Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Комп'ютерна система біометричної аутентифікації особи за відбитком пальця*

Виконала: студентка *IV* курсу, групи *СІс-44*
спеціальності *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

(підпис) *Костомаха М.В.* (прізвище та ініціали)

Керівник (підпис) *Луцків А.М.* (прізвище та ініціали)

Нормоконтроль (підпис) *Луцик Н.С.* (прізвище та ініціали)

Завідувач кафедри (підпис) *Осухівська Г.М.* (прізвище та ініціали)

Рецензент (підпис) *Стадник М.А.* (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
« » 2021 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Костомасі Марії Володимирівній*
(прізвище, ім'я, по батькові)

1. Тема роботи *Комп'ютерна система біометричної аутентифікації особи за відбитком пальця*

Керівник роботи *Луцків Андрій Мирославович, к.т.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*10*» *лютого* 2021 року № *4.7-97*

2. Термін подання студентом завершеної роботи *26.06.2021 р.*

3. Вихідні дані до роботи *Особливості відбитків пальців, міні-комп'ютер Raspberry PI, принцип сканування відбитків пальців*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз вимог технічного завдання та методів біометричної аутентифікації особи. 2. Розробка проекту комп'ютерної системи біометричної аутентифікації особи за відбитком пальців 3. Програмне забезпечення комп'ютерної системи біометричної аутентифікації особи за відбитком пальців. 4. Безпека життєдіяльності, основи охорони праці. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. *Структура відбитків пальців людини*
2. *Структурна схема системи біометричної аутентифікації особи*
3. *Архітектура комп'ютерної системи біометричної аутентифікації особи*
4. *Компонентна схема комп'ютерної системи*
5. *Схема з'єднань компонентів комп'ютерної системи*
6. *Зовнішній вигляд спроектованої системи*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	*Пилипець М.І., д.т.н., проф. каф. МТ*		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Розробка та аналіз вимог технічного завдання*	*10.02-21.02.2021*	
2	*Аналіз методів аутентифікації користувачів*	*21.02-07.03.2021*	
3	*Проектування архітектури комп'ютерної системи*	*08.03-20.03.2021*	
4	*Обґрунтування вибору апаратного забезпечення*	*20.03-26.03.2021*	
5	*Реалізація програмного забезпечення комп'ютерної системи*	*27.03-10.04.2021*	
6	*Розробка інструкцій з налаштування параметрів комп'ютерної системи біометричної аутентифікації*	*10.04-04.05.2021*	
7	*Безпека життєдіяльності, основи охорони праці*	*04.05-20.05.2021*	
8	*Оформлення кваліфікаційної роботи*	*27.05-10.06.2021*	
9	*Попередній захист кваліфікаційної роботи*	*10.06-20.06.2021*	
10	*Захист кваліфікаційної роботи*	*21.06-27.06.2021*	

Студент _____ *Костомаха Марія Володимирівна*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Луцків Андрій Мирославович*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Комп’ютерна система біометричної аутентифікації особи за відбитком пальця// Кваліфікаційна робота на здобуття освітнього ступеня бакалавр // Костомаха Марія Володимирівна // ТНТУ, спеціальність 123 «Комп’ютерна інженерія»// Тернопіль, 2021 // с.– 62, рис. – 21 , табл. – 6, аркушів А1 – 6, бібліогр. – 21.

Ключові слова: система, аутентифікація, біометрія, відбиток, палець.

У кваліфікаційній роботі спроектовано комп’ютерну систему біометричної аутентифікації особи за відбитком пальців, що відповідає вимогам технічного завдання. Досягти мети роботи вдалося шляхом застосування обґрунтованого апаратного і розробленого програмного забезпечення. Основними апаратними пристроями спроектованої системи є:

– сканер відбитків пальців на основі ZFM-20;

– пристрій керування процесом зчитування та аутентифікації особи Raspberry PI Model B;

– компонента виводу інформаційних повідомлень для взаємодії з користувачем LCD 2*16.

Взаємодію між сканером відбитків пальців і Raspberry PI забезпечено шляхом використання USB Serial адаптера.

Функції додавання та управління відбитками пальців на апаратному рівні реалізовано за допомогою відповідних чотирьох кнопок: реєстрації відбитка пальця, видалення та переходу між збереженими зображеннями. Успішність аутентифікації додатково сигналізує світлодіод.

Логіку роботи програмного забезпечення реалізовано засобами мови програмування Python, що підтримується обраним однокристальним міні-комп’ютером.

ABSTRACT

Computer-aided system of finger print-based person biometrical authentification // Bachelor's thesis // Kostomakha Mariia Volodymyrivna // TNTU, speciality 123 «Computer engineering»// Ternopil, 2021 // p.– 62 , fig. – 21 , tab. –6, posters A1 – 6, ref. – 21.

Keywords: system, authentication, biometric, fingerprints.

In the qualification work, a computer system of biometric authentication of a person by fingerprint is designed, which meets the requirements of the technical task. The goal of the work was achieved through the use of sound hardware and developed software.

The main hardware devices of the designed system are:

– fingerprint scanner based on ZFM-20;

– Raspberry PI Model B reading and authentication process control device;

– component for outputting information messages for interaction with the user LCD 2 * 16.

The interaction between the fingerprint scanner and the Raspberry PI is provided by using a USB Serial adapter. The functions of adding and managing fingerprints at the hardware level are implemented using the appropriate four buttons: fingerprint registration, deletion and transition between saved images.

The success of the authentication is additionally signaled by the LED. The logic of the software is implemented using Python programming language supported by the selected single-chip mini-computer.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ,
СИМВОЛІВ І СКОРОЧЕНЬ

БД	База даних
КС	Комп’ютерна система
ПЗ	Програмне забезпечення
GPIO	General purpose input/output
IoT	Internet of Things
Rpi	Raspberry PI
USB	Universal Serial Bus

ВСТУП

Сучасні комп’ютерні системи, впроваджені у виробництво, характеризуються широким спектром функціональної придатності, привабливості інтерфейсів, використанням різного стеку технологій при їх створенні. Особливо важливим компонентом будь-якого чи то програмного, чи апаратного комплексу є система безпеки. Теперішні системи безпеки базується не тільки на класичних методах і засобах аутентифікації чи ідентифікації користувачів за допомогою пін-кодів чи паролів, а й використовують особливості біометричних властивостей людини.

Актуальність застосування біометричних систем пов’язана з унікальністю фізіологічних особливостей людини, наприклад, відбитків пальців, сітківки ока, особливостей рис обличчя, поведінки і ходи. До фізіологічних властивостей також належать інші характеристики, однак вони здатні змінюватись з часом, зокрема, вага і зріст. При побудові систем біометричної аутентифікації необхідно обґрунтувати її структуру, обрати тип апаратного і програмного забезпечення, спроектувати схему зв’язків між компонентами і провести її тестування.

У даній роботі проектується комп’ютерна системи біометричної аутентифікації особи за відбитком пальців, що може бути окремим безпековим компонентом для більш комплексної системи, або використовуватись як окрема система авторизації користувача. Однією з важливих вимог до систем такого класу є точність, що полягає у здатності системи з визначеною достовірністю визначати біометричні характеристики людини. Тому проектування системи біометричної аутентифікації на основі відбитку пальців є актуальною задачею у сфері інформаційних технологій, оскільки дозволить забезпечити унікальність, визначену достовірність ідентифікації користувача при доступі до захищених ресурсів.

РОЗДІЛ 1 АНАЛІЗ ВИМОГ ТЕХНІЧНОГО ЗАВДАННЯ ТА МЕТОДІВ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ОСОБИ

1.1 Аналіз вимог технічного завдання на проектування комп'ютерної системи біометричної аутентифікації особи за відбитком пальця

Комп'ютерна система біометричної аутентифікації особи за відбитком пальця є різновидом систем, що призначені для ідентифікації особи за її унікальними характеристиками. У даному випадку в якості ідентифікатора виступає зображення відбитка пальця.

За ідентифікацію людини на основі її біометричних особливостей у комп'ютерних системах відповідають алгоритми машинного навчання. В основному вони побудовані на моделях нейронних мереж розпізнавання образів за візуальними зображеннями, в тому числі, і відбитків пальців.

Системи біометричної аутентифікації на основі розпізнавання відбитків пальців проектують і впроваджують для підвищення ефективності комп'ютерної та інформаційної безпеки, у сфері торгівлі, зокрема при аутентифікації користувачів при проведенні грошових транзакцій та операцій. У побуті, комп'ютерні системи на основі розпізнавання відбитків пальців, призначені для авторизації користувача комп'ютерів, смартфонів. Важливим призначенням системи біометричної аутентифікації особи за відбитком пальця є сфера авторизованого входу до приміщень з обмеженим доступом.

Комп'ютерна система біометричної аутентифікації особи за відбитком пальця, яка проектується у даній роботі, вимагає впровадження апаратно-програмного комплексу для зчитування зображення відбитка пальця, його аналізу засобами машинного навчання та порівняння результатів з наявними записами у базі даних. Основне призначення системи полягає у забезпеченні

точності та підвищенні ефективності аутентифікації осіб на основі її біометричних та фізіологічних особливостей.

Метою створення комп'ютерної системи біометричної аутентифікації особи за відбитком пальця є автоматизація, забезпечення точності і продуктивності авторизації людини з врахуванням її біологічних особливостей.

Для того, щоб досягнути цієї мети, необхідно:

– проаналізувати особливості відбитків пальців людини;

– дослідити переваги і недоліки технологій розпізнавання зображень;

– спроектувати архітектуру комп'ютерної системи біометричної аутентифікації особи;

– обґрунтувати вибір апаратних пристроїв системи;

– обґрунтувати та реалізувати інтелектуальну складову системи біометричної аутентифікації;

– реалізувати системне і прикладне програмне забезпечення системи;

– перевірити одержані результати розпізнавання відбитків пальців особи.

Основні задачі і функції системи біометричної аутентифікації полягають у забезпеченні процесів зчитування відбитків пальців людини, їх аналізу та прийняття рішення щодо надання доступу до ресурсів чи до приміщення. Фактично, дана система є частиною комплексу, що формує комп'ютерну та інформаційну безпеки підприємства.

При проведенні аутентифікації особи на основі аналізу її біометричних даних повинна бути забезпечена висока точність та надійність результатів розпізнавання відбитків пальців, а також швидкість опрацювання та одержання результатів щодо доступу до ресурсів.

Автоматизація процесу аутентифікації на основі біометричних даних передбачає застосування і налаштування апаратного забезпечення, зокрема:

– зчитувача відбитків пальців;

– мікроконтролера для управління процесом аутентифікації;

– дисплея для відображення сервісних повідомлень;

– кнопок управління записом та видаленням зображень відбитків;

– інших додаткових апаратних пристроїв.

В якості додаткових апаратних пристроїв можуть використовуватись:

– зумер;

– електромеханічний замок;

– кнопки ручного блокування та розблокування;

– інші пристрої аутентифікації користувача.

Зображення відбитків пальців може зберігатись на SD-картці, підключеній до плати прототипування, або інтегрованій у сканер відбитків пальців. Альтернативою є зберігання зображень відбитків пальців на зовнішньому сервері баз даних.

Програмне забезпечення комп'ютерної системи аутентифікації особи на основі відбитків пальців повинно забезпечувати ініціалізацію та моніторинг параметрів апаратних пристроїв, а також виконувати безпосередньо порівняння зчитаної інформації і порівняння з існуючими зображеннями.

Вимоги, які в цілому висуваються до системи біометричної аутентифікації полягають у здатності адекватно зчитувати зображення відбитку пальців, аналізувати їх, забезпечувати визначену швидкість та реакцію на результат ідентифікації особи.

Комп'ютерну систему можна реалізувати за допомогою як Raspberry PI, так і Arduino й інших плат макетування. Основна функція мікроконтролера – керування процесом ідентифікації відбитків пальців, які зчитуються відповідним сканером.

Для забезпечення зворотного зв'язку системи з користувачем потрібно використати дисплей для виводу повідомлень про успішність чи не успішність авторизації.

В загальному випадку, більш детально вимоги до комп'ютерної системи аутентифікації можна представити як:

– можливість сканування відбитків пальців;

– забезпечення продуктивності процесу аутентифікації до 1с;

– здатність запису відбитків пальців;

– можливість оновлення та видалення зображень відбитків пальців;

– організація зв’язку з локальною комп’ютерною мережею та мережею Інтернет;

– наявність авторизованих процедур для визначених груп користувачів при налаштуванні роботи комп’ютерної системи;

– надійність функціонування апаратних пристроїв комп’ютерної системи;

– можливість віддаленого оновлення програмного забезпечення сканера відбитків пальців;

– можливість підключення додаткових пристроїв біометричної ідентифікації людини.

Базова апаратна структура комп’ютерної система біометричної аутентифікації особи на основі відбитку пальця включає:

– однокристальний міні-комп’ютер Raspberry PI;

– Fingerprint Module ZFM-20;

– дисплей LCD 16x2;

– Bread Board або PCB;

– адаптер USB-Serial;

Комп’ютерна система біометричної аутентифікації повинна:

– показувати сталість і надійність результатів ідентифікації особи за відбитком пальця;

– здійснювати перевірку з наявними зображеннями заданої біометрії;

– виводити сервісні повідомлення про результат розпізнавання;

– надавати можливість обміну інформацією з ресурсами локальної комп’ютерної мережі та Інтернет.

Зв’язок між сканером відбитків пальців та Raspberry PI забезпечується комунікацією за допомогою USB Serial адаптера, а взаємодія з LCD дисплеєм – на основі шини I2C. За допомогою інтегрованого у Raspberry PI модуля WIFI

повинна виконуватись взаємодія з маршрутизатором локальної комп'ютерної мережі, який має доступ до мережі Інтернет.

Діагностика компонентів комп'ютерної системи біометричної аутентифікації особи на основі відбитків пальців повинна проводиться у випадках збоїв у їх роботі та у відповідності до розкладу регламентних робіт. Усунення неполадок працездатності системи повинні усуватись у найкоротші терміни.

Шляхами розвитку комп'ютерної системи біометричної аутентифікації особи за відбитком пальців є інтеграція додаткових пристроїв аналізу біометричних показників. Для цього можуть бути використані відеокамери та програмне забезпечення для виконання задач розпізнавання обличчя. Окрім цього, в якості біометричних даних можна використовувати голос і відповідний комплекс для його аналізу, а також сканування сітківки ока.

При інтеграції додаткових кінцевих пристроїв загальна архітектура комп'ютерної системи повинна бути незмінною, але підтримувати здатність до масштабування шляхом підключення апаратних пристроїв та імплементації програмного забезпечення. Модернізацію комп'ютерної системи аутентифікації особи можна виконувати за необхідності додавання інших керуючих пристроїв, наприклад, електромеханічних замків або інтеграції у більш складний комплекс комп'ютерної безпеки.

До вимог надійності комп'ютерної системи аутентифікації особи на основі відбитку пальця належать:

– точність результатів зчитування відбитків пальців на рівні 98%;

– час безперебійної експлуатації системи і її компонентів визначається виробничими графіками підприємства;

– здатність до відновлення у випадках виникнення не штатних ситуацій або відмов;

– продуктивність системи розпізнавання відбитків пальців і прийняття рішення повинно не перевищувати 2 с;

– забезпечення чіткості і зрозумілості сервісних повідомлень;

– наявність засобів сповіщення про збої у роботі компонентів системи;

– можливість аварійного відключення системи аутентифікації особи.

Вимогами до функцій та вимог, які висуваються до комп'ютерної системи біометричної аутентифікації особи на основі відбитку пальців є:

– можливість одержання адекватного відбитку пальця особи;

– здатність формування бази даних відбитків пальців осіб;

– можливість управління процесом біометричної аутентифікації;

– здатність запису, оновлення та видалення зображень відбитків з бази даних;

– можливість порівняння зчитаного відбитку з уже наявними у базі даних;

– забезпечення визначеної продуктивності роботи системи;

– наявність процедур авторизованого доступу для внесення змін у комп'ютерну систему;

– забезпечення доступу до ресурсів комп'ютерної мережі та Інтернет;

– вивід сервісних повідомлень на LCD екран;

– наявність засобів апаратного налаштування процесу запису та видалення відбитків пальців;

– можливість оновлення системного програмного забезпечення компонентів комп'ютерної системи.

Вимоги до апаратних пристроїв комп'ютерної системи біометричної аутентифікації особи на основі відбитків пальців повинні відображати базові технічні особливості таких компонентів як:

– однокристальний міні-комп'ютер на базі Raspberry PI 2 або Raspberry PI 3;

– сканер відбитку пальців ZFM-20, який сумісний з Raspberry PI;

– LCD-дисплей 16*2 на базі контролера HD44780;

– USB-Serial адаптер будь-якого виробника;

При проектуванні комп’ютерної системи біометричної аутентифікації необхідне застосування персонального комп’ютера, який відповідає наступній конфігурації:

– процесор з тактовою частотою процесора на рівні 2,4 ГГц;
– об’єм оперативної пам’яті – 4 ГБ;
– об’єм жорсткого диску - 500 ГБ.

За необхідності зберігання великої кількості зображень відбитків пальців необхідно використовувати сервер бази даних, апаратні характеристики якого відповідають наступним вимогам:

– процесор з тактовою частотою на рівні не менше 2,2 ГГц та кількістю потоків не менше 6;
– об’єм оперативної пам’яті – 16 ГБ;
– об’єм жорсткого диску – 2ТБ.

Вимогами до програмного забезпечення при проектуванні програмного забезпечення комп’ютерної системи біометричної аутентифікації на основі відбитку пальця є використання середовища розробки з підтримкою мови програмування Python. Особливих вимог до програмного забезпечення комп’ютера і сервера не висувається, однак повинна бути підтримка можливості розгортання та функціонування бази даних для зберігання відбитків пальців. При цьому можна використовувати операційні системи як Windows, так і Unix – подібні.

1.2 Методи і засоби аутентифікації особи

З ростом обсягу інформації, що зберігаються у комп'ютерних системах та з усе ширшим їх впровадженням у повсякденне життя, зростає необхідність у захисті інформації, зокрема у рольовому доступі до неї. Розрізняють наступні етапи взаємодії особи з інформаційною системою з рольовим доступом до її ресурсів: реєстрація, аутентифікація і авторизація.

Реєстрація – це створення нового запису в базі даних користувачів інформаційної системи. Такий запис включає у себе оригінальне реєстраційне ім'я користувача та сукупність його репрезентативних ознак. У більшості сучасних операційних систем на етапі реєстрації користувач вводить ім'я (login) і пароль. Не допускається наявності у базі даних користувачів з двома і більше однаковими реєстраційними іменами. Тобто на етапі реєстрації в інформаційну систему вводяться параметри нового користувача. За умови успішного проходження реєстрації у інформаційній системі, користувач зможе входити у систему пройшовши аутентифікацію.

Аутентифікація (підтвердження правдивості) особи в інформаційній системі – перевірка відповідності суб'єкта і того за кого він себе намагається видати, за допомогою деякої унікальної інформації (паролю, відбитку пальця, голосу і т.п.), у найпростішому випадку, за допомогою реєстраційного імені і паролю. Аутентифікацію в інформаційній системі може пройти зареєстрована особа або зловмисник, видавши себе за зареєстровану особу. У результаті успішної аутентифікацію система авторизує користувача.

Авторизація – надання користувачеві інформаційної системи доступу до певних системних ресурсів. Наприклад, процес авторизації в операційній системі передбачає завантаження середовища користувача, зокрема доступних йому мережевих файлових систем, системних змінних тощо. Підсистема аутентифікації є ключовим елементом інформаційної системи з рольовим доступом, оскільки забезпечує можливість доступу законних власників і неможливість несанкціонованого доступу зловмисників до її ресурсів. При розробці системи аутентифікації ставляться вимоги не лише до надійності роботи системи, а також до зручності роботи користувача з нею.

Переважна більшість методів аутентифікації користувачів базується на розпізнаванні [3]:

1) чогось, відомого лише користувачу;
2) чогось, що має лише користувач;
3) чогось, чим є користувач.

На цих трьох принципах побудовані три різні схеми аутентифікації, які мають певні рівні складності і характеристики безпеки. Щоб нанести шкоду інформаційній системі зловмиснику необхідно спочатку пройти аутентифікацію в ній. Це означає, що він має обійти використовувану в даній системі процедуру аутентифікації. Найширшого використання набула аутентифікація за чимось, що знає користувач – за паролем. Реалізація даного підходу полягає в організації централізованого зберігання списку пар (реєстраційне ім'я, пароль): введене ім'я відшукується у списку, а введений пароль порівнюється з наявним. Якщо паролі співпадають, реєстрація дозволяється, ні – в реєстрації відмовлено. Основною перевагою даного методу є простота реалізації, недоліком – можливість сторонньої особи, знаючої пароль, пройти реєстрацію.

Другий метод аутентифікації користувача полягає в перевірці деякого фізичного об'єкта (пластикова картка, смарт-картка, RFID-картка тощо). Даний метод зобов'язує користувача носити з собою об'єкт аутентифікації, який може бути викрадений зловмисником.

Третій метод аутентифікації базується на вимірюванні зовнішніх ознак або характеристичних особливостей користувача, які є унікальними для кожної особи і які складно підробити. Вони називаються біометричними параметрами. У біометричній підсистемі аутентифікації реалізується два етапи: реєстрація і аутентифікація. Під час першого етапу біометричні характеристики користувача вимірюються і оцифровуються. Потім зберігаються у базі даних, разом з реєстраційним іменем користувача. Другий етап процесу – це аутентифікація. Користувач вводить реєстраційне ім'я, система проводить заміри його біометричних даних і порівнює їх за деякими критеріями з даними, що отримані на етапі реєстрації. Якщо введені дані співпадають зі збереженими даними, реєстрація завершується успішно. В іншому разі користувачеві буде відмовлено в доступі. Біометрична аутентифікація поділяється на статичну, яка ґрунтується на статичних ознаках (папілярний малюнок пальця, малюнок судин руки, малюнок сітківки ока та інші) і динамічну, яка проводиться за динамічними

особливостями особи (відтворення голосом деякої фрази, відтворення підпису, клавіатурний почерк).

На сьогодні біометрична аутентифікація набуває все більшої популярності, оскільки має ряд суттєвих переваг:

1. Істотно підвищується захищеність систем і разом з тим спрощується процес ідентифікації користувача: він не повинен згадувати, набирати і періодично змінювати паролі доступу в різні системи.

2. В усіх випадках, крім випадків злому захисту, можна довести авторство тієї чи іншої електронної дії, підтверджене біометричною аутентифікацією.

3. Неможливо успішно пройти аутентифікацію іншою особою.

Системи динамічної біометричної аутентифікації на сьогодні є новими і перспективними, оскільки мають ряд переваг перед методами статичної біометричної аутентифікації: є зручними, природними і психологічно прийнятними для користувача. Крім того динамічний біометричний пароль може бути змінений особою на відміну від статичного.

Дана робота присвячена розробці математичної моделі і методів обробки, вибору аутентифікаційних ознак, а також розробці підходів до прийняття рішень, для розробки системи аутентифікації за динамічно введеним підписом, що передбачає реєстрацію і аутентифікацію особи [3].

Навички письма виробляються у кожної людини в результаті тривалого навчання і тренувань, та відносяться до числа складних механізмів вищої нервової діяльності. Почерк, як властиву кожній людині індивідуальну і динамічно стійку сукупність графічних і технічних навичок, яка відображена в рукописах, необхідно розглядати у світлі вчення сучасної фізіології про рухові навички. Зокрема, вчення фізіолога І.П. Павлова про динамічний стереотип, розвиненого Н.А. Берштейном [4], П.К. Анохіним та іншими ученими, які обґрунтовують передумови використання підпису як репрезентативної ознаки особи. Під динамічним стереотипом розуміється система умовно-рефлекторних зв'язків, що забезпечує пошук оптимального режиму руху і його відповідність поставленій задачі при повторенні руху в подібних умовах. Вчення про

динамічний стереотип пояснює одну із важливих для ідентифікації властивостей почерку – його відносну стійкість. Сформований почерк особи, набуває такої сукупності особливостей, які роблять його індивідуальним і відрізняють від почерку будь-якої іншої особи. Тому підпис використовується як репрезентативна ознака особи для різних задач [5, 6], зокрема криміналістики, психології, психіатрії тощо.

При письмі і відтворенні підпису, зокрема, людина задіює м'язи більшості пальців і частину м'язів передпліччя. Загальна кількість задіяних м'язів понад 50, проте найбільший вплив має група приблизно з 10 м'язів. Дії цих м'язів призводять до руху руки вздовж і впоперек площини написання, змінюють силу натиску при написанні, нахил пера і його орієнтацію у просторі. Процес відтворення підпису зображено на рис.1.1.

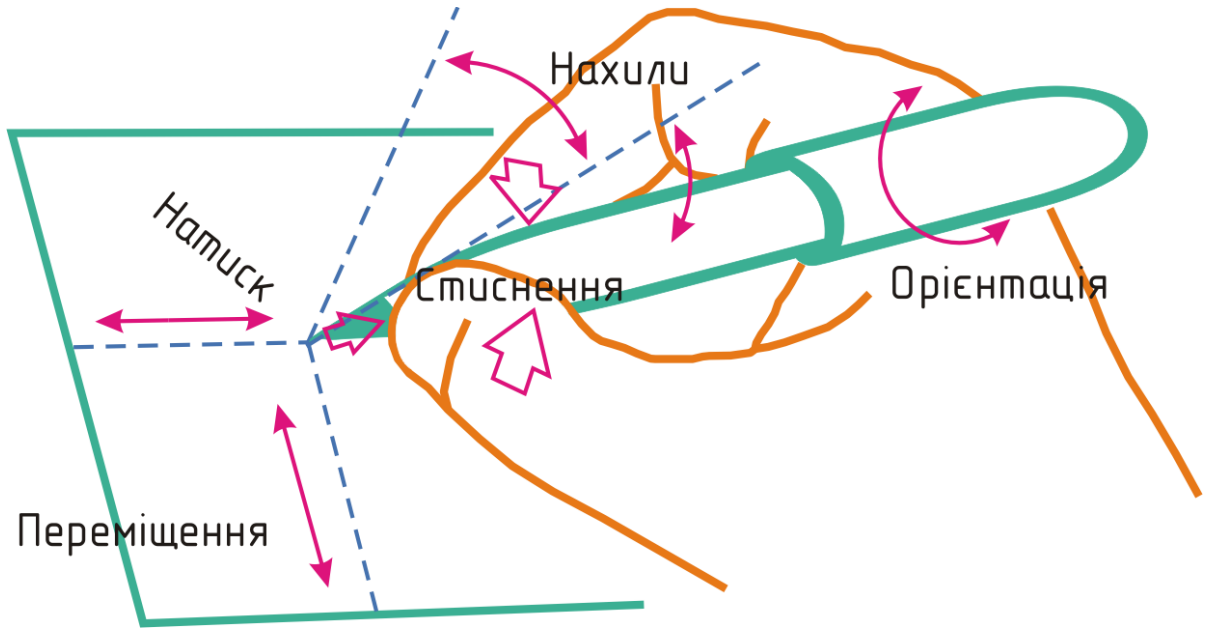

Рисунок 1.1 – Відтворення підпису і фактори, які впливають на нього

При аутентифікації особи на основі підпису розрізняють статичний підпис (off-line) і динамічний (on-line), на основі якого проводиться динамічна біометрична аутентифікація особи.

Розглянемо процес отримання динамічного підпису в ЕОМ (рис.1.1). Динамічний підпис отримується за допомогою пристрою вводу (пристрою-

вказівника) – графічного планшету, або за допомогою інших засобів вводу інформації. Планшет складається з поверхні, по якій особа малює і спеціального пера (стилуса), яким особа малює. Принцип роботи планшета аналогічний принципам роботи комп'ютерної миші: коли користувач пересуває перо по поверхні планшета, ЕОМ отримує координати місця знаходження пера, які одразу ж, у вигляді курсора, відображаються на екрані ЕОМ. Тобто, в момент переміщення пера, планшет інформує операційну систему ЕОМ про нове положення пера. Після запуску користувачем системи програм для аутентифікації особи за динамічно введеним підписом, вона синхронно відслідковує та фіксує моменти зміни положення курсора і з системного годинника (таймера) ЕОМ зчитує значення часу. Таким чином утворюється набір точок, кожна з яких визначається двома координатами місцезнаходження на площині планшета і значенням часу.

РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ КОМП'ЮТЕРНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ОСОБИ ЗА ВІДБИТКОМ ПАЛЬЦІВ

2.1 Архітектура комп'ютерної системи біометричної аутентифікації

Проаналізувавши методи аутентифікації та вимоги до комп'ютерної системи біометричної аутентифікації, важливим етапом є проектування архітектури та розробка алгоритмів функціонування.

На найвищому концептуальному рівні архітектура комп'ютерної системи можна представити, як показано на рис. 2.1.

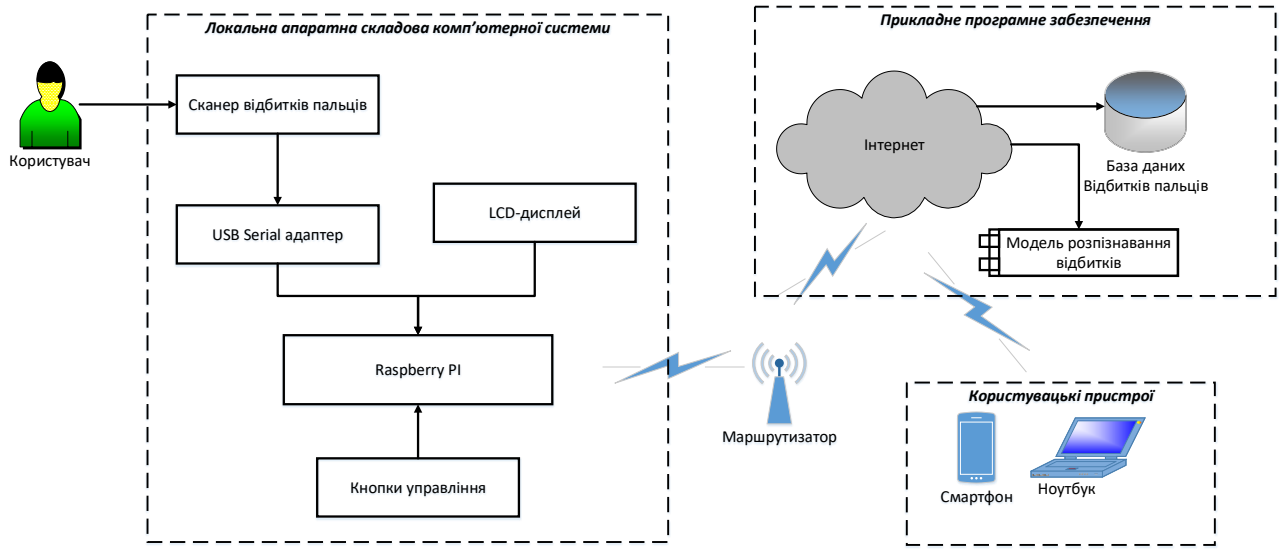

Рисунок 2.1 – Архітектура комп'ютерної системи біометричної аутентифікації особи за відбитком пальців

Складові архітектури комп'ютерної системи, зображеної на рис. 2.1, можна умовно поділити на три блоки:

– блок локальної апаратної складової;

– блок прикладного програмного забезпечення;

– блок користувацьких пристроїв.

Під локальною апаратною складовою комп’ютерної системи слід розуміти сукупність апаратних пристроїв, які безпосередньо здійснюють зчитування відбитку пальця і виконують функції управління передачею даних. При цьому кожен компонент даного блоку повинен використовувати системне програмне забезпечення, яке виконується за допомогою міні-комп’ютера Raspberry PI.

Структура блоку локальної апаратної складової включає наступні апаратні пристрої:

– сканер відбитку пальця;

– пристрій підключення сканера до Raspberry PI (USB Serial адаптер);

– однокристальний міні-комп’ютер Raspberry PI;

– LCD-дисплей;

– кнопки управління процесом сканування.

Сканер відбитку пальців виконує функції безпосереднього зчитування зображення та з’єднаний з Raspberry PI через USB Serial адаптер.

Raspberry PI виконує функцію управління та передачі/одержання даних зі сканера та взаємодії із прикладним ПЗ та базою даних.

USB Serial адаптер призначений для фізичного під’єднання сканера відбитків пальців з Raspberry PI.

LCD-дисплей виконує функцію відображення повідомлень про успішність аутентифікації особи за її відбитком пальця.

Блок прикладного програмного забезпечення включає програмне забезпечення для:

– інтелектуального аналізу і класифікації відбитків пальців;

– базу даних для накопичення та зберігання зображень і додаткової інформації про осіб;

– програмне забезпечення для віддаленого керування процесом управління скануванням.

Користувацькі пристрої по типу смартфонів виконують функції клієнтів, які можуть шляхом авторизованого доступу здійснювати моніторинг за процесом аутентифікації користувачів та керувати ним.

2.2 Обґрунтування вибору та аналіз технічних характеристики Raspberry PI

На сьогоднішній день Raspberry є однією з найпопулярніших вбудованих систем з підтримкою Linux. Підтримувані цим однокристальним міні-комп'ютером операційні системи засновані на дистрибутиві Linux з відкритим вихідним кодом – Debian. Відкриті операційні системи забезпечують гнучкість налаштування програмного забезпечення на системному і прикладному рівні.

На рис. 2.2 наведено зовнішній вигляд Raspberry PI 3.

Рисунок 2.2 – Зовнішній вигляд Raspberry PI 3

До основних технічних характеристик пристрою, наведеного на рис. 2.2 належать:

- SoC: Broadcom BCM2837;
- процесор: 4 × ARM Cortex-A53, 1,2 ГГц;
- графічний процесор: Broadcom VideoCore IV;
- оперативна пам'ять: 1 ГБ LPDDR2 (900 МГц);
- мережа: 10/100 Ethernet, бездротова мережа 2,4 ГГц 802.11n;

– Bluetooth: Bluetooth 4.1 Classic, Bluetooth з низьким енергоспоживанням;

– зберігання даних: microSD;

– GPIO: 40-контактний інтерфейс;

– порти: HDMI, аналоговий аудіо-відео роз'єм 3,5 мм, 4 × USB 2.0, Ethernet, послідовний інтерфейс камери (CSI), послідовний інтерфейс дисплея (DSI).

Модуль Broadcom BCM43438 (рис. 2.3) входить до складу Raspberry PI. Він настільки малий, що його позначення можна побачити лише під мікроскопом або за допомогою лупи. Однак він забезпечує підтримку бездротової локальної мережі у відповідності до протоколу 802.11n (2,4 ГГц), Bluetooth Low Energy та підтримку Bluetooth 4.1 Classic.

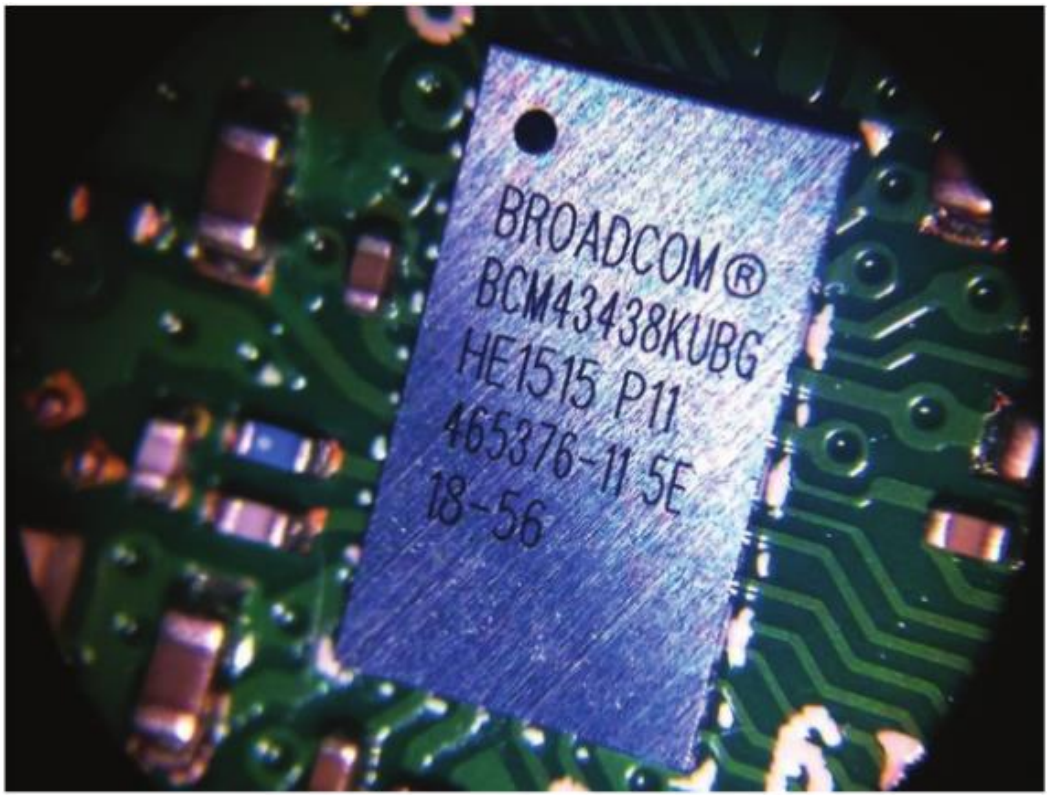

Рисунок 2.3 – Модуль Broadcom BCM43438

Побудована спеціально для нового Pi 3, система Broadcom BCM2837 на system-on-crystal (SoC) включає чотири високопродуктивних процесорних ядра ARM Cortex-A53, що працюють на частоті 1,2 ГГц, з кеш-пам'яттю першого

рівня 32 кБ і другого рівня 512 кБ, графічним процесором VideoCore IV, що підключений до модуля пам'яті LPDDR2 об’ємом 1 ГБ на задній панелі плати (рис. 2.4).

Рисунок 2.4 – Broadcom BCM2837

Немає необхідності підключати зовнішню антену до Raspberry Pi 3. Її радіомодулі підключені до мікросхеми, припаяної безпосередньо до плати, щоб мінімізувати розмір пристрою. Незважаючи на свій мінімальний розмір, ця антена здатна приймати сигнали бездротової локальної мережі та Bluetooth навіть через стіни.

Raspberry Pi 3 має той самий 40-контактний цифровий інтерфейс введення-виведення (GPIO) загального призначення, що і всі інші моделі Raspberry Pi.

Будь-яке існуюче обладнання GPIO працюватиме без змін. Єдине, що змінився перемикач для підключення UART до контактів GPIO, але це обробляється операційною системою внутрішньо.

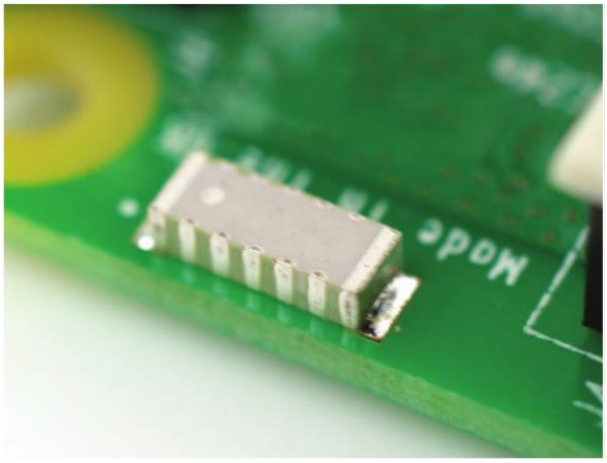

Рисунок 2.5 – Антена радіомодуля на Raspberry PI 3

USB у Raspberry Pi 3 використовує той самий чіп SMSC LAN9514 (рис. 2.6), що і його попередні моделі, додавши 10/100 Ethernet-з'єднання та чотири USB-канали на платі. Як і раніше, мікросхема SMSC підключається до SoC за допомогою одного USB-каналу, виконуючи роль адаптера USB-Ethernet та концентратора USB.

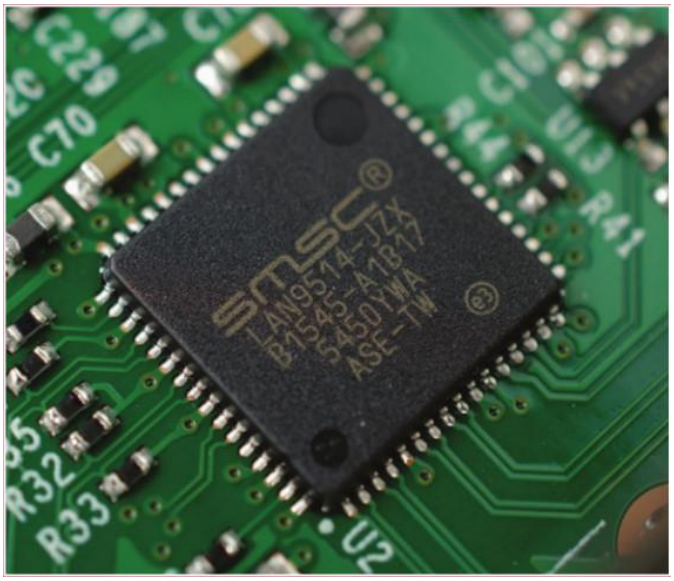

Рисунок 2.6 – Модуль SMSC LAN9514

Таким чином, у результаті аналізу технічних характеристик Raspberry PI 3, можна зробити висновок, що цього однокристального міні-комп’ютера цілком достатньо для побудови проекту комп’ютерної системи біометричної аутентифікації особи за відбитком пальця.

2.3 Аналіз технічних характеристик сканера відбитків пальців

Сканер відбитків пальців серії ZFM-20 представляє собою окремий модуль біометричної ідентифікації особи, запропонований Hangzhou Zhian Technologies Co., Ltd. Даний сканер побудований на Synochip DSP в якості центрального процесора та оптичного датчика із вбудованої інтелектуальною складовою розпізнавання відбитків. Даний модуль дозволяє виконувати ряд функцій, таких як реєстрація відбитків пальців, опрацювання зображень, узгодження відбитків пальців, обробка та зберігання шаблонів. На рис. 2.7 показано вигляд сканера відбитків пальців ZFM-20.

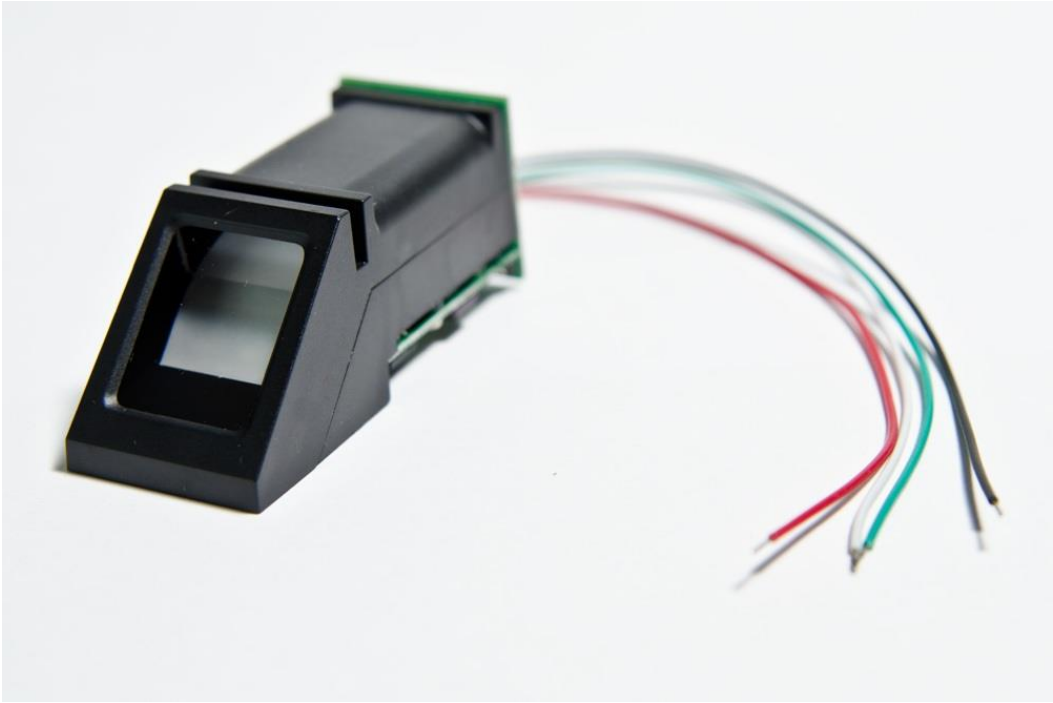

Рисунок 2.7 – Сканер відбитків пальців ZFM-20

Опрацювання відбитків пальців передбачає виконання двох типів процесів: реєстрація відбитків пальців та виявлення збігів (відповідність може бути 1: 1 або 1: N). У випадку наявності відповідності 1:N відбувається аутентифікація особи, в іншому випадку – ідентифікація. Під час реєстрації користувачеві потрібно два рази просканувати палець. Система опрацює два часові зображення, сформує шаблон відбитка на основі результатів обробки та

збереже шаблон. Під час сканування з метою аутентифікації користувач проводить пальцем через оптичний датчик, і система генерує його шаблон та здійснює порівняння з наявними патернами, що містяться у бібліотеці.

У випадку ідентифікації особи, система порівнює зчитаний відбиток і порівнює із наявним у модулі шаблоном. При аутентифікації – система виконує пошук на відповідність відбитка у всій бібліотеці патернів. І в тому, і в іншому випадку система поверне результат щодо успішності чи неуспішності відповідності зчитаного відбитку. Основні технічні характеристики сканера ZFM-20 наведено у табл. 2.1.

Таблиця 2.1 – Технічні параметри ZFM-20

№ з/п	Параметр	Значення
1.	Напруга живлення	Постійна 3,6В – 6 В
2.	Робочий струм	Нормальний: 100 мА Піковий: 150 мА
3.	Швидкість передачі даних	(9600*N) bsp, N=1..12 (за замовчуванням N=6)
4.	Час одержання зображення	<1с
5.	Об’єм сховища	120/375/880
6.	Коефіцієнт помилкового прийняття правильного рішення (FAR)	<0,001%
7.	Середній час пошуку патернів	<1с (1:800)
8.	Коефіцієнт відхилення (FRR)	<0,1%
9.	Температура навколишнього середовища	-10 C^0 … +40 C^0
10.	Відносна вологість	40%...85%
11.	Інтерфейс	UART (TTL на логічному рівні)/ USB 1.1
12.	Режим розпізнавання	1:1 або 1:N

Продовження таблиці 2.1

№ з/п	Параметр	Значення
13.	Розмір файлу символів	256 кБ
14.	Розмір шаблону	512 кБ
15.	Розмір вікна	14 мм*18 мм
16.	Рівень безпеки	5

З’єднання із зовнішніми пристроями можливе при використанні інтерфейсів UART або USB, які на PCB платі практично однакові. У випадку split з’єднання застосовується 5-контактний роз'єм (J1) з проміжком 2,0 мм між виводами, а для integral типу – 4-контактний роз'єм (J1) з проміжком між виводами 1,27 мм.

У випадку підключення сканера відбитків пальця до користувацького пристрою з використанням UART, використовується з’єднання контактів, як показано у табл. 2.2.

Таблиця 2.2 – Підключення сканера відбитків пальця з користувацьким пристроєм

Номер контакту	Назва	Тип	Функціональне призначення
1.	Vin	Вхід	Живлення (червоний провідник)
2.	TD	Вихід	Вихідні дані. TTL логічний рівень (зелений провідник)
3.	RD	Вхід	Вхідні дані. TTL логічний рівень (білий провідник)
4.	GND	-	Земля (чорний провідник).
5.	NC	-	Не з’єднується

Через послідовний інтерфейс сканер відбитків пальця може взаємодіяти з MCU потужністю 3,3 В або 5 В: TD (контакт 2 J1) з'єднується з RXD (контакт прийому MCU), RD (контакт 3 J1) з'єднується з TXD (передавальний контакт MCU).

При увімкненні живлення, для ініціалізації сканера потрібно близько 500 мс. Протягом цього періоду він не може приймати команди від зовнішніх пристроїв.

Електричні параметри живлення сканера відбитків пальців показано у табл. 2.3.

Таблиця 2.3 – Електричні параметри живлення сканера

Характеристика	Параметри			Од. вимір.	Примітка
	Мін.	Норм.	Макс.		
Напруга живлення (Vin)	3,6		6,0	В	Нормальний режим роботи
Максимальна напруга живлення	-0,3		7,0	В	Може спричинити перегрівання модуля
Робочий струм	90	100	110	мА	
Піковий струм			150	мА	

При підключенні сканера відбитків пальців із зовнішнім пристроєм через USB інтерфейс, з’єднання контактів виглядає так, як показано у табл. 2.4.

Таблиця 2.4 – З’єднання через USB інтерфейс

Номер контакту	Назва	Тип	Функціональне призначення
1.	Vin	Вхід	Живлення згідно параметрами табл. 2.3.
2.	DP+	Вхід/ Вихід	USB дані
3.	DP-	Вхід/ Вихід	USB дані
4.	GND	-	Земля (чорний провідник).
5.	END	-	Земля. Плаваюча або з підключенням до екранованого шару кабелю.

2.4 Особливості застосування LCD-дисплея

Рідкокристалічні дисплеї дуже часто використовуються при проектуванні вбудованих систем завдяки низькій вартості, зручності використання та програмування. Зовнішній вигляд типового LCD-дисплею 16*2 показано на рис. 2.8.

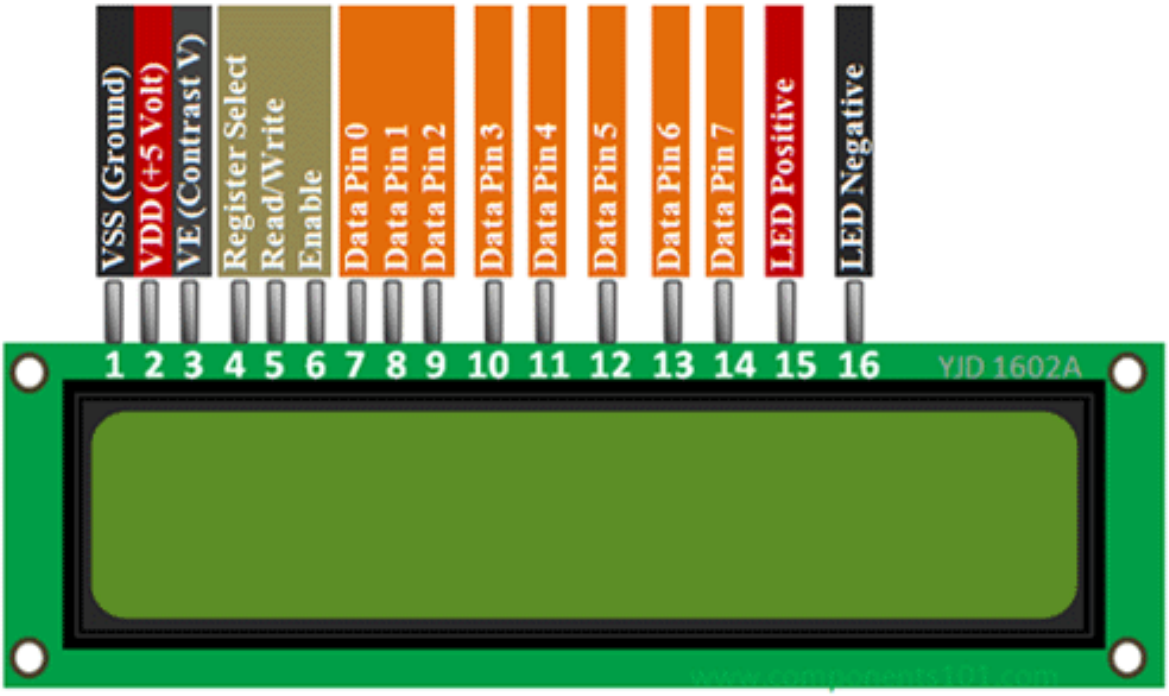

Рисунок 2.8 – LCD-дисплей 16*2

Рідкокристалічний дисплей 16*2 складається з 16 стовпчиків і 2 рядків. Загальна кількість символів, які можна відобразити за допомогою такого типу LCD-дисплеїв становить 32 символи, і кожен символ формується з 5*8 піксельних точок.

На рис. 2.9 наведено структурну схему дисплею 16*2.

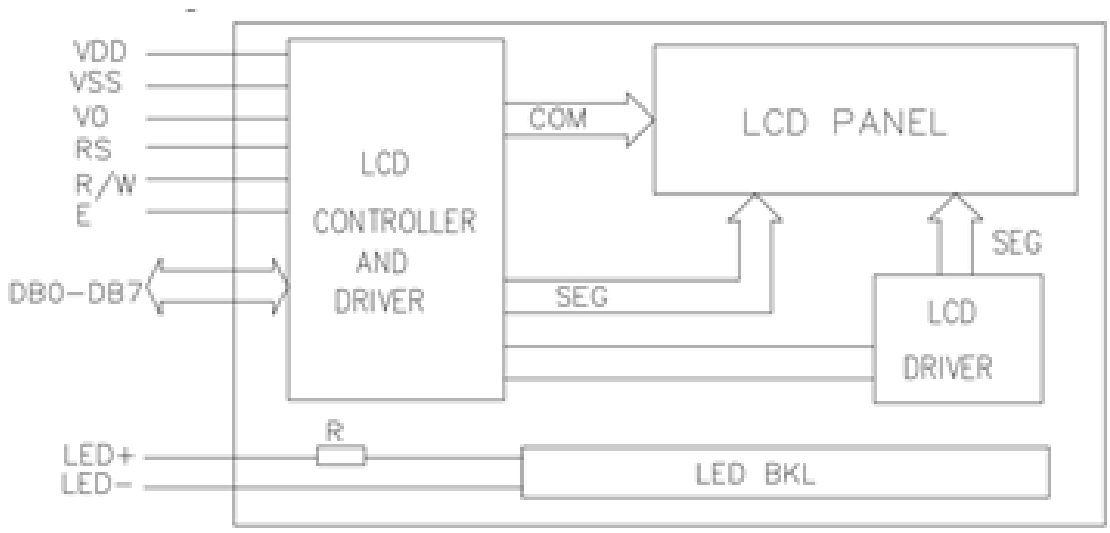

Рисунок 2.9 – Структурна схема LCD-дисплею

Як видно з рис. 2.9 основними компонентами LCD-дисплею 16*2 є:

– LCD-контролер і драйвер;
– Виводи різного призначення;
– LCD-панель.

Виводи LCD-дисплею показано у вигляді табл. 2.5.

Таблиця 2.5 – Технічні характеристики LCD 16*2

№ виводу	Назва виводу	Опис
1	Vss (Ground)	Контакт землі підключений до загальної землі системи
2	Vdd (+5 В)	Живлення дисплею +5В (4.7 В – 5.3 В)
3	VE (Контраст V)	Визначає рівень контрастності дисплея. Використовується заземлення для одержання максимальної контрастності.
4	Register Select	Підключається до мікроконтролера для перемикання між регістром команд/даних

Продовження таблиці 2.5

№ виводу	Назва виводу	Опис
5	Read/Write	Використовується для читання або запису даних. Зазвичай заземлений для запису даних на дисплей
6	Enable	Підключений до мікроконтролера вивід, що перемикається між 1 і 0 для підтвердження даних
7	Data Pin 0	Виводи даних від 0 до 7 утворюють 8-бітову шину даних. Їх можна підключити до мікроконтролера для передачі 8-бітових даних. Ці LCD-дисплеї також можуть працювати в 4-розрядному режимі, у такому випадку контактні дані 4,5,6 та 7 залишаться вільними
8	Data Pin 1	
9	Data Pin 2	
10	Data Pin 3	
11	Data Pin 4	
12	Data Pin 5	
13	Data Pin 6	
14	Data Pin 7	
15	LED Positive	Позитивний контакт світлодіодного підсвічування
16	LED Negative	Негативний контакт світлодіодного підсвічування

Основні властивості рідкокристалічного модуля 16*2:

– робоча напруга становить від 4,7 В до 5,3 В;
– споживання струму – 1 мА у режимі без підсвічування;
– здатність відображати букви і цифри;
– містить два рядки, кожен з яких може виводити 16 символів;
– кожен символ міститься у прямокутнику розміром 5*8 пікселів;
– здатність функціонувати у 8-бітному та в 4-бітному режимі;
– можливість відображати користувацькі символи;
– підсвітка екрану може бути зеленого або синього кольору.

Таким чином, для відображення сервісних повідомлень у комп’ютерній системі біометричної аутентифікації особи за відбитком пальця, цілком достатньо описаного вище пристрою.

2.5 Перетворювач USB – UART

Перетворювач USB – UART (USB Serial Adapter) дозволяє забезпечити зручність підключення різних пристроїв до GPIO Raspberry PI. Як варіант, можна використати USB-Serial перетворювач CP2102 TTL UART. Він дає змогу безпосередньо підключати пристрої з послідовною шиною до портів USB. Це хороший інструмент при проектуванні вбудованих систем, які потребують Serial пристроїв або сенсорів (наприклад, сканер відбитків пальців). На рис. 2.10 показано USB-UART перетворювач.

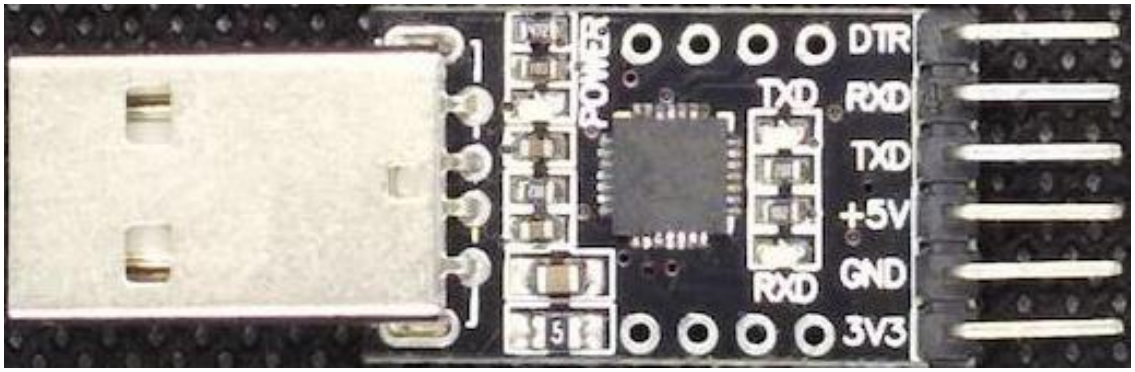

Рисунок 2.10 – USB Serial Adapter CP2102 TTL UART

До основних технічних параметрів CP2102 TTL UART належать:

– сумісність живлення 3,3 В/5 В;
– повношвидкісний USB 2.0;
– не потребує зовнішнього кристала;
– внутрішній EEPROM для ідентифікатора пристрою;
– швидкість передачі даних від 300 біт/с до 921600 біт/с.

Конвертер USB до послідовного TTL UART має чотири важливі виводи:

– RX вивід;
– Вивід TX;
– VCC;
– GND.

RX – це абревіатура для виводу, що приймає дані, а TX використовується для передачі. Виводи VCC і GND живлять модуль відбитків пальців. Цей

перетворювач може подавати 3 В або 5 В, залежно від потреб. На рис. 2.11 показано схему з'єднання USB Serial адаптера зі сканером відбитків пальців.

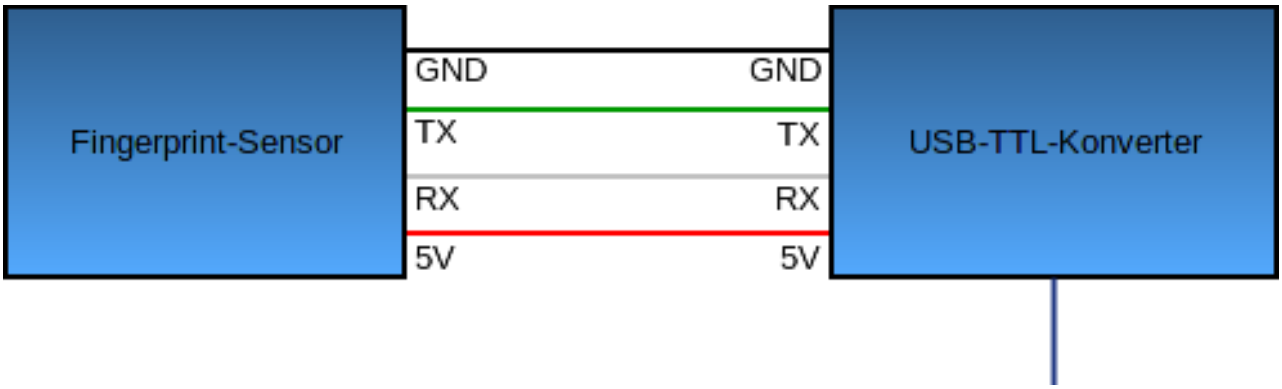

Рисунок 2.11 – Схема з'єднання USB Serial адаптера зі сканером відбитків пальців

При побудові комп'ютерної системи біометричної аутентифікації особи за відбитком пальця пропонується використовувати 3 В, тобто потужність, необхідну для функціонування сканера відбитків пальців.

2.6 Побудова схеми комп'ютерної системи біометричної аутентифікації особи за відбитком пальця

Обґрунтувавши вибір основних компонентів апаратного забезпечення комп'ютерної системи біометричної аутентифікації особи та провівши аналіз особливостей їх технічних характеристик, перейдемо до проектування схеми взаємодії між компонентами. Для проектування цієї схеми необхідно використання основних і допоміжних апаратних пристроїв:

- Raspberry Pi Model B;
- перетворювач USB в UART;
- сканер відбитків пальців;
- кнопки;
- LCD-дисплей 16x2;
- bread board або друкована плата;

– провідники;

– світлодіод;

– резистор 150 Ом –а 1 кОм.

На рис. 2.12 показано спроектовану схему компонентів комп'ютерної системи біометричної аутентифікації особи. При проектуванні системи взаємодії сканера відбитків пальців з Raspberry Pi запропоновано використати 4 кнопки:

– Enrol/Ok – для реєстрації нового відбитка пальця,

– Delete – для видалення вже наявних зображень відбитків пальців;

– Increment/Decrement – дві кнопки для збільшення/зменшення кількості уже наявних відбитків пальців.

Світлодіод використовується в якості індикатора того, що сканер відбитків пальців готовий зчитати відбиток пальця.

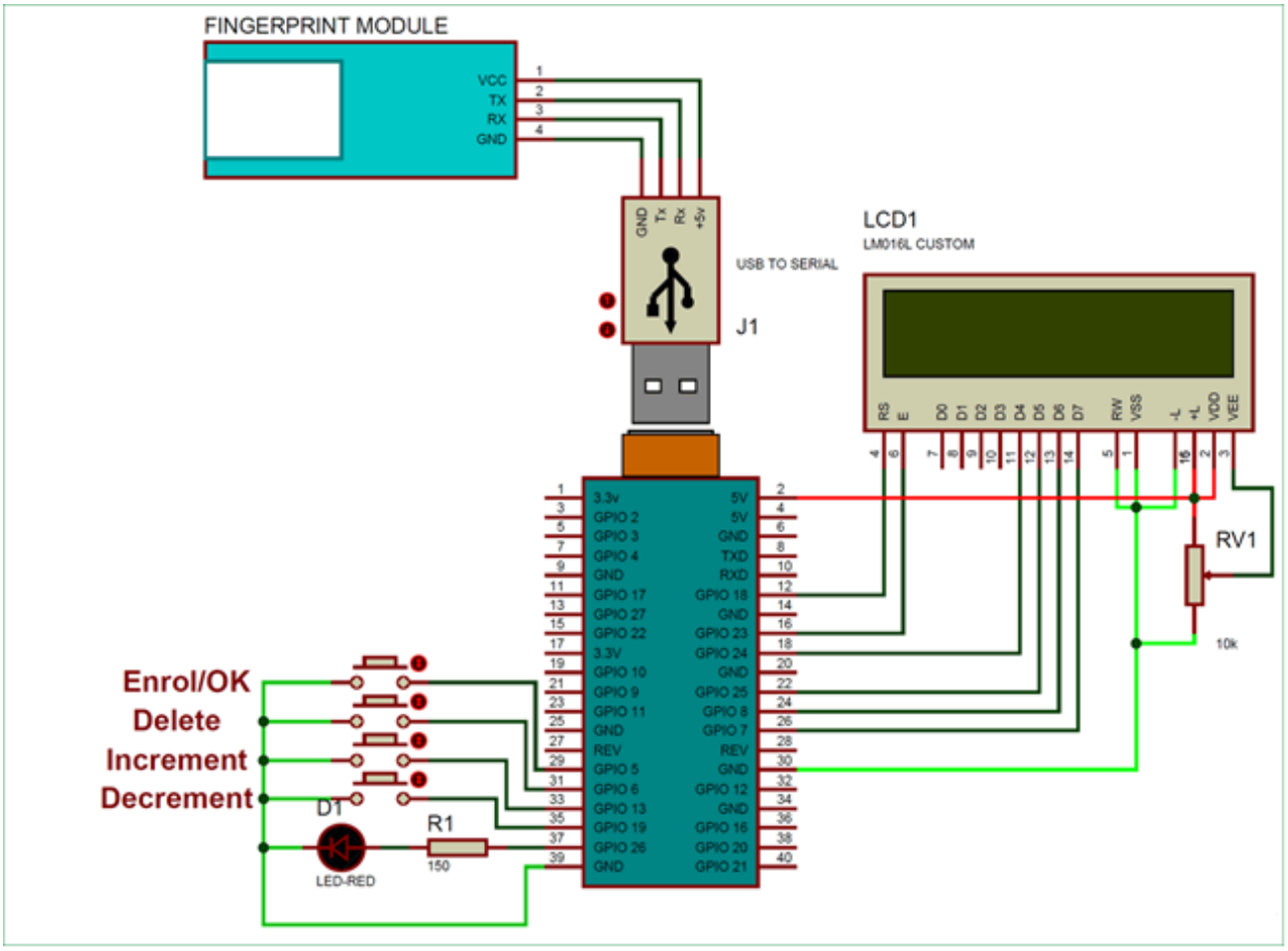

Рисунок 2.12 – Схема комп'ютерної системи біометричної аутентифікації особи за відбитком пальців

Для зчитування відбитку пальця і передачі даних до Raspberry PI використовується USB Serial адаптер (UART).

LCD-дисплей 16*2 використовується для відображення повідомлень, а резистор 10 Ом забезпечує контроль його контрастності.

Виводи LCD-дисплею RS, EN, d4, d5, d6 та d7 підключені до виводів GPIO 18, 23, 24, 25, 8 та 7 Raspberry Pi відповідно.

Чотири кнопкові кнопки підключені до GPIO 5, 6, 13 та 19 Raspberry Pi. Світлодіод також підключений на виводі 26.

У табл. 2.6 показано підключення виводів кінцевих пристроїв з однокристальним міні-комп'ютером Raspberry PI.

Таблиця 2.6 – З'єднання виводів кінцевих пристроїв з Raspberry PI

Пристрій	Вивід	Вивід Raspberry PI
LCD-дисплей	RS	18
	EN	23
	D4	24
	D5	25
	D6	8
	D7	7
Кнопка Enroll/OK		5
Кнопка Delete		6
Кнопка Increment		13
Кнопка Decrement		19
Світлодіод		26

Після встановлення всіх з'єднань потрібно увімкнути Raspberry Pi т відкрити термінал. Далі необхідно проінсталювати бібліотеку для роботи зі

сканером відбитків пальців для Raspberry Pi, виконавши наведені нижче дії. Для того, щоб встановити цю бібліотеку, потрібні права адміністратора (рис. 2.13).

```
sudo bash
```

Рисунок 2.13 – Виконання команд від імені root

Після цього необхідно завантажити бібліотеки, використавши команди, як показано на рис. 2.14.

```
wget -O - http://apt.pm-codeworks.de/pm-codeworks.de.gpg | apt-key add -
wget http://apt.pm-codeworks.de/pm-codeworks.list -P /etc/apt/sources.list.d/
```

Рисунок 2.14 – Завантаження необхідних бібліотек

Результат завантаження пакетів представлено на рис. 2.15.

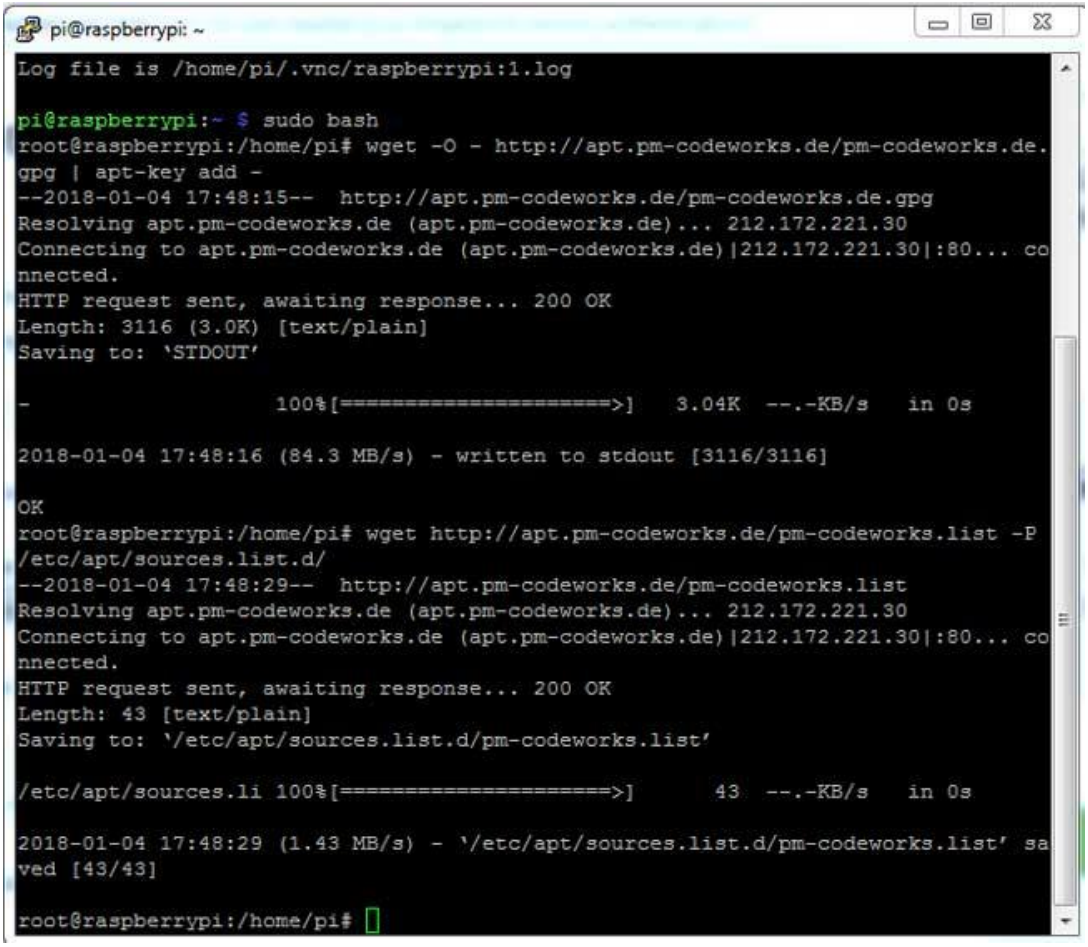

Рисунок 2.15 – Результат завантаження бібліотек

Після цього потрібно оновити Raspberry PI і встановити завантажену бібліотеку сканера відбитків пальців шляхом виконання команд, наведених на рис. 2.16.

```
sudo apt-get update
sudo apt-get install python-fingerprint -yes
```

Рисунок 2.16 – Оновлення Raspberry PI та інсталяція бібліотеки для роботи зі сканером відбитків пальців

Результат виконання команд, наведених на рис. 2.16, показано на рис. 2.17.

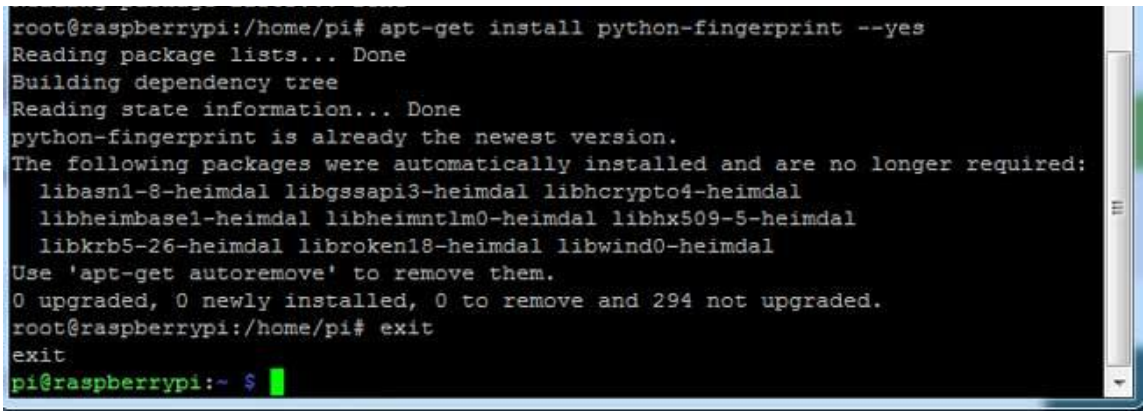

Рисунок 2.17 – Результат виконання команд

Після встановлення бібліотеки потрібно перевірити USB-порт, до якого підключений сканер відбитків пальців, за допомогою команди, наведеної на рис. 2.18.

```
ls /dev/ttyUSB*
```

Рисунок 2.18 – Перевірка підключення до USB-порта

Одержаний номер USB-порту був раніше використаний при написанні програмного забезпечення для біометричної аутентифікації особи за відбитком пальців.

РОЗДІЛ 3 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ОСОБИ ЗА ВІДБИТКОМ ПАЛЬЦІВ

3.1 Реалізація логіки роботи програмного забезпечення комп'ютерної системи біометричної аутентифікації

Розробку програмного забезпечення комп'ютерної системи біометричної аутентифікації особи за відбитком пальця запропоновано реалізувати за допомогою мови програмування Python.

Для взаємодії сканера відбитків пальців з Raspberry PI можна скористатись готовою бібліотекою, а у випадку застосування власного алгоритму розпізнавання відбитку пальця – побудувати та інтегрувати власну модель за допомогою інструментів тієї ж мови програмування.

Перед тим, як перейти до безпосередньої реалізації логіки роботи програмного забезпечення необхідно імпортувати бібліотеки для роботи зі сканером відбитків пальців, GPIO та часом. Імпорт бібліотек показаний у лістингу 1.1.

Лістинг 3.1 – Імпорт бібліотек

```
import time
from pyfingerprint.pyfingerprint import PyFingerprint
import RPi.GPIO as gpio
```

Після цього, потрібно визначити виводи для роботи з LCD-дисплеєм, світлодіодом та кнопками управління (лістинг 3.2).

Лістинг 3.2 – Програмне оголошення виводів

```
RS =18
EN =23
D4 =24
D5 =25
D6 =8
D7 =7
enrol=5
delet=6
inc=13
dec=19
led=26
HIGH=1
LOW=0
```

Після оголошення виводів потрібно виконати їх ініціалізацію, як показано у лістингу 3.3.

Лістинг 3.3 – Ініціалізація виводів

```
gpio.setwarnings(False)
gpio.setmode(gpio.BCM)
gpio.setup(RS, gpio.OUT)
gpio.setup(EN, gpio.OUT)
gpio.setup(D4, gpio.OUT)
gpio.setup(D5, gpio.OUT)
gpio.setup(D6, gpio.OUT)
gpio.setup(D7, gpio.OUT)

gpio.setup(enrol, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(delet, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(inc, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(dec, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(led, gpio.OUT)
```

Ініціалізація сканера відбитків пальців наведена у лістингу 3.4.

Лістинг 3.4 – Ініціалізація сканера відбитків пальців

```
try:
    f = PyFingerprint('/dev/ttyUSB0', 57600, 0xFFFFFFFF,
0x00000000)
    if ( f.verifyPassword() == False ):
        raise ValueError('The given fingerprint sensor
password is wrong!')
except Exception as e:
    print('Exception message: ' + str(e))
    exit(1)
```

Для керування рідкокристалічним дисплеєм необхідно реалізувати наступні функції:

– begin () – основна функція при роботі з дисплеєм, що забезпечує виклик інших функцій та виводить повідомлення у зрозумілій для користувача формі;

– lcdcmd (ch) – функція для зчитування вхідних даних та управління відображенням символів на екрані;

– lcdwrite (ch) – функція формування повідомлень, які в подальшому використовуються функцією lcdprint (Str);

– lcdprint (Str) – функція, що відповідає за безпосередній вивід повідомлення на екран;

– setCursor (x,y) – функція управління курсором;

– lcdclear () – функція очищення дисплею від символів.

Програмний код функції lcdclear () показано у лістингу 3.5.

Лістинг 3.5 – Функція lcdclear()

```
def lcdclear():
  lcdcmd(0x01)
```

Функція lcdclear() не приймає на вхід жодних параметрів, а лише викликає функцію lcdcmd () з параметром 0x01, що вказує на очищення символів на LCD-екрані.

Функція setCursor(x,y) має програмну реалізацію як показано у лістингу 3.6.

Лістинг 3.6 – Функція setCursor (x,y)

```
def setCursor(x,y):
    if y == 0:
        n=128+x
    elif y == 1:
        n=192+x
    lcdcmd(n)
```

Вхідними параметрами функції, наведеної у лістингу 3.6 є координати поточного положення курсора. Логіка роботи функції полягає у перевірці значення y, а після цього формування значення змінної n шляхом додавання зміщення по осі абсцис. У результаті цього, обчислений параметр n передається у функцію управління дисплеєм lcdcmd () і відбувається її виклик.

Програмна реалізації функції виводу на екран показана у лістингу 3.7.

Лістинг 3.7 – Програмна реалізація функції lcdprint()

```
def lcdprint(Str):
  l=0;
  l=len(Str)
  for i in range(l):
    lcdwrite(ord(Str[i]))
```

Як видно з коду лістингу 3.7 вхідним параметром функції є змінна Str, яка інтерпретує повідомлення, що необхідно відобразити на екрані. Алгоритм виконання функції наступний:

– створення локальної змінної для зберігання значення довжини стрічки, що міститься у параметрі Str;

– циклічний виклик функції lcdwrite (ch) у діапазоні, що відповідає значенню локальної змінної l.

Варто зауважити, що значення параметра ch у функції lcdwrite () формується шляхом посимвольного зчитування стрічки і перетворенням типу символа у цілочисельний тип за допомогою функції ord().

Реалізація функції lcdwrite () наведена у лістингу 3.8.

Лістинг 3.8 – Програмний код функції lcdwrite ()

```
def lcdwrite(ch):
  gpio.output(RS, 1)
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
  gpio.output(D7, 0)
  if ch&0x10==0x10:
    gpio.output(D4, 1)
  if ch&0x20==0x20:
    gpio.output(D5, 1)
  if ch&0x40==0x40:
    gpio.output(D6, 1)
  if ch&0x80==0x80:
    gpio.output(D7, 1)
  gpio.output(EN, 1)
  time.sleep(0.005)
  gpio.output(EN, 0)
  # Low bits
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
  gpio.output(D7, 0)
  if ch&0x01==0x01:
    gpio.output(D4, 1)
```

```
if ch&0x02==0x02:
  gpio.output(D5, 1)
if ch&0x04==0x04:
 gpio.output(D6, 1)
if ch&0x08==0x08:
 gpio.output(D7, 1)
 gpio.output(EN, 1)
 time.sleep(0.005)
 gpio.output(EN, 0)
```

З аналізу лістингу 3.8 видно, що вхідним параметром функції lcdwrite () є цілочисельне представлення символу ch, який необхідно відобразити на екрані. Після цього виконуються перевірки відносно того, який символ за яким виводом інтерфейсу GPIO закріплено. У результаті виконання функція повертає символи з підтримкою англійського алфавіту.

Програмний код реалізації функції управління формуванням повідомлень представлено у вигляді лістингу 3.9.

Лістинг 3.9 – Програмний код lcdcmd()

```
def lcdcmd(ch):
  gpio.output(RS, 0)
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
  gpio.output(D7, 0)
  if ch&0x10==0x10:
    gpio.output(D4, 1)
  if ch&0x20==0x20:
    gpio.output(D5, 1)
  if ch&0x40==0x40:
    gpio.output(D6, 1)
  if ch&0x80==0x80:
    gpio.output(D7, 1)
  gpio.output(EN, 1)
```

```
    time.sleep(0.005)
    gpio.output(EN, 0)
    # Low bits
    gpio.output(D4, 0)
    gpio.output(D5, 0)
    gpio.output(D6, 0)
    gpio.output(D7, 0)
    if ch&0x01==0x01:
      gpio.output(D4, 1)
    if ch&0x02==0x02:
      gpio.output(D5, 1)
    if ch&0x04==0x04:
      gpio.output(D6, 1)
    if ch&0x08==0x08:
      gpio.output(D7, 1)
    gpio.output(EN, 1)
    time.sleep(0.005)
    gpio.output(EN, 0)
```

Ще одна функція, яка відповідає за процес управління відображенням повідомлень на LCD-дисплеї, наведена у лістингу 3.10.

Лістинг 3.10 – Функція begin()

```
def begin():
  lcdcmd(0x33)
  lcdcmd(0x32)
  lcdcmd(0x06)
  lcdcmd(0x0C)
  lcdcmd(0x28)
  lcdcmd(0x01)
  time.sleep(0.0005)
```

Основне призначення функції begin() полягає у послідовному виклику функції lcdcmd() з різними вхідними параметрами.

Здійснивши реалізацію функцій щодо роботи з LCD-дисплеєм, далі необхідно впровадити програмну реалізацію логіки роботи зі сканером відбитків пальців. Для цього створено наступні функції:

– def enrollFinger () – функція, що використовується для реєстрації або збереження нових відбитків пальців;

– def searchFinger () – функція, що використовується для пошуку вже збережених відбитків пальців;

– def deleteFinger () – функція для знищення вже збереженого відбитка пальця шляхом натиснення відповідної кнопки.

Лістинг 3.11 демонструє логіку реєстрації або додавання відбитку пальця зчитаного зі сканера.

Лістинг 3.11 – Функція def enrollFinger ()

```
def enrollFinger():
        lcdcmd(1)
        lcdprint("Enrolling Finger")
        time.sleep(2)
        print('Waiting for finger...')
        lcdcmd(1)
        lcdprint("Place Finger")
        while ( f.readImage() == False ):
            pass
        f.convertImage(0x01)
        result = f.searchTemplate()
        positionNumber = result[0]
        if ( positionNumber >= 0 ):
            print('Template already exists at position #' +
    str(positionNumber))
            lcdcmd(1)
            lcdprint("Finger ALready")
            lcdcmd(192)
            lcdprint("   Exists     ")
```

```
        time.sleep(2)
        return
    lcdcmd(1)
    lcdprint("Remove Finger")
    time.sleep(2)
    print('Waiting for same finger again...')
    lcdcmd(1)
    lcdprint("Place Finger")
    lcdcmd(192)
    lcdprint("   Again    ")
    while ( f.readImage() == False ):
        pass
    f.convertImage(0x02)
    if ( f.compareCharacteristics() == 0 ):
        print "Fingers do not match"
        lcdcmd(1)
        lcdprint("Finger Did not")
        lcdcmd(192)
        lcdprint("   Mactched   ")
        time.sleep(2)
        return
    f.createTemplate()
    positionNumber = f.storeTemplate()
    print('Finger enrolled successfully!')
    lcdcmd(1)
    lcdprint("Stored at Pos:")
    lcdprint(str(positionNumber))
    lcdcmd(192)
    lcdprint("successfully")
    print('New template position #' + str(positionNumber))
    time.sleep(2)
```

Наведена у лістингу 3.11 функція перевіряє коректність зчитаного відбитку пальця і якщо такого ще немає у базі даних, виконує реєстрацію. У випадку наявності такого зображення відбитку пальця, його можна замінити

новим. Для цього передбачено оператори для видалення зображення і на його місце запису іншого.

Пошук відбитків пальців на основі зчитаного зі сканера виконується функцією searchFinger (), програмний код якої наведено у лістингу 3.12.

Лістинг 3.12 – Функція searchFinger ()

```
def searchFinger():
    try:
        print('Waiting for finger...')
        while( f.readImage() == False ):
            #pass
            time.sleep(.5)
            return
        f.convertImage(0x01)
        result = f.searchTemplate()
        positionNumber = result[0]
        accuracyScore = result[1]
        if positionNumber == -1 :
            print('No match found!')
            lcdcmd(1)
            lcdprint("No Match Found")
            time.sleep(2)
            return
        else:
            print('Found template at position #' +
str(positionNumber))
            lcdcmd(1)
            lcdprint("Found at Pos:")
            lcdprint(str(positionNumber))
            time.sleep(2)
    except Exception as e:
        print('Operation failed!')
        print('Exception message: ' + str(e))
        exit(1)
```

Для видалення наявних відбитків пальців застосовуються кнопки інкременту і декременту для руху по базі даних. Після знаходження потрібного номеру відбитку виконується його вибір шляхом натиснення кнопки реєстрації, яка одночасно працює як кнопка підтвердження дії користувача. Програмна реалізація описаного алгоритму наведена у лістингу 3.13.

Лістинг 3.13 – Функція deleteFinger()

```
def deleteFinger():
    positionNumber = 0
    count=0
    lcdcmd(1)
    lcdprint("Delete Finger")
    lcdcmd(192)
    lcdprint("Position: ")
    lcdcmd(0xca)
    lcdprint(str(count))
    while gpio.input(enrol) == True:    # here enrol key means ok
        if gpio.input(inc) == False:
            count=count+1
            if count>1000:
                count=1000
            lcdcmd(0xca)
            lcdprint(str(count))
            time.sleep(0.2)
        elif gpio.input(dec) == False:
            count=count-1
            if count<0:
                count=0
            lcdcmd(0xca)
            lcdprint(str(count))
            time.sleep(0.2)
    positionNumber=count
    if f.deleteTemplate(positionNumber) == True :
        print('Template deleted!')
        lcdcmd(1)
```

```
    lcdprint("Finger Deleted");
    time.sleep(2)
```

Після успішного видалення відбитку на дисплеї з’явиться відповідне повідомлення Наступного змісту «Fingerprint deleted». Реалізувавши функції для роботи зі сканером та дисплеєм, наступний крок полягає у написанні основної функції програми, яка приведена у лістингу 3.14.

Лістинг 3.14 – Основне тіло програми

```
begin()
lcdcmd(0x01)
lcdprint("FingerPrint ")
lcdcmd(0xc0)
lcdprint("Interfacing ")
time.sleep(3)
lcdcmd(0x01)
lcdprint("Circuit Digest")
lcdcmd(0xc0)
lcdprint("Welcomes You  ")
time.sleep(3)
flag=0
lcdclear()

while 1:
    gpio.output(led, HIGH)
    lcdcmd(1)
    lcdprint("Place Finger")
    if gpio.input(enrol) == 0:
        gpio.output(led, LOW)
        enrollFinger()
    elif gpio.input(delet) == 0:
        gpio.output(led, LOW)
        while gpio.input(delet) == 0:
            time.sleep(0.1)
```

```
            deleteFinger()
        else:
            searchFinger()
```

У результаті написання програмного забезпечення реалізовано функціональність та взаємодію між апаратними пристроями комп'ютерної системи біометричної аутентифікації особи за відбитком пальця, що відповідає вимогам, зазначених у технічному завданні.

3.2 Тестування комп'ютерної системи аутентифікації особи

Для перевірки і тестування розробленої комп'ютерної системи біометричної аутентифікації особи за відбитком пальця потрібно запустити програмний код мовою програмування Python. У випадку успішного запуску, на LCD-дисплеї з'являються сервісні повідомлення, а після того користувачеві буде запропоновано зісканувати палець за допомогою зчитувача відбитків пальців, як показано на рис. 3.1.

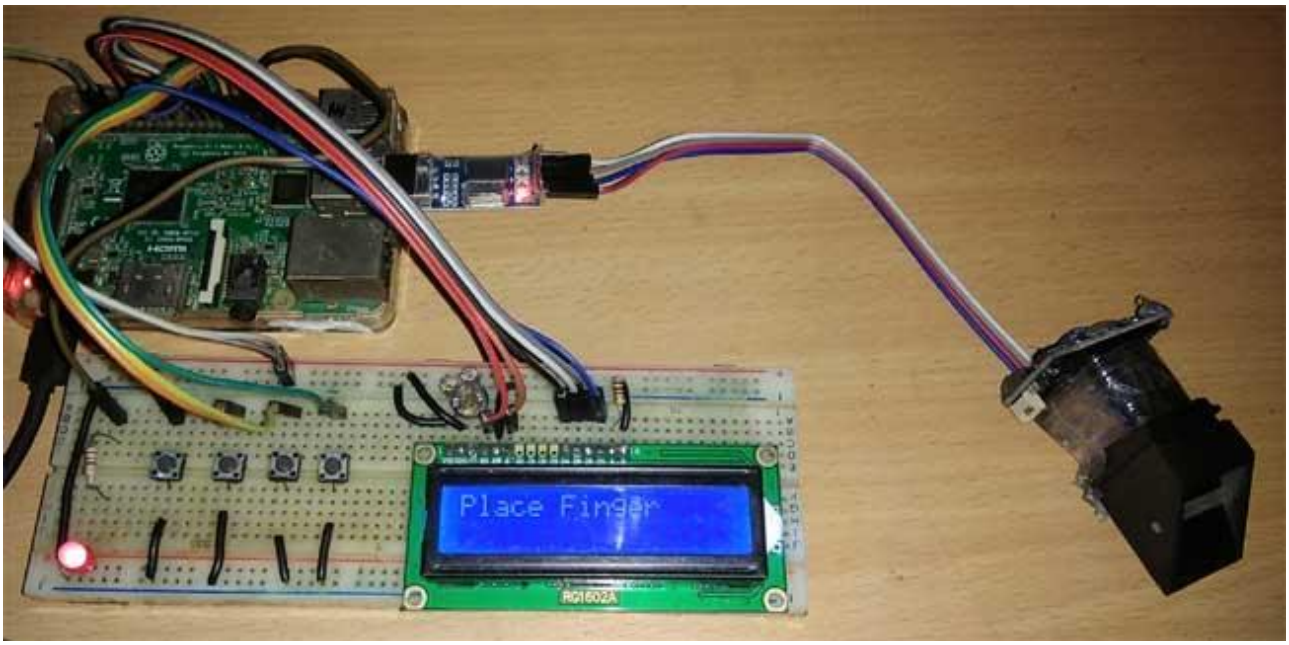

Рисунок 3.1 – Вивід сервісного повідомлення

Приклавши палець на сканер можна перевірити, чи зберігаються відбитки пальців чи ні. Якщо відбиток пальця зберігається, тоді на дисплеї відображатиметься повідомлення з позицією зберігання відбитка, наприклад, «Save at Pos: 2», в іншому випадку – відображатиметься «No Match Found».

Для того, щоб зареєструвати відбиток пальця, користувачеві потрібно натиснути кнопку реєстрації та виконувати інструкції, які з'являються на рідкокристалічному екрані.

Якщо користувач хоче видалити будь-який з відбитків пальців, то для цього потрібно натиснути кнопку видалення. Як результат, на екрані буде відображено повідомлення про те, який саме відбиток потрібно знищити. Вказавши номер запису відбитка за допомогою кнопок «Increment» або «Decrement» обирається позиція з якої буде видалено зображення. Для підтвердження операції видалення використовується кнопка реєстрації відбитку пальця, що в даному випадку, працює як «ОК».

Схематично взаємодію між пристроями комп'ютерної системи біометричної аутентифікації особи на програмному та апаратному рівні показано на рис. 3.2.

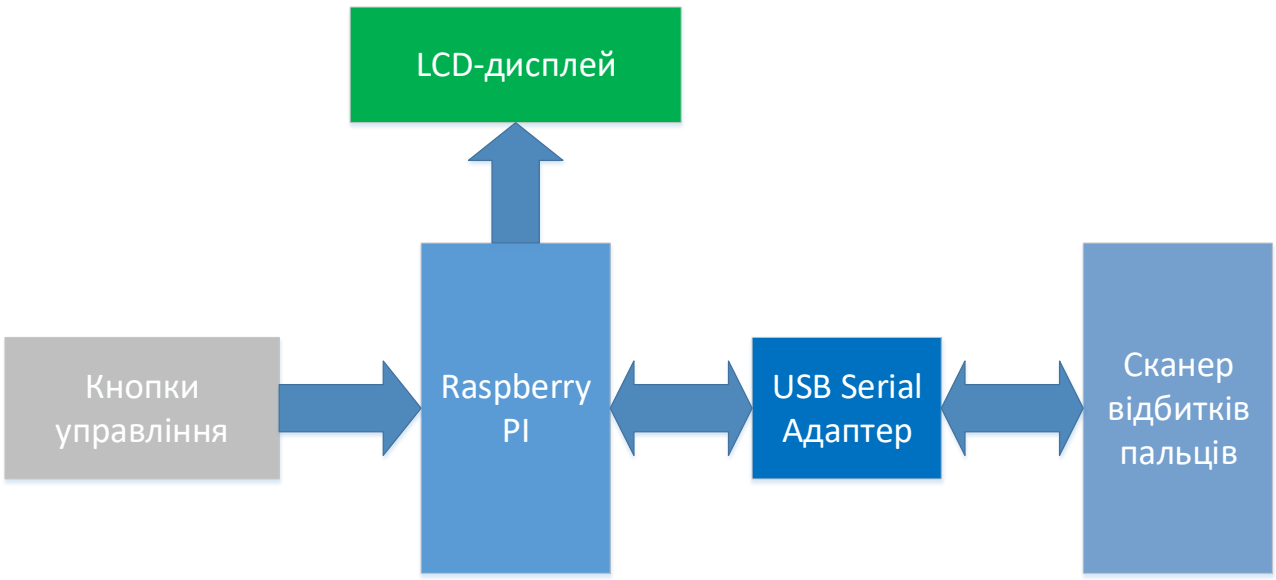

Рисунок 3.2 – Взаємодія між компонентами комп'ютерної системи

Таким чином, у результаті тестування комп’ютерної системи біометричної аутентифікації встановлено відповідність результатів функціонування системи вимогам до неї, а взаємодія між її компонентами відповідає запропонованій архітектурі.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вплив виробничого середовища на працездатність та здоров'я користувачів комп'ютерів

Трудова діяльність користувачів комп'ютерів відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі — фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників. Вплив хімічних та, особливо, біологічних факторів виробничого середовища на користувачів комп'ютерів —значно менший.

Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп'ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями, недостатньою руховою активністю, напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями.

Професійні якості та виробничий досвід, які визначають внутрішні засоби діяльності, обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи розв'язання виробничих завдань навіть у нестандартних ситуаціях.

Зовнішні засоби діяльності, які в основному визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його елементів, просторового розташування основного і допоміжного устаткування,

можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів.

У професійних операторів частіше зустрічаються порушення органів зору, опорно-рухового апарату, центральної нервової, серцево-судинної, імунної та статевої систем, захворювання шкіри. Зафіксована значна кількість скарг операторського персоналу на загальне недомагання, передчасне стомлювання, головний біль, порушення функцій органів зору, які здійснювали несприятливий психофізіологічний вплив на само почуття та працездатність операторів. Сучасна професія користувача ВДТ належить до розумової праці, яка характеризується:

– високою напруженістю зорових функцій;

– одноманітною позою;

– великою кількістю стереотипних висококоординованих рухів, що виконуються лише м'язами кистей рук на фоні малої загальної рухової активності;

– значним нервово-емоційним компонентом, особливо в умовах дефіциту часу;

– роботою з великими масивами інформації, що викликає активізацію уваги та інших вищих психічних функцій.

Крім того, при роботі з дисплеями на електронно - променевих трубках виникає вплив на користувача цілої низки факторів фізичної природи — електростатичні поля, радіочастотне та рентгенівське випромінювання тощо. Діяльність професіоналів можна поділити на три групи:

– діяльність, яка пов'язана з виконанням нескладних багаторазово повторюваних операцій, що не вимагають великого розумового напруження, зокрема, робота операторів комп'ютерного набору, працівників довідкових служб.

– діяльність, яка пов'язана із здійсненням логічних операцій, що постійно повторюються. Це робота інженера - економіста, інженера - проектувальника, оператора автоматизованого виробництва.

– діяльність, коли в процесі роботи необхідно приймати рішення за відсутності заздалегідь відомого алгоритму: робота інженера - програміста, диспетчерів руху залізничного транспорту, аеропортів тощо.

У користувачів, які інтенсивно використовують комп'ютер в умовах значних розумових напружень досить часто (40 — 70%) виникають психологічні та поведінкові порушення (нервозність, роздратування, тривога, нерішучість, замкнутість тощо). Серед користувачів ВДТ в США і Європі значного поширення набуло специфічне захворювання, яке отримало назву синдром комп'ютерного стресу (СКС). СКС супроводжується головним болем, запаленням очей, алергією, роздратованістю, млявістю і депресією. Інформаційне перевантаження користувачів ВДТ супроводжується низкою специфічних захворювань, які називають інформаційними. Першим симптомом їх є головний біль. Дослідження, проведені в США, Німеччині, Швейцарії та інших країнах, показали, що робота з обслуговування ВДТ супроводжується підвищеним напруженням зору, інтенсивністю і монотонністю праці, збільшенням статичних навантажень, нервово-психічним напруженням, впливом різного виду випромінювань та ін . Внаслідок цього серед операторів ВДТ, як зазначають фахівці Всесвітньої організації охорони здоров'я, частіше, ніж в інших групах працюючих, трапляються такі професійні захворювання, як передчасна стомлюваність, погіршення зору, м'язові і головні болі, психічні й нервові розлади, хвороби серцево-судинної системи, онкологічні захворювання [21].

Вважається, що стан організму операторів ВДТ визначається комплексним впливом факторів трудового процесу і середовища, значення яких є неоднаковим. На операторів з малим стажем роботи на ВДТ домінуючий вплив чинять фактори середовища, а на операторів зі стажем понад 5 років – фактори трудового процесу.

Для захисту людини від шкідливого впливу електромагнітних полів приймаються нормативи та стандарти. Треба зазначити, що будь-які норми та стандарти, пов’язані із захистом людини від небезпечного впливу, завжди представляють собою компроміс між перевагами використання нових

технологій та нової техніки і можливим ризиком, спричиненим цим використанням.

ГОСТ 12.1.006-84 “Електромагнітні поля радіочастот” охоплює діапазон частот 60 кГц-300МГц. Він встановлює, що оцінка ЕМП в діапазоні 60 кГц-300МГц проводиться окремо з електричних і магнітних складових поля. Допустимі рівні протягом робочого дня по електричній складовій не повинні перевищувати 50 В/м знижуючись ступенями 5 В/м на міру підвищення частоти. По магнітній складовій встановлені рівні тільки для окремих ділянок діапазону: 5 А/м для частот 60 кГц-1.5 Мгц та 0,3 А для частот 30-50 МГц. Допускається перевищення цих стандартів, але не більше ніж двократне, при скороченні робочого дня не менш як на 50% [21].

Для зменшення впливу електромагнітних полів на персонал, який знаходиться у зоні дії деяких радіоелектронних засобів необхідним є ряд захисних заходів: організаційні, інженерно-технічні та лікувально-профілактичні. У приміщеннях з комп’ютерами має бути забезпечений 3-кратний обмін повітря за годину. Під час розумової праці мозок людини споживає в 9-10 разів більше кисню, а ПК його забирає, спричиняючи кисневе голодування.

Для забезпечення нормованого мікроклімату та рівня іонізації повітря на робочих місцях користувачів рекомендується застосовувати припливно-витяжну вентиляцію чи систему кондиціонування повітря, прилади зволоження та/або установки генерації негативних іонів (аероіонізатори). Знизити деіонізацію повітря в зоні дихання користувача ПК дозволяє також встановлений на монітор захисний заземлений екран.

4.2 Захист населення у надзвичайних ситуаціях від впливу радіації

При виникненні надзвичайної ситуації, зокрема, при аварійному викиданні в атмосферу радіоактивних речовин можливі такі види радіоактивного впливу на населення:

– зовнішнє опромінення при проходженні радіоактивної хмари;

– внутрішнє опромінення при вдиханні радіоактивних аерозолів (інгаляційна небезпека);

– контактне опромінення внаслідок радіоактивного забруднення шкіри і одягу;

– зовнішнє опромінення, зумовлене радіоактивним забрудненням поверхні землі, будівель, споруд та ін.;

– внутрішнє опромінення при використанні забруднених продуктів харчування і води.

Розрахункові дані та результати прямих вимірювань рівня радіації і дози опромінення мають бути основою для вжиття заходів захисту населення від зовнішнього і внутрішнього опромінення, в тому числі й профілактичне застосування стабільного йоду.

Основою розробки заходів захисту населення в умовах радіоактивного забруднення при ядерній аварії є рекомендації Міжнародного агентства з атомної енергії (МАГАТЕ) 1988 р., а також норми радіаційної безпеки України (НРБУ—1997).

Враховуючи рівень радіації, а також прогноз можливих аварійних викидів радіоактивних речовин та метеорологічні дані, приймається рішення про проведення таких термінових і невідкладних заходів захисту в умовах ранньої фази радіаційної аварії:

– укриття населення;

– обмеження перебування населення на відкритій місцевості;

– евакуація у разі загрози здоров'ю;

– проведення йодової профілактики;

– тимчасова заборона вживання продуктів харчування і води із зони радіоактивного забруднення.

Крім цих заходів у період ранньої і пізньої фази проводяться довгострокові заходи:

– тимчасове відселення;

– евакуація — переселення на постійне місце проживання;

– обмеження вживання води і продуктів харчування забруднених радіоактивними речовинами;

– заходи захисту при виробництві продукції тваринництва, рослинництва і лісогосподарської діяльності;

– дезактивація території і будівель;

– інші заходи: гідрологічні, протиповіневі, обмеження лісокористування, полювання, рибної ловлі, перебування у полі при проведенні сільськогосподарських робіт.

Критерієм для прийняття рішення про заходи захисту населення на ранній і середніх фазах після аварії є дози зовнішнього і внутрішнього опромінення (табл. 4.1) з установленими двома рівнями радіаційного впливу — нижнім і верхнім — згідно з рекомендацією МАГАТЕ і НРБУ—1997.

При прогнозованому опроміненні, що не перевершує нижнього рівня, заходи, перелічені в табл. 4.1 не проводяться. Якщо прогнозоване опромінення перевищує нижній рівень, але не досягає верхнього рівня, то проведення вказаних заходів може бути відкладене.

Таблиця 4.1 – Критерії для прийняття рішень на ранній фазі розвитку аварії

Захисні заходи	Дозові критерії (прогнозована доза за перші 10 діб), мЗв			
	Все тіло		Окремі органи (легені, щитовидна залоза, шкіра)	
	Нижній рівень	Верхній рівень	Нижній рівень	Верхній рівень
Укриття, захист органів дихання і шкіри	5	50	50	500
Йодова профілактика:				
дорослі	—	—	50*	500*
діти, вагітні жінки	—	—	50*	250*
Евакуація:				
дорослі діти, вагітні жінки	50 10	500 50	500 200*	5000 500*

Радіаційний захист населення включає в себе:

– організацію безперервного контролю, виявлення та оцінку радіаційної та хімічної обстановки в районах розміщення радіаційно-небезпечних об'єктів;

– завчасне накопичення, підтримання в готовності і використання при необхідності засобів індивідуального захисту, приладів радіаційної розвідки і контролю;

– створення, виробництво та застосування уніфікованих засобів захисту, приладів і комплектів радіаційної розвідки і дозиметричного контролю;

– придбання населенням у встановленому порядку в особисте користування засобів індивідуального захисту та контролю за використанням їх за призначенням;

– своєчасне впровадження і застосування засобів і методів виявлення та оцінки масштабів і наслідків аварій на радіаційно-небезпечних об'єктах;

– створення і використання на радіаційно-небезпечних об'єктах систем (переважно автоматизованих) контролю обстановки і локальних систем оповіщення;

– розробку і застосування, за необхідності, режимів радіаційного захисту населення і функціонування об'єктів економіки та інфраструктури в умовах забрудненості (зараженості) місцевості;

– завчасне пристосування об'єктів комунально-побутового обслуговування і транспортних підприємств для проведення спеціальної обробки одягу, майна і транспорту, проведенням цієї обробки в умовах аварій;

– навчання населення використання засобів індивідуального захисту і правилам поведінки на забрудненій (зараженої) території.

Радіація на сьогодні є чи не найнебезпечнішим фактором впливу не тільки на людину, але й на усі живі організми на планеті. Підтвердженням цього є аварія на Чорнобильській АЕС, наслідки якої відчувають до сьогодні як в Україні, так і за її межами. Дотримання рекомендацій щодо захисту населення від впливу радіації, які проаналізовано вище, дає змогу мінімізувати ризики, пов’язані із загибеллю великої кількості людей, а також зберегти їхнє здоров’я.

ВИСНОВКИ

У кваліфікаційній роботі спроектовано комп’ютерну систему біометричної аутентифікації особи за відбитком пальців, що відповідає вимогам технічного завдання. Досягти мети роботи вдалося шляхом застосування обґрунтованого апаратного і розробленого програмного забезпечення. Основними апаратними пристроями спроектованої системи є:

– сканер відбитків пальців на основі ZFM-20;

– пристрій керування процесом зчитування та аутентифікації особи Raspberry PI Model B;

– компонента виводу інформаційних повідомлень для взаємодії з користувачем LCD 2*16.

Взаємодію між сканером відбитків пальців і Raspberry PI забезпечено шляхом використання USB Serial адаптера.

Функції додавання та управління відбитками пальців на апаратному рівні реалізовано за допомогою відповідних чотирьох кнопок: реєстрації відбитка пальця, видалення та переходу між збереженими зображеннями. Успішність аутентифікації додатково сигналізує світлодіод.

Логіку роботи програмного забезпечення реалізовано засобами мови програмування Python, що підтримується обраним однокристальним міні-комп’ютером.

Результати тестування комп’ютерної системи біометричної аутентифікації особи за відбитком пальця показали її працездатність та можливість застосування на практиці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shah D., Bharadi V. IoT Based Biometrics Implementation on Raspberry Pi/ 7th International Conference on Communication, Computing and Virtualization. 2016. PP. 328-333.

2. Biometrics. URL: https://www.dhs.gov/biometrics (дата звернення 20.03.2021 р.).

3. How to use fingerprint sensor for Arduino and Raspberry Pi. URL: https://www.seeedstudio.com/blog/2019/12/02/try-this-fingerprint-sensor-for-your-arduino-raspberry-pi/ (дата звернення 29.03.2021 р.)

4. Learn all about biometrics and how to build a security system that uses your fingerprints as the key in this tutorial. URL: https://maker.pro/raspberry-pi/projects/raspberry-pi-fingerprint-scanner-using-a-usb-to-serial-ttl-converter (дата звернення 08.04.2021 р.)

5. How to use a Raspberry Pi Fingerprint Sensor for Authentication. URL: https://tutorials-raspberrypi.com/how-to-use-raspberry-pi-fingerprint-sensor-authentication/ (дата звернення 10.04.2021 р.).

6. Луцків А.М. Математичне моделювання і обробка динамічно введеного підпису для задачі аутентифікації особи у інформаційних системах: автореф. дис... канд. техн. наук: 01.05.02. Терноп. держ. техн. ун-т ім. І. Пулюя. Т., 2008. 20 с.

7. Суслина А. Обзор систем биометрической идентификации. URL: https://www.anti-malware.ru/analytics/Market_Analysis/biometric-identification-systems (дата звернення 10.05.2021 р.)

8. Магда Ю. Raspberry Pi. Руководство по настройке и применению. Litres. 2017 р. 161 с.

9. Тиммонс-Браун М. Робототехника на Raspberry Pi для юных конструкторов и программистов Робототехника на Raspberry Pi для юных конструкторов и программистов. БХВ-Петербург. 2020. 208 с.

10. Петин В. Датчики для Arduino и Raspberry Pi в проектах Internet of Things. БХВ-Петербург. 2016. 320 с.

11. Дисплей LCD 2×16 – 1602A. URL: https://3d-cnc.pro/product/displej-lcd-2x16-1602a/?attribute_tsvet-displeya=%D0%A1%D0%B8%D0%BD%D0%B8%D0%B9&gclid=CjwKCAjwg4-EBhBwEiwAzYAlsjWRO80mG-smvO0_h3bNVwrRu11zlkzH5Zvqv6tQdptvdYsjOyFwEhoCaMYQAvD_BwE (дата звернення 17.04.2021 р.)

12. ZFM-20 SeriesFingerprint Identification Module User Manual. URL: https://cdn-shop.adafruit.com/datasheets/ZFM+user+manualV15.pdf (дата звернення 05.05.2021 р.)

13. Shelgaonkar S.K. Creating a smart home environment with IOT driven home appliances. GRIN Verlag. 2016 p. 80 p.

14. IoT-шлюзы: автоматизация производства на уровне Индустрии 4.0 - Control Engineering Russia URL: http://www.controlengrussia.com/internet-veshhej/iot_gateways/ (дата звернення 15.10.2020 р.).

15. Waher P. Learning Internet of Things. Packt Publishing. 2015. 286 p.

16. Тиммонс-Браун М. Робототехника на Raspberry Pi для юных конструкторов и программистов Робототехника на Raspberry Pi для юных конструкторов и программистов. БХВ-Петербург. 2020. 208 с.

17. Васильев В. И. Распознающие системы : справочник. К. : Наукова думка, 1983. 230 с.

18. Шапиро Л. Компьютерное зрение : пер. с англ. БИНОМ. Лаборатория знаний, 2006. 752 с.

19. Python Tutorial. URL: https://www.w3schools.com/python/default.asp (дата звернення 15.04.2021 р.).

20. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Київ. 2018.

21. Бедрій Я. Основи охорони праці користувачів персональних комп’ютерів: навчальний посібник для студентів ВНЗ та інженерів-практиків. Навчальна книга-Богдан. 2014. 144 с.

Додаток А.

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп’ютерно-інформаційних систем і програмної інженерії

Кафедра комп’ютерних систем та мереж

“Затверджую”

Завідувач кафедри КС

_____ Осухівська Г.М.

“___” _____2021 р

КОМП’ЮТЕРНА СИСТЕМА БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ОСОБИ ЗА ВІДБИТКОМ ПАЛЬЦЯ

ТЕХНІЧНЕ ЗАВДАННЯ

на _*11*_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студентка групи СІс-44
_____ к.т.н., доц. Луцків А.М.	_____ Костомаха М.В.
«____» _____ 2021 р.	«____» _____ 2021 р.

Тернопіль 2021

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Комп’ютерна система біометричної аутентифікації особи за відбитком пальця».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.172.00.00

1.2 Виконавець

Студентка групи СІс-44, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Костомаха Марія Володимирівна.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№ 4.7-97 від 10.02.2021 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 10.02.2021 р.

Плановий термін завершення виконання кваліфікаційної роботи – 23.06.2021 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ІСО, ГОСТ, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи.

Попередній захист кваліфікаційної роботи відбувається при готовності роботи на 90% , наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Комп’ютерна система біометричної аутентифікації особи за відбитком пальця є різновидом систем, що призначені для ідентифікації особи за її унікальними характеристиками. У даному випадку в якості ідентифікатора виступає зображення відбитка пальця.

За ідентифікацію людини на основі її біометричних особливостей у комп’ютерних системах відповідають алгоритми машинного навчання. В основному вони побудовані на моделях нейронних мереж розпізнавання образів за візуальними зображеннями, в тому числі, і відбитків пальців.

Системи біометричної аутентифікації на основі розпізнавання відбитків пальців проектують і впроваджують для підвищення ефективності комп’ютерної та інформаційної безпеки, у сфері торгівлі, зокрема при аутентифікації користувачів при проведенні грошових транзакцій та операцій. У побуті, комп’ютерні системи на основі розпізнавання відбитків пальців, призначені для авторизації користувача комп’ютерів, смартфонів.

Важливим призначенням системи біометричної аутентифікації особи за відбитком пальця є сфера авторизованого входу до приміщень з обмеженим доступом.

Комп’ютерна система біометричної аутентифікації особи за відбитком пальця, яка проектується у даній роботі, вимагає впровадження апаратно-програмного комплексу для зчитування зображення відбитка пальця, його аналізу засобами машинного навчання та порівняння результатів з наявними записами у базі даних. Основне призначення системи полягає у забезпеченні точності та підвищенні ефективності аутентифікації осіб на основі її біометричних та фізіологічних особливостей.

2.2 Мета створення системи

Метою створення комп’ютерної системи біометричної аутентифікації особи за відбитком пальця є автоматизація, забезпечення точності і продуктивності авторизації людини з врахуванням її біологічних особливостей.

Для того, щоб досягнути цієї мети, необхідно:

– проаналізувати особливості відбитків пальців людини;

– дослідити переваги і недоліки технологій розпізнавання зображень;

– спроектувати архітектуру комп’ютерної системи біометричної аутентифікації особи;

– обґрунтувати вибір апаратних пристроїв системи;

– обґрунтувати та реалізувати інтелектуальну складову системи біометричної аутентифікації;

– реалізувати системне і прикладне програмне забезпечення системи;

– перевірити одержані результати розпізнавання відбитків пальців особи.

2.3 Характеристика об'єкту

2.3.1 Основні задачі та функції об’єкту

Основні задачі і функції системи біометричної аутентифікації полягають у забезпеченні процесів зчитування відбитків пальців людини, їх аналізу та прийняття

рішення щодо надання доступу до ресурсів чи до приміщення. Фактично, дана система є частиною комплексу, що формує комп'ютерну та інформаційну безпеки підприємства.

При проведенні аутентифікації особи на основі аналізу її біометричних даних повинна бути забезпечена висока точність та надійність результатів розпізнавання відбитків пальців, а також швидкість опрацювання та одержання результатів щодо доступу до ресурсів.

Автоматизація процесу аутентифікації на основі біометричних даних передбачає застосування і налаштування апаратного забезпечення, зокрема:

– зчитувача відбитків пальців;
– мікроконтролера для управління процесом аутентифікації;
– дисплея для відображення сервісних повідомлень;
– кнопок управління записом та видаленням зображень відбитків;
– інших додаткових апаратних пристроїв.

В якості додаткових апаратних пристроїв можуть використовуватись:

– зумер;
– електромеханічний замок;
– кнопки ручного блокування та розблокування;
– інші пристрої аутентифікації користувача.

Зображення відбитків пальців може зберігатись на SD-картці, підключеній до плати прототипування, або інтегрованій у сканер відбитків пальців. Альтернативою є зберігання зображень відбитків пальців на зовнішньому сервері баз даних.

Програмне забезпечення комп'ютерної системи аутентифікації особи на основі відбитків пальців повинно забезпечувати ініціалізацію та моніторинг параметрів апаратних пристроїв, а також виконувати безпосередньо порівняння зчитаної інформації і порівняння з існуючими зображеннями.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Вимоги, які в цілому висуваються до системи біометричної аутентифікації полягають у здатності адекватно зчитувати зображення відбитку пальців, аналізувати їх, забезпечувати визначену швидкість та реакцію на результат ідентифікації особи.

Комп’ютерну систему можна реалізувати за допомогою як Raspberry PI, так і Arduino й інших плат макетування. Основна функція мікроконтролера – керування процесом ідентифікації відбитків пальців, які зчитуються відповідним сканером.

Для забезпечення зворотного зв’язку системи з користувачем потрібно використати дисплей для виводу повідомлень про успішність чи не успішність авторизації.

В загальному випадку, більш детально вимоги до комп’ютерної системи аутентифікації можна представити як:

– можливість сканування відбитків пальців;

– забезпечення продуктивності процесу аутентифікації до 1с;

– здатність запису відбитків пальців;

– можливість оновлення та видалення зображень відбитків пальців;

– організація зв’язку з локальною комп’ютерною мережею та мережею Інтернет;

– наявність авторизованих процедур для визначених груп користувачів при налаштуванні роботи комп’ютерної системи;

– надійність функціонування апаратних пристроїв комп’ютерної системи;

– можливість віддаленого оновлення програмного забезпечення сканера відбитків пальців;

– можливість підключення додаткових пристроїв біометричної ідентифікації людини.

3.1.1 Вимоги до структури та функціонування системи

Базова апаратна структура комп’ютерної система біометричної аутентифікації особи на основі відбитку пальця включає:

– однокристальний міні-комп’ютер Raspberry PI;
– Fingerprint Module ZFM-20;
– дисплей LCD 16x2;
– Bread Board або PCB;
– адаптер USB-Serial;

Комп’ютерна система біометричної аутентифікації повинна:

– показувати сталість і надійність результатів ідентифікації особи за відбитком пальця;
– здійснювати перевірку з наявними зображеннями заданої біометрії;
– виводити сервісні повідомлення про результат розпізнавання;
– надавати можливість обміну інформацією з ресурсами локальної комп’ютерної мережі та Інтернет.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Зв’язок між сканером відбитків пальців та Raspberry PI забезпечується комунікацією за допомогою USB Serial адаптера, а взаємодія з LCD дисплеєм – на основі шини I2C. За допомогою інтегрованого у Raspberry PI модуля WIFI повинна виконуватись взаємодія з маршрутизатором локальної комп’ютерної мережі, який має доступ до мережі Інтернет.

3.1.3 Вимоги по діагностуванню системи

Діагностика компонентів комп’ютерної системи біометричної аутентифікації особи на основі відбитків пальців повинна проводиться у випадках збоїв у їх роботі та у відповідності до розкладу регламентних робіт. Усунення неполадок працездатності системи повинні усуватись у найкоротші терміни.

3.1.4 Перспективи розвитку, модернізація системи

Шляхами розвитку комп’ютерної системи біометричної аутентифікації особи за відбитком пальців є інтеграція додаткових пристроїв аналізу біометричних показників. Для цього можуть бути використані відеокамери та програмне забезпечення для виконання задач розпізнавання обличчя. Окрім цього, в якості біометричних даних можна використовувати голос і відповідний комплекс для його аналізу, а також сканування сітківки ока.

При інтеграції додаткових кінцевих пристроїв загальна архітектура комп’ютерної системи повинна бути незмінною, але підтримувати здатність до масштабування шляхом підключення апаратних пристроїв та імплементації програмного забезпечення. Модернізацію комп’ютерної системи аутентифікації особи можна виконувати за необхідності додавання інших керуючих пристроїв, наприклад, електромеханічних замків або інтеграції у більш складний комплекс комп’ютерної безпеки.

3.1.5 Вимоги до надійності системи

До вимог надійності комп’ютерної системи аутентифікації особи на основі відбитку пальця належать:

– точність результатів зчитування відбитків пальців на рівні 98%;

– час безперебійної експлуатації системи і її компонентів визначається виробничими графіками підприємства;

– здатність до відновлення у випадках виникнення не штатних ситуацій або відмов;

– продуктивність системи розпізнавання відбитків пальців і прийняття рішення повинно не перевищувати 2 с;

– забезпечення чіткості і зрозумілості сервісних повідомлень;

– наявність засобів сповіщення про збої у роботі компонентів системи;

– можливість аварійного відключення системи аутентифікації особи.

3.1.6 Вимоги до функцій та задач, які виконує система

Вимогами до функцій та вимог, які висуваються до комп’ютерної системи біометричної аутентифікації особи на основі відбитку пальців є:

– можливість одержання адекватного відбитку пальця особи;
– здатність формування бази даних відбитків пальців осіб;
– можливість управління процесом біометричної аутентифікації;
– здатність запису, оновлення та видалення зображень відбитків з бази даних;
– можливість порівняння зчитаного відбитку з уже наявними у базі даних;
– забезпечення визначеної продуктивності роботи системи;
– наявність процедур авторизованого доступу для внесення змін у комп’ютерну систему;
– забезпечення доступу до ресурсів комп’ютерної мережі та Інтернет;
– вивід сервісних повідомлень на LCD екран;
– наявність засобів апаратного налаштування процесу запису та видалення відбитків пальців;
– можливість оновлення системного програмного забезпечення компонентів комп’ютерної системи.

3.1.7 Вимоги до апаратного забезпечення

Вимоги до апаратних пристроїв комп’ютерної системи біометричної аутентифікації особи на основі відбитків пальців повинні відображати базові технічні особливості таких компонентів як:

– однокристальний міні-комп’ютер на базі Raspberry PI 2 або Raspberry PI 3;
– сканер відбитку пальців ZFM-20, який сумісний з Raspberry PI;
– LCD-дисплей 16*2 на базі контролера HD44780;
– USB-Serial адаптер будь-якого виробника;

При проектуванні комп’ютерної системи біометричної аутентифікації необхідне застосування персонального комп’ютера, який відповідає наступній конфігурації:

– процесор з тактовою частотою процесора на рівні 2,4 ГГц;
– об’єм оперативної пам’яті – 4 ГБ;
– об’єм жорсткого диску - 500 ГБ.

За необхідності зберігання великої кількості зображень відбитків пальців необхідно використовувати сервер бази даних, апаратні характеристики якого відповідають наступним вимогам:

– процесор з тактовою частотою на рівні не менше 2,2 ГГц та кількістю потоків не менше 6;
– об’єм оперативної пам’яті – 16 ГБ;
– об’єм жорсткого диску – 2ТБ.

3.1.8 Вимоги до програмного забезпечення

Вимогами до програмного забезпечення при проектуванні програмного забезпечення комп’ютерної системи біометричної аутентифікації на основі відбитку пальця є використання середовища розробки з підтримкою мови програмування Python. Особливих вимог до програмного забезпечення комп’ютера і сервера не висувається, однак повинна бути підтримка можливості розгортання та функціонування бази даних для зберігання відбитків пальців. При цьому можна використовувати операційні системи як Windows, так і Unix – подібні.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;
– графічного матеріалу:

1. Структура відбитку пальця людини.
2. Структурна схема системи біометричної аутентифікації особи.
3. Архітектура комп’ютерної системи біометричної аутентифікації особи.
4. Компонентна схема комп’ютерної системи.

5. Схема з’єднань компонентів комп’ютерної системи.
6. Зовнішній вигляд спроектованої системи.

*Примітка: У комплект документації можуть вноситися міни та доповнення в процесі розробки.

5 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1	Розробка та аналіз вимог технічного завдання	10.02-21.02.2021
2	Аналіз методів аутентифікації користувачів	21.02-07.03.2021
3	Проектування архітектури комп’ютерної системи	08.03-20.03.2021
4	Обґрунтування вибору апаратного забезпечення	20.03-26.03.2021
5	Реалізація програмного забезпечення комп’ютерної системи	27.03-10.04.2021
6	Розробка інструкцій з налаштування параметрів комп’ютерної системи біометричної аутентифікації	04.05-20.05.2021
7	Безпека життєдіяльності, основи охорони праці	20.05-27.05.2021
8	Оформлення кваліфікаційної роботи	27.05-10.06.2021
9	Попередній захист кваліфікаційної роботи	10.06-20.06.2021
10	Захист кваліфікаційної роботи	21.06-27.06.2021

6 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.

Додаток Б.

Програмне забезпечення комп'ютерної системи біометричної аутентифікації особи за відбитком пальця

```
import time
from pyfingerprint.pyfingerprint import PyFingerprint
import RPi.GPIO as gpio

RS =18
EN =23
D4 =24
D5 =25
D6 =8
D7 =7

enrol=5
delet=6
inc=13
dec=19
led=26

HIGH=1
LOW=0

gpio.setwarnings(False)
gpio.setmode(gpio.BCM)
gpio.setup(RS, gpio.OUT)
gpio.setup(EN, gpio.OUT)
gpio.setup(D4, gpio.OUT)
gpio.setup(D5, gpio.OUT)
gpio.setup(D6, gpio.OUT)
gpio.setup(D7, gpio.OUT)

gpio.setup(enrol, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(delet, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(inc, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(dec, gpio.IN, pull_up_down=gpio.PUD_UP)
gpio.setup(led, gpio.OUT)

try:
    f = PyFingerprint('/dev/ttyUSB0', 57600, 0xFFFFFFFF, 0x00000000)

    if ( f.verifyPassword() == False ):
        raise ValueError('The given fingerprint sensor password is
wrong!')
```

```
except Exception as e:
    print('Exception message: ' + str(e))
    exit(1)

def begin():
  lcdcmd(0x33)
  lcdcmd(0x32)
  lcdcmd(0x06)
  lcdcmd(0x0C)
  lcdcmd(0x28)
  lcdcmd(0x01)
  time.sleep(0.0005)

def lcdcmd(ch):
  gpio.output(RS, 0)
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
  gpio.output(D7, 0)
  if ch&0x10==0x10:
    gpio.output(D4, 1)
  if ch&0x20==0x20:
    gpio.output(D5, 1)
  if ch&0x40==0x40:
    gpio.output(D6, 1)
  if ch&0x80==0x80:
    gpio.output(D7, 1)
  gpio.output(EN, 1)
  time.sleep(0.005)
  gpio.output(EN, 0)
  # Low bits
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
  gpio.output(D7, 0)
  if ch&0x01==0x01:
    gpio.output(D4, 1)
  if ch&0x02==0x02:
    gpio.output(D5, 1)
  if ch&0x04==0x04:
    gpio.output(D6, 1)
  if ch&0x08==0x08:
    gpio.output(D7, 1)
  gpio.output(EN, 1)
  time.sleep(0.005)
  gpio.output(EN, 0)

def lcdwrite(ch):
  gpio.output(RS, 1)
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
```

```
  gpio.output(D7, 0)
  if ch&0x10==0x10:
    gpio.output(D4, 1)
  if ch&0x20==0x20:
    gpio.output(D5, 1)
  if ch&0x40==0x40:
    gpio.output(D6, 1)
  if ch&0x80==0x80:
    gpio.output(D7, 1)
  gpio.output(EN, 1)
  time.sleep(0.005)
  gpio.output(EN, 0)
  # Low bits
  gpio.output(D4, 0)
  gpio.output(D5, 0)
  gpio.output(D6, 0)
  gpio.output(D7, 0)
  if ch&0x01==0x01:
    gpio.output(D4, 1)
  if ch&0x02==0x02:
    gpio.output(D5, 1)
  if ch&0x04==0x04:
    gpio.output(D6, 1)
  if ch&0x08==0x08:
    gpio.output(D7, 1)
  gpio.output(EN, 1)
  time.sleep(0.005)
  gpio.output(EN, 0)
def lcdclear():
  lcdcmd(0x01)

def lcdprint(Str):
  l=0;
  l=len(Str)
  for i in range(l):
    lcdwrite(ord(Str[i]))

def setCursor(x,y):
    if y == 0:
        n=128+x
    elif y == 1:
        n=192+x
    lcdcmd(n)

def enrollFinger():
    lcdcmd(1)
    lcdprint("Enrolling Finger")
    time.sleep(2)
    print('Waiting for finger...')
    lcdcmd(1)
    lcdprint("Place Finger")
    while ( f.readImage() == False ):
```

```
        pass
    f.convertImage(0x01)
    result = f.searchTemplate()
    positionNumber = result[0]
    if ( positionNumber >= 0 ):
        print('Template already exists at position #' +
str(positionNumber))
        lcdcmd(1)
        lcdprint("Finger ALready")
        lcdcmd(192)
        lcdprint("   Exists     ")
        time.sleep(2)
        return
    print('Remove finger...')
    lcdcmd(1)
    lcdprint("Remove Finger")
    time.sleep(2)
    print('Waiting for same finger again...')
    lcdcmd(1)
    lcdprint("Place Finger")
    lcdcmd(192)
    lcdprint("   Again    ")
    while ( f.readImage() == False ):
        pass
    f.convertImage(0x02)
    if ( f.compareCharacteristics() == 0 ):
        print "Fingers do not match"
        lcdcmd(1)
        lcdprint("Finger Did not")
        lcdcmd(192)
        lcdprint("   Mactched   ")
        time.sleep(2)
        return
    f.createTemplate()
    positionNumber = f.storeTemplate()
    print('Finger enrolled successfully!')
    lcdcmd(1)
    lcdprint("Stored at Pos:")
    lcdprint(str(positionNumber))
    lcdcmd(192)
    lcdprint("successfully")
    print('New template position #' + str(positionNumber))
    time.sleep(2)

def searchFinger():
    try:
        print('Waiting for finger...')
        while( f.readImage() == False ):
            #pass
            time.sleep(.5)
            return
        f.convertImage(0x01)
```

```
        result = f.searchTemplate()
        positionNumber = result[0]
        accuracyScore = result[1]
        if positionNumber == -1 :
            print('No match found!')
            lcdcmd(1)
            lcdprint("No Match Found")
            time.sleep(2)
            return
        else:
            print('Found template at position #' +
str(positionNumber))
            lcdcmd(1)
            lcdprint("Found at Pos:")
            lcdprint(str(positionNumber))
            time.sleep(2)

    except Exception as e:
        print('Operation failed!')
        print('Exception message: ' + str(e))
        exit(1)

def deleteFinger():
    positionNumber = 0
    count=0
    lcdcmd(1)
    lcdprint("Delete Finger")
    lcdcmd(192)
    lcdprint("Position: ")
    lcdcmd(0xca)
    lcdprint(str(count))
    while gpio.input(enrol) == True:   # here enrol key means ok
        if gpio.input(inc) == False:
            count=count+1
            if count>1000:
                count=1000
            lcdcmd(0xca)
            lcdprint(str(count))
            time.sleep(0.2)
        elif gpio.input(dec) == False:
            count=count-1
            if count<0:
                count=0
            lcdcmd(0xca)
            lcdprint(str(count))
            time.sleep(0.2)
    positionNumber=count
    if f.deleteTemplate(positionNumber) == True :
        print('Template deleted!')
        lcdcmd(1)
        lcdprint("Finger Deleted");
        time.sleep(2)
```

```
begin()
lcdcmd(0x01)
lcdprint("FingerPrint ")
lcdcmd(0xc0)
lcdprint("Interfacing ")
time.sleep(3)
lcdcmd(0x01)
lcdprint("Circuit Digest")
lcdcmd(0xc0)
lcdprint("Welcomes You  ")
time.sleep(3)
flag=0
lcdclear()

while 1:
    gpio.output(led, HIGH)
    lcdcmd(1)
    lcdprint("Place Finger")
    if gpio.input(enrol) == 0:
        gpio.output(led, LOW)
        enrollFinger()
    elif gpio.input(delet) == 0:
        gpio.output(led, LOW)
        while gpio.input(delet) == 0:
            time.sleep(0.1)
        deleteFinger()
    else:
        searchFinger()
```