МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра комп'ютерної інженерії

ДОПУЩЕНО ДО ЗАХИСТУ
Завідувач кафедри,
канд. техн.наук, доцент
_____ Я. М.Крайник
« __ » _____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

« Вбудована система двофакторної ідентифікації користувача лабораторного устаткування»

Спеціальність 123 Комп'ютерна інженерія

123 – КР.1 – 405з21920504

Студент _____ Решетняк О.Є.
підпис

«__»_____2022р.

Керівник ст. викладач _____Старченко В.В.
підпис

«__»_____2022р.

Миколаїв 2022

ЗАВДАННЯ

на виконання бакалаврської роботи

НЕ ВИДАЛЯТИ цю СТОРІНКУ з файлу !!!!!!!!!!!!!!!!!!

ЗАРЕЗЕРВОВАНА Сторінка 1

ця сторінка після друку буде замінена

ЗАВДАННЯ

на виконання бакалаврської роботи

НЕ ВИДАЛЯТИ цю СТОРІНКУ з файлу !!!!!!!!!!!!!!!!!!

ЗАРЕЗЕРВОВАНА Сторінка 2

ця сторінка після друку буде замінена

АНОТАЦІЯ

Актуальність: Під час роботи у дослідницькій лабораторії часто виникають питання збереження комерційної таємниці, підтвердження кваліфікації персоналу, дотримання техніки безпеки, тощо. Для вирішення таких питань використовується різноманітні системи допуску та ідентифікації співробітників. Однак традиційні системи, що використовують лише один фактор для ідентифікації легко можуть бути подолані. Тому з плином часу все більше поширення набувають системи багатофакторної ідентифікації користувачів. Такі системи використовують для ідентифікації одночасно декілька факторів і подолати їх значно складніше.

Цифрове забезпечення покращується кожного дня і можливості його використання стають все більш всеохоплюючими та необмеженими. Використовуючи різноманітні сервіси, програми, сайти, додатки, користовучі створюють персональні кабінети для ідентифікування особи, можливості використання потрібного забезпечення та збереження персональних даних. Для ідентифікації користовуча завжди створюються логін та пароль для входу, які зберігаються в пам’яті сервіса, який використовується для повторного використання на сайті, у програмі, тощо.

В свою чергу, користувач повинен запам’ятовувати чи записувати ці данні для використання свого аккаунту на конкретній платформі. Бувають випадки втрати паролів або навіть втрати доступу до особистого кабінету користувача.

Основними недоліками зберігання паролів є можливість їх втратити. Для зберження паролів та подальшого їх застосування використовуються різні способи збереження паролів: на комп'ютері, телефоні, у спеціальних програмах,на папері, у голові.

Одні з них більш безпечні чи практичні, інші меньш практичні,

безпечніше всього використовувати спеціальні менеджери паролів, але всі вони мають свої недоліки.

Мета: Розробка впровадження методів багатофакторної автентифікації.

Завдання:

1. провести аналіз рішень, що існують для систем двофакторної ідентифікації користувача лабораторного устаткування;
2. за результатами аналітичного огляду літератури та патентної інформації визначити склад та загальне компонування системи;
3. розробити інформаційну модель системи;
4. визначити зовнішні та внутрішні протоколи та інтерфейси системи;
5. оглянути наявну компонентну базу та обрати необхідні компоненти для побудови прототипу системи;
6. розробити прототип апаратно-програмного комплексу для двофакторної ідентифікації користувача лабораторного устаткування;
7. розробити алгоритми роботи системи, навести блок-схему та дати їх опис.
8. розробити програмне забезпечення мікроконтролера апаратно- програмного комплексу для системи двофакторної ідентифікації користувача лабораторного устаткування.

Об'єкт: Промислові системи багатофакторної ідентифікації персоналу.

Предмет: Промислові системи багатофакторної ідентифікації персоналу.

Методи дослідження: Під час виконання дипломної роботи були використані методи математичної статистики, технічного моделювання та проектування, а також програмування для вбудованих мікроконтролерних систем.

Наукова новизна: Система з можливістю гнучкої генерації даних для збереження за допомогою спеціального алгоритму шифрування.

Практичне значення: На основі розробленого прототипу системи багатофакторної ідентифікації користувача лабораторного устаткування може бути побудований конкурентоспроможний промисловий зразок.

Ключові слова: сенсор, спектр, система допуску.

ABSTRACT

Relevance: While working in a research laboratory, there are often questions about trade secrets, confirmation of staff qualifications, compliance with safety, etc. Various systems of admission and identification of employees are used to address such issues. However, traditional systems that use only one factor for identification can easily be overcome. Therefore, over time, multi-factor user identification systems are becoming more widespread. Such systems use several factors to identify at the same time and are much more difficult to overcome.

Digital security is improving every day and the possibilities of its use are becoming more comprehensive and unlimited. Using a variety of services, programs, sites, and applications, users create personal accounts to identify the person, and the ability to use the necessary software and store personal data. To identify the user, a login and login password are always created, which are stored in the memory of the service, which is used for reuse on the site, in the program, etc. In turn, the user must remember or record this data to use their account on a particular platform. There are cases of loss of passwords or even loss of access to the user's account.

The main disadvantages of storing passwords are the possibility of losing them. To save passwords and their subsequent use, different ways of saving passwords are used: on a computer, phone, in special programs, on paper, in the head. Some of them are more secure or practical, others are less practical, and it is safest to use special password managers, but they all have their drawbacks.

Objective: Development of implementation of multifactor authentication methods.

Task:

1. to analyze the solutions that exist for two-factor identification systems for users of laboratory equipment;

2. based on the results of the analytical review of the literature and patent information to determine the composition and general layout of the system;

3. develop an information model of the system;

4. define external and internal protocols and interfaces of the system;

5. inspect the existing component base and select the necessary components to build a prototype system;

6. to develop a prototype of a hardware-software complex for two-factor identification of the user of laboratory equipment;

7. develop algorithms for system operation, provide a block diagram and describe them.

8. to develop the software of the microcontroller of the hardware-software complex for the system of two-factor identification of the user of the laboratory equipment.

Object: Industrial systems of multifactor personnel identification. Subject: Industrial systems of multifactor identification of personnel.

Research methods: During the thesis methods of mathematical statistics, technical modeling and design, as well as programming for embedded microcontroller systems were used.

Scientific novelty: A system with the ability to flexibly generate data for storage using a special encryption algorithm.

Practical value: Based on the developed prototype of the system of multifactor identification of the user of the laboratory equipment a competitive industrial design can be constructed.

Keywords: sensor, spectrum, tolerance system.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AFIS - Automatic Fingerprint Identification System

РОО - Райдужна оболонка ока

СКУД - Система контрольованого управління доступом.

RFID - Radio frequency Identification (Радіочастотна ідентифікація)

USB – Universal serial bus (Універсальна послідовна шина)

RS232, UART – послідовний інтерфейс комп'ютера та мікроконтролера

ID - Identificational data (Ідентифікаційні дані)

DSP - Digital signal processing (Цифровий сигнальний процессор)

АКБ - Акумуляторна батарея

AC - Alternating Current (Змінний струм)

DC - Direct Current (Постійний струм)

SPI - Serial Peripheral Interface (Послідовний периферійний інтерфейс)

ЕРС - Електрорушійна сила

ВСТУП

Під час роботи у дослідницькій лабораторії часто виникають питання збереження комерційної таємниці, підтвердження кваліфікації персоналу, дотримання техніки безпеки, тощо. Для вирішення таких питань використовується різноманітні системи допуску та ідентифікації співробітників. Однак традиційні системи, що використовують лише один фактор для ідентифікації легко можуть бути подолані. Тому з плином часу все більше поширення набувають системи багатофакторної ідентифікації користувачів. Такі системи використовують для ідентифікації одночасно декілька факторів і подолати їх значно складніше.

Цифрове забезпечення покращується кожного дня і можливості його використання стають все більш всеохоплюючими та необмеженими. Використовуючи різноманітні сервіси, програми, сайти, додатки, користовучі створюють персональні кабінети для ідентифікування особи, можливості використання потрібного забезпечення та збереження персональних даних. Для ідентифікації користовуча завжди створюються логін та пароль для входу, які зберігаються в пам'яті сервіса, який використовується для повторного використання на сайті, у програмі, тощо.

В свою чергу, користувач повинен запам'ятовувати чи записувати ці данні для використання свого аккаунту на конкретній платформі.

Мета: Розробка впровадження методів багатофакторної автентифікації.

Завдання:

9. провести аналіз рішень, що існують для систем двофакторної ідентифікації користувача лабораторного устаткування;
10. за результатами аналітичного огляду літератури та патентної інформації визначити склад та загальне компонування системи;
11. розробити інформаційну модель системи;

12. визначити зовнішні та внутрішні протоколи та інтерфейси системи;
13. оглянути наявну компонентну базу та обрати необхідні компоненти для побудови прототипу системи;
14. розробити прототип апаратно-програмного комплексу для двофакторної ідентифікації користувача лабораторного устаткування;
15. розробити алгоритми роботи системи, навести блок-схему та дати їх опис.
16. розробити програмне забезпечення мікроконтролера апаратно- програмного комплексу для системи двофакторної ідентифікації користувача лабораторного устаткування.

Об'єкт: Промислові системи багатофакторної ідентифікації персоналу.

Предмет: Промислові системи багатофакторної ідентифікації персоналу.

Методи дослідження: Під час виконання дипломної роботи були використані методи математичної статистики, технічного моделювання та проектування, а також програмування для вбудованих мікроконтролерних систем.

Наукова новизна: Система з можливістю гнучкої генерації даних для збереження за допомогою спеціального алгоритму шифрування.

Практичне значення: На основі розробленого прототипу системи багатофакторної ідентифікації користувача лабораторного устаткування може бути побудований конкурентоспроможний промисловий зразок.

Ключові слова: сенсор, спектр, система допуску.

Розділ 1

АНАЛІТИЧНИЙ ОГЛЯД

Важливим елементом забезпечення цілісності конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та автентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання користувач або отримує доступ до певних ресурсів інформаційної системи, або не отримує.

Ідентифікація – процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається системою. Вона є початковою процедурою надання доступу до системи, після неї здійснюється автентифікація та авторизація.

Автентифікація – це процедура перевірки належності ідентифікатора об'єкту, тобто встановлення чи підтвердження дійсності, і перевірка чи є об'єкт або суб'єкт, що перевіряється, справді тим, за кого він себе видає.

Останнім часом все частіше застосовується, так звана, розширена або багатофакторна автентифікація. Вона побудована на спільному використанні декількох факторів автентифікації. Це значно підвищує захищеність системи.

Сучасні методи ідентифікації особи не спроможні забезпечити необхідний рівень надійності. Одним із можливих рішень цієї проблеми є застосування біометричних технологій для ідентифікації особи. Біометричні технології, на відміну від парольної ідентифікації, є більш надійними та дозволяють значно підвищити певність процесу ідентифікації особи, для них вже створена розвинена база технічних рішень. Звідси можна зробити

висновок, що в інфокомунікаційних мережах процес ідентифікації особи буде реалізовуватися саме на базі біометричних технологій.

Є дев’ять рівнів біометричної ідентифікації:

- ✓ ідентифікація за допомогою відбитків пальців;
- ✓ ідентифікація на основі параметрів геометрії ока;
- ✓ ідентифікація за допомогою голосу;
- ✓ ідентифікація за параметрами обличчя;
- ✓ ідентифікація за параметрами вуха;
- ✓ ідентифікація з рукописним почерком;
- ✓ ідентифікація з клавіатурним почерком;
- ✓ ідентифікація за геометрією долоні;
- ✓ ідентифікація за ДНК.

1.1 БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ ЗА ДОПОМОГОЮ ВІДБИТКІВ ПАЛЬЦІВ

1.1.1 Характеристика відбитків пальців

Як уже зазначалось, ідентифікація за відбитками пальців застосовується досить давно, тому вже існує відповідна їх класифікація відбитків пальців. Кожний відбиток унікальний сам по собі, не існує двох однакових відбитків, проте кожний відбиток має певні ознаки, за допомогою яких і проводить ідентифікацію. Звичайно ці ознаки поділяють на дві групи – *локальні* та *глобальні*.

Глобальні ознаки – це ознаки, які можна побачити очима, до них відносяться:

- папілярний узор;
- область зразка – відокремлений фрагмент відбитка, в якому локалізовано всі ознаки;
- ядро – точка локалізована у середині відбитку або в деякій відокремленій області;
- дельта (або дуга) – початкова точка, місце, в якому починається розділення або поєднання папілярних ліній;
- тип ліній – дві найбільші лінії, які розпочинаються як паралельні, а потім розходяться й оминають усю область образу;
- лічильник ліній – число ліній на області образу, або між ядром та дельтою.

Проте глобальні ознаки не дають можливості провести стовідсоткову ідентифікацію. Більш важливими для ідентифікації є локальні ознаки. Локальні ознаки або мінуції – це ознаки, які унікальні для кожного відбитка. Ці ознаки визначають пункти зміни папілярних ліній, такі як роздвоєння або розрив, орієнтація папілярних ліній.

Ці дві локальні ознаки є основними і найбільш частіше за все використовуються, на рис. 1.1 показано кінцеві точки та точки розгалуження.

Крім цих двох локальних ознак досить часто використовують ще декілька:

гребінь – це коли лінія відбитка піднімається уверх, створюючи бугорок;

боріздка – жолоб між гребнями;

дельта – місце, де гребінь поділяється на три лінії;

центр – точка найбільшої кривизни гребня.

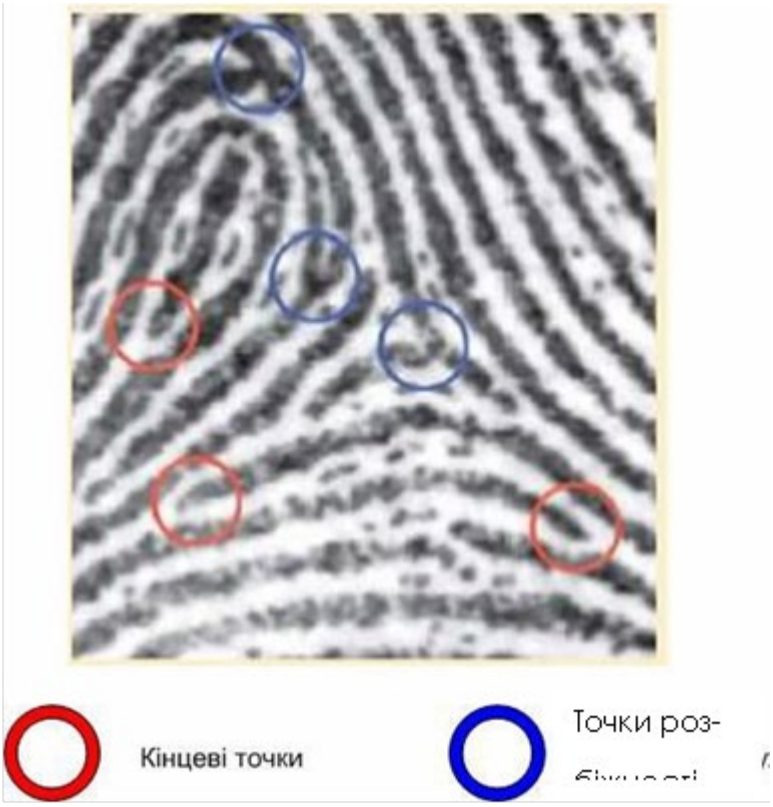


Рисунок 1.1 – Кінцеві точки та точки розгалуження

На рис. 1.2 показано відбиток пальців з наявними на ньому усіма можливими локальними ознаками.

Отже, розпізнавання відбитків пальців здійснюється за допомогою локальних (в першу чергу) та глобальних ознак. Як показує досвід, відбитки пальців різних осіб можуть мати однакові глобальні ознаки і різні локальні. Тому глобальні ознаки використовують для розподілу відбитків на класи, а локальні вже безпосередньо для ідентифікації особи.

Рисунок 1.2 – Локальні ознаки відбитків пальців

1.1.2. Класифікація відбитків пальців

Класифікація відбитків пальців – це метод, який дозволяє віднести відбиток пальця до одного з заздалегідь сформованих класів на основі його ознак, якізможуть забезпечити подальший механізм ідентифікації. Класична системакласифікації відбитків була запропонована фахівцями криміналістики. Спираючись на глобальні ознаки, властиві відбиткам пальців, було проведено їхню класифікацію. Класифікація проводилася за типом папілярного узору, всього існує три основних класи відбитків пальців:

- дугові – у такому узорі звичайно відсутня дельта і він утворюєтьсядвома потоками (лініями);
- петльові – розрізняють за напрямом ніжок петлі та її формою;
- завиткові – бувають прості (колові, овальні, спіральні) та складні.

За існуючими даним близько 5 % усіх відбитків відносяться до дугових, 65 % до петльових та 35 % до завиткових. Кожний з цих трьох класів має декілька підкласів. На рис. 1.3 показані відбитки усіх трьох класів.

Рисунок 1.3 – Три основні класи відбитків пальців

У кожного з трьох основних класів існує декілька підкласів, проте слід за- значити, що найчастіше використовують підкласи:

– права петля;
– ліва петля;
– подвійна петля;
– напівсфера.

Всі ці підкласи відносяться до найбільш розповсюдженого петльового класу. Подібна класифікація використовується у криміналістиці. Коли виникла ідея використовувати ідентифікацію за відбитками пальців в інформаційних системах та системах автоматизації подібна класифікація виявилась надто складною. Тому для інформаційних систем та систем автоматизації було запропоновано наступний спосіб класифікації – усі відбитки поділяються на п’ять класів: W (це подвійна петля та завиткові узори); R (права петля); L (ліва петля); A (дуга); T (напівсфера). Саме ці 5 класів використовуються для створення систем біометричної ідентифікації за відбитками пальців. На рис. 1.4 показано приклад відповідних відбитків пальців.

Слід зазначити, що зображення відбитків пальців повинно також відповідати деяким стандартам. Переважно це стандарти ANSI. Вони висувають на- ступні вимоги до зображення відбитка:

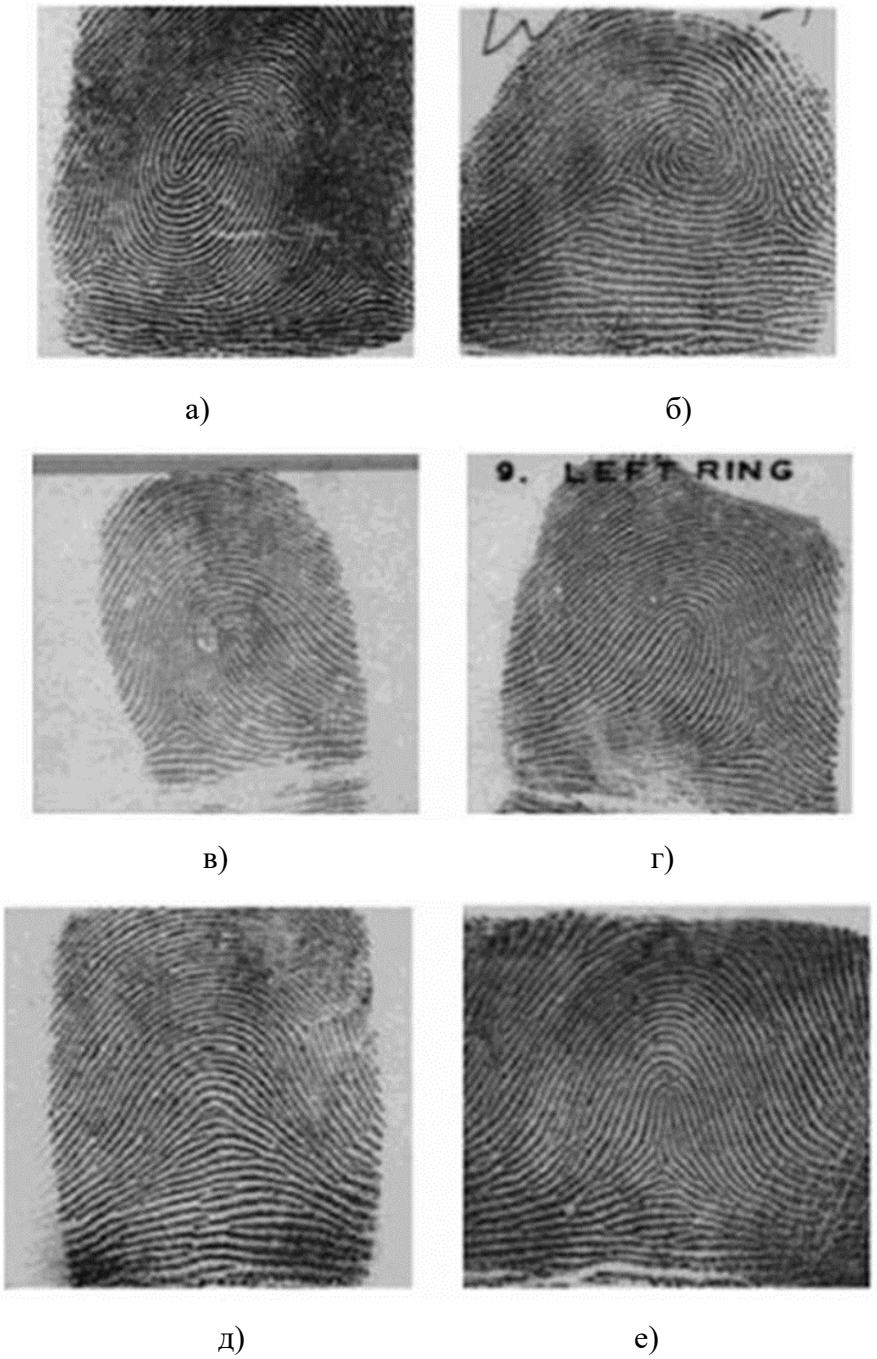
відбитки повинні бути надані у форматі TIFS;

зображення відбитків повинно мати дозвіл не менше 500 пікселів на дюйм;

образ повинен бути напівтоновим з 256 рівнями яскравості;

мінімальний кут відбитка відносно вертикальної осі – 15 градусів;

основні типи локальних ознак – це кінцеві точки та точки розбіжності.



а) б) в) г) д) е)

а) подвійна петля – W; б) завиток – W; в) права петля – R; г) ліва петля – L; д) дуга – A і е) на півсфера – T;

Рисунок 1.4 – Основні класи відбитків пальців, які використовуються в інформаційних системах

1.1.3 Методи та класифікатори автоматизованої класифікації відбитків пальців

Автоматизація класифікації відбитків пальців є досить складною проблемою, тому що незначні відміни у середині класу та значні відміни між класами необхідно дуже чітко враховувати. Як уже зазначалось, для автоматизованої класифікації використовується лише п’яти класів відбитків. Сам процес класифікації полягає у наступному – спочатку відбиток на основі відповідних ознак відноситься до одного з класів, а потім за локальними ознаками здійснюється порівняння відбитка з відбитками, які є у базі даних, поки не буде знайдено відповідність. Зараз існує декілька підходів до автоматичної класифікації, усі ці підходи поділено на п’ять категорій:

1.На основі моделі – цей підхід заснований на використанні моделі розташування особливих точок (ядер та розбіжностей). Цей підхід використовує знання людини-експерта, він застосовує правила для класифікації відбитків на базі створеної вручну моделі, тому потребує вивчення.

2.На основі структури – цей підхід використовує оцінку орієнтаційного поля на відбитку, для того щоб віднести його до відповідного класу, безпосередня класифікація відбувається на основі нейронної мережі.

3.На основі частоти – даний підхід використовує спектр частот відбитків пальців та ряди Фур’є для проведення класифікації.

4.Синтаксичний підхід – використовує формальну граматику для подання та класифікації відбитків пальців.

5.Гібридні підходи – використовують комбінацію двох або більше підходів для проведення класифікації відбитків пальців. Найбільш перспективний серед цих підходів багатоканальний підхід.

Кожен із цих підходів здійснює класифікацію відбитків спираючись на спеціальну методологію, яка називається класифікатор. Класифікатор

визначає яким чином буде встановлюватися приналежність відбитка до того чи іншого класу. Існує декілька видів класифікаторів:

- класифікатор "К-найближчий";
- класифікатор нейронна мережа;
- двоетапний класифікатор;
- класифікатор на основі прихованої моделі Маркова;
- класифікатор на основі «дерева рішень»;
- гібридні класифікатори. Класифікатор "К-найближчий"

Класифікатор нейронна мережа

У даному випадку для класифікації використовується багатошарова (багаторівнева) нейронна мережа з прямим розповсюдженням та алгоритмом навчання швидкого розповсюдження. Нейронна мережа має один прихований прошарок з 20 нейронами, 192 нейронами вхідних та 5 нейронами вихідних, які відповідають п'яти класам відбитків пальців. Точність класифікаціє сягає 86,4 %.

Класифікатор на основі прихованої моделі Маркова (ПММ)

Приховані моделі Маркова (ПММ) – це форма стохастичного кінцевого автомата стана, які використовуються для розпізнавання образи моделі, якіі здатні класифікувати дані, засновані на значній кількості ознак, число яких є змінним і має певні типи основної структури. У відбитку пальця, основна інформація класу може бути виведена з синтаксичного аналізу особливих точок, або може застосовувати статичне моделювання структури зразка. В загальному випадку спочатку відбувається виділення виступів (або виступу) на зображенні відбитка. Для цього існує декілька різних способів. Потім для виділеного виступу відбувається виділення ознак. ПММ може статистично моделювати різні структури зразків виступів по цілому відбитку.

Далі створюється ПММ двовимірної структури, бо дані про ознаки є двовимірним масивом. Причому для кожного з п'яти класів створюється своя окрема ПММ. Після чого здійснюється порівняння масиву виділених ознак з ПММ і приймається рішення до якого класу віднести відбиток пальця.

Класифікатор *«дерева рішень»*

Рисунок 1.5 – Приклад виділення ознак для «дерева рішень»

В даному випадку для класифікації відбитка пальця спочатку відбувається виділення характерних ознак відбитка пальця (рис. 1.5), а потім створюється ієрархічне «дерево питань». Ці питання об'єднані в ієрархічній манері і формують «дерево рішення», які використовуються для класифікації. До ознак у даному випадку відносять кривизну та точки повороту верхні, нижні, ліві та праві.

Питання для створення «дерева рішень» – є логічними думками про ознаки, які можуть бути присутні на відбитку пальця. Відповідь на питання – це або істина, або неправда. Відповідно кожне питання породжує розбіжність, тобто тестовий зразок відбитка пройшовши усе дерево досягає кінцевої точки, які відмічені відповідно до класів відбитків. Питання являють собою інформацію про відношення між ознаками відбитка, які були виділені. Відношення між ознаками задається напрямом. Через те, що класичні напрями верх, низ, вправо та вліво виступають в ролі ознак, то при побудові питання використовують як напрями південь, північ, схід та захід. Північ відповідає напряму пересування вверх, південь – вниз, схід – вправо, а захід – вліво. Перше питання формується наступним чином – випадковим способом обирається одна з ознак відбитка і формується питання її розташування відносно напряму.

Приклад створення «дерева рішень» показано на рис. 1.6.

Двоетапний класифікатор

Цей класифікатор застосовується досить часто. Основна ідея полягає в наступному. Спочатку здійснюється класифікація за допомогою

"К– найближчого" класифікатора, а потім отриманий результат уточнюється за допомогою нейронної мережі.

Рисунок 1.6 – Приклад формування «дерева рішень»

Перша стадія використовує класифікатор "К–найближчий" (K = 10), за допомогою цього класифікатора отримується два класи, які володіють найбільшою ймовірністю того, що відбиток відноситься до цих класів. Тобто ми отримуємо два класи з п'яти до яких імовірно може відноситися відбиток. Далі для подальшої класифікації застосовується 10 нейронних мереж (з п'яти класів можна скласти 10 комбінацій по два класи). Кожна з 10 нейронних мереж має 192 нейрона входу, 20-40 прихованих нейронів та 2 нейрона виходу. Спираючись на внутрішню навчальну множину, нейронні мережі також визначають два класи, до яких найбільш імовірно відноситься відбиток пальця. Після чого результати двох порівнянь мультиплексуються та отримується кінцевий результат класифікації. У даному випадку ймовірність правильної класифікації становить 95 %.

На рис. 1.7 надана схема функціонування двоетапного класифікатора.

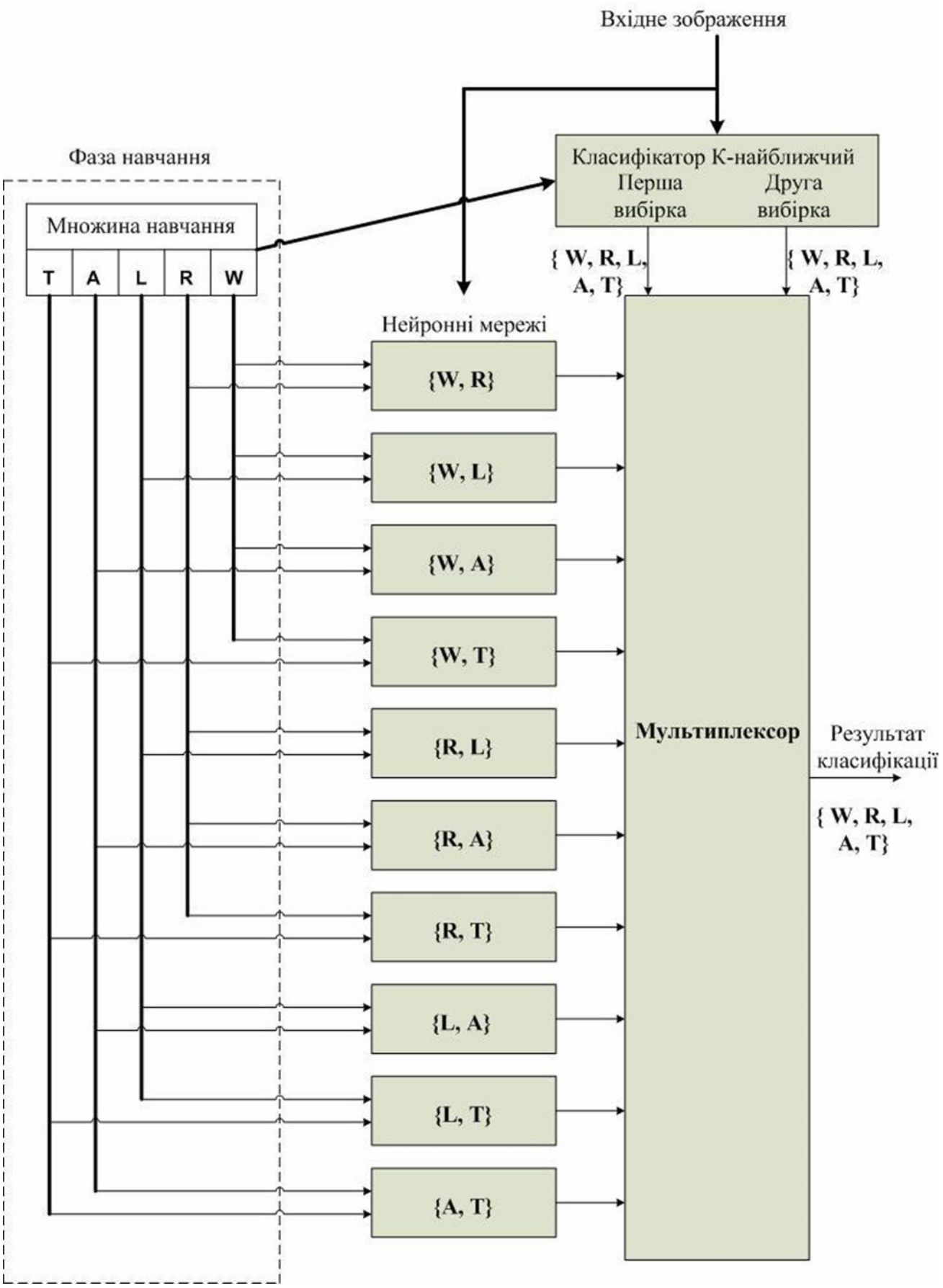


Рисунок 1.7 – Схема двоетапного класифікатора

1.1.4 Алгоритми ідентифікації відбитків у рамках обраного класу

Після того як відбиток пальця віднесено до відповідного класу, необхідно провести ідентифікацію у рамках обраного класу, тобто встановити особу, якій належить цей відбиток. Ця процедура здійснюється алгоритмами ідентифікації. На сьогодні існує декілька найбільш популярних алгоритмів ідентифікації за відбитками. До них відносяться:

- кореляційне порівняння;
- порівняння за особливими точками;
- порівняння за узором;
- порівняння за шаблоном;
- порівняння на основі графів.

Суть методу полягає в наступному. Отриманий відбиток пальця накладається на кожен еталон з бази даних по черзі, після чого безпосередньо за пікселями зображень здійснюється прорахунок відмінностей між ними. Проте слід враховувати одну особливість даного методу. Людина кожний раз може прикладати палець до сканера під різними кутами, а це означає, що отриманий відбиток буде відрізнятися від оригіналу.

Отже, процес порівняння відбитка її пальця з еталонами повинен включати безліч ітерацій, на кожній з яких зображення, отримане зі сканера, повертається під невеликим кутом або трохи зміщується.

Таким чином, підраховується кореляція (за рівнем інтенсивності) між відповідними пікселями, обчислена для різних вирівнювань зображень один відносно одного (наприклад, шляхом різних зсувів та поворотів), а потім за відповідним коефіцієнтом приймається рішення про ідентичність відбитків.

Порівняння за особливими точками

У цьому алгоритмі на базі одного або декількох зображень відбитка пальця зі сканера формується шаблон (карта), який є двовимірною поверхнею, на якій виділені кінцеві точки та точки розбіжності. Процедура порівняння полягає в тому, що на наданому зображенні відбитка виділяються особливі точки, складається тимчасова карта цих точок, яка порівнюється з шаблоном і

закількістю точок, що збіглися, приймається рішення з ідентичності відбитків. Результатом порівняння, як правило, є набір ключових точок. Потім використовується поріг, що визначає, наскільки великим має бути це число, щоб було можливо порівняти відбиток пальця з шаблоном. У роботі алгоритмів даного класу реалізуються механізми кореляційного порівняння, але при порівнянні розташування кожної з можливо відповідних одна одній точок. Даний алгоритм поділяється на декілька етапів:

- ✓ покращення якості вихідного зображення відбитка, тобто підвищується чіткість та різкість меж папілярних ліній;
- ✓ розрахунок поля орієнтації папілярних ліній відбитка, тобто зображення розбивається на квадратні блоки зі стороною понад 4 пікселів і за градієнтами яскравості обчислюється кут орієнтації ліній для фрагмента відбитка;
- ✓ бінаризація зображення відбитка, тобто приведення до чорно-білого зображення (1 bit) з пороговим обробленням;
- ✓ стоншення ліній зображення відбитка, тобто необхідно отримати товщину ліній 1 піксель;
- ✓ отримання деталей – зображення розбивається на блоки 9×9 пікселів у яких знаходяться локальні ознаки – кінцеві точки та точки розбіжності. Для цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центра.

Піксель у центрі вважається деталлю, якщо він сам ненульовий, і сусідніх ненульових пікселів один (кінцева точка) або два (точка розгалуження). На рис. 1.8 показано процес отримання деталей відбитка пальця.

Координати виявлених деталей та їх кути орієнтації записуються у вектор:

$$W(p) = [(x1, y1, \ldots\theta1), (x2, y2, \ldots\theta2), \ldots (xp, yp, \ldots\theta p)], \qquad (3.1)$$

де p – число деталей. При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає поточний відбиток.

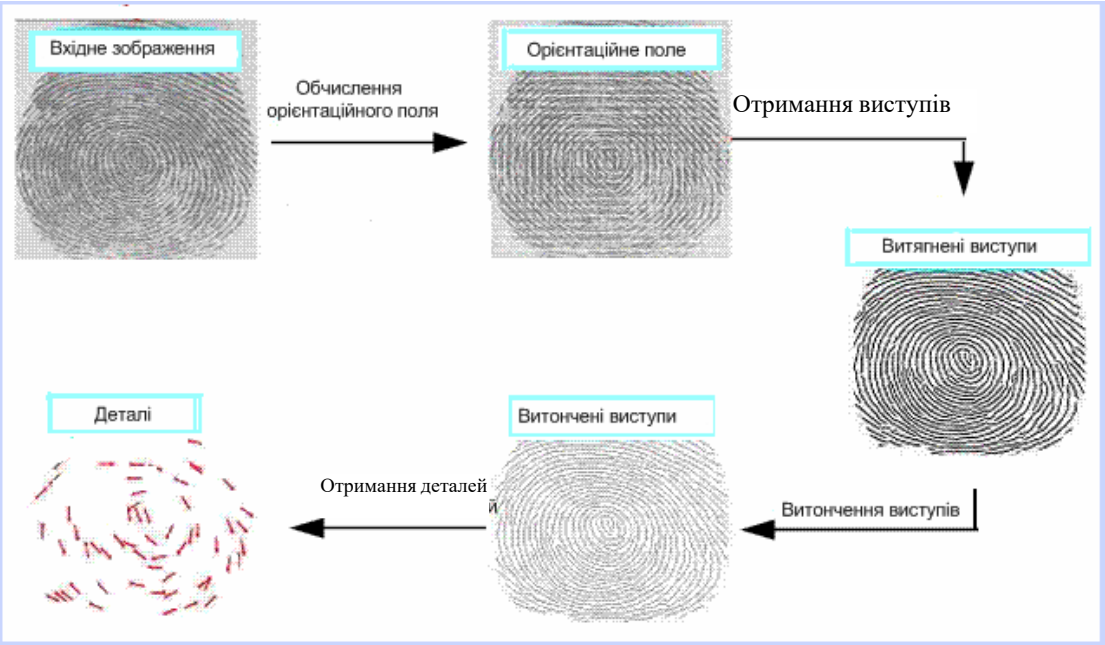


Рисунок 1.8 – Процес отримання деталей відбитка пальця

Після отримання деталей відбувається порівняння деталей. Два відбитки одного пальця відрізнятимуться один від одного поворотом, зсувом, зміною масштабу і площею зіткнення залежно від того, як користувач прикладає палець до сканера. Тому не можна сказати, чи належить відбиток людині чи ні на підставі простого їх порівняння (вектори еталона і поточного відбитка можуть відрізнятися за довжиною, мати невідповідні деталі тощо). Через це процес порівняння має бути реалізований для кожної деталі окремо і включати наступні етапи порівняння:

– реєстрація даних. Визначаються параметри афінних перетворень (кут повороту, масштаб та зсув), за яких деяка деталь з одного вектора відповідає деякій деталі з іншого;
– пошук пар відповідних деталей. При пошуку для кожної деталі потрібно перебрати до 30 значень повороту (від –15 градусів до +15), 500 значень зсуву (від –250 пікселів до +250 пікселів) і 10 значень масштабу (від 0,5 до 1,5 з кроком 0,1). Разом до 150 000 кроків для кожної з 70 можливих деталей;
– оцінка відповідності відбитків. Оцінка відповідності відбитків виконується за формулою:

$$K = (D*D*100\%)/(p*q), \quad (3.2)$$

де D – кількість деталей, що збіглися; p – кількість деталей еталона; q –кількість деталей відбитка, що ідентифікується). У випадку, якщо результат перевищує 65 %, відбитки вважаються ідентичними (поріг може бути збільшено виставлянням іншого рівня пильності).

Приклад порівняння деталей між введеним і шаблонним зображеннями відбитків пальців показаний на рис. 1.9.

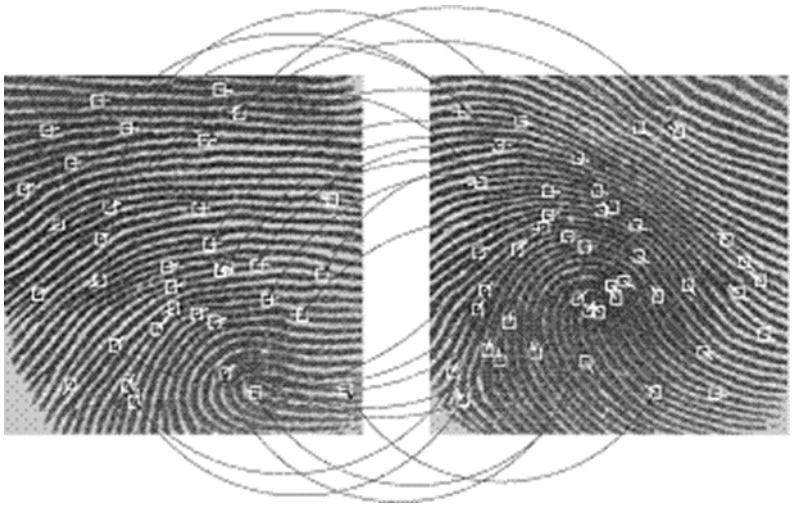


Рисунок 1.9 – Приклад порівнянн деталей

Якщо виконувалася аутентифікація, то на цьому все і закінчується. Для ідентифікації необхідно повторити цей процес для всіх відбитків, що знаходяться в базі даних. Потім вибирається користувач, у якого найбільший рівень відповідності (зрозуміло, його результат має бути вище за поріг 65%). Головною перевагою алгоритму порівняння відбитків пальців за особливими точками є швидкість його роботи. Більше всього часу в процесі ідентифікації займає перебір еталонів у пошуку відбитка, ідентичного тимчасовому. Проте набагато простіше і швидше порівняти декілька десятків окремих точок, ніж ціле зображення. Тим більше, що в цьому випадку використовуються спеціальні алгоритми кореляційного порівняння.

Вони враховують положення ймовірно точок, що збігаються, для повороту або зсуву тимчасової карти. А це дозволяє ще більше прискорити процес ідентифікації. До достоїнств можна також віднести те, що метод є досить

відомим і добре дослідженим. Тому через простоту реалізації і швидкості роботи – алгоритми даного класу є найбільш поширеними.

До недоліків слід віднести високі вимоги до якості зображення папілярного узору (дозволу) і розмірів чутливого датчика. Для їх задоволення сканер повинен забезпечувати дозвіл не менше 500 пікселів.

Порівняння за узором

У даному випадку для порівняння використовуються безпосередньо особливості папілярного узору пальця. Отримане зображення відбитка пальця поділяється на безліч малих комірок (розмір комірки залежить від вимог точності). Розташування ліній у кожній комірці описується параметрами деякої синусоїдальної хвилі, тобто задається початковий зсув фази, довжина хвилі та напрям її поширення. Отриманий відбиток вирівнюється и приводиться до того ж виду що й шаблон.

Спеціальний модуль розглядає папілярні лінії у комірках по черзі і кожну з них описує рівнянням синусоїдальної хвилі, тобто визначає початковий зсув фази, довжину хвилі та напрям її поширення. А саме, ці параметри використовуються для порівняння з відбитком пальця, що зберігається у базі. Порівняння відбувається покомірково.

На рис. 1.10 показано приклад розбиття відбитка пальця на комірки.

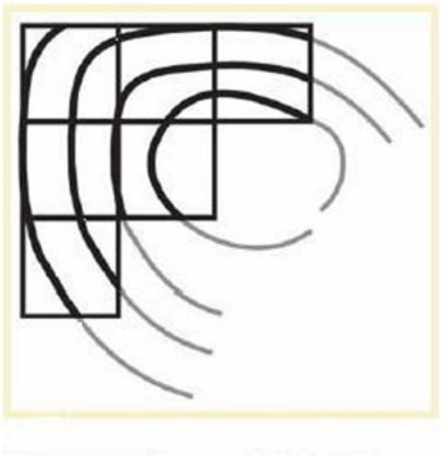


Рисунок 1.10 – Розбиття папілярного узору пальця на комірки

Основними перевагами цього алгоритму є досить висока швидкість роботи та низькі вимоги до якості зображення відбитка пальця. Проте цей алгоритм не надто поширений через те, що для його реалізації потребується досить складний математичний апарат.

Порівняння за шаблоном

У цьому алгоритмі до уваги беруться не тільки окремі точки, а й загальна характеристика відбитка пальця, яка може включати до себе відповідний відсоток додаткових даних, наприклад, товщину ліній папілярного узору, їхню щільність та кривизну. Під час роботи даний алгоритм визначає наявність додаткових ознак відбитка замість реєстрації ключових точок. Невеликі частини відбитка і відстань між ними виділяється з відбитка з метою максимально збільшити кількість унікальної інформації.

Найбільш важливі ділянки навколо ключових точок та ділянки з невеликим радіусом вигину.

Процес ідентифікації розпочинається з попереднього оброблення відбитка пальця. Спочатку отримане зображення відбитка порівнюється із шаблоном з бази, щоб визначити наскільки він з ним збігається. Поріг, який описує найменше відхилення яке можливо, використовується для визначення ступеня відповідності відбитка із шаблоном з бази.

Основною перевагою цього алгоритму є те, що він може працювати з будь-якими типами сканерів відбитків та з будь-якою якістю зображення відбитка пальця. А недоліком – що цей алгоритм досить погано працює з так званим багатоканальним пошуком.

Порівняння на основі графів

У даному алгоритмі зображення відбитка пальця спочатку збільшується, потім виділяється орієнтація папілярних ліній. Потім увесь відбиток поділяється на області, які мають однакову орієнтацію папілярних ліній. Після цього в кожній області виділяють центр, після чого центри суміжних областей з'єднуються між собою, внаслідок чого отримуємо граф. Отриманий граф

порівнюється з еталонними графами з бази даних, поки не буде встановлено ідентифікацію особи. Даний алгоритм відносно простий, дуже швидко працює і тому він також є одним із найпоширених алгоритмів. На рис 1.11 надано приклад роботи цього алгоритму.

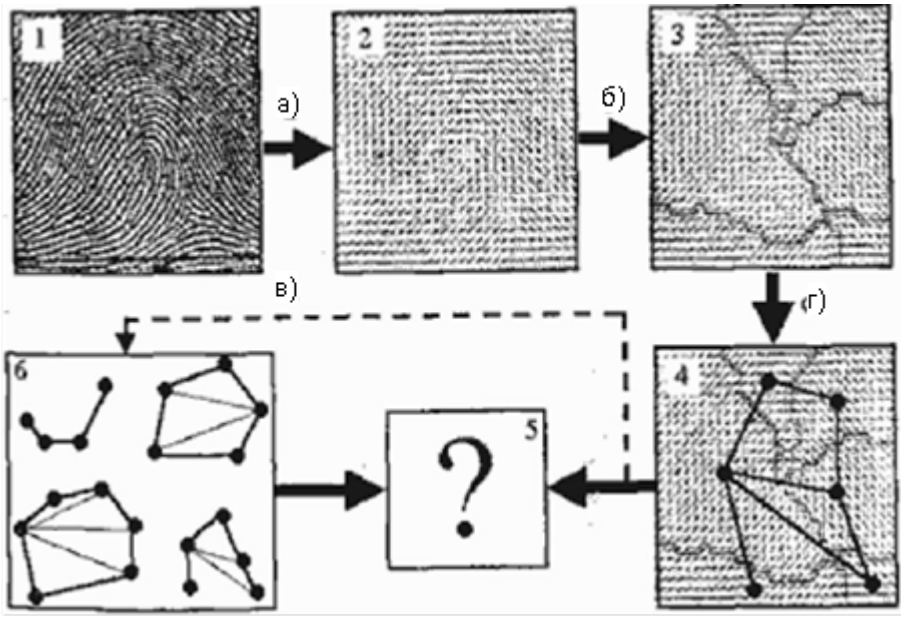


Рисунок 1.11 – Принцип порівняння на основі графів

Як видно з рис. 3.11, спочатку ми отримуємо орієнтаційне поле, потім поділяємо його на області, які мають у середині однакову орієнтацію. Далі в кожній області знаходимо центр, а потім центри суміжних областей поєднуємо між собою, як результат ми отримали граф, який можна порівнювати з елементами, що зберігаються у базі.

1.2 ІДЕНТИФІКАЦІЯ НА ОСНОВІ ПАРАМЕТРІВ ГЕОМЕТРІЇ ОКА

1.2.1 Ідентифікація на основі параметрів ока

У даному випадку в якості біометричного ідентифікатора використовуються такі параметри ока, як:

– райдужна оболонка ока (РОО);

– сітківка ока.

Райдужна оболонка являє собою тонку рухливу діафрагму ока з отвором (зіницею) в центрі, яка розташована за рогівкою, між передньою і задньою камерами ока, перед кришталиком. Практично світлонепроникна. Містить пігментні клітини, колові м'язи, що звужують зіницю, і радіальні, що розширюють її. Сітківка (лат. retina) – внутрішня оболонка ока, яка є периферичним відділом зорового аналізатора. Містить фоторецепторні клітини, що забезпечують сприйняття і перетворення електромагнітного випромінювання видимої частини спектра в нервові імпульси, а також забезпечує їх первинне оброблення. Має унікальне розташування кровоносних судин.

Ідентифікація на основі райдужної оболонки ока

Роговиця ока розташована на передній частині очного яблука, має приблизно кільцеву форму і розмір близько 11 міліметрів. Форма і розміри зовнішньої межі роговиці постійні (не змінюються з часом) і практично однакові для всіх людей. Внутрішня межа райдужки задається зіницею, що знаходиться приблизно в її центрі. У загальному вигляді внутрішню і зовнішню межу роговиці можна вважати концентричними колами (рис. 1.12).

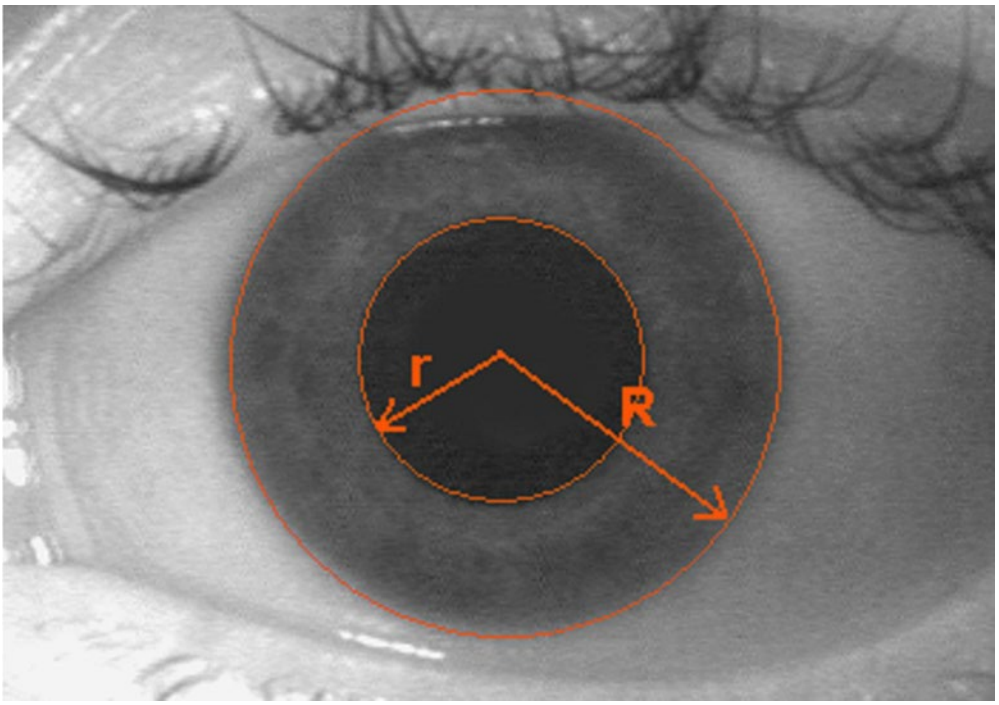


Рисунок 1.12 – Райдужна оболонка ока з радіусом R ≈ 5,5 мм зовнішньої межі й радіусом внутрішньої межі r = 0,1R…0,7R

Роговиця складається з пігментованої з’єднувальної тканини, яка може організовувати різні елементи, розташування яких унікальне для кожної людини. До таких елементів відносяться:

– поглиблення, буває двох типів – лакуни й крипти;
– гребінчасті стяжки або гребені;
– борозни (боріздки);
– кільця;
– промені;
– веснянки;
– корони.

На рис. 1.13 показані деякі з елементів райдужної оболонки.

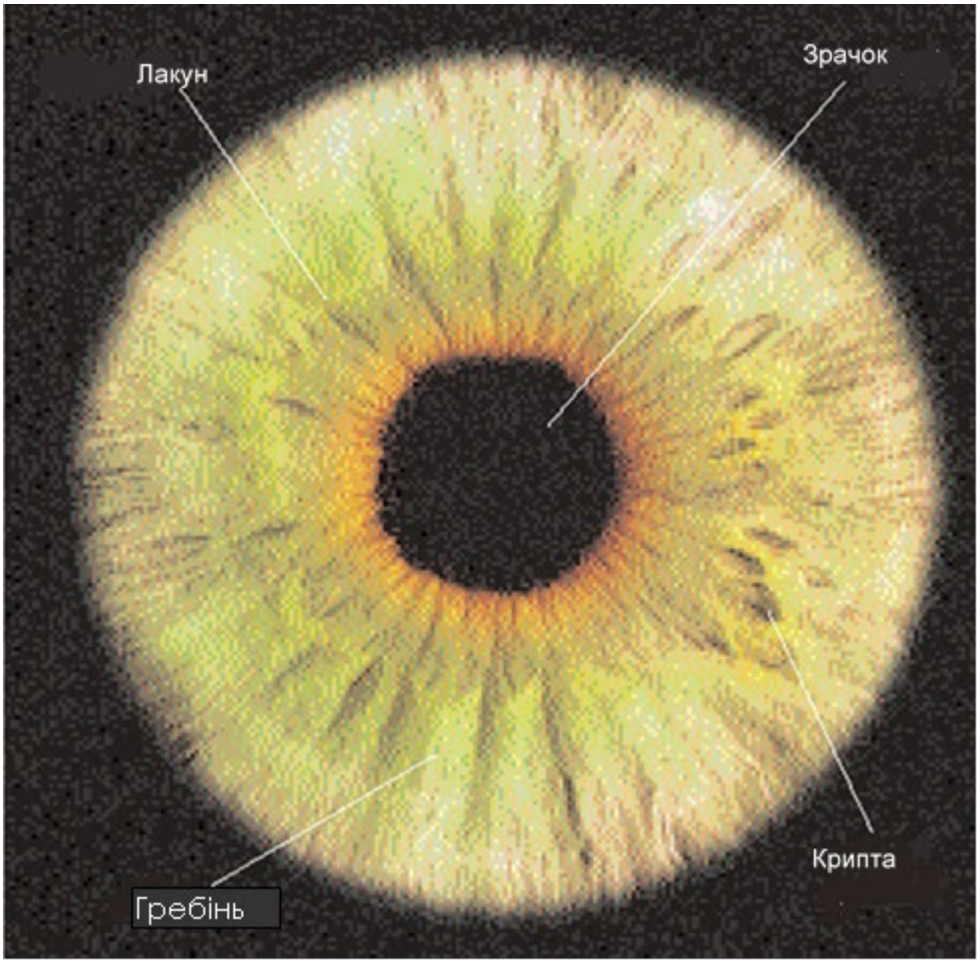


Рисунок 1.13 – Елементи райдужної оболонки

Будь-який біометричний ідентифікатор повинен мати такі властивості:

– стійкість, тобто він повинен не змінюватися з часом;
– виразність;
– інформативність.

Райдужна оболонка практично не змінюється протягом усього життя людини. Таким чином, райдужна оболонка є параметром, який є найбільш важливим для біометричної ідентифікації, – стійкість, тобто форма роговиці залишається постійною протягом усього життя людини.

Роговиця є плоским об'єктом простої форми і практично незмінних розмірів. Варіації її зображення, створювані зміною умов реєстрації, малі і відносно легко можуть бути компенсовані, дозволяючи відокремити

інформацію, що відноситься до індивідуальних особливостей даної роговиці від випадкових спотворень при спостереженні, тобто райдужна оболонка має виразність.

Зображення роговиці містить значну кількість структурних елементів унікальних ознак, тобто райдужна оболонка має великий ступінь інформативності.

Наявність цих властивості у райдужної оболонки призвело до того, що на неї звернули значну увагу як на об'єкт автоматичного біометричного розпізнавання. Використання райдужної оболонки для біометричної ідентифікації почалося тільки у 1994 році, проте вже розроблено низку надійних та стійких методів ідентифікації на основі РОО і відповідні програмно-апаратні комплекси автоматичного розпізнавання.

1.2.2 Методи розпізнавання на основі райдужної оболонки ока

На сьогодні як ми вже зазначали, існує кілька методів ідентифікації на основі РОО. Проте у загальному випадку всі вони діють за однією і тією ж самою схемою, яка показана на рис. 1.14.

Рисунок 1.14 – Спрощена схема процеса ідентифікації на основі РОО

Дана схема складається з кількох етапів:

– отримання зображення ока;
– аналіз якості зображення РОО;
– виділення райдужної оболонки на зображенні;
– нормування розмірів зображення райдужної оболонки;
– обчислення ознак і формування з них набору роговиці;
– порівняння отриманого набору з еталонним.

Виділення роговиці на зображенні

Даний етап полягає у пошуку на отриманому зображенні відносно темного об'єкта, близького за формою до кола, що містить усередині себе ще один концентричний темніший об'єкт (зіницю). У більшості систем на даному етапі необхідно забезпечити виконання тільки однієї умови –

усередині зіниці повинен знаходитися яскравий відблиск певної форми (відблиск від освітлювача).

Дане завдання може бути вирішене багатьма способами, наприклад, пошук концентричних кіл за допомогою перетворення Хафа, або використання корелятора для пошуку відблиску заданої форми з подальшим виявленням контурів зіниці, що містить цей відблиск, і далі – концентричної зіниці райдужної оболонки.

Методи виділення зіниці і зовнішньої межі РОО базуються на детекторах краю і виділення кіл за допомогою перетворення Хафа. Проте для перетворення Хафа потрібно багато часу. Алгоритми виділення зіниці орієнтовані на діаметр зіниці 10…60 пікселів. Як правило, межі зіниць таких розмірів мають досить чіткі перепади яскравості або зафарбовані одним відтінком вручну (як у базі зображень CASIA). Тому для виділення меж зіниці більшість алгоритмів використовує стандартні детектори краю (Canny, Sobel тощо). Зображення, що надходять на обробку в таких системах, мають діаметр зіниці 150…500 пікселів і детектори краю, застосовані до них, не дозволяють виділити чіткі перепади, або їх виділяють надмірно багато.

Специфічним є наявність повік, які у більшості випадків закривають верхню і нижню частини роговиці. Деякі системи, можуть виділяти повіки явним чином і відкидають помилкові дані із закритих ділянок. Інші системи виділення повік як такі не використовують, а закриті частини виявляють за великою відмінністю при порівнянні декількох послідовних знімків.

На рис. 1.15 показано зображення ока і результати виділення роговиці.

Нормування розмірів зображення райдужної оболонки

Нормування розмірів зображення райдужної оболонки необхідне за двох причин:

– через розходження масштабів знімків;
– через зміну відносного розміру зіниці.

Нормування до єдиного масштабу здійснюється досить просто, на етапі виділення роговиці був отриманий еліпс, що наближає зовнішній контур райдужної оболонки, завдання вирішується афінним перетворенням цього еліпса до деякого заданого кола.

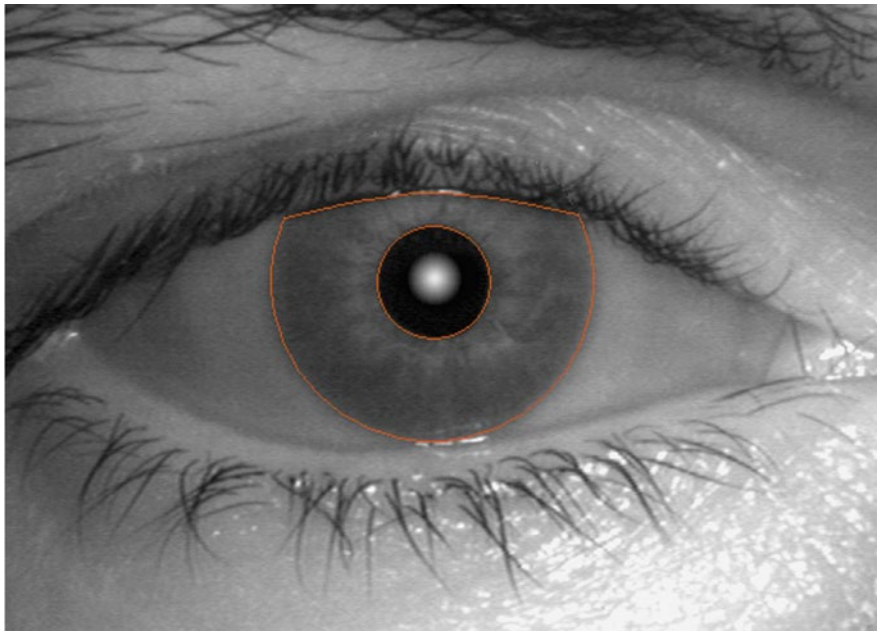
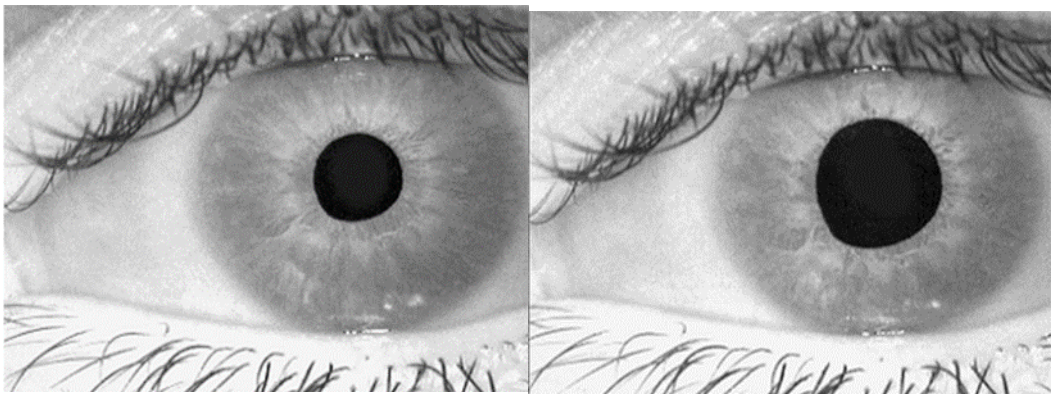


Рисунок 1.15 – Виділення РОО на зображенні ока

Значно складніше усунути варіації, викликані зміною розмірів зіниці. Фізично роговиця являє собою нерівномірне за товщиною кільце. Переміщення елементів кільця при зміні внутрішнього радіуса нелінійне. Більше того, при пульсації зіниці деякі елементи роговиці можуть здійснювати не тільки поступальні рухи уздовж радіусів, а й обертальні відносно цента. Це є однією з основних перешкод підвищення точності систем розпізнавання за роговицею.

На рис. 1.16 надане зображення одного і того ж самого ока, отримані з однієї і тієї самої камери з інтервалом у кілька хвилин, але за різних умов освітлення.



а) б)

Рисунок 1.16 – Зміна розмірів РОО й зіниці при зміні умов освітлення

Оскільки роговиця є майже круглим об'єктом, з добре вираженою варіацією структури уздовж радіусів і практично однорідними текстурами уздовж концентричних кіл, має сенс розглядати її у полярній системі координат. Перетворення системи координат може бути зроблено явно або неявно, як це робиться, обчислюючи диференціальні ознаки уздовж концентричних кіл.

Обчислення ознак і формування еталона

На етапі обчислення ознак і формування еталона роговиці вирішується завдання факторизації, тобто обчислення набору характеристик зображення, що мають найменший розкид для знімків даної людини і найбільший розкид між знімками різних людей. Оскільки кількість ознак досить мала порівняно з розмірами зображення, попутно вирішується завдання зменшення розмірності даних. Якщо всі попередні етапи стосувалися лише геометричної, але не яскравішої нормалізації зображення, то на даному етапі необхідно обчислювати ознаки інваріантні до змін яскравості (яскравість, контрастність, нерівномірність освітлення). Також можливо буде позбутися шумів зображення. Цим умовам добре задовольняють спектральні і близькі до них вейвлет-перетворення. Найбільш часто використовують перетворення Габора і перетворення Хаара.

1.2.3 Проблеми ідентифікації на основі райдужної оболонки ока

Ідентифікація особистості на основі райдужної оболонки має дуже великий ступінь надійності й точності, проте існує й низка проблем. У першу чергу, це те, що для успішної ідентифікації необхідно щоб око потрапило у поле зору об'єктива камери під певним діапазоном кутів. Решта проблем пов'язані з особливостями структури ока людини і показані на рис. 1.17.

Рисунок 1.17 – Проблеми ідентифікації на основі райдужної оболонки

1.Затінювання роговиці повіками. Ця проблема може вирішуватися спеціальним алгоритмом пошуку повік або відбраковуванням частин зображення при порівнянні послідовних кадрів.

2.Затінювання роговиці віями, що стирчать донизу. Алгоритм пошуку повік на подібних знімках відпрацьовує успішно і з великою впевненістю, проте виділена ним область, не підходить для розпізнавання. Проблема може вирішуватися алгоритмом відбраковування за послідовністю зображень. Роговиця і повіки з віями рухаються відносно одна одної, тому ті частини зображення, де вії і повіки нависають над роговицею, постійно змінюються (вії поперемінно закривають різні частини роговиці). Навпаки, відкриті ділянки роговиці на нормованому зображенні відносно стабільні.

3.Відблиски від навколишніх предметів на роговиці. Роговиця працює як сферичне дзеркало, відбиваючи навколишній світ. Ці відбиття (особливо

відображення джерел світла, плям сонячного світла і ділянок денного неба) можуть бути в кілька разів яскравішими деталей роговиці і повністю пригнічувати їх. Для вирішення цієї проблеми застосовують високо інтенсивне у вузькій області спектра освітлення (що значно перевершує сонячне за освітленістю, найчастіше використовують інфрачервоне випромінювання) і реєстрацію зображення у цій самій області спектра.

4.Різний розмір зіниці при змінних умовах зйомки. Як уже зазначалось, афінне перетворення зображення роговиці до стандартного розміру вирішує цю проблему лише у першому наближенні, тому що розтягування роговиці підпорядковується нелінійному, надто складному закону. Для вирішення цієї проблеми пропонується, наприклад, запам'ятовувати розмір зіниць людини при реєстрації у системі, а при розпізнаванні домагатися акомодації (розширення чи звуження) зіниць до цього розміру, маніпулюючи яскравістю спеціального джерела видимого світла.

5.Патологічні й вікові зміни. На роговиці дуже чітко відбивається стан організму, у тому числі різного роду патології (хвороби, травми, отруєння). У зв'язку з цим виникає питання про стійкість (за часом) розпізнавання об'єкта, підданого цим змінам. Проте, на роговиці існує значна кількість вроджених ознак і ознак, які не змінюються протягом усього життя. Вроджені та набуті ознаки розділити практично неможливо, проте людину можна розпізнавати на підставі збігу навіть незначної кількості ознак. Необхідний мінімум – це 30% і навіть у цьому випадку ймовірність помилкового допуску не перевищує 10–6.

6.Невизначеність кута повороту роговиці. У системі з реєстрацією двох роговиць або у системі, що комбінує роговицю й обличчя, цієї проблеми не існує. Для так званої «одноокої» системи можна визначати кут за конфігурацією повік, децентрацією зіниці або за якоюсь важливою характерною ознакою на роговиці. Всі ці ознаки можуть змінюватися з часом. У такому випадку залишається перебирати кути повороту (істотно

збільшується час роботи системи) або вираховувати ознаки, інваріантні до повороту (таких ознак в десятки разів менше, отже, сильно знижується надійність системи).

Крім усього вищеперерахованого системи біометричної ідентифікації повинні бути стійкими до використання підробок. Для систем ідентифікації на основі райдужної оболонки в якості підробки можуть застосовувати або об'ємну фотографію роговиці або макет ока, так само можуть застосовувати відчуження біометричних ознак (у даному випадку «вирване» око).

Існує два способи вирішення цієї проблеми:

1.За спектром відбиття роговиці. Роговиця «живого» ока постійно зволожується, «мертве» око швидко пересихає. Спектри відбиття вологої і сухої роговиць відрізняються.

2. За реакцією ока на освітлення. Зіниця певним чином і з певним запізненням реагує на зовнішні подразники (спалах світла, гучний звук і т.д.), причому ця реакція керується головним мозком.

Будуючи графік реакції зіниці (пупілограму) і відносячи її до моменту, коли був поданий імпульс-подразник, то можна з високою надійністю відкинути спроби фальсифікації. Пупілограми дають ще одну цікаву можливість. Як відомо, пупілограма служить характеристикою фізичного функціонального стану людини (норма, перезбуджена, пригноблена). За пупілограмою з великою точністю можна встановити, наскільки працездатна людина на даний момент, а також визначити стан сп'яніння або впливу стимуляторів. Така можливість цін- на для систем безпеки, що встановлюються на об'єктах, де потрібен не тільки допуск певних осіб, але й перевірка їх працездатності (операторські АЕС, авіадиспетчерські тощо).

ВИСНОВОК ДО РОЗДІЛУ 1

В результаті аналізу, досліджено сучасні системи біометричні ідентифікації користувачів та принципи їх роботи. На даний час є 9 рівнів біометричної ідентифікації. Як показує практика, кожний користувач сучасних інформаційно – комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та автентифікації. Такі користувачі все частіше застосовують, так звану, розширену або багатофакторну автентифікацію.

Для подальшої реалізації системи двофакторної ідентифікації було обрано такі фактори:

- ідентифікація за допомогою відбитків пальців;
- ідентифікація на основі параметрів геометрії ока.

РОЗДІЛ 2
РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ

2.1 Пристрої для отримання відбитків пальців в електронному вигляді

Отримання електронного образу відбитка пальця з добре помітним папілярним узором – досить складне завдання. Оскільки відбиток пальця дуже малий, для отримання його якісного зображення доводиться використовувати досить витончені методи. До недавнього часу це було досить складно реалізувати, подібні системи з'явилися у 80-х роках минулого століття, вони називалися сканерами і були досить громіздкі та дорогі. Проте з розвитком мікроелектронної бази подібні пристрої стало значно проще реалізовувати, при чому вони стали менш габаритними та більш дешевими. З кінця 90-х років минулого століття такі пристрої почали випускатися масово.

На сьогодні існує декілька десятків різних типів сканерів відбитків пальців. Усі існуючі сканери відбитків пальців можна поділити на три класи, які відрізняються між собою фізичними принципами функціонування та отримання зображення відбитка пальця. На рис. 2.1 надано класифікацію сканерів відбитків пальців.

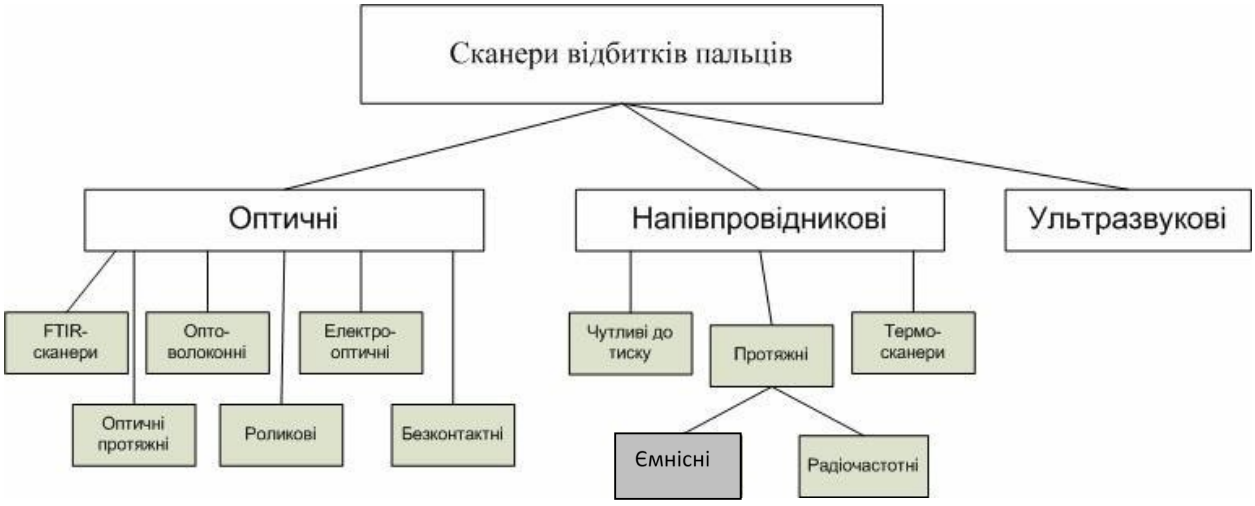


Рисунок 2.1 – Класифікація сканерів відбитків пальців

Розглянемо принципи роботи цих типів сканерів більш детальніше.

В даний час існують наступні технології реалізації оптичних сканерів:

Ftir-сканери (frustrated total internal reflection) – це пристрої, в яких використовується ефект порушеного повного внутрішнього віддзеркалення. Розглянемо даний ефект детальніше, щоб пояснити повний алгоритм роботи таких сканерів.

Проте при контакті більш щільного оптичного середовища (у нашому випадку поверхня пальця) з менш щільним (поверхня призми) в точці повного внутрішнього віддзеркалення пучок світла проходить через цю межу. Таким чином, від межі відіб'ються лише пучки світла, що попали в такі точки повного внутрішнього віддзеркалення, до яких не були прикладені лінії папілярного узору поверхні пальця. Для фіксації, світлової картинки, що вийшла таким чином, використовується спеціальна камера. Принцип роботи FTIR-сканера показано на рис. 2.2.

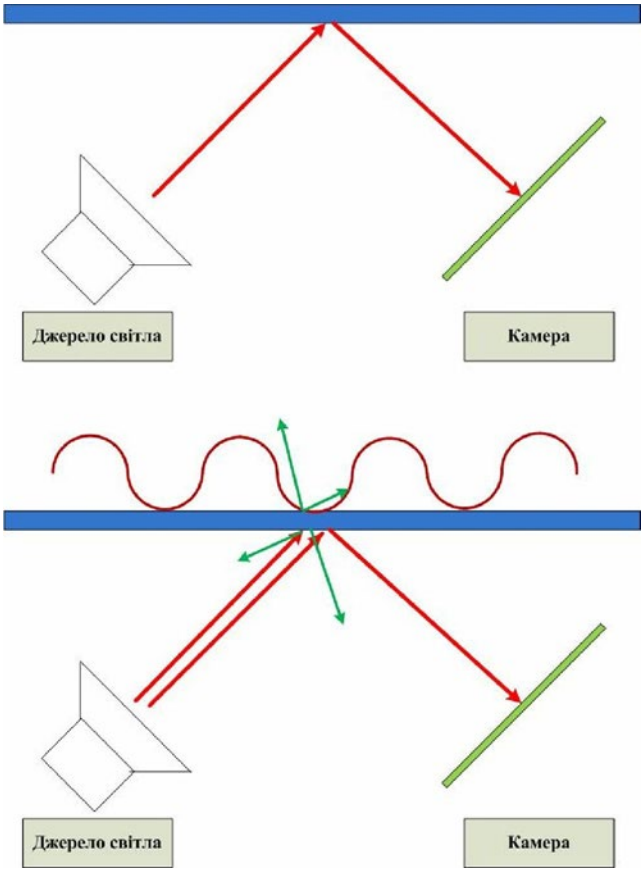


Рисунок 2.2 – Принцип роботи FTIR-сканерів

Оптоволоконні сканери (fiber optic scanners) -- являють собою оптоволоконну матрицю, кожне з волокон якої закінчується фотоелементом. Чутливість кожного фотоелемента дозволяє фіксувати залишкове світло, що проходить через палець, в точці дотику рельєфу пальця до поверхні сканера. Зображення відбитка пальця формується за даними кожного з елементів. На рис. 2.3 показано принцип формування зображення оптоволоконними сканерами.

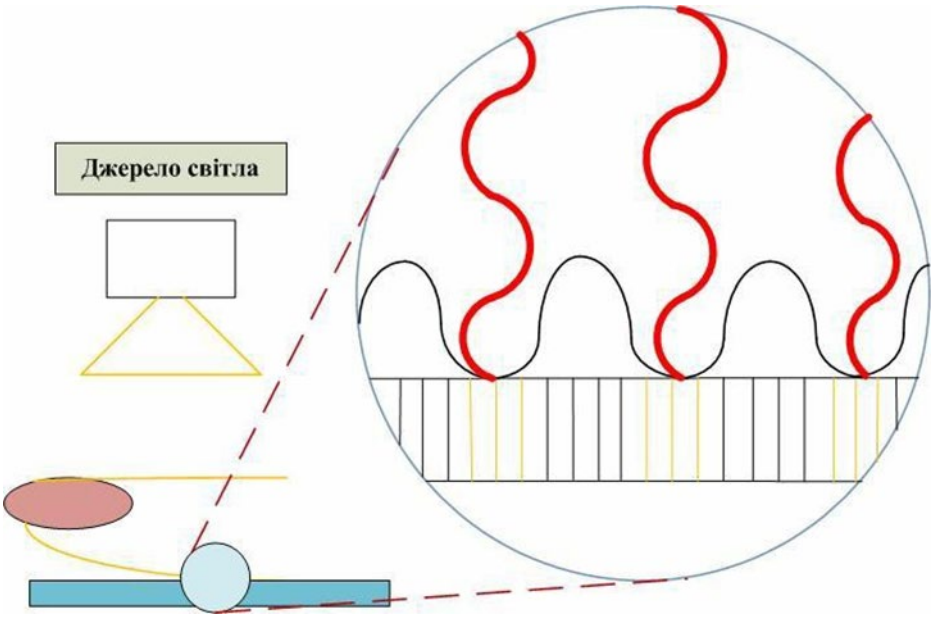


Рисунок 2.3 – Механізм роботи оптоволоконних сканерів

Електрооптичні сканери (electro-optical scanners) – в основі даної технології лежить використання спеціального електрооптичного полімеру, до складу якого входить світловипромінюванний шар. При дотику пальця до сканера неоднорідність електричного поля в його поверхні (різниця потенціалів між горбками і западинами) відбивається на світінні цього шару так, що він висвічує відбиток пальця. Потім масив фотодіодів сканера перетворить це світіння в цифровий вигляд.

Оптичні протяжні сканери (sweep optical scanners) – в цілому аналогічні FTIR-пристроям. Їх особливість в тому, що палець потрібно не просто прикладати до сканера, а проводити ним по вузькій смужці – зчитувачу. При русі пальця по поверхні сканера робиться серія миттєвих знімків (кадрів). При цьому сусідні кадри, знімаються з деяким накладенням, тобто

перекривають один одного, що дозволяє значно зменшити розміри використовуваної призми і самого сканера.

Роликові сканери (roller-style scanners) – в цих мініатюрних пристроях сканування пальця відбувається при прокатуванні пальцем прозорого тонкостінного циліндра, що обертається (ролика). Під час руху пальця по поверхні ролика робиться серія миттєвих знімків (кадрів) фрагмента папілярного узору, який торкається поверхні у цей час. Аналогічно протяжному сканеру сусідні кадри знімаються з накладенням, що дозволяє без спотворень зібрати повне зображення відбитка пальця. При скануванні використовується проста оптична технологія: усередині прозорого циліндрового ролика знаходяться статичне джерело світла, лінза і мініатюрна камера. Зображення ділянки пальця, яка освітлюється фокусується лінзою на чутливий елемент камери. Після повної «прокрутки» пальця, «збирається картинка» його відбитка. На рис. 2.4 показано структура роликового сканера.

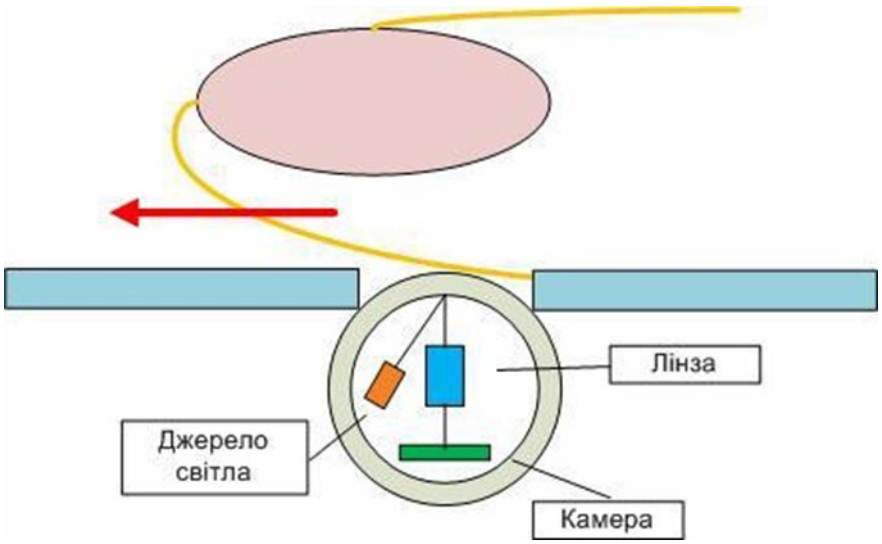


Рисунок 2.4 – Роликовий сканер

Безконтактні сканери (touchless scanners) – в них не вимагається безпосереднього контакту пальця з поверхнею скануючого пристрою. Палець прикладається до отвору у сканері, декілька джерел світла підсвічують його знизу з різних сторін, у центрі сканера знаходиться лінза, через яку зібрана інформація проектується на камеру, яка перетворює отримані дані в зображення відбитка пальця. Схема роботи оптичного сканера показана на рис. 2.5.

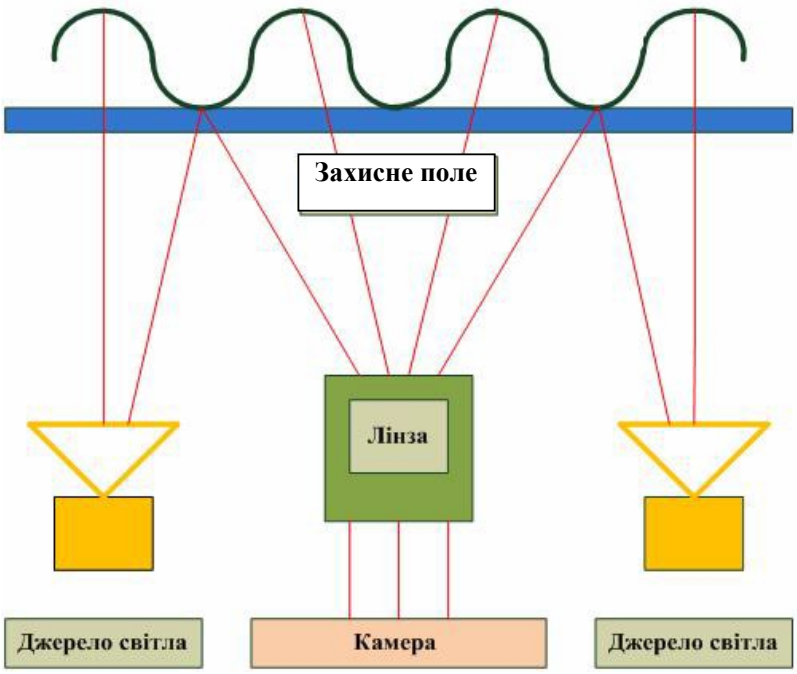


Рисунок 2.5 – Схема роботи безконтактного сканера

Напівпровідникові сканери

В їх основі лежить використання властивостей напівпровідників для отримання зображення поверхні пальця, що змінюються в місцях контакту гребенів папілярного узору з поверхнею сканера. В даний час існує декілька технологій реалізації напівпровідникових сканерів.

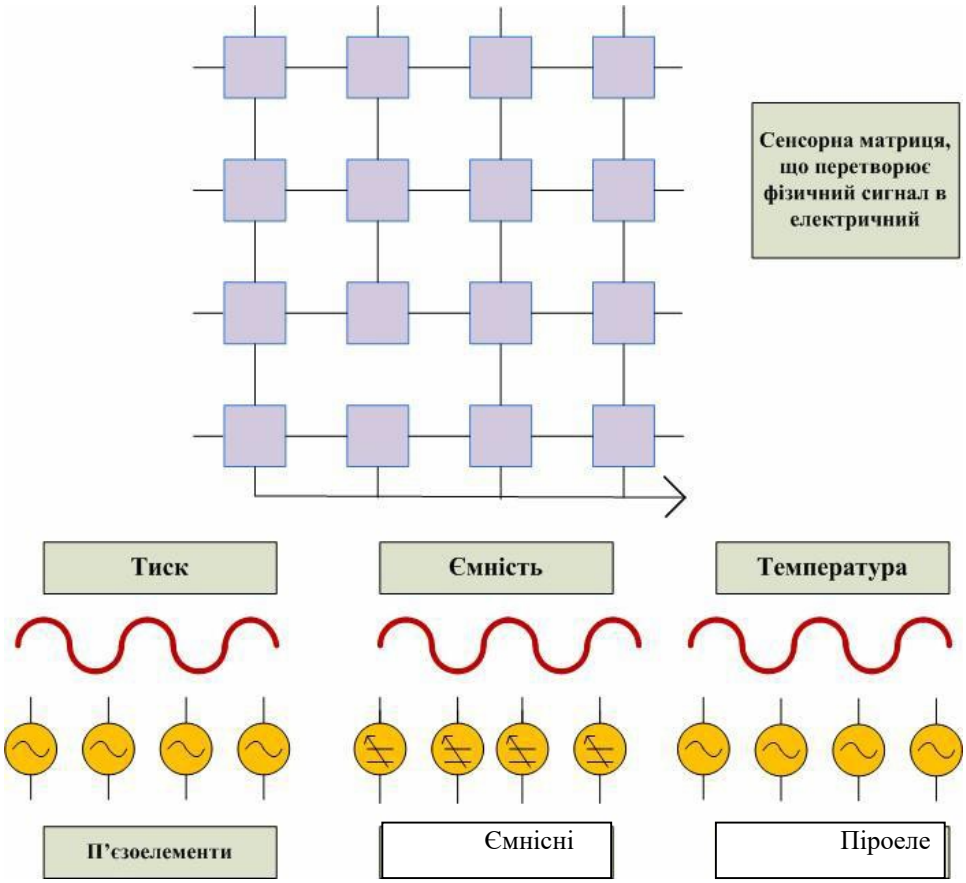


Рисунок 2.6 – Загальна схема роботи напівпровідникових сканерів

Ємнісні сканери (capacitive scanners) – найбільш розповсюджений тип напівпровідникових сканерів, в яких для отримання зображення відбитка пальця використовується ефект зміни ємності pn-переходу напівпровідникового приладу при зіткненні гребеня папілярного узору з елементом напівпровідникової матриці. Існують модифікації описаного сканера, в яких кожен напівпровідниковий елемент у матриці сканера виступає в ролі однієї пластини конденсатора, а палець – в ролі іншої. При дотику пальця до сенсора між кожним чутливим елементом і виступом-западиною папілярного узору утворюється деяка ємність, величина якої визначається відстанню між поверхнею пальця й елементом. Матриця цих ємностей перетвориться в зображення відбитка пальця.

Чутливі до тиску сканери (pressure scanners) – в цих пристроях використовуються сенсори, що складаються з матриці п'єзоелементів. При дотику пальця до поверхні виступи папілярного узору утворюють тиск на деякі підмножинні елементи поверхні, відповідно впадини жодного тиску не

чинять. Матриця отриманої з п'єзоелементів напруги, перетвориться в зображення поверхні пальця.

Термосканери (thermal scanners) – в них використовуються сенсори, які складаються з піроелектричних елементів, що дозволяють фіксувати різницю температури і перетворювати її в напругу. При дотику пальця до сенсора за температурою виступів папілярного узору, що торкаються до піроелектричних елементів, і температурою повітря, яка знаходиться в западинах, будується температурна карта поверхні пальця, що перетвориться в цифрове зображення.

У цілому можна сказати, що в усіх напівпровідникових сканерах використовуються деяка матриця чутливих мікроелементів (тип яких визначається способом реалізації) і перетворювач сигналів, які отримала матриця в цифрову форму.

Радіочастотні сканери (RF-Field scanners) – в таких сканерах використовується матриця елементів, кожен з яких працює як маленька антена. Сенсор генерує слабкий радіосигнал і спрямовує його на скановану поверхню пальця, кожен з чутливих елементів приймає відбитий від папілярного узору сигнал. Величина наведеної в кожній мікроантені ЕРС залежить від наявності або відсутності поблизу неї гребеня папілярного узору. Отримана таким чином матриця напруги перетвориться в цифрове зображення відбитка пальця.

Протяжні термосканери (thermal sweep scanners) – різновид термосканерів, в яких використовується, як і в оптичних протяжних сканерах, проведення пальця по поверхні сканера, а не просто дотик.

Ємнісні протяжні сканери (capacitive sweep scanners) – використовують аналогічний спосіб покадрового збирання зображення відбитка пальця, але кожен кадр зображення виходить за допомогою ємнісного напівпровідникового сенсора.

Ультразвукові сканери

Ця група в даний час представлена всього одним методом сканування, який так і називається – ультразвукове сканування. У даному випадку сканування поверхні пальця ультразвуковими хвилями і вимір відстані між джерелом хвиль і впадинами та виступами на поверхні пальця по віддзеркаленому від них еху. Якість отримуваного в такий спосіб зображення в 10 разів краще, ніж отриманого будь-яким іншим представленим нам методом розглянутим раніше. Крім цього слід відзначити, що даний спосіб практично повністю захищений від муляжів, оскільки дозволяє крім відбитка пальця отримувати і деякі додаткові характеристики про його стан (наприклад, пульс усередині пальця). На рис. 2.7 показано загальний принцип роботи ультразвукового сканера.

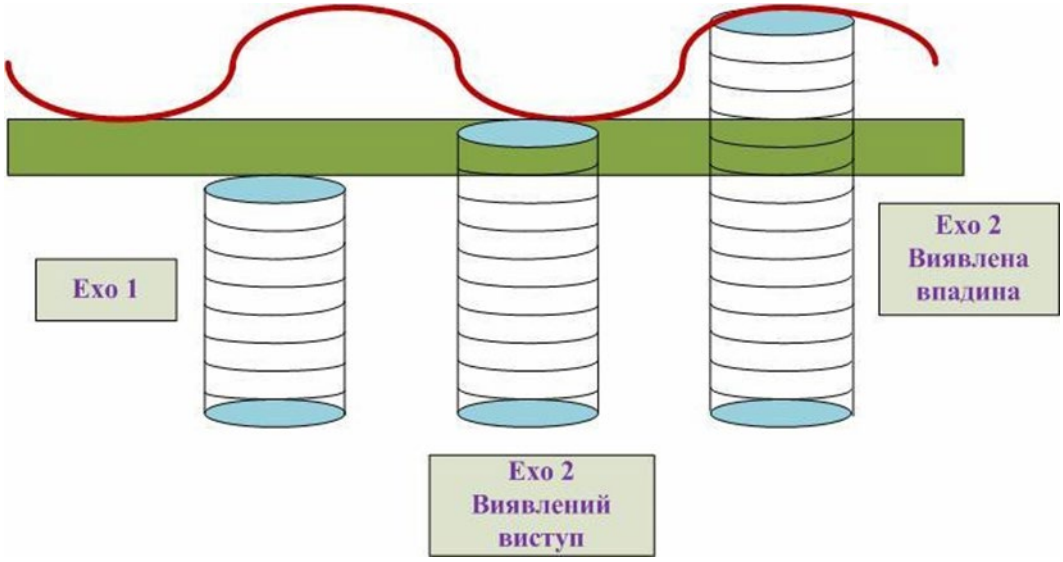


Рисунок 2.7 – Схема роботи ультразвукового сканера

2.2 Приклади систем біометричної ідентифікації за допомогою відбитків пальців та геометрії ока

2.2.1 Система біометричної ідентифікації BioLink IDenium

Система BioLink IDenium є системою біометричної ідентифікації за відбитками пальців, при цьому вона дозволяє також утворювати і систему контролю доступу. Архітектурно система BioLink IDenium складається з декількох блоків, а саме:

- індивідуальних сканерів відбитків;
- групових сканерів відбитків;
- сервера системи;
- підсистеми контролю доступу;
- підсистеми біометричної ідентифікації.

Програмне забезпечення системи BioLink IDenium функціонує під управлінням операційних систем Microsoft Windows XP/2003/Vista/7/8, а сама система дозволяє реалізувати наступні функції:

- біометричну ідентифікацію особи за відбитками пальців (в якості ідентифікатора можна застосовувати як і один відбиток, так і комбінацію відбитків різних пальців);
- можливість реалізації схеми двофакторної ідентифікації – за паролем та за відбиткам пальців;
- ефективне розмежування доступу до інформаційних ресурсів корпоративних мереж;
- організація централізованої системи контролю доступу;
- можливість біометричної ідентифікації для вилучених користувачів у режимі роботи «сервер терміналів» (підтримуються протоколи Windows RDS та Citrix);

– одноразова реєстрація користувачів та їх біометричних ідентифікаторів з подальшим наданням зареєстрованим користувачам доступу до інформаційних ресурсів мережі з будь-якого з вхідних до її складу комп'ютерів;
– повна інтеграція зі службою Active Directory;
– можливість автономної роботи сканера при втраті зв’язку з сервером (сканер дозволяє зберігати у пам’яті до 10 останніх біометричних ідентифікаторів);
– протоколювання подій доступу й аудит.

На рис. 2.8 надано структурну схему системи BioLink IDenium. Програмний модуль авторизації у системі BioLink Win Logon – призначений для ідентифікації особи та допуску її у систему.

Модуль авторизації прав на запуск ПЗ BioLink SDK – призначений для перевірки прав користувач на запуск того чи іншого програмного продукту або до доступу того чи іншого ресурсу.

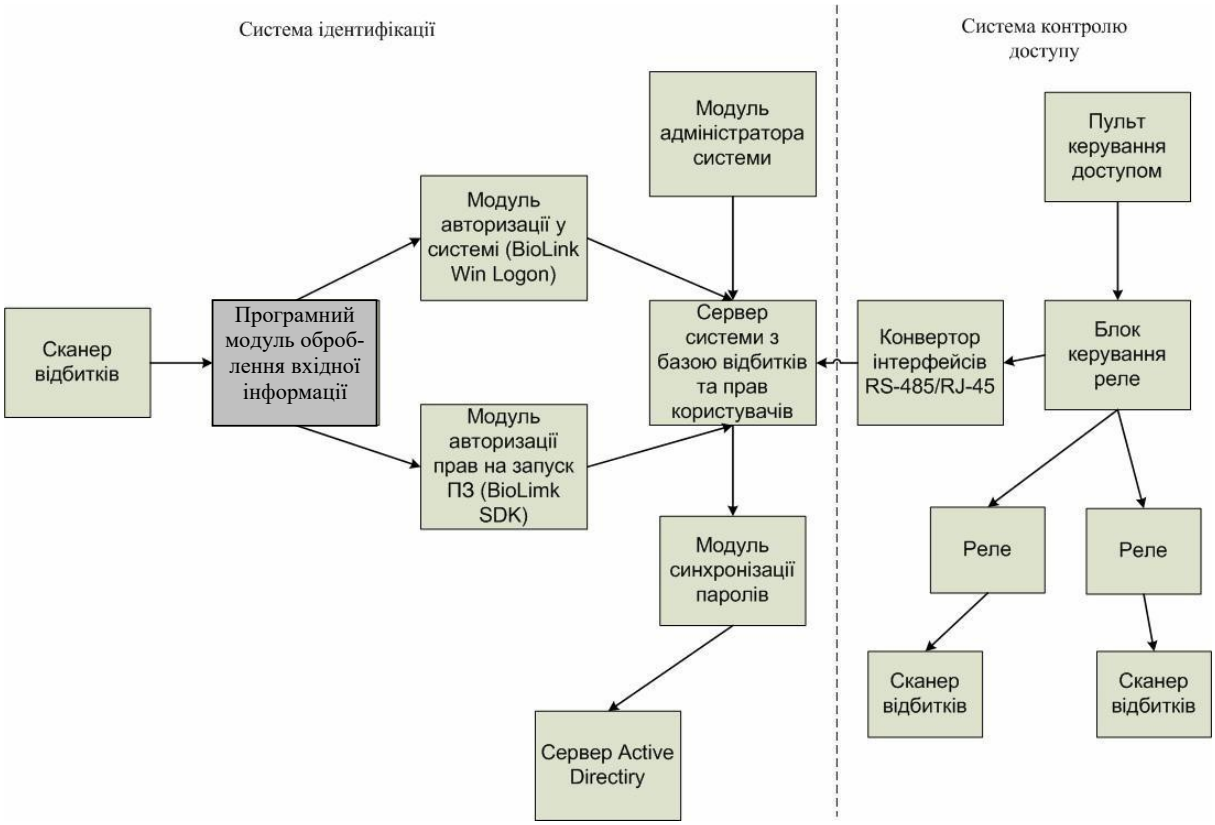


Рисунок 2.8 – Структурна схема системи BioLink IDenium

Модуль синхронізації паролів – призначений для синхронізації інформації про користувача, яка зберігається на сервері Active Directory та сервері BioLink IDenium.

Слід зазначити, що особливістю системи BioLink IDenium є те, що вона дозволяє використовувати для біометричної ідентифікації комбінацію з десятьох різних відбитків. Тобто користувач може надати системі зразки декількох відбитків пальців, при чому задати послідовність їх надання.

На рис. 2.9 та 2.10 показано вигляд діалогових вікон системи BioLink IDenium при отриманні зразків відбитків пальців.

На рис. 2.11 надано вікно ідентифікації користувача при вході до системи, а на рисунку 2.12 приклад повідомлення системи за неможливості розпочати ідентифікацію користувача.

Рисунок 2.9 – Вибір пальців для ідентифікації

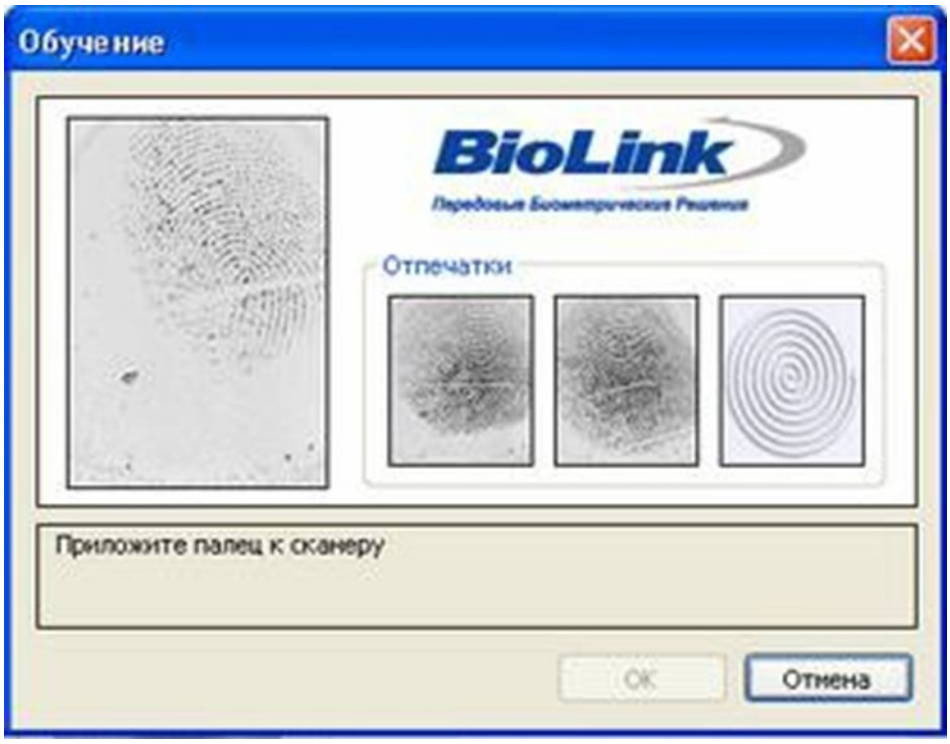


Рисунок 2.10 – Створення біометричного ідентифікатора

Рисунок 2.11 – Стартове вікно ідентифікації користувача

Рисунок 2.12 – Повідомлення системи за неможливості розпочати ідентифікацію користувача

Алгоритм роботи BioLink IDenium (рис. 2.13) полягає у наступному:

- користувач притискає палець до сканера відбитків пальців, що встановлений на робочому місці та є підключений до робочої станції (1);
- зображення відбитка пальця перетворюється у цифрову модель. Яка передається на сервер ідентифікації (2);
- сервер біометричної ідентифікації (IDenium Server) порівнює сформовану модель з моделлю раніше зареєстрованого відбитка та приймає рішення про ідентифікацію користувача;
- у разі позитивного рішення про ідентифікацію формується пакет, що містить облікові дані користувача;
- облікові дані користувача отримуються з каталогу Active Directory, актуальність цих облікових даних забезпечується синхронізацією цього каталогу та IDenium Server (3);
- IDenium Server транслює облікові дані користувача на робочу станцію (4);
- отримані облікові дані передаються системі, що ініціювала запит про ідентифікацію користувача;
- локальна система отримує облікові дані користувача у звичному вигляді – ім'я (логін), пароль (password) та перелік прав, на базі цих даних система перевіряє ідентичність користувача та приймає рішення про надання йому доступу

до запитаних ресурсів (5).

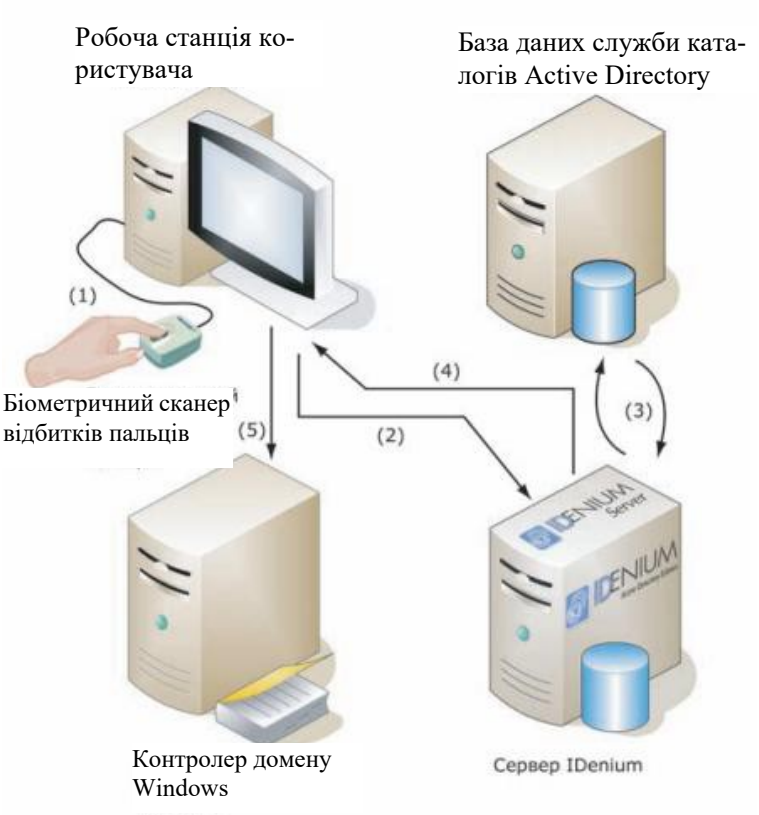


Рисунок 2.13 – Алгоритм роботи системи BioLink IDenium

На рис. 2.14 показано приклад інтеграції системи BioLink IDenium в існуючу інфраструктуру підприємства та створення єдиної інтегрованої системи контролю доступу на базі біометричних ознак.

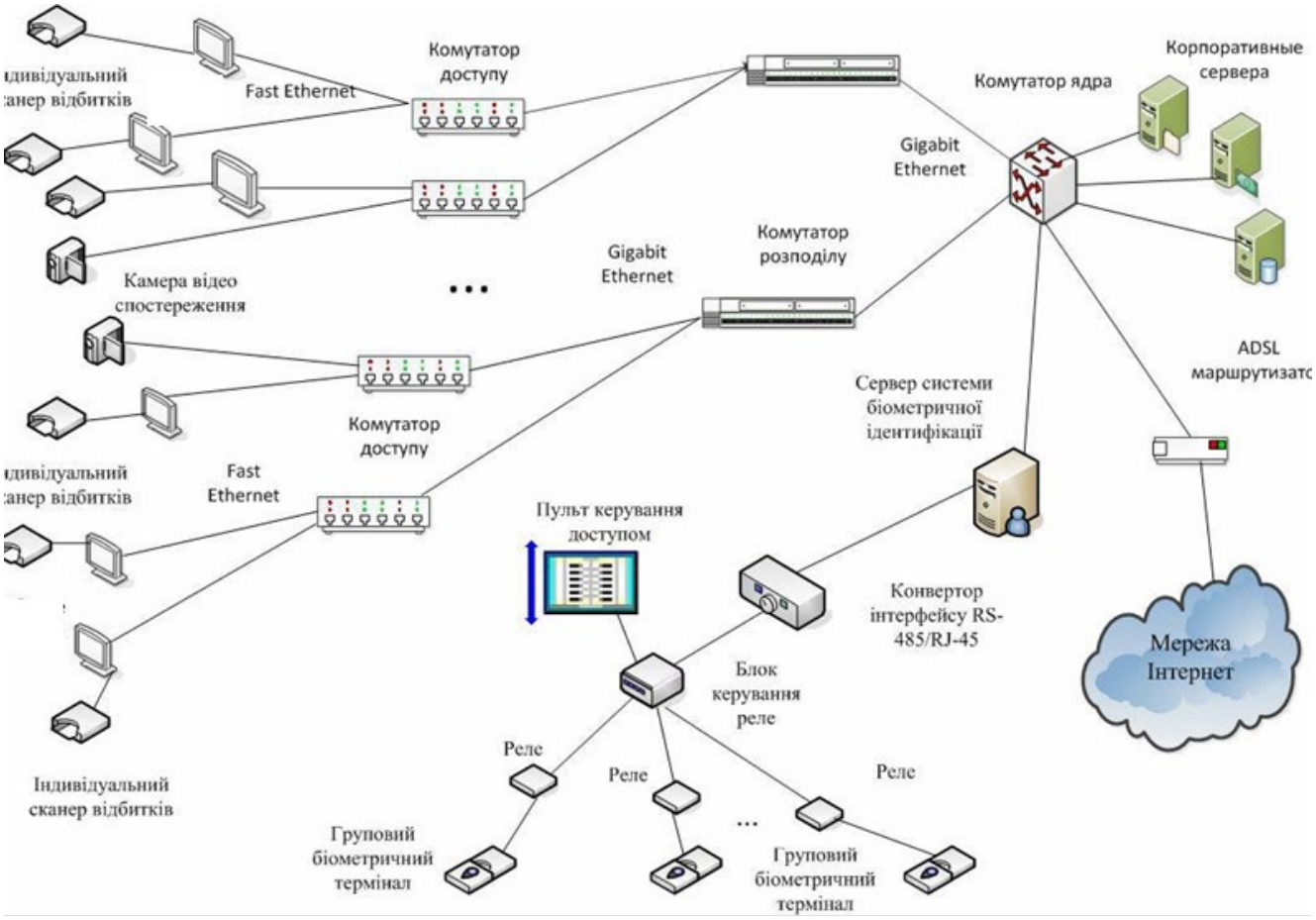


Рисунок 2.14 – Структурна схема мережі з використанням системи біометричної ідентифікації

У системі застосовуються індивідуальні (рис. 2.15) та групові (рис. 2.16) сканери відбитків пальців

Рисунок 2.15 – Індивідуальні сканери системи BioLink IDenium

Рисунок 2.16 – Групові сканери відбитків пальців системи BioLink IDenium

Слід відзначити, що система BioLink IDenium має можливість реалізовувати функцію обліку робочого часу. Система здійснює функцію обліку та аналізу використання робочого часу – вона фіксує час приходу та уходу працівників з роботи, відсутність працівників на робочому місці протягом робочого дня тощо. На базі цієї інформації система визначає реально відпрацьований час кожним працівником.

2.2.2 Система біометричної ідентифікації АДИС ПАПИЛОН

Система ідентифікації АДИС ПАПИЛОН створена на базі ідентифікації за відбитками пальців. АДИС ПАПИЛОН забезпечує створення, зберігання та функціонування електронної бази даних відбитків пальців та дозволяє вирішувати широке коло задач для розв’язання значного кола задач:

- ✓ ідентифікацію користувачів інформаційних мереж;
- ✓ створення систем контролю доступу на територію підприємств;
- ✓ створення територіально-розподіленої системи ідентифікації.

У АДИС ПАПИЛОН застосовується детальний опис папілярних візерунків і ієрархічний підхід до їх порівняння. Перший рівень ієрархії порівняння – тип візерунка, потім слідують положення дельт і центрів, гребневий рахунок дельта-дельта і дельта-центр, масив напрямів потоку папілярних ліній і маска невикористовуваних місць, розташування й напрям дрібних особливостей, і потім – гребневий рахунок і зв'язаність між дрібними

особливостями – топологічні характеристики, що є найпотужнішим інструментом при порівнянні (рис. 2.17).

Тип візерунка, розташування дельт та центрів | Потоки | Гребневий рахунок та в’язкість

Рисунок 2.17 – Принцип порівняння відбитків пальців у системі АДИС ПАПИЛОН

Топологічний підхід до опису візерунків та ієрархічний спосіб їх порівняння забезпечують дуже високу вибірковість пошуку, що перевершує вибірковість систем, які описують тільки положення і напрям дрібних особливостей.

Архітектура системи

В основу побудови системи покладено архітектуру «клієнт-сервер», що підтримує незалежне звернення робочих станцій до обслуговуючого запити серверу.

Введення інформації, оброблення зображень та приведення одиниці зберігання до стандартної форми відбувається на робочій станції. Автоматичний процес введення в базу даних запускається на сервері. За кожним, знову уведеним до БД об'єктом, здійснюються пошуки. Об'єкт вважається уведеним до БД тільки після завершення пошуків.

Серверні функції (уведення, зберігання, пошуки, зв'язок і комунікації) у великих розподілених АДІС виконують окремі підсистеми:

– сервер БД;
– пошукова підсистема;
– підсистема зберігання даних;

– підсистема зв'язку і комунікацій.

У невеликих за обсягом БД програмно-апаратних комплексах серверні функції забезпечуються ресурсами єдиного серверного блока або розподіляються між робочими станціями.

Сервер БД забезпечує:

– підтримку електронного масиву пошукових образів об'єктів зберігання БД (індексних даних) на дисковому масиві;

– прийом до виконання запитів робочих станцій і віддалених користувачів;

– розподіл обчислювальних завдань;

– формування результатів пошуків і передачу їх на робочі станції відповідно до запитів.

Залежно від обсягу БД до складу серверного блока може входити зовнішня дискова підсистема для зберігання індексних даних під керуванням RAID-контролера.

Пошукова підсистема забезпечує порівняння записаних у базу шаблонів за зразком наданих для проведення ідентифікації. Обчислювальний процес організований за технологією паралельних обчислень. По АДИС ПАПИЛОН забезпечує використання n-ї кількості багатопроцесорних обчислювачів (метчерів) як єдиного обчислювального ресурсу. Метчери побудовані на базі модульних серверів, монтуються у стійки. Кількість обчислювачів залежить від розміру БД і необхідної пропускної спроможності системи. Вихід з ладу одного обчислювача не призводить до зупинки комплексу, навантаження рівномірно розподіляється між рештою. Таке рішення застосовується у разі організації розподіленої системи ідентифікації. У випадку невеликого проекту функції пошукової системи можуть реалізовуватися одним сервером.

Підсистема зберігання даних складається з дискових накопичувачів – мембоксів і Oracle-сервера, призначеного для вивантаження текстової супровідної інформації. Кожен мембокс являє собою пристрій з масивом

жорстких дисків, що монтується у стійки, працює під управлінням ОС Linux і спеціального програмного забезпечення «MemoryBox». Кількість мембоксів визначається розміром БД.

Підсистема комунікацій і зв'язку складається з комутаторів і сервера комунікацій і забезпечує:

– взаємодію серверу БД з іншими вузлами системи;

– взаємодію АДІС з робочими станціями, пунктами групової ідентифікації та зі станціями віддаленого доступу.

На рис. 2.18 надано структурну схему простої мережевої версії системи АДИС ПАПИЛОН.

Проста мережева версія розрахована на загальний обсяг бази даних у 25- 100 тис. відбитків пальців. До складу входять індивідуальні сканери відбитків пальців, які підключаються до робочих станцій та групові сканери відбитків пальців, які дозволяють організовувати систему контролю доступу. Функції системи ідентифікації виконуються окремим єдиним сервером.

Розподілена мережева версія забезпечує можливість організувати глобальну систему ідентифікації. Розподілений варіант системи забезпечує зберігання у базі даних від одного до десятків мільйонів відбитків пальців. Система створюється за принципом централізації – присутній центральний вузол системи, який виконує функції пулу серверів БД, пошукової системи, системи зв’язку та комунікації. До центрального вузла через глобальну мережу Інтернет підключаються регіональні філії, які мають власні локальні сервери системи.

Рисунок 2.18 – Структурна схема простої мережевої версії системи АДИС ПАПИЛОН

На рис. 2.19 надано структурну схему розподіленої мережевої версії системи АДИС ПАПИЛОН.

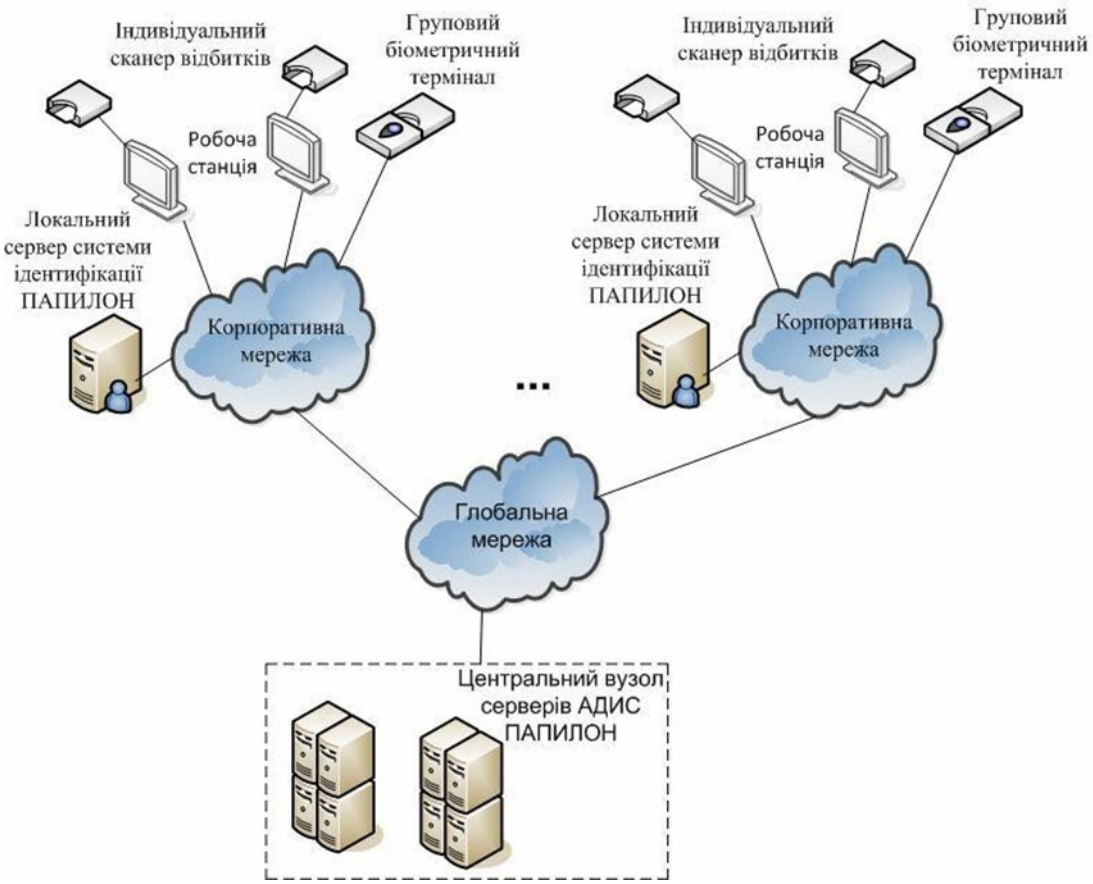


Рисунок 2.19 – Структурна схема розподіленої мережевої версії системи АДИС ПАПИЛОН

На рис. 2.20 показано зовнішній вигляд індивідуального сканера відбитків пальців, що застосовується системою.

Рисунок 2.20 – Індивідуальний сканер відбитків пальців

2.2.3 Система ідентифікації за райдужною оболонкою ока ПАПИЛОН «Циркон»

Однією з переваг методу ідентифікації особи за роговицею є його "неагресивність" до перевіряного – немає безпосереднього контакту людини з апаратурою, захоплення зображення райдужної оболонки проводиться просто при розгляданні в об'єктив сканера. Сканер аналізує якість зображення ока у кадрі, визначає центр зіниці, центр райдужної оболонки та її межі (рис. 2.21). Потім відбувається супроводжуване сигналом захоплення зображення, його кодування і перевірка за БД.

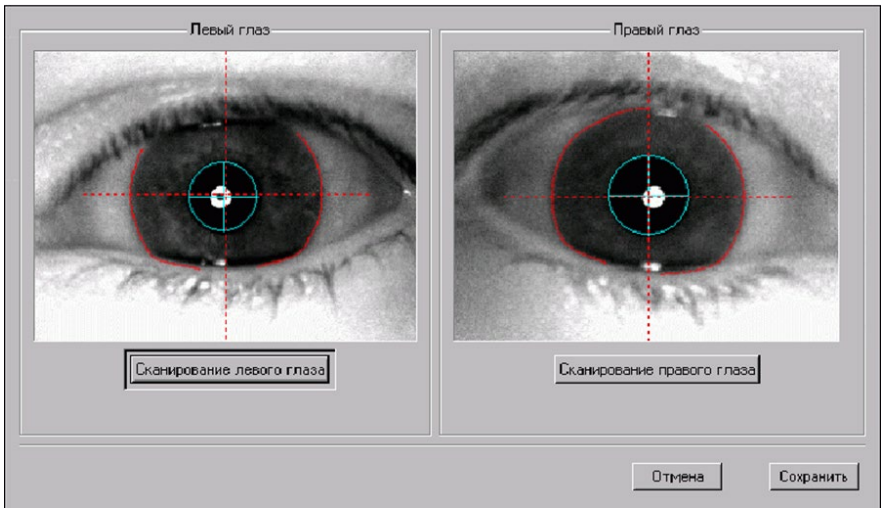


Рисунок 2.21 – Сканування райдужної оболонки ока системою

Можливості системи

Система Папилон «Циркон» надає наступні можливості:

– реєстрація та цифрове кодування зображення райдужної оболонки ока;

– створення і зберігання в електронній БД масиву записів, кожен з яких містить: закодоване зображення райдужної оболонки, текстові дані, фотографії зареєстрованої особи;

– перевірка коду райдужної оболонки за БД у режимі «один-до-багатьох»;

– перевірка коду райдужної оболонки за БД у режимі «один-до-одного»;

– робота з БД: отримання вибірок з БД, сортування списків БД, видалення і редагування записів тощо.

Система Папилон «Циркон» адаптована для інтеграції в автоматизовані системи контролю та управління доступом (СКУД). Для цього розроблено спеціалізоване програмне забезпечення ПАПИЛОН ЦИРКОН SDK, яке поставляться разом з блоком доступу ЦИРКОН-3Е.

Інгерація системи Папилон «Циркон» у діючу СКУД здійснюється шляхом встановлення ПО Папилон ЦИРКОН SDK на сервер та звернення до функцій Папилон ЦИРКОН SDK з боку клієнтського додатка.

Функції сервера покладаються на центральний вузол СКУД. Взаємодія вбудованого в ЦИРКОН-3Е обчислювача і центрального вузла СКУД здійснюється в локальній мережі за протоколом Ethernet. Передача команд між обчислювачем і кінцевим обладнанням СКУД – через інтерфейсний порт RS-232 (RS- 485).

Кожен блок доступу підтримує захоплення зображення райдужної оболонки ока як в режимі реєстрації, так і в режимах верифікації (порівняння з контрольним шаблоном "один-до-одного") або ідентифікації ("один-до-багатьох"). Для роботи в режимі верифікації блок доступу доповнюється вузлом зчитування персональних ID-карт.

Кожен блок доступу містить власну БД біометричних даних, чим забезпечується гнучкість налаштування системи і виключаються втрати часу,

пов'язані з внутрішньо мережевою взаємодією. У практичній реалізації СКУД доцільно залишити функцію реєстрації на одному або декількох блоках доступу. На інших здійснюється тільки операція ідентифікації/верифікації.

Територіальне масштабування системи забезпечується введенням додаткових блоків доступу з підключенням їх до центрального вузла СКУД по будь- яких доступних лініях зв'язку, що підтримують протокол TCP/IP. Кількість блоків доступу у системі не обмежується.

Типова схема інтеграції блоків доступу ЦИРКОН-3Е в діючу СКУД показана на рис. 2.22.

Блок доступу за райдужною оболонкою ока ЦИРКОН-3Е (рис. 2.23) являє собою кінцевий вузол реєстрації та розпізнавання за малюнком райдужної оболонки ока. Він призначений для захоплення й автоматичного порівняння зображень райдужної оболонки ока як в автономному режимі, так і у складі автоматизованої системи контролю та управління доступом (АСКУД) в режимах верифікації (порівняння з контрольним шаблоном «один-до-одного») або ідентифікації («один-до-багатьох »).

В автономному режимі реєстрація користувачів, створення та зберігання бази ключів здійснюється локально на блоці доступу. Блок завжди працює в режимі ідентифікації та за успішного розпізнавання керує електронним замком. При роботі блока у складі АСКУД в режимі верифікації база даних ключів може створюватися на пункті реєстрації і зберігатися на сервері. АСКУД взаємодіє з блоком доступу за протоколом, описаним в SDK. Ключ райдужної оболонки ока порівнюється «один-до-одного» з контрольним шаблоном за допомогою додаткового ідентифікатора – безконтактної картки, брелка і т. п.

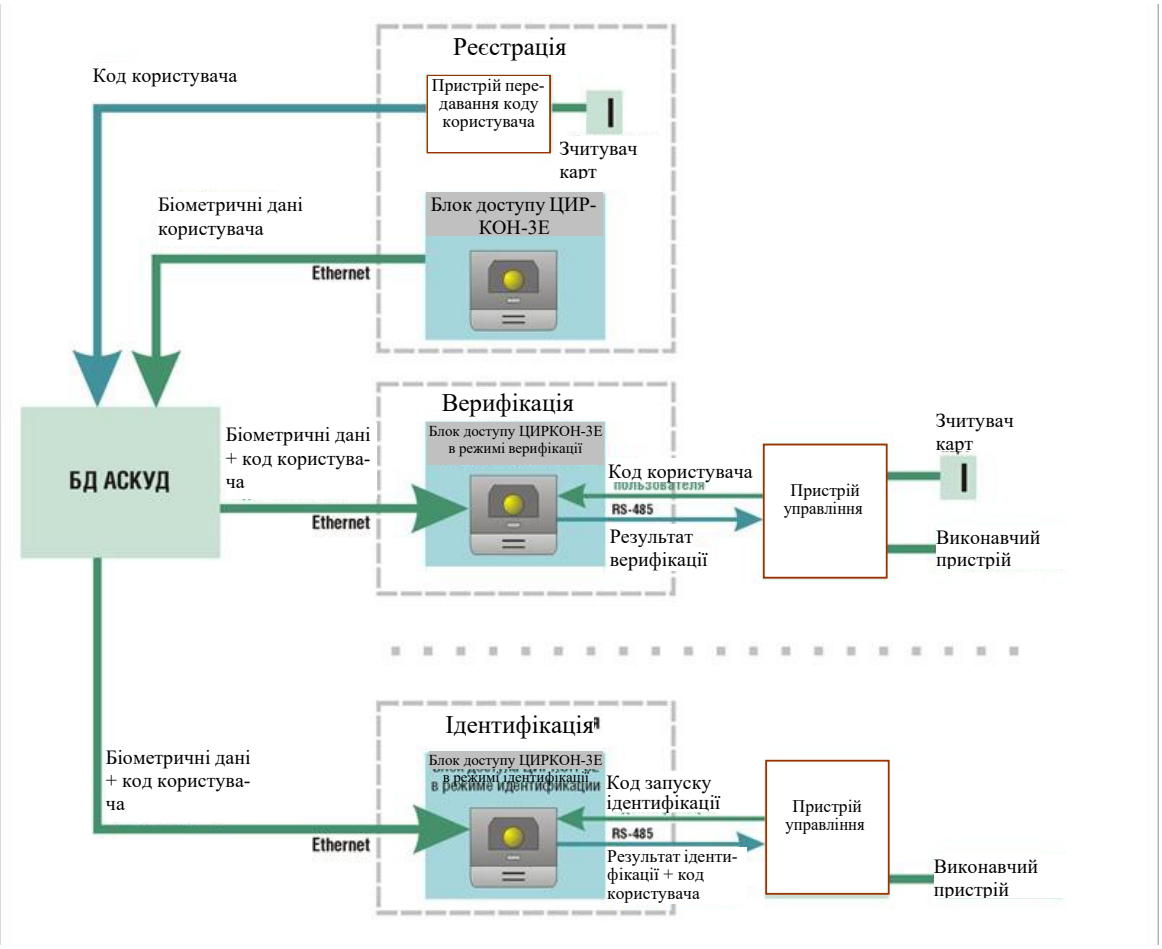


Рисунок 2.22 – Типова схема інтеграції блоків доступу ЦИРКОН-3Е до діючих СКУД

Рисунок 2.23– Блок доступу за радужною оболонкою ока ЦИРКОН-3Е

Відмінність роботи блоку в складі АСКУД в режимі ідентифікації полягає у тому, що ключ райдужної оболонки ока ідентифікованого суб'єкта порівнюється «один-до-багатьох» з усіма записами БД, завантаженими у блок доступу АСКУД.

Блок доступу розміщується в контрольованій точці перетину охоронного периметра і кріпиться на вертикальній поверхні в безпосередній близькості від обладнаного проходу в приміщення, із зовнішнього його боку.

Блок доступу обладнаний дзеркалом позиціонування і блоком світлодіодної індикації, також реалізована функція голосової підказки. Всі ці інструменти використовуються для спрощення позиціонування об'єкта в робочій області сканера. Для запуску процедури захоплення зображення достатньо підійти до блока доступу і побачити у дзеркалі позиціонування відображення свого ока. Захоплення зображення відбувається на відстані 200…300 мм від передньої панелі блока доступу в полі зору його оптичного блока.

Світлодіодна індикація «ближче-далі» функціонує за принципом: задіяна верхня група світлодіодів – «підійти ближче», нижня – «відійди далі».

У сканері райдужної оболонки реалізована функція автофокуса. Використовуване інфрачервоне підсвічування безпечне для зору. Сканер повертається у вертикальній площині для настроювання положення камери на зріст конкретної людини. У системі використовуються тільки чорно-білі зображення для того, щоб на результат ідентифікації особи не впливала колірна зміна райдужної оболонки, яка відбувається в результаті перенесених захворювань.

2.2.4 Система ідентифікації EyeSwipe Nano

EyeSwipe-Nano є локальною системою біометричної ідентифікації по базі райдужної оболонки ока. Розробником системи є компанія Eyelock.

EyeSwipe- Nano являє собою мініатюрну систему розпізнавання на основі аналізу райдужної оболонки ока, яка здатна забезпечити в режимі реального часу ідентифікацію та аутентифікацію особистості в русі й на відстані.

EyeSwipe Nano є ідеальною заміною для систем керування і контролю доступу (СКУД), заснованих на використанні персональних карт, і легко контролює доступ до об'єктів через турнікети та інші засоби доступу, вхід у серверні кімнати й будь-які інші приміщення, які потребують захисту.

Основу системи складає переносний сканер райдужної оболонки ока EyeLock (рис. 2.24).

Рисунок 2.24 – Сканер райдужної оболонки ока EyeLock

Пристрій є потужним і досить компактним, щоб забезпечити безпеку транзакцій підвищеної вартості та значущості, захистити критично важливі бази даних, мережеві робочі станції або будь-які інші інформаційні системи. Так само до складу системи входить пакет програмного забезпечення, яке

забезпечує роботу системи. EyeSwipe Nano є нейтральним відносно використовуваних алгоритмів і може використовуватися у поєднанні з будь-якими алгоритмами або існуючими базами даних. Сканер підключається за допомогою USB інтерфейсу до робочої станції. Ідентифікація користувача здійснюється за допомогою програмного забезпечення, яке встановлено на сервері.

Так само система EyeSwipe Nano має групові пристрої ідентифікації EyeSwipe Nano-TS. EyeSwipe Nano-TS (рис. 2.25) є турнікетним пристроєм ідентифікації й аутентифікації особистості, який здійснює в реальному часі зчитування й аналіз райдужної оболонки ока на відстані та у русі.

Рисунок 2.25 – Груповий термінал EyeSwipe Nano-TS

Пристрій був розроблений для встановлення на турнікетах або інших системах з великою пропускною здатністю і має широкий діапазон захоплення для підвищення простоти у використанні під час руху. EyeSwipe Nano-TS включає в себе інтегрований кардрідер для підтримки старих користувачів персональних карт і забезпечити плавний перехід до використання біометричних технологій допуску.

Використання індивідуальніх та групових сканерів райдужної оболонки ока та системного програмного забезпечення дозволяє реалізувати надійну й ефективну систему контролю доступу.

ВИСНОВОК ДО РОЗДІЛУ 2

Під час аналізу апаратної частини, було розглянуто пристрої для авторизації за допомогою відбитків пальців та параметрів геометрії ока.

Усі сканери відбитків пальців поділяється на 3 види:

- ✓ оптичні;
- ✓ напівпровідникові;
- ✓ ультразвукові.

Усі сканери ідентифікації за допомогою параметрів геометрії ока поділяються на два види:

- ✓ За радужною оболонкою ока;
- ✓ За сітківкою ока.

Для подальшої реалізації системи було обрано оптичний сканер відбитків пальців та сканер ідентифікації за радужною оболонкою ока.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ПРОЄКТУВАННЯ ПРИСТРОЮ

3.1. Визначення головних задач на проектування

Відповідно до завдання та на основі огляду літератури та патентної інформації за темою дипломного проєкту, визначено головні задачі на проектування:

1. Розробити апаратно - програмну систему ідентифікації на основі RFID технології та сенсора відбитків пальця.
2. Розробити концептуальну та функціональну схеми пристрою СКУД з двофакторною автентифікацією.
3. Представити концепцію та алгоритм роботи програмного забезпечення на основі відлагоджувальної плати Arduino.
4. Розробити програмне забезпечення для мікроконтролера Arduino.

Проєктування даної системи вирішить наступні задачі:

- Дозволить вирішити питання підвищення рівня безпеки лабораторного обладнання за рахунок інтеграції додаткового рівня ідентифікації персоналу.
- Забезпечить можливість моніторингу відвідування лабораторного приміщення персоналом.
- Унеможливлює несанкціоноване проникнення сторонніх осіб до контрольованого системою приміщення.
- Система має широкі можливості для модернізації

Таким чином, розробка є актуальною, адже більшість лабораторних приміщень в Україні контролюється особисто працівниками та лаборантами, натомість пропонується автоматизувати контроль доступу до приміщення з метою нівелювання людського фактору та пов'язаних з ним помилок, а також ведення електронного журналу відвідування.

3.2. Розробка функціональної схеми роботи пристрою та структурної схеми розташування елементів системи СКУД для лабораторного приміщення.

Згідно завдання на проектування та враховуючи можливі недоліки, переваги та вимоги до подібних розробок, запропонована система має складатися з наступних функціональних блоків:

- Драйвер інтерфейсу карток Mifare MFRC522;
- Сенсор відбитків пальця R307
- Відлагоджувальна плата Arduino UNO;
- Перетворювач USB-RS232;
- Двострочний дисплей 1602 з інтерфейсом i2c
- Світлозвуковий індикатор, кнопки
- Реле
- Електромагнітний замок
- Блок автономного живлення

На рис.3.1. зображено функціональну схему роботи пристрою СКУД, що відображає необхідні процеси та дії для проходження двофакторної автентифікації людини за допомогою персональної RFID картки та відбитка пальця.

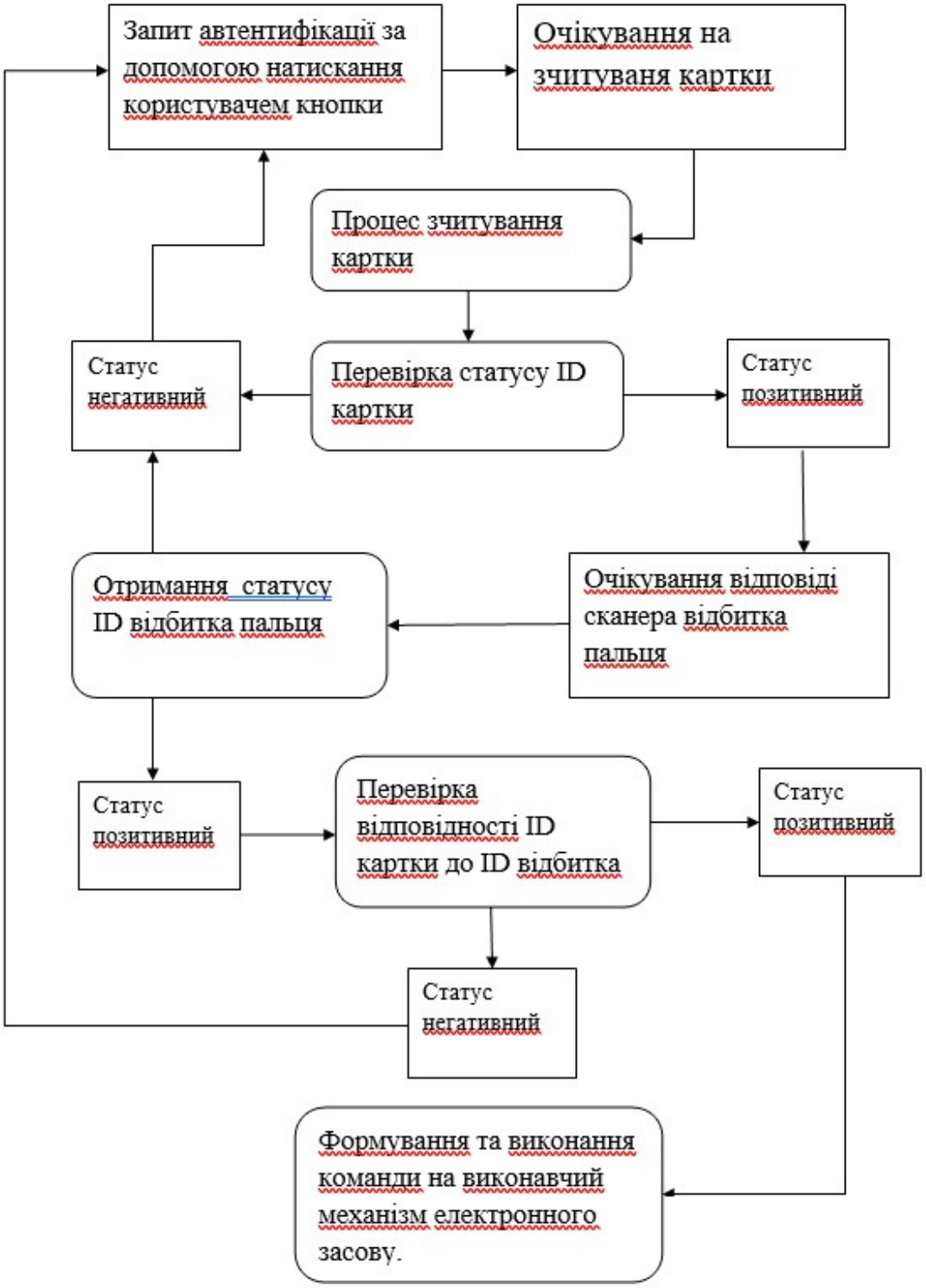


Рис.3.1. Функціональна схема роботи пристрою

Згідно даної схеми, працівник, що має доступ до захищеного цією системою приміщення, отримує доступ до цього приміщення тільки тоді, коли співпадуть обидва фактори автентифікації, тобто авторизуватися ключ-картою іншого працівника, при цьому скориставшись власним відбитком пальця є неможливим.

Для проходження процедури двофакторної автентифікації необхідно активувати користувацьку панель за допомогою натиснення кнопки запиту автентифікації, піднести до зчитувача свою ключ-картку, дочекатися індикації успішного зчитування картки та активації сканера відбитків пальця, покласти до сканера відбитків пальця саме той палець, який було зареєстровано в системі, дочекатися індикації розблокування електронного замка та відчинити двері. Блокування дверей відбудеться автоматично за допомогою пневматичного доводчика дверей та електронного засову.

Структурна схема (Рис.3.2.) системи ілюструє блоки пристрою та зв'язки між ними, де сенсори знаходяться у зовнішньому антивандальному блоці, який є доступним для взаємодії між системою та людиною, тобто знаходиться поза межі приміщення до якого має надаватись або не надаватись доступ. А також внутрішній блок, який містить автоматичну систему прийняття рішень на основі мікроконтролера та його програмного забезпечення, автономне джерело живлення, основне джерело живлення від побутової мережі 220\230В, захищений від впливу мережевих та інших радіозавад виконавчий механізм - електромагнітний засов.

Відлагоджувальна плата Arduino UNO вже містить базовий фільтр, що захищає схему від мережевих завад, а також стабілізатор напруги 5В, AMS1117-5,0. Тому стабілізатор напруги 5 В встановлювати додатково немає потреби, також можна виключити зі складу схеми стабілізатор 12В, оскільки електромагнітний замок може працювати у широкому діапазоні напруг, як правило від 9В до 28В, без змін у надійності спрацьовування.

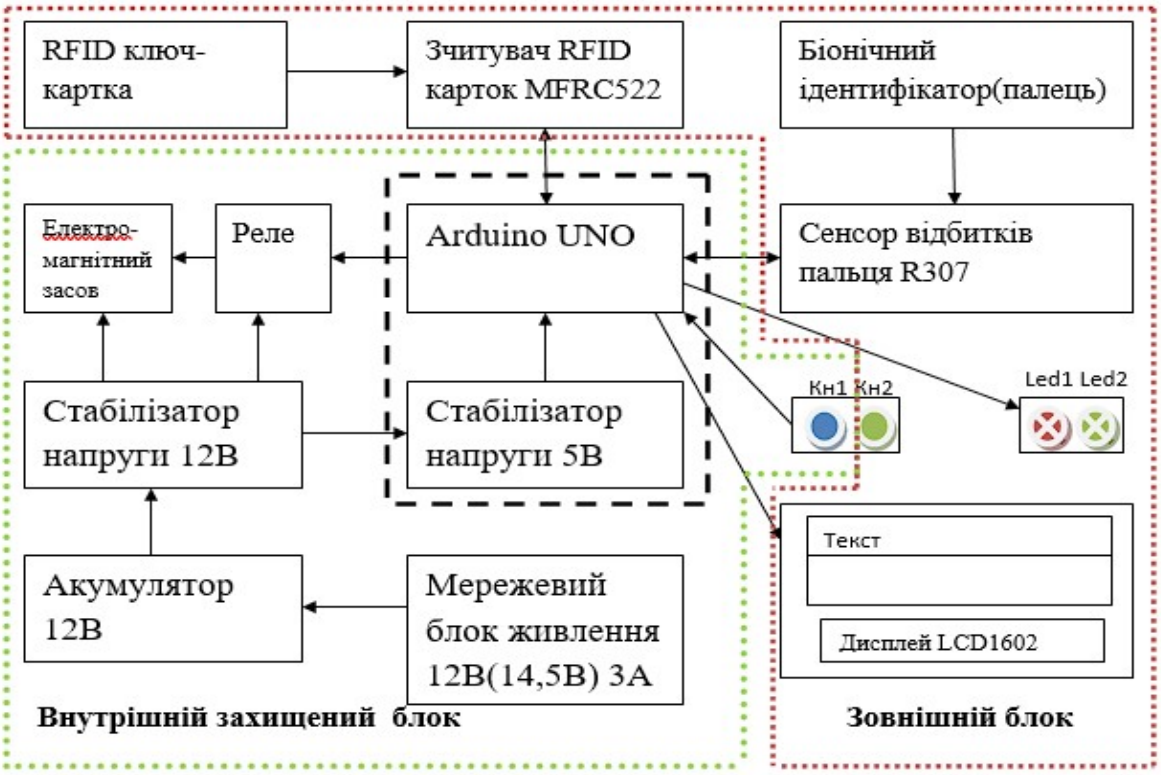


Рис.3.2. Структурна схема розташування елементів

3.3. Технічні дані елементів системи

Для побудови принципової схеми пристрою необхідно розглянути основні технічні дані блоків, модулів та інших елементів системи, їх переваги і недоліки, а також дослідити принцип роботи деяких з них.

Сенсор відбитків пальця R307

Ці сенсори включають DSP чіп, який обробляє зображення, виконує необхідні розрахунки для виявлення відповідності між записаними і поточними даними. Недорогі датчики відбитків пальців дозволяють записати до 162 різних відбитків пальців.

Сенсор(Рис.3.3.) поставляється із софтом для Windows, що значно полегшує його тестування. За допомогою рідного софту можна навіть відобразити фотографію відсканованого відбитка на моніторі ПК. Існує

окрема бібліотека для Arduino, з використанням якої можна налаштувати датчик менше ніж за 5 хвилин.

Технічні характеристики:

- Напруга живлення: 3.6 – 6.0 В (постійний струм);
- Робоча сила струму: 120 мА;
- Максимальна сила струму: 150 мА;
- Час обробки зображення відбитка: < 1.0 секунд;
- Розмір вікна: 14 мм х 18 мм;
- Кількість файлів, що одночасно записуються: 162 файлів;
- Вибір рівня безпеки (від 1 до 5);
- Інтерфейс (підключення): TTL послідовний;
- Швидкість передачі (Baud rate): 9600, 19200, 28800, 38400, 57600
- Робочий діапазон температур: від -20 °C до +50 °C;
- Допустимий рівень вологості: 40% - 85% RH;
- Габаритні розміри: 56 х 20 х 21.5 мм;
- Вага: 20 грам.

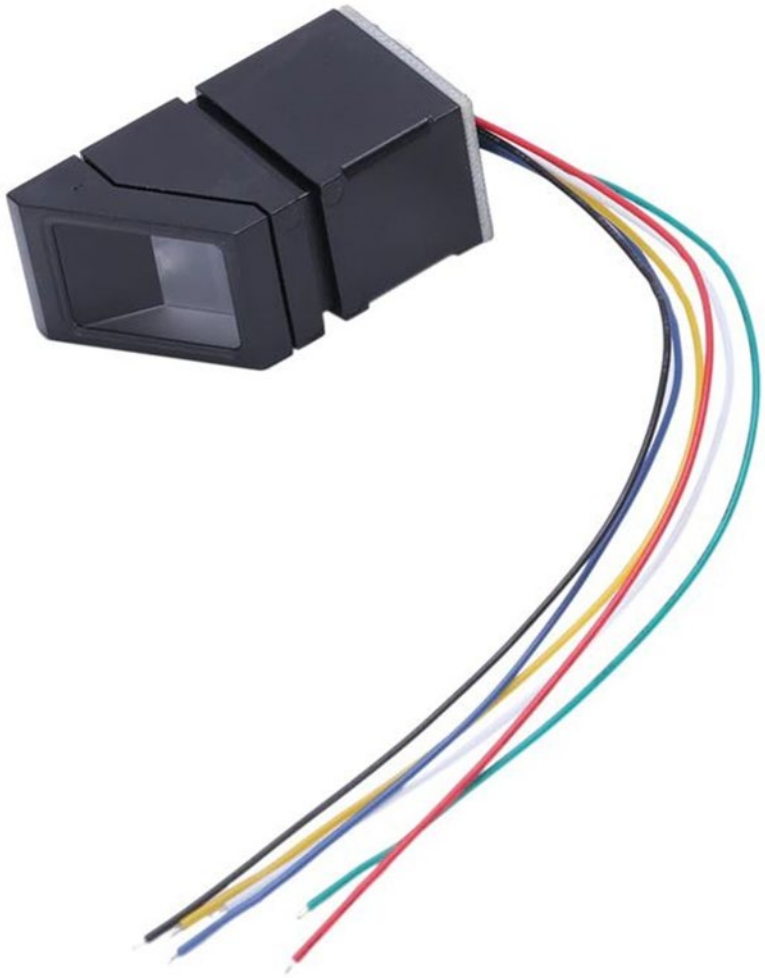


Рис.3.3. Сканер відбитків пальців R307

При використанні датчика відбитка пальців є два основні кроки. Спочатку вам треба записати дані в пам'ять сенсора, тобто присвоїти свій унікальний ID кожному відбитку, який ви використовуватимете для співставлення надалі. Після запису даних, можна переходити до 'пошуку', порівнюючи поточне зображення відбитка з тими, які записані в пам'яті датчика.

Переваги:

- Простота у використанні
- Низька ціна
- Потужний DSP

Недоліки:

- Недостатньо захищений інтерфейс команд, потребує додаткової обробки мікроконтролером

Зарядний пристрій UKC Battery Charger MA-1205A 12V, 5A

Рис.3.4. Зарядний пристрій

Зарядний пристрій UKC Battery Charger MA-1205A (Рис.3.4.) для 12-вольтового свинцевого акумулятора. У приладі є захист від перегріву, також додатково встановлений потужний вентилятор для активного охолодження.

Має вбудований датчик заряду, при повному зарядженні акумулятора прилад автоматично вимикається. Зарядний пристрій має якісний мікропроцесор, який стійкий до перепадів температур -40°C до +105°C.

Технічні характеристики:

- Захист від замикання
- Струм заряду до: 5A
- Напруга, вольт: 12V
- Спосіб заряджання: Автоматична зарядка
- Тип зарядного пристрою: Імпульсні

- Наявність активного охолодження: Є
- Чотири рівні заряду
- Захист від неправильної полярності
- Вхідна напруга: AC 220V
- Витримує перепади температури: -40°C. +105°C
- Колір корпусу: чорний
- Матеріал корпусу: Пластик

Переваги:

- Низька ціна
- Активне охолодження
- Автоматичне вимкнення при високому рівні заряду АКБ

Недоліки: не виявлено.

RFID-модуль RC522

Радіочастотна ідентифікація (RFID) – технологія безконтактної ідентифікації об'єктів за допомогою радіочастотного каналу зв'язку. Ідентифікація об'єктів здійснюється за унікальним ідентифікатором, який має кожна електронна мітка. Зчитувач випромінює електромагнітні хвилі певної частоти. Мітки надсилають у відповідь інформацію – ідентифікаційний номер та дані пам'яті.

Мітки бувають двох типів: активні та пасивні (без вбудованого джерела енергії, живляться від струму, індукованого в антені сигналом від зчитувача).

Мітки працюють на різній частоті:

- LF (125 – 134 кГц)
- HF (13.56 МГц)
- UHF (860 – 960 МГц)

Мітки бувають лише для читання або читання та запису. В середовищі Arduino в якості зчитувача використовують популярний модуль RFID-RC522.

Модуль виконаний на мікросхемі MFRC522 фірми NXP, яка забезпечує роботу з мітками HF (на частоті 13,56 МГц). У комплекті з модулем RFID-

RC522(Рис.3.5.) йдуть дві мітки, одна у вигляді карти, інша у вигляді брелока(Рис.3.6.).

Рис.3.5. Зовнішній вигляд модуля RFID-RC522.

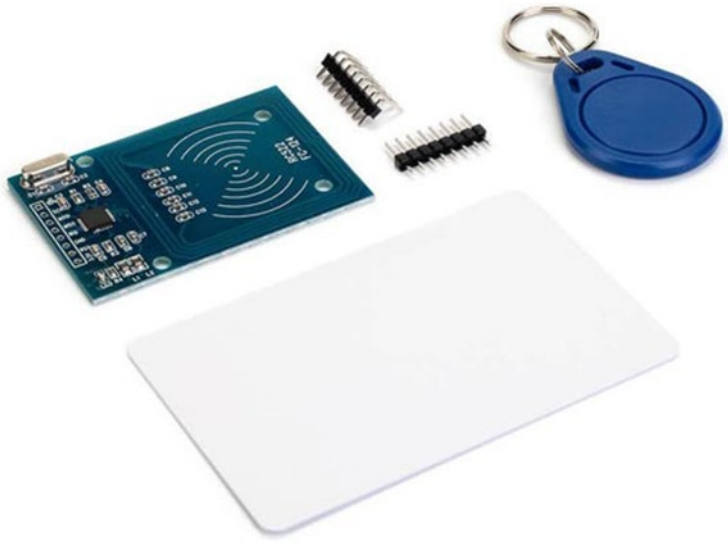


Рис.3.6. Загальне фото модуля RFID-RC522 та міток

Мікросхема MFRC522 підтримує інтерфейси SPI, UART та I2C. Вибір інтерфейсу здійснюється встановленням логічних рівнів певних контактах мікросхеми. В Arduino зазвичай використовують SPI.

Технічні характеристики:

- Напруга живлення: 3.3V
- Споживаний струм :13-26mA
- Робоча частота: 13.56MHz
- Дальність зчитування: до 6 см
- Інтерфейс: SPI
- Швидкість передачі: максимальна 10Мбіт/с
- Розмір: 40мм х 60мм

Переваги:

- Наднизька ціна зчитувача та міток
- Компактні розміри
- Висока точність

Недоліки:

- Мала робоча відстань
- Несумісність з деякими мітками інших виробників

Модуль реле 5В 10А з оптозв'язкою

Реле-модуль(Рис.3.7.). Може керуватися безпосередньо більшістю мікроконтролерів: Arduino, AVR, PIC, ARM і MSP430.

Рис.3.7. Модуль реле

Характеристики:

- Струм спрацьовування: 15-20мА при напрузі 12 В
- Керування: 5В TTL, який може бути поданий безпосередньо з виходу мікроконтролера
- Комутоване навантаження: 10А при 250В
- Розміри модуля: 39.5 мм х 51 мм

Акумуляторна батарея

Особливість герметичних кислотно-свинцевих акумуляторів(рис.3.8.) полягає в тому, що електроліт у них не рідкий, а гелеподібний. Корпус акумуляторів герметичний. Ці якості дозволяють використовувати акумуляторну батарею в будь-якому положенні, не побоюючись витоку електроліту. Гелієві кислотно-свинцеві батареї не вимагають періодичного поповнення електроліту.

Крім перерахованих якостей герметичні свинцево-кислотні акумулятори не бояться глибокого розряду, можуть тривалий час зберігатися в зарядженому стані при малому струмі саморозрядження. Також гелієві акумулятори позбавлені "ефекту пам'яті".

За рахунок використання електродів із ефективного свинцево-кальцієвого сплаву акумуляторні батареї мають тривалий термін служби та працездатні при інтервалі температур від -200 °С до +500 °С.

Рис.3.8. Кислотно-свинцевий акумулятор X-Digital SPb 12-100

Характеристики:

- Номінальна напруга 12 V
- Місткість 100 Ah
- Внутрішній опір 4.5 mΩ
- Тип клем T10, T60
- Габаритні розміри 173 x 331 x 213 мм
- Вага 28.5 кг

Переваги:

- Надійність
- Велика ємність

Недоліки: Вага

3.4. Принципова електрична схема

На основі розробленої структурної та функціональної схеми розроблено електричну принципову схему(див. Додаток 1).

Оскільки система побудована за модульною структурою, тому необхідно виконати схему з'єднань та узгоджень модулів, таких як Arduino

UNO, що має відому стандартизовану принципову схему, яку окремо розглядати немає потреби.

Окремо слід розглянути схему модуля реле, захищеного від стрибків напруги(Рис.3.9.), що дозволяє підключати навантаження з високим ЕРС самоіндукції.

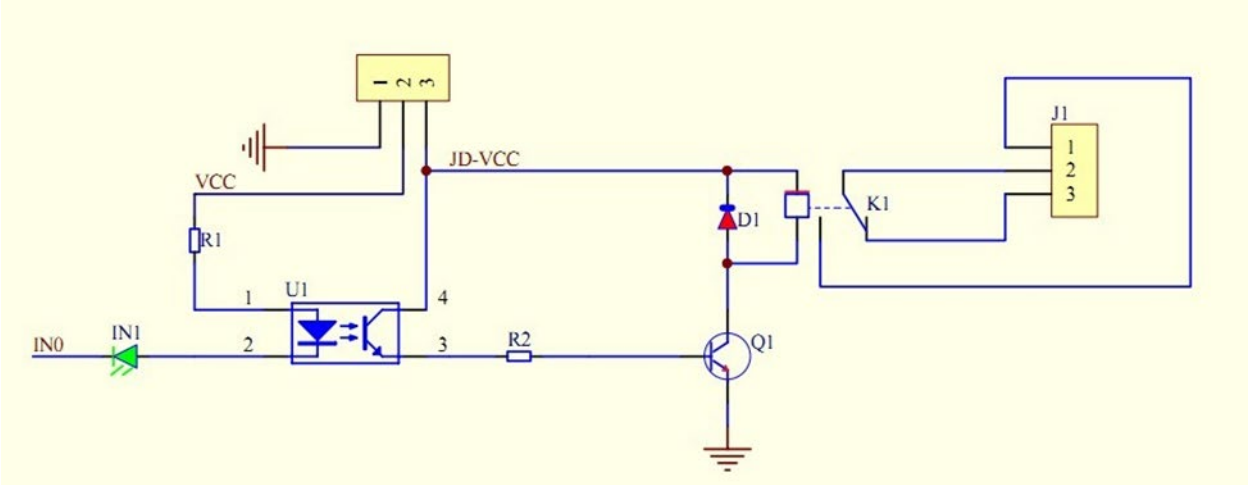
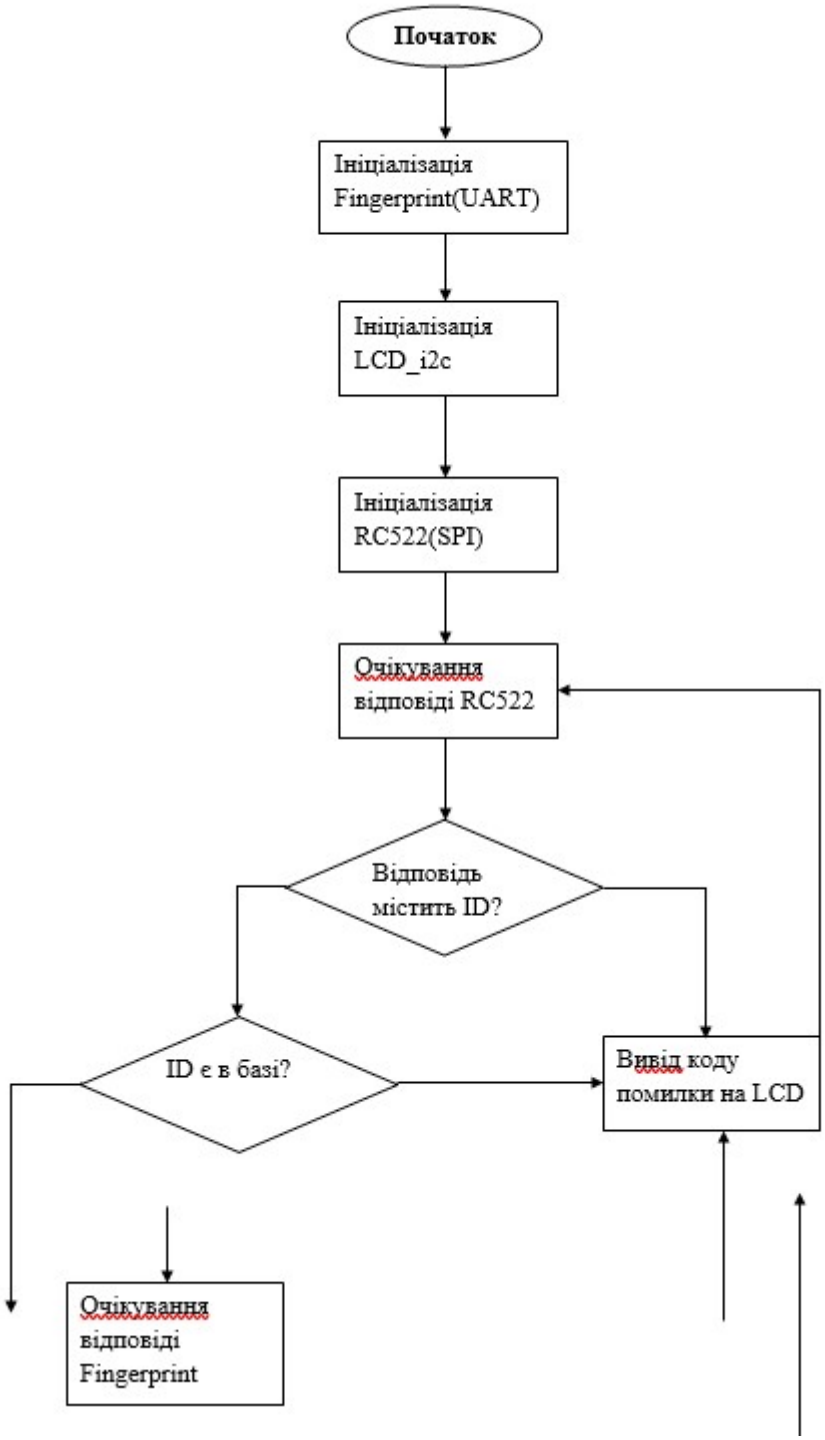


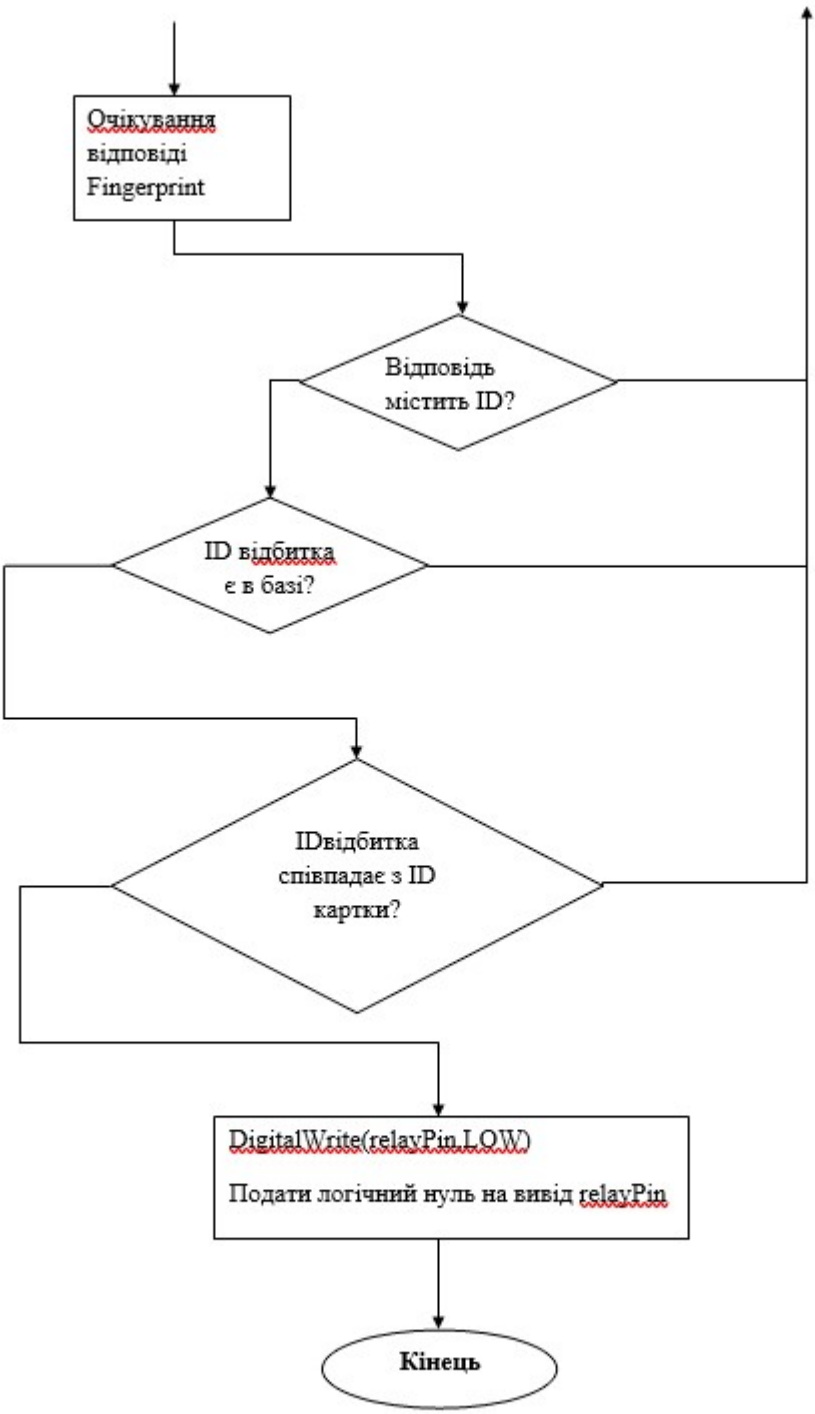
Рис.3.9. Схема модуля реле

На даній схемі напруга на котушку реле подається не напряму з вивода мікроконтролера, а спочатку гальванічно відокремлюється від самого реле за допомогою оптопари U1 , але струм колектор-еміттер оптопари все ще недостатній для спрацювання котушки реле К1, тому для підсилення використовується транзистор Q1, а також діод D1 для погашення ЕРС самоіндукції, яка може виникати в котушці реле після того як закривається транзистор Q1, і спрямована на U1 та Q1.

Таким чином електромагнітні завади, що створюються роботою реле, а також електромагнітним навантаженням, не впливають на роботу мікроконтролера, оскільки відсутній гальванічний зв'язок між ними, адже схема даного реле може бути заживлена від окремого стабілізатора напруги.

3.5. Блок – схема алгоритму роботи пристрою




Очікування відповіді Fingerprint
Відповідь містить ID?
ID відбитка є в базі?
IDвідбитка співпадає з ID картки?
DigitalWrite(relayPin,LOW)
Подати логічний нуль на вивід relayPin
Кінець

3.6. Розробка програмного забезпечення для мікроконтролера Arduino

Для вирішення завдання програмування необхідно завантажити середовище програмування ARDUINO IDE версії не нижче 1.6.2, а також завантажити та підключити необхідні для роботи бібліотеки :

- Adafruit_fingerprint.h
- LiquidCrystal_i2c.h
- MFRC522.h
- Wire.h
- SPI.h
- SoftwareSerial.h

Перед початком програмування необхідно виготовити макет пристрою за допомогою макетної плати або з'єднати дротами всі модулі за схемою (див. ДОДАТОК 1).

Під'єднати до ПК за допомогою USB кабеля плату Arduino UNO, встановити відповідний драйвер(в даному випадку для CH340).

Дослідивши основні необхідні класи та функції платформи та бібліотек, наведені далі, вирішено розробити програмне забезпечення для відлагоджувальної плати ARDUINO UNO, адже всі бібліотеки задовольняють вимоги апаратного забезпечення.

Також для забезпечення роботи з модулем R307 необхідно завантажити в його базу кілька тестових відбитків пальців, для цього треба скористатись спеціальним скетчем для Ардуїно, який створює міст між ПК та модулем в обхід мікроконтролера, а також фірмовим програмним забезпеченням SFGDemo.exe, завантаженим з офіційного сайту. Заведення відбитків в базу а також налаштування модуля проводяться за допомогою цього ПЗ.

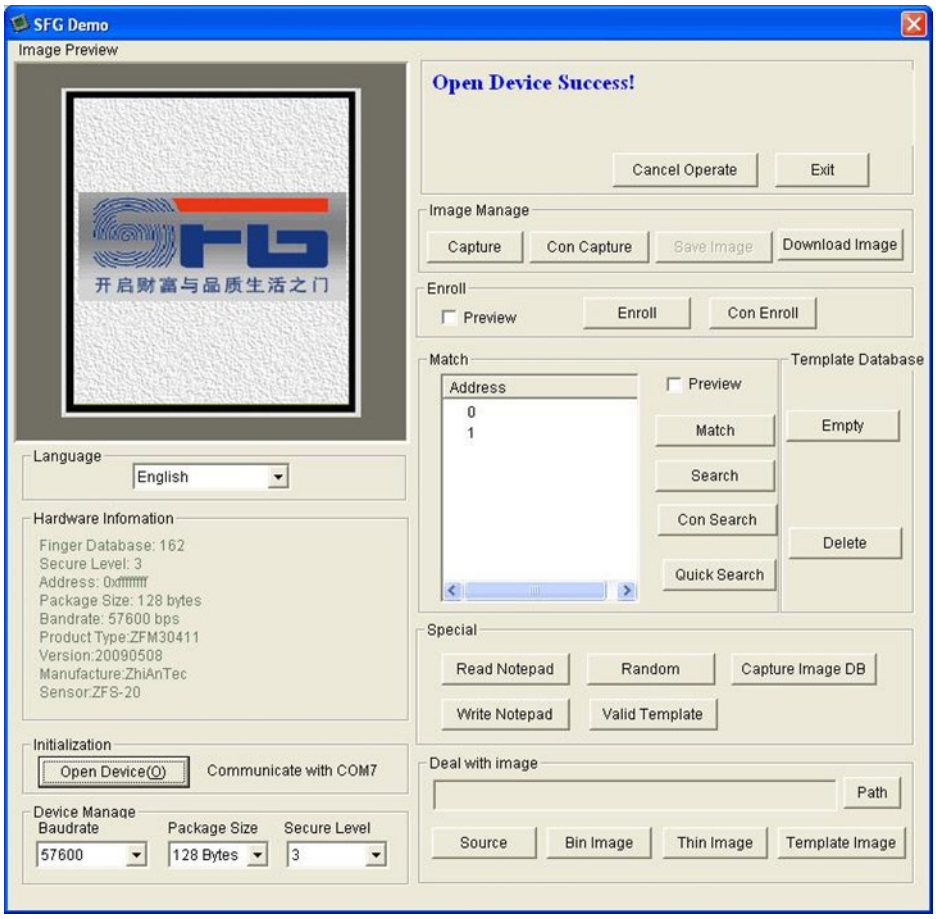


Рис.3.11. Головне вікно SFGDemo

Код програми - моста:

```
#include <SoftwareSerial.h>
SoftwareSerial mySerial(2, 3);
void setup() {
mySerial.begin(9600);
Serial.begin(9600);
}
void loop()
{
while (Serial.available())
mySerial.write(Serial.read());
while (Serial1.available())
Serial.write(mySerial.read());
}
```

За допомогою цього скетчу та програми SFGDemo завантажимо декілька відбитків пальців у сканер:

1. Необхідно підключити плату до ПК, запустити програму та обрати відповідний COM - порт плати у меню програми як указано на (Рис.3.12)

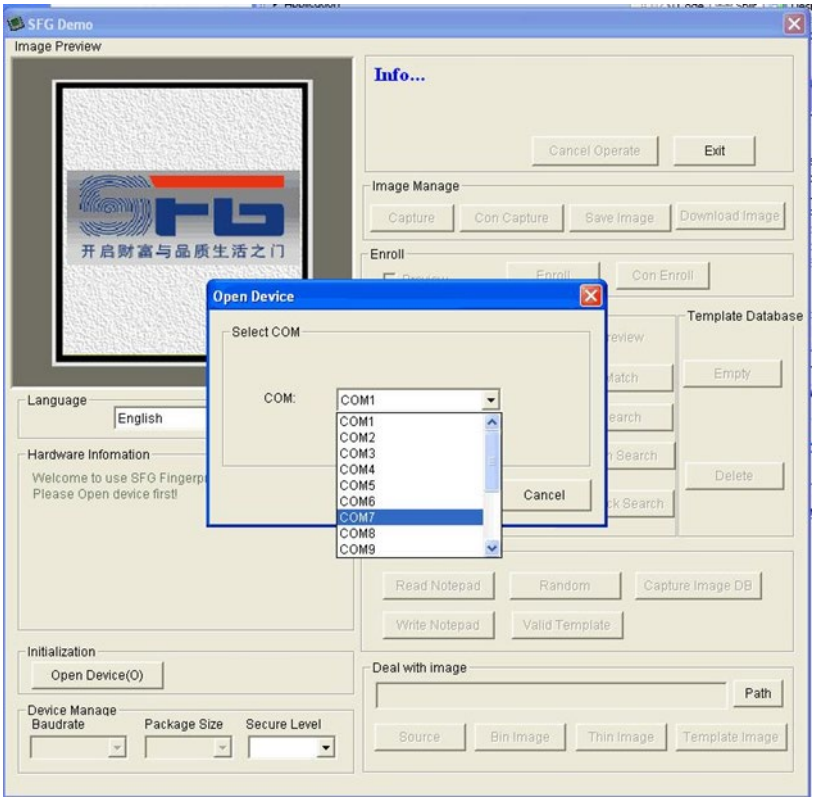


Рис.3.12. Вікно вибору COM – порта

Після вибору натисніть OK. В результаті має відобразитися синій напис про успішне відкриття пристрою та системні дані про пристрій. Можна змінити швидкість передачі даних (baund rate) у нижньому лівому куті та рівень безпеки (security level), але не рекомендується чіпати ці налаштування, поки ви не переконаєтесь, що все працює.

За замовчуванням швидкість передачі даних дорівнює 9600 baud, а рівень безпеки дорівнює 2.

2. Тепер потрібно завантажити відбиток пальця. Виберіть пункт меню Preview і натисніть кнопку Enroll поряд (Con Enroll означає 'Continuous' (без зупинки). Зручна опція, якщо ви збираєтеся записувати багато відбитків пальців). Коли з'явиться нове меню, вказати ID #(Рис.3.13), який потрібно використовувати. Максимум можна використовувати 162 ID номери.

Рис.3.13. Вікно вводу ID

3. Потім програма запропонує покласти палець до сканера(Рис.3.14)

Рис.3.14. Вікно статусу сканера

Після даної процедури можна побачити попередній перегляд вашого відбитка пальця(Рис.3.15.).

Далі потрібно буде повторити процес із тим самим пальцем, це необхідно для підвищення точності образу. Після успішного завершення, ви побачите повідомлення на Рис.3.16.

Рис.3.15. Вікно попереднього перегляду

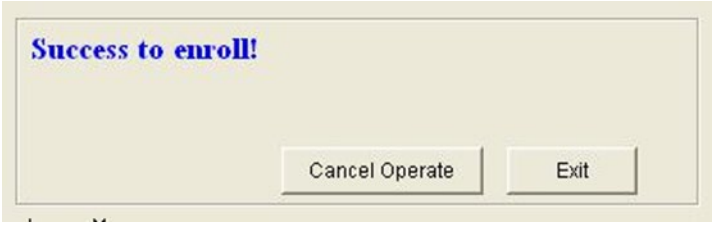


Рис.3.16. Вікно повідомлення успішного запису

4. Після завантаження зображення бажано перевірити, чи з'явилося воно у базі сенсора. Для цього потрібно кнопку Search, що знаходиться праворуч.

Коли з'явиться запит, прикладіть інший палець до датчика відбитка пальця.

Якщо це той самий палець, має з'явитися вікно з ID # (Рис.3.17.)

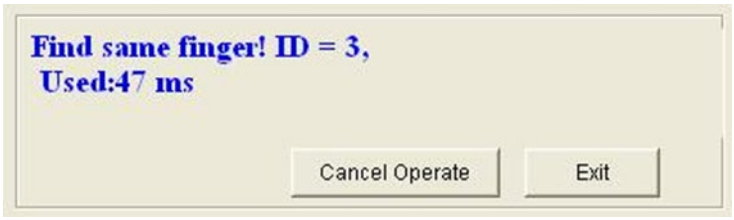


Рис.3.17. Вікно повідомлення, ID підтверджено

Якщо цього відбитка немає у базі даних, з'явиться вікно із попередженням(Рис.3.18.)

Рис.3.18. Вікно повідомлення, ID не підтверджено

Таким чином маємо можливість легко додавати та видаляти відбитки користувачів у базі без застосування всієї апаратної частини, це може бути корисним, тому що образи відбитків немає потреби зберігати у пам'яті мікроконтролера.

5. Також необхідно додати до системи RFID мітки, в даній роботі додаватимемо картки за допомогою зчитування ID картки та запису їх до ПЗП мікроконтролера вручну, скориставшись скетчем, що зчитує картку та виводить ID картки у COM порт. Отримані ідентифікаційні номери додаються

до масиву - таблиці співпадінь. Тобто під час перевірки, якщо порядковий номер ID картки співпадає з порядковим номером відбитка то функція видає TRUE, інакше - FALSE.

Деякі необхідні функції класів розглянемо більш детально:

Adafruit_fingerprint.h

Для роботи цієї бібліотеки необхідно підключити відповідний модуль, а також прописати в заголовку програми бібліотеку "SoftwareSerial.h", так як

вона забезпечує обмін даними між модулем R307 та платою ARDUINO UNO, у той час як "Adafruit_fingerprint.h" забезпечує обробку отриманих даних та надсилає команди модулю. Для цього необхідно об'явити її за наступним зразком:

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

// оголошуємо об'єкт finger до роботи з бібліотекою Adafruit_Fingerprint ІМ'Я_ОБ'ЄКТА = Adafruit_Fingerprint(ПАРАМЕТР); // ПАРАМЕТР - посилання об'єкт до роботи з UART якого підключений модуль, наприклад: &Serial1

За тим необхідно у секції Setup() розпочати роботу з модулем :

"finger.begin(9600);", де 9600 - швидкість UART в бод.

Після цього можна працювати з даним об'єктом.

finger.getImage(); - захоплюємо зображення, якщо результат виконання дорівнює константі FINGERPRINT_OK (коректне завантаження зображення), то проходимо далі, інакше повертає помилку:

FINGERPRINT_PACKETRECIEVEERR: - помилка з'єднання,

FINGERPRINT_NOFINGER: - помилка піротехніка, не вдалося знайти палець:),

FINGERPRINT_IMAGEFAIL:, FINGERPRINT_INVALIDIMAGE: - помилка образу,

Коди цих помилок можуть бути виведені на дисплей пристрою з метою інформування про помилкові діїї користувача.

finger.image2Tz(); - Конвертуємо отримане зображення, якщо результат виконання дорівнює константі FINGERPRINT_OK (зображення конвертовано), то проходимо далі, інакше - починаємо з початку.

finger.fingerFastSearch(); - Знаходимо відповідність у базі даних відбитків пальців, якщо результат виконання дорівнює константі FINGERPRINT_OK (знайдено відповідність), то проходимо далі, інакше - починаємо з початку.

finger.fingerID - ідентифікаційний номер відбитка в базі, функція "finger.fingerFastSearch();" повертає його у разі співпадіння.

finger.confidence - рівень безпеки образувід 0 до 5, чим мешне цей індекс тим швидше проходить зчитування та порівняння, чим він більший тим більше шанс на помилку при зчитуванні та порівнянні. зазвичай індекс 1-2 достатньо для нормальної роботи.

MFRC522.h:

Для роботи цієї бібліотеки необхідно підключити відповідний модуль, а також прописати в заголовку програми бібліотеку ***"SPI.h"***, так як

вона забезпечує обмін даними між модулем RFID та мікроконтролером.

MFRC522 mfrc522(SS_PIN, RST_PIN); - Створюємо об'єкт

SPI.begin(); - активуємо шину SPI

mfrc522.PCD_Init(); - ініціюємо об'єкт

mfrc522.PICC_IsNewCardPresent() - повертає статус присутності мітки у зоні дії електромагнітного поля зчитувача

mfrc522.PICC_ReadCardSerial() - зчитує та повертає ID мітки у форматі BYTE

mfrc522.PICC_HaltA() - зупиняє взаємодію з міткою

mfrc522.PICC_DumpToSerial() - виводить всі дані мітки до терміналу COM порта.

LiquidCrystal_I2C.h:

Для роботи цієї бібліотеки необхідно підключити відповідний модуль, а також прописати в заголовку програми бібліотеку ***"Wire.h"***, так як

вона забезпечує обмін даними між модулем дисплея та мікроконтролером.

LiquidCrystal_I2C lcd(0x27,16,2); - створюємо об'єкт дисплею, де: 0x27 - адреса дисплея на шині, 16 - кількість знакомісць у строках, 2 - кількість строк.

lcd.init(); - ініціювання шини та дисплею.

lcd.clear(); - очищення буфера дисплея.

lcd.write("дані"); - записує в буфер дисплея текст та виводить його на LCD.

lcd.setCursor(x,y); - встановлює курсор на строку "y" та символ "x".

lcd.print("Text") - виводить на LCD текст з вбудованої таблиці знаків.

3.7. Перспективи розвинення та покращення запропонованої системи

У подальному, під час підготовки до захисту дипломної роботи Магістратури, планую виконати наступні модернізації та покращення розробленої системи:

1. Реалізувати налаштування системи та додавання і видалення користувачів без ПК, за допомогою майстер-ключа.

2. Реалізувати можливість віддаленого контролю та моніторингу користувачів, за допомогою бездротових мережевих технологій.

3. Додати можливість взіємодії системи з пропонованими на ринку України стандартизованими охоронними та протипожежними системами, або інтеграції у такі системи за відповідністю до загальноприйнятих стандартів.

4. Додати можливість ідентифікації за допомогою райдужної оболонки ока.

ВИСНОВОК ДО РОЗДІЛУ 3

Відповідно до завдання в вирішено наступні задачі:

- Розглянуто особливості RFID модуля безконтактної ідентифікації та сканера відбитків пальців.
- Досліджено та вирішене питання сполучення модулів з периферійним обладнанням за допомогою USB та UART протоколу.
- Вирішено питання програмування мікропроцесорних модулів на базі ATmega328 в середовищі Arduino.
- Розроблено концептуальну та функціональну схеми пристрою СКУД з двофакторною автентифікацією.
- Розроблено покрокові інструкції налаштування та перевірки роботи системи у складі комплексу: мікропроцесорний модуль – сканер відбитків, та RFID модуль
- Представлено концепцію та алгоритм роботи програмного забезпечення на основі відлагоджувальної плати Arduino.
- Розробити програмне забезпечення для мікроконтролера Arduino.

Охорона праці

Спеціальний розділ до дипломної роботи бакалавра

на тему: «Охорона праці та безпека в недзвичайних ситуаціях»

Спеціальність «Комп'ютерна інженерія»

123 – БР.ПЗ.00 – 405з.21920504

Студент _____

«» червня 2022 р.

Керівник _____В.В.Старченко

ст. викладач

«» червня 2022 р.

Консультант _____А. О. Алексеєва

ст. викладач

«» червня 2022 р.

МИКОЛАЇВ – 2022

РОЗДІЛ 4

ОХОРОНА ПРАЦІ

Науково-технічний прогрес відіграє важливу роль у можливості безпечного виконання людьми своїх трудових обов'язків. Охорона праці – найважливіша державна задача, так як у її основі лежить турбота про здоров'я і життя людей. Значимість цієї функції держави підтверджується прийнятими і чинними у нашій країні законодавчими актами, що визначають основні положення з питань охорони праці, а саме, загальні закони України, а також спеціальні законодавчі акти. До загальних законів, що визначають основні положення про охорону праці, належать: Конституція України, Закони України «Про охорону праці», «Про охорону здоров'я», «Про пожежну безпеку», «Про використання ядерної енергії та радіаційний захист», «Про забезпечення санітарного та епідемічного благополуччя населення», «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності», Кодекс законів про працю України (КЗпП). Спеціальними законодавчими актами у галузі охорони праці є нормативно-правові акти з охорони праці, Державні стандарти Системи стандартів безпеки праці, Будівельні норми та правила, Санітарні норми, Правила безпечної експлуатації електроустановок споживачів та інші нормативно-правові акти, якими регламентуються загальнообов'язкові правила (норми) [1]. Також в Україні створено спеціальну службу – Державний комітет нагляду з охорони праці.

Сьогодні велика кількість людей працює у маленьких офісах та, як правило, організація робочого місця працівників, на перший погляд, не спричиняє будь-яких ускладнень для роботодавців. Але від правильної організації робочих місць залежить продуктивність праці, здоров'я, комунікабельність і мобільність працівників, задіяних у виконанні трудових

функцій. Отже, у цьому розділі будуть розглядатися загальні підходи до організації праці на прикладі працівників, які виконують роботи з написання застосунків з використанням ЕОМ та інших мобільних пристроїв. Також особливу увагу буде приділено нормам освітлення у виробничих приміщеннях.

4.1 Основні положення Закону України «Про охорону праці»

Специфічною особливістю Закону України «Про охорону праці», що регламентує правову основу охорони праці, є високий рівень прав і гарантій працівників. Уперше в історії держави працівнику було надано право відмовитися від дорученої роботи, якщо створилася виробнича ситуація небезпечна для його життя чи здоров'я, або для людей, які його оточують, і навколишнього природного середовища. Розширено права працівників у соціальних гарантіях відшкодування збитків у випадках ушкодження їх здоров'я на виробництві. Передбачається нова система фінансування охорони праці, формування системи страхування від нещасних випадків і профзахворювань, посилюється централізація планування. Договірне регулювання з питань охорони праці поставлено на високий рівень. Передбачається значна участь громадських інституцій у цьому процесі [2].

З позицій законодавчої регламентації прав і гарантій працівників у сфері охорони праці та їх забезпечення Закон України «Про охорону праці» та нормативно-правові акти щодо його реалізації одержали високу оцінку експертів Міжнародної організації праці.

До позитивних аспектів Закону України «Про охорону праці», безперечно, належить закріплення за державою функції нагляду за охороною праці.

В умовах роздержавлення, приватизації, утворення великої кількості суб'єктів підприємницької діяльності з різними формами недержавної власності роль держави у вирішенні завдань охорони праці суттєво зростає.

Держава виступає гарантом створення безпечних та нешкідливих умов праці для працівників підприємств, установ, організацій усіх форм власності [3].

4.2 Організація охорони праці на підприємстві

В організації охорони праці на підприємстві беруть участь роботодавці, їх заступники, головні спеціалісти, керівники виробничих дільниць, окремих структурних підрозділів та служб, профспілки та інші органи, що певним чином впливають на організацію охорони праці.

Основним завданням з питань організації охорони праці є створення здорових і безпечних умов праці. Цього можна досягти:

- навчанням всіх працюючих на підприємстві, перевіркою їх знань та пропагандою охорони праці;
- розробкою і виконанням комплексних (перспективних), річних та оперативних планових заходів з охорони праці;
- аналізом показників і причин виробничого травматизму та захворювань;
- оперативним контролем стану охорони праці на підприємстві і негайним усуненням шкідливостей та небезпек, виявлених на робочих місцях;
- проведенням паспортизації санітарно-технічного стану виробничих приміщень, технологічного обладнання та окремих робочих місць;
- впровадженням заходів морального і матеріального заохочення за зразковий стан охорони праці на робочому місці, дільниці, структурному підрозділі;
- проведенням спеціальних заходів з охорони праці жінок та молоді, виховної роботи з питань охорони праці та трудової дисципліни, а також притягненням до відповідальності осіб, які порушили існуючі норми і правила охорони праці;
- забезпеченням усіх працюючих необхідними захисними засобами згідно з існуючими нормами.

Виконання цих заходів необхідно здійснювати на основі новітніх досягнень науки та передового досвіду, включаючи технічні засоби інформатики, спеціальні засоби сигналізації, блокування та ін. [4].

4.3 Аналіз шкідливих та небезпечних факторів, які супроводжують роботу програміста

Відповідно до встановлених гігієнічно-санітарних вимог, визначених у Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98), затверджених Постановою Головного державного санітарного лікаря України від 10 грудня 1998 р. № 7 [5], роботодавець зобов'язаний забезпечити в приміщеннях з ВДТ оптимальні параметри виробничого середовища (табл. 4.1 – табл. 4.4).

Таблиця 4.1 – Норми мікроклімату для приміщень з ВТД

Пора року	Категорія робіт	Температура повітря, °С, не більше	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодна	Легка – 1а	22…24	4…6	0,1
	Легка – 1б	21…23	4…6	0,1
Тепла	Легка – 1а	23…25	4…6	0,1
	Легка – 1б	22…24	4…6	0,2

Таблиця 4.2 – Рівні іонізації повітря приміщень при роботі на ВДТ

Рівні	Число іонів в 1 $см^3$ повітря	
	п+	п–
Мінімально необхідні	400	600
Оптимальні	1500–30000	3000–5000
Максимально допустимі	50000	50000

Таблиця 4.3 – Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот

Вид трудової діяльності	Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц								
	63	125	250	500	1000	2000	4000	8000	Рівні звуку, еквівалентні рівні звуку, дБА/дБАекв.
Програмісти ЕОМ	7	61	54	49	45	42	40	38	50
Оператори в залах обробки інформації на ЕОМ та оператори комп'ютерного набору	83	74	68	63	60	57	55	54	65
В приміщеннях для розташування шумних агрегатів ЕОМ	91	83	77	73	70	68	66	64	75

Таблиця 4.4 – Допустимі параметри електромагнітних випромінювань і електричного поля

Види поля	Допустимі параметри поля		Допустима поверхнева щільність потоку енергії (інтенсивність потоку енергії), Вт/м^2
	за електричною складовою (Е), В/м	за магнітною складовою (Н), А/м	
Напруженість електромагнітного поля при частоті:6 кГц...3 МГц	50	5	
3 МГц...30 МГц	2	–	
30 МГц...5 ГГц	–	–	10
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру: УФ-С (220...280 мм)			0,001
УФ-В (280...320 мм)			0,01
УФ-А (320...400 мм)			10,0
в інфрачервоній частині спектру: 0,76…10,0 мкм			35,0...70,0
Напруженість електричного поля ВДТ			20 В/м

4.4 Засоби регулювання метеорологічних умов в приміщеннях, де працюють програмісти

Параметри мікроклімату можуть мінятися в широких межах, у той час як необхідною умовою життєдіяльності людини є підтримка постійності

температури тіла завдяки терморегуляції, тобто здатності організму регулювати віддачу тепла в навколишнє середовище. Принцип нормування мікроклімату – створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем [6].

Обчислювальна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вологості у приміщенні. У приміщеннях, де встановлені комп'ютери, повинні дотримуватися певні параметри мікроклімату (табл. 4.5 – табл. 4.6). У санітарних нормах «Санітарні норми мікроклімату виробничих приміщень» (ДСН 3.3.6.042-99) встановлені величини параметрів мікроклімату, що створюють комфортні умови. Ці норми встановлюються в залежності від пори року, характеру трудового процесу і характеру виробничого приміщення [7].

Таблиця 4.5 – Параметри мікроклімату для приміщень, де встановлені комп'ютери

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря у приміщенні Відносна вологість Швидкість руху повітря	22...24°С 40...60 % до 0,1 м/с
Теплий	Температура повітря у приміщенні Відносна вологість Швидкість руху повітря	23 ... 25°С 40 ... 60 % 0,1 ... 0,2 м/с

Таблиця 4.6 – Норми подачі свіжого повітря в приміщення, де розташовані комп'ютери

Характеристика приміщення	Об'ємна витрата подається в приміщення свіжого повітря, $м^3$ / на одну людину в годину
Об'єм до 20 $м^3$ на особу	Не менше 30
20 ... 40 $м^3$ на особу	Не менше 20
Більш 40 $м^3$ на особу	Природнавентиляція

Об'єм приміщень, в яких розміщені працівники обчислювальних центрів, не повинен бути меншим 19,5 м^3 на людину з урахуванням максимального числа одночасно працюючих в зміну.

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт залежно від пори року і доби, чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціювання повітря, опалювальна система).

4.5 Визначення розряду зорової праці відповідно нормативним вимогам

Правильно спроектоване і виконане виробниче освітлення покращує умови зорової роботи, знижує стомлюваність, сприяє підвищенню продуктивності праці, благотворно впливає на виробниче середовище, надаючи позитивну психологічну дію на працюючого, підвищує безпеку праці і знижує травматизм.

Недостатність освітлення приводить до напруги зору, ослабляє увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає засліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань, тому такий важливий правильний розрахунок освітленості.

Існує три види освітлення – природне, штучне і поєднане (природне і штучне разом) [8].

Природне освітлення – освітлення приміщень денним світлом, що потрапляє через світлові прорізи в зовнішніх огороджуючих конструкціях приміщення. Природне освітлення характеризується тим, що змінюється в широких межах залежно від часу дня, пори року, характеру області і ряду інших чинників.

Штучне освітлення застосовується при роботі в темний час доби і вдень, коли не вдається забезпечити нормовані значення коефіцієнта природного освітлення (похмура погода, короткий світловий день). Освітлення, при якому недостатнє за нормами природне освітлення доповнюється штучним, називається змішаним освітленням.

Штучне освітлення підрозділяється на робоче, аварійне, евакуаційне, охоронне. Робоче освітлення, у свою чергу, може бути загальним або комбінованим. Загальне – освітлення, при якому світильники розміщуються у верхній зоні приміщення рівномірно, або, як розташоване устаткування. Комбіноване – освітлення, при якому до загального додається місцеве освітлення.

Згідно з СНіП II-4-79 [9] в приміщень обчислювальних центрів необхідно застосувати систему комбінованого освітлення.

При виконанні робіт категорії високої зорової точності (найменший розмір об'єкту розрізнення 0,3 ... 0,5 мм) величина коефіцієнта природного освітлення (КЕО) повинна бути не нижче 1,5 %, а при зоровій роботі середньої точності (найменший розмір об'єкту розрізнення 0,5 ... 1,0 мм) КЕО повинен бути не нижче 1,0 %. В якості джерел штучного освітлення звичайно використовуються люмінесцентні лампи типу ЛБ, або ДРЛ, які попарно об'єднуються в світильники, які повинні розташовуватися рівномірно над робочими поверхнями.

Вимоги до освітленості в приміщеннях, де встановлені комп'ютери, наступні: при виконанні зорових робіт високої точності загальна освітленість повинна складати 300 лк, а комбінована – 750 лк; аналогічні вимоги при виконанні робіт середньої точності – 200 і 300 лк відповідно.

Крім того, все поле зору повинне бути освітлено достатньо рівномірно – ця основна гігієнічна вимога. Іншими словами, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими, оскільки

яскраве світло в районі периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності.

Отже, для того щоб праця робітників була успішною та комфортною, роботодавець повинен урахувати всі норми при освітленні приміщення, тому є доцільним обрахувати необхідну площу вікон для забезпечення бокового природного освітлення приміщення, де працює програміст, що займається написанням застосунків із використанням мобільних пристроїв. Довжина приміщення L = 12 м; глибина приміщення B = 5 м; висота підвіконня – 1 м. Площа приміщення – 60 м^2; 3 вікна розміром 2×1,5 м кожне. Відстань до протилежної будівлі D = 30 м, висота карнизу протилежного будинку над підвіконням приміщення H = 20 м.

По-перше, потрібно визначити необхідні значення для розрахунку:

1) За нормативними значеннями КПО у СНиП 23-05-95 для виробничого приміщення III розряду зорової роботи визначаємо нормоване значення коефіцієнта природного освітлення: $(КПО)_{норм} = 2,0$ %.

2) Для IV поясу світлового клімату (м. Миколаїв) та орієнтації вікон на південний захід знаходимо коефіцієнт світлового клімату: $m_N = 0,85$.

3) Нормоване значення за формулою

$$КПОN = (КПО)норм \times mN ,$$

де $(КПО)_{норм}$ — нормоване значення КПО;

m_N — коефіцієнт світлового клімату, що враховує особливості світлового клімату.

$$(КПО)_N = (КПО)_{норм}\ m_N = 2,0 * 0,85 = 1,7\ \%.$$

4) Для нормальних умов середовища коефіцієнт запасу $К_з = 1,2$.

5) Умовна робоча поверхня розташована на висоті 0,8 м від підлоги, висота підвіконня — 1 м, вікон — 1,5 м, тому висота від рівня робочої поверхні до верхнього краю вікна h = 1 + 1,5 – 0,8 = 1,7 м. Приймаємо, що розрахункова точка М умовної робочої поверхні розміщується на відстані 1 м від стіни, найвіддаленішої від вікон, тобто відстань від точки М до зовнішньої стіни приміщення

$$b = B - 1 = 5 - 1 = 4 \text{ м.}$$

Тоді $\frac{L}{B} = \frac{12}{5} = 2.4 \approx 2$ $\frac{B}{h} = \frac{5}{1.7} = 2.94 \approx 3.$

Для цих значень знаходимо світлову характеристику вікон: $\eta_в = 10,5$.

6) Розраховуємо коефіцієнт r. Для цього визначаємо спочатку відношення

$$\frac{h}{B} = \frac{4}{5} = 0.8.$$

7) Потім визначаємо площу стін $S_{стін}$, стелі $S_{стелі}$, підлоги $S_{підлоги}$ та відповідні коефіцієнти відбиття $\rho_{стелі}$, $\rho_{стін}$, $\rho_{підлоги}$. Бокові стіни мають площу $2 \times 5 \times 3 = 30$ м^2 , протилежна від вікон стіна — $12 \times 3 = 36$ м^2 , тоді загальна площа стін $S_{стін.} = 30 + 36 = 66$ м^2 ;

$S_{стелі} = S_{підлоги} = 60$ м^2 . Для свіжопобіленої стелі $\rho_{стелі} = 0,7$; для стін, що обклеєні світлими шпалерами, $\rho_{стін} = 0,3$, для підлоги $\rho_{підл} = 0,25$.

Середнє значення коефіцієнта відбиття $\rho_{сер\ стелі}$, стін і підлоги розраховуємо за формулою:

$$\rho_{сер} = \frac{\rho_{стелі}S_{стелі} + \rho_{стін}S_{стін} + \rho_{підлоги}S_{підлоги}}{S_{стелі} + S_{стін} + S_{підлоги}} = \frac{0.7 * 60 + 0.3 * 66 + 0.25 * 60}{60 + 66 + 60} \approx 0.4.$$

Тепер визначаємо, що $r_1 = (1,7–2,45)$, за правилом інтерполяції $r_1 = 2,1$.

8) Відношення геометричних параметрів D/H = 30/20 = 1,5.
Визначаємо коефіцієнт Кбуд = 1,2.

9) Отже, знаходимо необхідну розрахункову площу вікон за формулою:

$$S_{вік\ розр} = \frac{(КПО)_N * К_З * \eta_В * К_{БУД} * S_{підл}}{\tau_{заг} * r_1 * 100} = \frac{1,7 * 1,2 * 10,5 * 1,2 * 60}{0,48 * 2,1 * 100} = 15,7 \text{ м}^2.$$

Оскільки розрахункова площа вікон перевищує фактичну для приміщення (9 м^2) більше як на 10 %, доходимо висновку, що для запропонованих умов потрібне значення КПО = 1,7 % не може бути забезпечене, природне освітлення для заданого розряду зорової роботи недостатнє. Можна запропонувати виконання суміщеного освітлення або виконувати у приміщенні зорові роботи іншого розряду.

4.6 Потужність електричних приладів за ступенем небезпеки

Більшість вчених вважають, що як короткочасне, так і тривалий вплив усіх видів випромінювання від екрану монітора не небезпечно для здоров'я

персоналу, що обслуговує комп'ютери. Проте, вичерпних даних щодо небезпеки дії випромінювання від моніторів на працюючих з комп'ютерами не існує і дослідження в цьому напрямі продовжуються .

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітора комп'ютера представлені в табл. 4.7 [5].

Максимальний рівень рентгенівського випромінювання на робочому місці оператора комп'ютера звичайно не перевищує 10 мкбер/год, а інтенсивність ультрафіолетового і інфрачервоного випромінювань від екрану монітора лежить в межах 10...100 мВт/м$^{2.}$.

Таблиця 4.7 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань (відповідно до ДСанПіН 3.3.2-007-98)

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні відеомонітора	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні відеомонітора	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати: для дорослих користувачів	20 кВ/м
для дітей дошкільних установ і таких, які вчаться у середніх спеціальних і вищих навчальних закладів	15 кВ/м

Для зниження дії цих видів випромінювання рекомендується застосовувати рідкокристалеві LCD-монітори зі зниженим рівнем випромінювання (ТСО-92 та вище, до ТСО'03, ТСО'04, ТСО'05, ТСО'06 включно), а також дотримуватися регламентованих режимів праці та відпочинку [10].

4.7 Ергономічні вимоги до робочого місця програміста

Проектування робочих місць, забезпечених відеотерміналами (ВДТ), відноситься до числа важливих проблем ергономічного проектування в області обчислювальної техніки.

Робоче місце і взаємне розташування усіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи. Зокрема, при організації робочого місця програміста повинні бути дотримані наступні основні умови: оптимальне розміщення устаткування, що до складу робочого місця і достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення [10].

Ергономічними аспектами проектування відеотермінальних робочих місць, зокрема, є: висота робочої поверхні, розміри простору для ніг, вимоги до розташування документів на робочому місці (наявність і розміри підставки для документів, можливість різного розміщення документів, відстань від очей користувача до екрану, документа, клавіатури та ін.), характеристики робочого крісла, вимоги до поверхні робочого столу, урегульованість елементів робочого місця.

Головними елементами робочого місця програміста є стіл і крісло. Основним робочим положенням є положення сидячи.

Ергономічні вимоги до робочого місця оператора ЕОМ визначені у ДСТУ ISO 9241-5:2004 «Вимоги до компонування робочого місця та до робочої пози»[11] та ДСТУ 7951:2015 «Дизайн і ергономіка. Крісло оператора. Загальні ергономічні вимоги» чинних в Україні [12].

4.8 Вступний інструктаж з пожежної безпеки.

Вступний є найбільш масовим. Він проводиться з усіма співробітниками компаній і підприємств, які зараховуються в штат на тимчасове або постійне місце роботи, з співробітниками інших компаній або організацій, які беруть участь в процесі виробництва в будинку або споруді, з учасниками екскурсій, студентами, учнями професійних училищ та інших навчальних закладів . Він проводиться силами штатних фахівців служби охорони праці, а його проведення відбивається в журналі реєстрації вступного інструктажу.

ВИСНОВОК ДО РОЗДІЛУ 4

У цьому розділі дипломної роботи були викладені вимоги до робочого місця інженера-програміста. Створені умови повинні забезпечувати комфортну роботу. На підставі вивчення літератури з цієї теми, було визначено оптимальні розміри робочого столу і крісла, робочої поверхні, а також проведено вибір системи і розрахунок оптимального освітлення виробничого приміщення. Дотримання умов, визначає оптимальну організацію робочого місця інженера-програміста, що дозволить зберегти максимальну працездатність протягом всього робочого дня, підвищить, як у кількісному, так і в якісному відношенні, продуктивність праці програміста, що у свою чергу сприятиме швидкій розробці та налагодженню програмного продукту.

ВИСНОВКИ

Дослідивши можливості апаратного та програмного інструментів розробки, класів, об'єктів та їх функцій прийнято рішення розробити програму - скетч для мікроконтролера Arduino на прикладі двофакторної ідентифікації за допомогою RFID -мітки та сканера відбитків пальця, оскільки ідентифікація за допомогою сканера райдужної оболонки ока потребує більших ресурсів, та є занадто дорогою.

Використовуючи перелічені елементи, з метою відлагодження системи вцілому, а також подальшому виготовленні діючого макета системи та апробації з допомогою реальних осіб на фізичному об'єкті під час підготовки до захисту диплома магістратури.

Опрацьовано теоретичні технічні можливості обраної платформи, визначені необхідні компоненти для побудови діючого макета системи.

На основі аналізу програмних інструментів та бібліотек розроблено тестовий зразок програмного забезпечення, повний вихідний код якого, наведено у Додатку 2.

У розділі з охорони праці було розглянуто такі питання:

1. Основні положення Закону України «Про охорону праці»;
2. Організація охорони праці на підприємстві;
3. Аналіз шкідливих та небезпечних факторів, які супроводжують роботу програміста;
4. Засоби регулювання метеорологічних умов в приміщеннях, де працюють програмісти;
5. Визначення розряду зорової праці відповідно нормативним вимогам;
6. Потужність електричних приладів за ступенем небезпеки;
7. Ергономічні вимоги до робочого місця програміста;
8. Вступний інструктаж з пожежної безпеки;

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Галатенко В.А. Идентификация и автентификация, управление доступом лекция из курса «Основы информационной безопасности». - Интернет Университет Информационных Технологий, 2010г.

2. Двухфакторная автентификация [Электронный ресурс]. – Режим доступа: http://www.aladdin-rd.ru/solutions/ authentication/.

3. Двухфакторная автентификация при удаленном доступе [Электронный ресурс]. – Режим доступа: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166/.

4. Евсеев С. П. Исследование методов двухфакторной автентификации / С. П. Евсеев, О. Г. Король // Системи обробки інформації. – 2014. – № 2(118). – С. 81– 87.

5. Настройка двухфакторной автентификации [Электронный ресурс]. – Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factorauthentication-gransden.html?locale=ru.

6. Семь методов двухфакторной автентификации [Электронный ресурс]. – Режим доступа: http://www.infosecurityrussia.ru/news/29947.

7. Тихонов И.А. Информативные параметры биометрической автентификации пользователей информационных систем 2010. № 9. С. 26-32.

8. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. - Феникс, 2008 г.

9. Face Recognition.[Электронный ресурс]. - Режим доступа: https://play.google.com/store/apps/details?id=com.vinisoft.facesdk.demo&hl=ru.

10. Hyvdrinen A, Karhunen J., and Oja E., Independent Component Analysis, A Volume in the Wiley Series on Adaptive and Learning Systems for

Signal Processing, Communications, and Control. — John Wiley & Sons, Inc., 2001.

11. Muresan D. D., Parks T. W., Adaptive Principal Components and Image Denoising, in: Image Processing, 2003, Proceedings 2003 IEEE International Conference on Image Processing (ICIP), 14-17 Sept. 2003, V. 1, pp. I-101-104

12. Rao, K., Yip P. (eds.), The Transform and Data Compression Handbook, CRC Press, Baton Rouge, 2001.

13. Scholz M., Fraunholz M., Selbig J., Nonlinear Principal Component Analysis: Neural Network Models and Applications, In: Gorban A. N. et al (Eds.), LNCSE 58, Springer, 2007 ISBN 978-3-540-73749-0

14. Zinovyev A., Cluster structures in genomic word frequency distributions, 14- 17 Sept. 2003, V. 1, pp. I-101-104.

15. Марат Давлетханов. Идентификация по радужке глаза. Часть 1, 2 / Ма- рат Давлетханов // www. infobez. ru

16. Матвеев И. Распознавание человека по радужке/

И. Матвеев, К. Ганькин // Системы безопасности. – 2004. – № 5. – С. 33-37.

17. Болл Р.М. Руководство по биометрии / Р.М. Болл [и др.]. – М., 2007.

18. Introduction to Biometrics [Электронный ресурс]

//Режим доступа:

http://www.biometrics.gov/Documents/biofoundationdocs.pdf, свободный, яз. англ.

19. Кухарев Г.А. Биометрические системы: Методы и средства индентификации личности человека / Кухарев Г.А. – СПб.: Политехника, 2001.

20. J.P. Campbell, J.P. Jr. Speaker Recognition: A Tutorial/ J.P. Campbell, Jr.//Proceedings of the IEEE. – 1997. – Vol. 85, № 9. – P. 1437–1462.

21. Ландэ Д.В. О цифровой идентификация личности // Д.В. Ландэ, В.Н. Фурашев. – Харьков: НАКУ, 2007. – Вып. 34. – С. 127 – 135.

22. Biometrics catalog [Электронный ресурс]. – Режим доступа:http://www.biometricscatalog.org/, яз. англ.

23. Задорожный В. Обзор биометрических технологий // Защита инфор- мации. Конфідент. – 2003. – № 5. – С. 19-25.

24. Muller Stefan, Wallhoff Frank, Hulsken Frank. Facial Expression Recognition Using Pseudo 3-D Hidden Markov Models. Dep. of Computer Science, Faculty of Electrical Engineering.

25. Samaria F. Face recognition using Hidden Markov Models. PhD thesis. Engineering department, Cambrige University. Oct. 1994.

26. Nefian Ara V., Hayes III Monson H. Hidden Markov Models For Face Recognition. Center for Signal and Image Processing School of Electrical and Computer Engineering Georgia Institute of Technology, Atlanta.

27.http://www.accessexcellence.org/RC/AB/BA/Use_of_DNA_Identification.php. Use of DNA in Identification.

28. http://www.papillon.ru

29. http://www.biolink.ru/

30. http://www.vocord.ru/

31. http://iss.ru/

32. http://www.eyelock.com/

33. Методичні вказівки з курсу "Охорона праці" / В. С. Джигирей та ін. Львів, 1992. 88 с.

34. Жидецький В. Ц., Джигирей В. С., Мельников О. В. Основи охорони праці: навч. посіб. Вид.4-те, допов. Львів, 2000. 350 с.

35. Правові та організаційні питання охорони праці. Навчальні матеріали онлайн : веб-сайт. URL: http://pidruchniki.com/1783102438245/bzhd/pravovi_organizatsiyni_pitannya_ohoroni_pratsi.

36. Практикум з охорони праці: навч. посіб. / В. С. Джигирей, В. М. Сторожук , Х. І. Лико, Л. В. Туряб; за ред. В. Ц. Жидецького. Львів: Афіша, 2000. 352 с.

37. ДСанПІН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. Нормативно-директивні документи МОЗ України : веб-сайт. URL:http://mozdocs.kiev.ua/view.php?id=2445.

38. Жидецький В. Ц. Охорона праці користувачів комп'ютерів. Львів, 2000. 176 с.

39. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. Верховна Рада України : офіційний сайт. URL: http://zakon5.rada.gov.ua/rada/show/va042282-99.

40. ДБН В.2.5-28:2018. Природне і штучне освітлення. Державні будівельні норми України : веб-сайт. URL: http://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_28/1-1-0-1188.

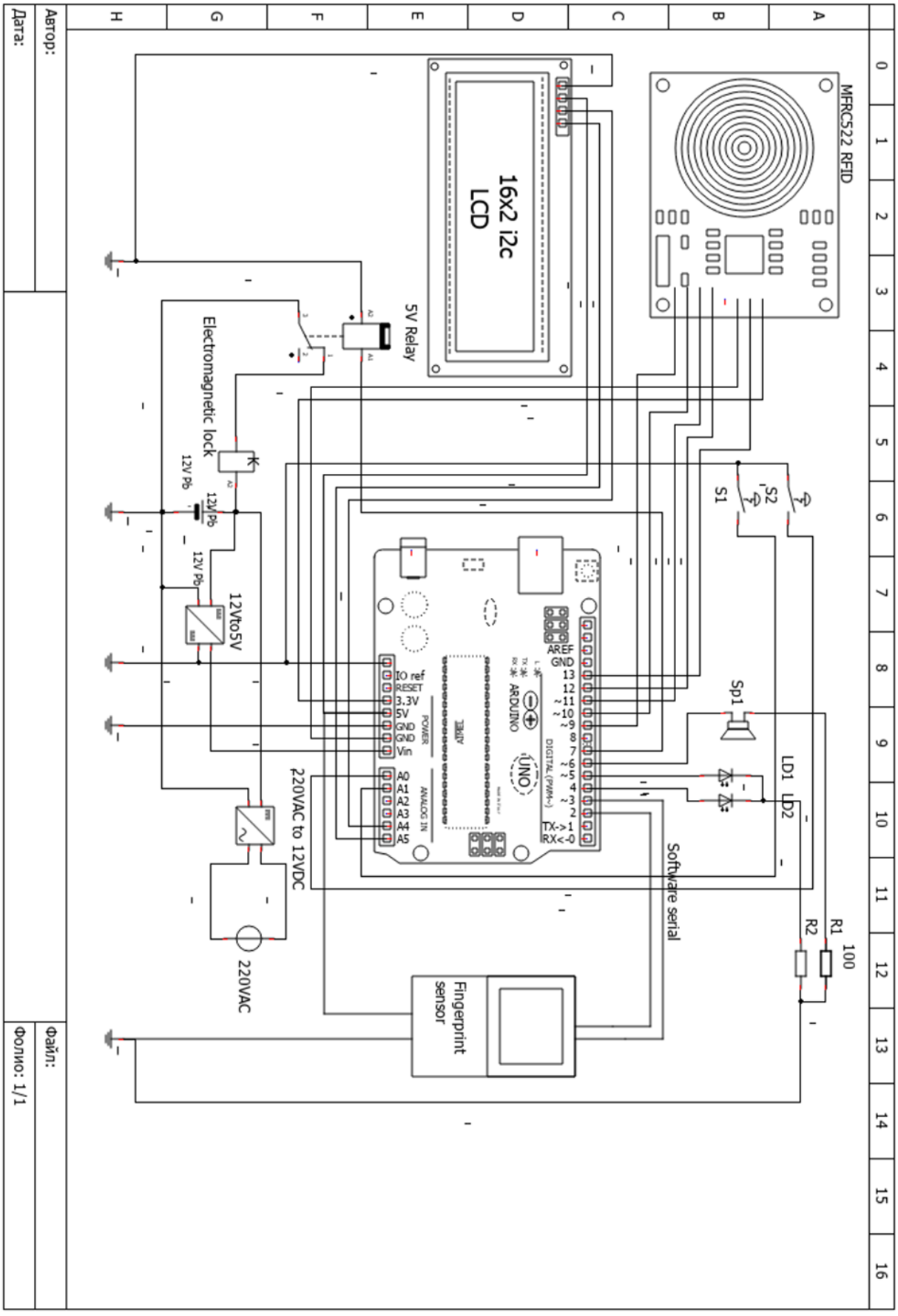
41. СНиП II-4-79. Естественное и искусственное освещение. Build.org.ua : веб-сайт. URL: http://www.build.org.ua/docs/stroitelstvo_358-.html.

42. ГОСТ 12.1.002-84. ССБТ. Электрические поля промышленной частоты. Допустимые уровни напряженности и требования к проведению контроля на рабочих местах. БУДСТАНДАРТ Online : веб-сайт. URL: http://online.budstandart.com/ru/catalog/doc-page?id_doc=48129.

43. ДСТУ ISO 9241-5:2004 Вимоги до компонування робочого місця та до робочої пози. Каталог НД України online : веб-сайт. URL: http://csm.kiev.ua/nd/nd.php?z=%D0%94%D0%A1%D0%A2%D0%A3+ISO+9241-5%3A2004&st=0&b=1.

44. Правила пожежної безпеки в Україні https://zakon.rada.gov.ua/laws/show/z0252-15

ДОДАТОК 1


MFRC522 RFID
16x2 i2c LCD
5V Relay
Electromagnetic lock
12V Pb
12V Pb
12V Pb
12Vto5V
220VAC to 12VDC
220VAC
S1
S2
Sp1
LD1
LD2
R1 100
R2
Software serial
Fingerprint sensor
IO ref
RESET
3.3V
5V
GND
GND
Vin
A0
A1
A2
A3
A4
A5
AREF
GND
13
12
~11
~10
~9
8
7
~6
~5
4
~3
2
TX->1
RX<-0
ARDUINO
UNO
Автор:
Дата:
Файл:
Фолио: 1/1

ДОДАТОК 2

Вихідний код програми

```
#include <SPI.h>
#include "MFRC522a.h"
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

#define RST_PIN         9
#define SS_PIN          10
#define relay 7
#define MaxCards 3
#define MaxLength 7

byte UIDs[MaxCards][MaxLength]=
  {{0x04,0xD3,0xD3,0xE2,0x72,0x26,0x82},
   {0x34,0x51,0xF4,0x71,0xED,0x51,0x26},
   {0x04,0x72,0x10,0xD2,0x4A,0x33,0x86}
  };

byte nID = 0;

LiquidCrystal_I2C lcd(0x27,20,4);
MFRC522 mfrc522(SS_PIN, RST_PIN);
SoftwareSerial      mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);



void setup() {
 Serial.begin(115200);
 SPI.begin();
 mfrc522.PCD_Init();
```

```
  mfrc522.PCD_SetAntennaGain(mfrc522.RxGain_max);
  Serial.println("RFID init");
  lcd.init();
 while(!Serial);
  delay(500);
  Serial.begin(9600);
  Serial.println("Scan sensor...");
  finger.begin(9600);
 }//setup

 void loop() {
  byte cardN=-1;
  // Look for new cards
  if ( ! mfrc522.PICC_IsNewCardPresent()) {
   return; // do nothing
  }//if
  if ( ! mfrc522.PICC_ReadCardSerial()) {
   return; // do nothing
  }//if

  // Card UID info
  Serial.print("Card UID: ");
  for (int i = 0; i < mfrc522.uid.size; i++) {
   if(mfrc522.uid.uidByte[i] < 0x10) Serial.print("0"); //Add leading 0
   Serial.print(mfrc522.uid.uidByte[i], HEX);
   Serial.print(" ");
   lcd.print(mfrc522.uid.uidByte[i], HEX);
  }//for
  Serial.println();
  mfrc522.PICC_HaltA(); // Already done if it was a MIFARE Classic PICC.

  // try to identify this card
  for (int n=0; n<MaxCards; n++){
```

```
  if (ThisCard(n)){ cardN=n; break; }// if ThisCard
 }// for n

 // Card name
 switch (cardN){
  case 0:
   Serial.println("Red");
   FingerPrint_ID();
   if (nID==1){
    granted();
   } else{
    denied();
   }
   break;
  case 1:
   Serial.println("Blue");
   FingerPrint_ID();
   if (nID==2){
    granted();
   } else{
    denied();
   }
   break;
  case 2:
   Serial.println("Green");
   FingerPrint_ID();
   if (nID==3){
    granted();
   } else{
    denied();
   }
   break;
  default:
```

```
    Serial.println("Unknown");
    denied();
    softRst();
  }//switch

}//loop
//-------------------------------------------------------------
boolean ThisCard(byte N){
  boolean test=true;
  for (int i = 0; i < mfrc522.uid.size; i++) {
   if (i>=MaxLength) break;
   if (mfrc522.uid.uidByte[i]!=UIDs[N][i]) {
    test=false; //mismatch
    break;
   }//if
  }//for i
  return test;
}//ThisCard

void FingerPrint_id(){
  if(finger.verifyPassword()){Serial.println("Found sensor!");}
  else{lcd.print("Did not find sensor :("); delay(1500); softRst();}
  if(finger.getImage()       == FINGERPRINT_OK){
  if(finger.image2Tz()       == FINGERPRINT_OK){
  if(finger.fingerFastSearch() == FINGERPRINT_OK){
   Serial.print("Found ID=");
   Serial.print(finger.fingerID);
   Serial.print(", with confidence of ");
   Serial.println(finger.confidence);
   nID = finger.fingerID;
  }}}
  delay(500);
}
```

```
void granted(){
  digitalWrite(relay, HIGH);
  delay(5000);
  lcd.print("Acess granted");
  digitalWrite(relay, LOW);
  softRst();
}
void denied(){
  lcd.print("Acess denied!");
  delay(1000);
  softRst();
}
void softRst(){
  __asm__ __volatile__ ("jmp 0");
}
```