupa/biometricheskie/schityvateli/
25. http://aiconstructor.ru/page14247059.html
26. https://ru.wikipedia.org/wiki/Аутентификация_по_сетчатке_глаза#:~:text=Аутентификация%20по%20сетчатке%20глаза%20—%20это,физиологический%20параметр%20—%20уникальность%20сетчатки%20глаза.
27. http://fingerprint.com.ua/article/schaccessterminal.htm
28. https://neolight.kiev.ua/mag-280/?gclid=CjwKCAjws8yUBhA1EiwAi_tpEfu_aY7Wz-C4RCsoI4bkCf3-x6M9ujfn4cccwpZFR1DNinELPBbFpRoClv0QAvD_BwE
29. https://nadzor.ua/product/hikvision-ds-k2801?gclid=CjwKCAjws8yUBhA1EiwAi_tpESKM4BPIhEnZz6ORMNr1bXEczcroQ8tDQeVmsXZddiYtT3ySdl3pDRoCFK0QAvD_BwE
30. https://nadzor.ua/product/hikvision-ds-k1200ef?gclid=CjwKCAjws8yUBhA1EiwAi_tpEVIbNVMhvPHx8zNWO5haKu7sef3R5RNLxJj8WlSyQO1kX746lVNzuRoCsnkQAvD_BwE
31. https://rozetka.com.ua/ua/tyto_ds264232/p216376015/
32. https://komplektservice.com.ua/dovodchiki/geze/dvernoy-dovodchik-geze-ts-1000/
33. https://secur.ua/datchik-otkrytija-magnitokontaktnyj-satel-b-3-a.html?gclid=Cj0KCQjw1tGUBhDXARIsAIJx01nlOfHDArr4CUviYjMF2ejOuAV6DgcAVwFQfzy1_vmTzcz_Ez0XtKcaAoxwEALw_wcB
34. https://uawest.com/usb-rs485-konverter.html?gclid=Cj0KCQjw1tGUBhDXARIsAIJx01k4ShgR4IBaIru9-Ai8ufnMGoO8q-4ECypbGgYcPJPRyf4txvGBYQcaAkFoEALw_wcB
35. https://www.forter.com.ua/aksessuary-alarm/altronics-sr-03/?gclid=Cj0KCQjw1tGUBhDXARIsAIJx01knzQSsroq34LQogh3cxEm9ZyUR77_5K9ueoLo7kBeJaVA91zR9GV4aAvakEALw_wcB
36. https://hard.kiev.ua/server-hp-proliant-dl80-gen9-12-lff-2u/#characteristics
37. Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. Руководство по биометрии. — М.: Техносфера, 2007. — С. 20 - 63. — 368 с. — ISBN 978-5-94836-109-3.
38. Алексеев В.Н., Астахов Ю.С., Басинский С.Н. Глава 2. Анатомия органа зрения // Офтальмология: Учебник для студ. мед. вузов / Е.А.Егоров. — М.: ГЭОТАР-Медиа, 2008. — С. 12 - 29. — 240 с.