НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Радіотехнічний факультет

Кафедра прикладної радіоелектроніки

До захисту допущено:

В.о. зав.кафедри

_____ Михайло СТЕПАНОВ

«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньою програмою «Радіозв`язок і оброблення сигналів»

за спеціальністю172 «Телекомунікації та радіотехніка»

на тему: Біометрична система контролю доступу

Виконав:
студент IV курсу, групи РА-81
Кириленко О.А.

Керівник: доцент, к.т.н., доцент кафедри ПРЕ

Сушко Ірина Олександрівна
Посада, науковий ступінь, вчене звання
Прізвище, ім'я, по батькові

Рецензент доцент, к.т.н., доцент кафедри РІ

Гусєва Олена Володимирівна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент

Київ – 2022 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського »

Радіотехнічний факультет

Кафедра прикладної радіоелектроніки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність 172 “Телекомунікації та радіотехніка”

Освітньо-професійна програма «Радіозв’язок та обробка сигналів»

ЗАТВЕРДЖУЮ

В.о.зав. кафедри

_____ Михайло СТЕПАНОВ

«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу

Кириленка Олександра Анатолійовича

1. Тема роботи: «Біометрична система контролю доступу»

Керівник роботи доцент кафедри прикладної радіоелектроніки Сушко Ірина Олександрівна, затверджена наказом по університету №822-с від01.06.2022р.

2. Термін подання студентом проєкту 13 червня 2022року

3. Вихідні дані до роботи: біометрична система контролю доступу.

4. Зміст пояснювальної записки: вступ, аналіз ринку, огляд типів біометричних сканерів, загальні відомості про біометрію за відбитками пальців, макетування системи біометричного доступу з використанням інтерфейсу обміну даними Weagand, висновки.

5. Графічний матеріал: структурна схема

6. Дата видачі завдання 01 травня 2022 року

7. Календарний план

6.

№	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Актуальність тематики	1.05.22 – 13.05.22	
2	Огляд існуючих рішень	14.05.22 – 18.05.22	
3	Загальні відомості про біометрію відбитків пальців	19.05.22 – 29.05.22	
4	Вибір та обгрунтування елементів системи	30.05.22 – 6.06.22	
5	Розробка системи	7.06.22 – 10.06.22	
6	Розробка алгоритму управління	11.06.22– 12.06.22	

ВІДОМІСТЬ ДИПЛОМНОЇ РОБОТИ

№ з/п	Формат	Найменування	Кількість листів	Примітка
1	А4	Завдання на дипломну роботу	2	
2	А4	Пояснювальна записка	47	
3	А3	Схема структурна	1	
4	А4	Технічне завдання	4	

АНОТАЦІЯ

В дипломному проєкті на тему «Біометрична система контролю доступу» кінцевою метою є опрацювання підвищення ефективності контролю до об’єктів з обмеженим доступом з можливістю використанні кінцевих пристроїв, що затверджені в технічній документації на об’єкт, та подальшим використанням в роботі ситем новітніх контролерів віддаленого управління. В роботі проведено аналіз існуючих методів та засобів контролю, розглянуто макетування набору стандартних кінцевих виконавчих пристроїв об’єкту та їх управління через контролер Arduino, розроблено та описано алгоритм формування команд обміну даними для інтерфейсу Wiegand26 і подальшу роботу підпрограми із стандартним програмним забезпеченням Arduino та, як результат, можливість обміну даними з контролерами віддаленого управління SG314GI-WR.

Ключові слова: СКУД (система контролю віддаленого доступу), Wiegand, аутентифікація.

ANNOTATION

In this diploma project the ultimate goal is to increase the effectiveness of objects control with limited access with the possibility of using end devices approved in the technical documentation for the object, and further use of the latest remote controllers. The existing methods and means of control are analyzes, the layout of a set of standard terminal actuators and their control through the Arduino controller are considered, the algorithm for generating communication commands for the Wiegand26 interface is developed and further work of the subroutine with standard Arduino software result is described, the ability to exchange data with remote controllers SG314GI-WR is presented.

Keywords: ACS, Wiegand, authentication.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проєкту

на тему: Біометрична система контролю доступу

Київ – 2022 року

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

СКВД — Система контролю віддаленого доступу

FRR — False Rejection Rate

FAR — False Acceptance Rate

ТЗ — технічне завдання

ВСТУП

Тенденції світового ринку пришвидшили розвиток галузей сучасних технологій, однією з яких є біометрія.

Біометрія – сфера науки та сукупність технологій з розпізнавання людини за її біометричними параметрами. Свій початок біометрія бере ще з часів Стародавнього Китаю, коли завдяки відбитку пальця на глині люди проводили торгові операції та могли визначати причетність до злочину. Вже на початку 20 століття у США з'явився спеціальний відділ по зберіганню та аналізу відбитків пальців підозрюваних у злочинах. Але до другої половини особливого розвитку в біометрії не спостерігалося.

Завдяки впровадженню напівпровідників та подальшого розвитку напівпровідникових технологій відбувся ривок у виробництві комп'ютероної техніки та електроніки, що надало можливість розвитку в тому числі і біометричних технологій.

Створення автоматичних систем, які б змогли знімати біометричні параметри людини, перетворювати їх у цифровий вигляд та виконувати подальший аналіз, стало можливим і суттєво підвищило попит на біометрику.

Сьогодні важливий період для розвитку біометрії. Сенсори швидко дешевшають, комп'ютери досягли високого рівня продуктивності, розвиваються нанотехнології, а технологічна інфраструктура стала невід'ємною частиною нашого життя. Біометричні технології виконують не тільки функції заміщення паролів, а й функції повноцінного компоненту систем безпеки, інтеграція яких потребує серйозного підходу [1]. Застосування біометрії на всіх рівнях побуту людини є питанням часу

1 АКТУАЛЬНІСТЬ ТЕМАТИКИ

Надійна авторизація та аутентифікація є необхідним атрибутом повсякденного життя. Сьогодні людство використовує підтвердження особи для різноманітних цілей: розблакування телефону, проведення банківських та інших розрахункових операцій, отримання доступу до приміщень, т.і. Зазвичай користувач не хоче щоб зловмисник отримав доступ до персональних даних, оскільки їх викрадення несе фінансові та моральні збитки. Одночасно з цим процедура аутентифікації повинна мати високу швидкодію, достатню точність та максимальну мобільність. Користувач не повинен відчувати дискомфорт під час проходження процедури.

Біометрична ідентифікація добре зарекомендувала себе, оскільки саме цей тип розпізнавання має високу ступінь надійності, де використовується унікальність фізіологічних особливостей людини та виключення їх повторення. Наприклад, навіть близнюки мають різний папілярний візерунок пальців чи геометрію зіниці. Використання особливостей нашого тіла у якості ідентифікатора доступу до різного роду ресурсів є мобільним та практичним процесом, який потребує мінімум часу та сил користувача.

Основними для використання в системах розпізнавання та захисту є шість біометричних параметрів, які, в свою чергу, розділяються на фізіологічні та параметри поведінки [1].

Фізіологічні біометричні параметри:

— структура обличчя

— відбиток пальців

— геометрія руки

— райдужна оболонка ока,

Параметри поведінки:

— підпис

— голос.

Технології з розпізнавання деяких зазначених параметрів вже майже досягли досконалості та активно застосовуються у повсякденному житті, а деякі знаходяться в розробці.

Приклад: сканер розпізнавання обличчя та сканер відбитка пальців в смартфонах, які кожен з нас використовує багаторазово на день.

Слід згадати і про біометричні параметри, які вивчаються та мають велику перспективу застосування:

— ДНК;

— форма вуха;

— запах;

— сітківка ока;

— шкірне відображення;

— термограма;

— хода.

Розвиток електроніки та алгоритмів розпізнавання поки що не дійшов до такого рівня, щоб згадані біометричні параметри були впроваджені в сьогоденне життя. Варто зазначити, що навіть звичні сканери відбитка ще не надають гарантії безпомилкової роботи, але є відносно надійними. Розвиток науки, особливо цифрових технологій та статистики, впровадження рішень в програмне забезпечення, суттєво підвищать надійність роботи систем.

Параметрів, що використовуються, багато, але усі вони мають як переваги, так і недоліки.

На стадії розробки систем доступу тип ідентифікації вибирається згідно вимог, що задаються у технічному завданні на розробку систему.

Зазначаємо, що важливим є вимоги не тільки до вибору типу ідентифікації, а також вимоги до інших організаційних заходів, якими в системах є відповідність вимогам, що на багатьох об’єктах телекомунікацій оформлюється як комплексна система захисту інформації. Складовою такої системи є вимоги доступу на об’єкт телекомунікацій та технічного захисту

інформації. Також зважаємо, що проектування, погодження, побудова та подальша експлуатація об’єктів здійснюються виключно до положень та вимог затвердженої документації. Тому будь-яка заміна активних елементів (датчиків, сенсорів, серверів, т.і.) потребують окремих погоджень, затверджень з подальшим внесення змін в дозвільну документацію.

Важливим є можливість використання нового периферійного обладнання та його підключення до вже діючого без порушення затверджених вимог.

Сучасна модернізація існуючих об’єктів потребує забезпечення можливості роботи існуючих елементів контролю доступу з пристроями, які працюють з протоколами Weagand, радіо-доступом та хмарними технологіями з відповідним рівнем захисту інформації. Крім того, обмін інформацією повинен забезпечити швидку передачу достатньо великого масиву даних для здійснення ідентифікації з подальшим прийняттям рішення щодо прав доступу.

Основними елементами таких систем є датчик, пристрій аналізу з виконанням функцій порту обміну інформацією, сигнальні датчики, пристрій радіо-доступу з функціями доступу до хмарних технологій.

Поетапний аналіз побудови такої системи з обґрунтуваннями наведено в наступних розділах.

2 ТИПИ БІОМЕТРИЧНИХ СКАНЕРІВ

2.1 Оптичні

Оптичні сканери відбитків пальців є одними з найпоширеніших наряду з ємнісними. Принцип роботи цих пристроїв побудований на оптичних методах отримання зображення з подальшим аналізом.

Оптичні сканери умовно поділяються на 3 типи, принцип роботи яких однаковий, але присутні суттєві відмінності в методиці реалізації.

2.1.1 FTIR

В перекладі з англійської Frustrated Total Internal Reflection, FTIR – «порушене повне внутрішнє відбиття». Ефект полягає у тому, що при падінні світла на межу поділу двох середовищ (пагорбів і западин папілярного візерунка пальця) частина енергії відбивається від границі (пагорбу), інша частина проникає через межу у інше середовище (западини). Значення відбитої енергії залежить від кута падіння світлового променю. Починаючи з певного значення цього кута, уся світлова енергія відбивається від межі поділу [2].

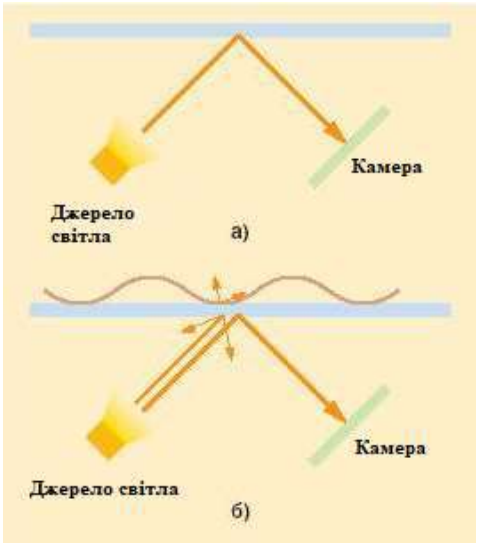


Рисунок. 2.1 — Принцип роботи FTIR сканеру

Таким чином, від межі відіб’ються лише пучки світла, які потрапили в зони повного внутрішнього відбиття, до яких не був прикладений папілярний візерунок пальця.

Недоліком цього виду сканерів є невисокий рівень захищеності та чутливість до забруднень на екрані.

Перевага – невисока вартість.

2.1.2 Сканери з використанням оптичного волокна

Ці сканери складаються з оптоволоконної матриці, яка являє собою велику кількість мікроскопічних фотодатчиків, щільно розташованих поряд один з одним та з'єднаних на вході з хвилеводами. Чутливість кожного елемента дозволяє фіксувати залишкове світло, яке проходить через палець, у точці дотику його візерунка до поверхні сканеру [3]. Так інформація зчитується з кожного фотодатчика та за допомогою певних алгоритмів відбувається генерація зображення відбитку (рис. 2.2)

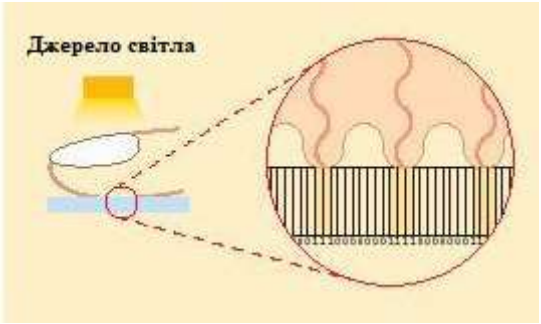


Рисунок 2.2 — Ілюстрація сканеру на базі оптичного волокна

Переваги: відносно висока надійність зчитування та роздільна здатність.

Недоліки: складність конструкції, висока ціна.

2.1.3 Безконтактні оптичні сканери

Сканери цього типу не потребують безпосереднього дотику до контактної поверхні пристрою. Користувач розташовує палець напроти спеціального отвору Всередині отвору знаходяться джерела світла, які рівномірно підсвічують палець з різних сторін, та спеціальна лінза всередині. Отримане зображення проектується на світлочутливу матрицю, виконану за КМОП технологією, та перетворюється на зображення (рис. 2.3).

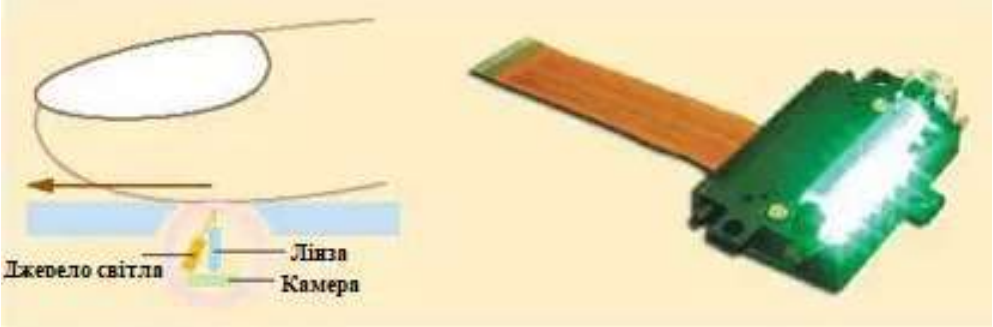


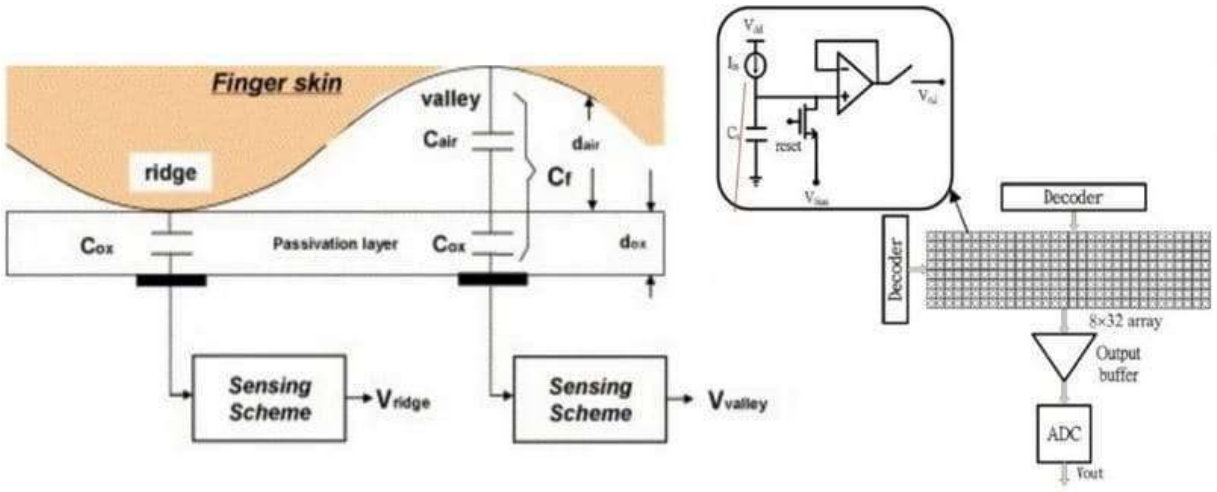
Рисунок 2.3 — Безконтактний оптичний сканер

Переваги: ефективний у випадку інтенсивного використання великою кількістю людей, більш гігієнічний.

Недоліком є висока вартість.

2.2 Ємнісні сканери

Ємнісні сканери є досить популярними, часто використовуються у смартфонах. Принципом роботи - розпізнавання нерівностей пальця з використанням індивідуальної провідності людини та створення електростатичного поля та цифрового зображення на основі цього поля.



а б

Рисунок 2.4 — Схема ємнісного сканеру відбитків пальців (а), матриця ємностей (б)

Ємнісний сканер використовує малі за розміром конденсатори, що утворюють своєрідний масив, (рис. 2.4). При піднесенні пальця до екрану, ті ділянки провідної пластини, що торкаються виступів папілярного візерунку, змінюють свою ємність, а ті що залишаються недоторканими, тобто зона впадин, залишають заряд на конденсаторі незмінним. Схема інтегратора операційного підсилювача фіксує зміни. Отримана матриця ємностей кодується у цифровий вигляд завдяки АЦП та аналізуються системою [4].

Переваги: складні в підробці, мають більш високу точність у порівнянні з оптичними.

Недолік: висока вартість виробництва.

2.3 Ультразвукові сканери

Цей тип опромінює поверхню пальця ультразвуковими хвилями та вимірює відстань між джерелом випромінювання та западинами і виступами на поверхні пальця по відбитій від них звуковій хвилі. Якість отриманого зображення у багато разів вища за інші типи сканерів (рис. 2.5).

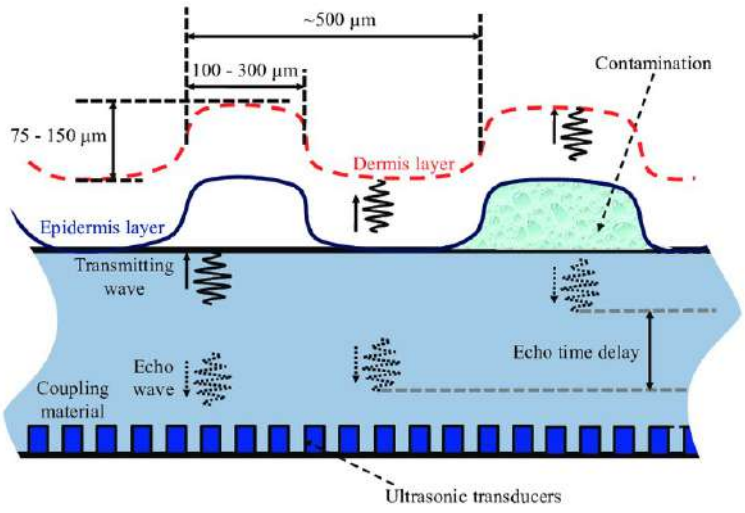


Рисунок 2.5 — Ілюстрація роботи ультразвукового сканеру відбитків пальців

Переваги: неможливо підробити, дозволяє вимірювати пульс.

Недоліки: висока ціна, низька швидкість роботи.

2.4 Термосканери

Принцип роботи подібний до ємнісного. Контактна поверхня пристрою складається з набору мікроскопічних піроелектричних елементів. В момент прикладання пальця до сканеру в місцях контакту з папілярним візерунком (горбки), палець передає на поверхню піроелектричних елементів своє тепло, а у місцях западин, де присутній повітряний прошарок, тепла передається набагато менше. Піроелектричні датчики фіксують зміни тепла та переводять їх у електричні імпульси з подальшою побудовою теплової карти папілярного візерунку (рис. 2.6).

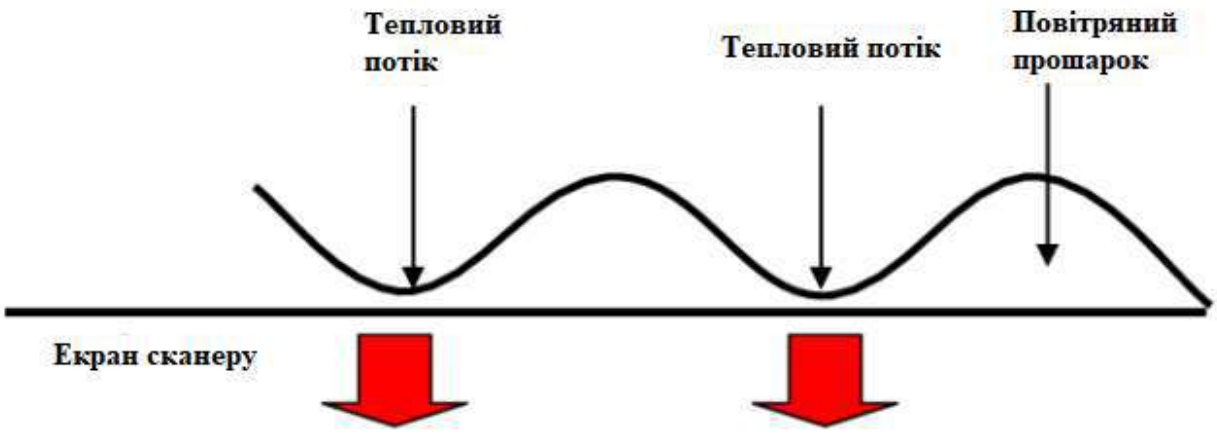


Рисунок 2.6 — Ілюстрація принципу роботу термічного сканеру

Переваги: ефективний захист від підробок, можливість роботи при більш широкому діапазоні температур навколишнього середовища, висока стійкість до електро-статистичних розрядів

Недоліки: через невелику різницю температур палець та датчик за долі секунд приходять до теплової рівноваги. Теплове зображення зникає, можливі помилки зчитування, вірогідність повторного зчитування.

2.5 Аутентифікація з використанням ока людини

Такий метод має два види: ідентифікація по райдужній оболонці та по зіниці ока.

2.5.1 Ідентифікація по райдужній оболонці

Райдужна оболонка являє собою м’язову пластину біля передньої частини ока та розташована між рогівкою та отвором (зіницею). Виконує функцію своєрідної природньої діафрагми, що регулює надходження світла в око [5].

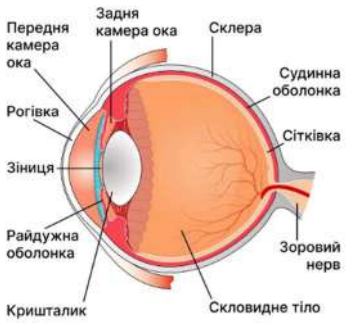


Рисунок 2.6 — Око людини

Структурно райдужна оболонка є трабекулярною мережею. Це сіткове утворення та складається з багатьох рельєфних унікальних рис, таких як кільця, гребінчасті стяжки, борозни, кільця, зморшки, ластовиння, судини. Сукупність цих фрагментів трабекулярної мережі утворює унікальний візерунок райдужної оболонки ока кожної людини (рис. 2.7).

Рисунок 2.7 — Райдужна оболонка

Незважаючи на те, що колір райдужної оболонки ока може змінюватися ще у ранньому дитинстві, візерунок трабекулярної мережі залишається незмінним на протязі всього життя.

Важливо, що зміна структури візерунку можлива, але із застосуванням хірургічного втручання.

Три типи ідентифікації з використанням радужної оболонки ока:

- отримання зображення: за допомогою монохромної, чутливої до інфрачервоного випромінювання CCD камери для максимально якісного знімку робиться декілька фотографій радужної оболонки [5];

- етап сегментації: виділяється зображення райдужної оболонки, визначаються її верхня та нижня границі; для запобігання помилки прибираються зайві деталі;

- фінальний етап: отримується шаблон райдужної оболонки, закодований у цифровий вигляд.

В ході аутентифікації отриманий шаблон порівнюється з вже занесеним у базу шаблоном. Мірою, за допомогою якої визначається ступінь відмінності двох райдужних оболонок, є відстань Хеммінгу [6].

2.5.2 Метод аутентифікації за сітківкою ока

Сітківка – внутрішня оболонка ока, що є периферичним відділом зорового аналізатора та містить фоторецепторні клітини, які забезпечують сприйняття електромагнітного випромінювання видимої частини спектра та його перетворення в нервові імпульси. Сітківка відповідає за забезпечення їх первинної обробки.

Аутентифікація особи по сітківці здійснюється ляхом порівняння зображень кровеносних сосудів дна ока – хлоридальної системи. Процес відбувається шляхом сканування сітківки спеціальною камерою, що працює у ближньому інфрачервоному діапазоні [7] та завдяки якій отримується якісне зображення кровоносних судин дна ока та переводиться у цифровий шаблон.

Недолік: високі вимоги до процесу сканування.

Перевага: сітківка не змінює свою структуру протягом усього життя, візерунок хлоридальної системи неможливо змінити шляхом хірургічного втручання.

2.6 Метод аутентифікації за ходою

В методі використовується методика аналізу ходи людини. Оскільки це поведінковий біометричний параметр, кожна особа має свої особливості ходи. Комп'ютер на основі відеозапису формує скелет, що складається із з'єднання контрольних точок кінцівок тіла людини. Нейромережі, що аналізують дані, аутентифікують користувача за ходою.

Перевага: можливість розпізнавання через відеозапис.

Недолік: недостатня розвиненість, часті помилки.

2.7 Метод аутентифікації за геометрією обличчя

Цей метод популярний та використовується для розпізнавання осіб серед натовпу по звичайній фотографії з камер відеоспостереження.

Принцип заснований на побудові тривимірної моделі обличчя з подальшим виділенням контурів носу, губ, брів, очей, підборіддя, т.і. з обчисленням відстані та інших параметрів співвідношення між ними. Враховується до 40 особливостей лиця та голови особи [8].

2.8 Метод аутентифікації за геометрією руки

Типові параметри кістки руки включають довжину та ширину пальців, співвідношення розмірів кістки чи пальців, ширину, товщину кістки, відстань між суглобами, структура кістки, зморшки, папілярні візерунки, і інші [1].

До системи входять камера та світлодіоди, які рівномірно підсвічують прикладену руку. На основі отриманих зображень моделюється тривимірна модель та подальший аналіз [8].

Основний недолік: рука може піддаватися травмам, що збільшує ймовірність помилки.

2.9 Метод аутентифікації за голосом

Голос – поведінковий біометричний параметр та залежить від фізичних характеристик. Властивості голосу такі, як частота (залежить від характеристик мовленнєвоготракту, детально оцінюється у деяких системах), носовий звук, модуляція, інтонація і т.і. є унікальними властивостями людини.

Недолік: невисока точність. Голос змінюється протягом віку, хвороб. хвороб. Наявність стороннього шуму може негативно впливати на процес розпізнавання.

2.10 Метод аутентифікації за підписом

Підпис виконується на спеціальній поверхні з використанням цифрової ручки, що є чутливою до тиску на поверхню. Підпис порівнюється з оригінальним шаблоном та враховуються другорядні поведінкові ознаки.

3 ОГЛЯД ІСНУЮЧИХ АНАЛОГІВ ТА ВИБІР КОМПОНЕНТУ

Оскільки макет системи біометричного доступу повинен мати компактні розміри, та передбачати швидку процедуру доступу до системи, вибір методу аутентифікації обмежуємо сканерами відбитку пальців та райдужки ока.

Такі типи біометричного доступу розповсюджені та найчастіше використовуються, датчики мають невеликі розміри, а технології досягли достатньо високого рівня захисту.

3.1 Аналоги систем розпізнавання райдужки

— **Anviz UltraMatch S2000.** Біометричний термінал для систем контролю доступу, обліку робочого часу та масової ідентифікації зі сканером райдужної оболонки ока та зчитувачем безконтактних карток. Технологія підтримує всі кольори очей, легко ідентифікує особу навіть в окулярах, масках або контактними лінзами.

Ціна пристрою: 3300 доларів США

Рисунок 3.1 — Сканер Anviz UltraMatch S2000

— **EyeLock Nano NXT**. Біометричний пристрій розпізнавання райдужної оболонки ока на відстані та в режимі реального часу. При використанні

даного пристрою час розпізнавання зведено до мінімуму. Nano NXT розпізнає швидко і безпомилково. Автономна пам'ять зчитувача дозволяє зберігати до 20 000 шаблонів райдужної оболонки, реєстрація користувача може проходити по 1 або2 очах.

Ціна: 1654 доларів США

Рисунок 3.2 — Сканер EyeLock Nano NXT

— **EyeSwipe-Nano.** Сканер є мініатюрною системою розпізнавання на основі аналізу райдужної оболочки ока, яка здатна забезпечити в режимі реального часу ідентифікацію та автентифікацію особистості в русі та на відстані. Для розпізнавання користувачу необхідно подивитись на пристрій з відстані 30 см.

Пропускна здатність: 20 осіб за хвилину.

Ціна: 1500 доларів США

Рисунок 3.3 — Сканер EyeSwipe-Nano

— **EF-45.** Біометричний термінал розпізнавання райдужної оболонки

обох очей на відстані 35-40 см. Пристрій дозволяє реалізовувати безпечні системи контролю доступу за принципом «вільні руки». Термінал незамінний при використанні в зонах із високим рівнем забруднення або в місцях, де аутентифікація здійснюється без застосування рук.

Ціна: 1247 доларів США

Рисунок 3.4 — Сканер EF-45

— EyeLock Myris. Комп'ютерний пристрій розпізнавання райдужної оболонки. Має USB інтерфейс, сумісний із операційними системами Windows, MacOS та основними інтернет браузерами. Ідентифікація райдужної оболонки відбувається на пристрої, що забезпечує повну конфіденційність даних. Пам'ять розрахована на зберігання до 5 шаблонів.

Ціна: 74 долари США

Рисунок 3.5 — Сканер EyeLock Myris

3.2 Аналоги систем розпізнавання відбитків пальців

— **SENSOR FPM10A.** Сумісний з Arduino модуль відбитків пальців. Завдяки високошвидкісному DSP процесору може працювати з послідовними пристроями типу MSP430, 51, AVR, PIC, STM32, ARM і FPGA а також окремо без основного комп’ютера чипрограмного забезпечення для ПК. Може зберігати 1000 відбитків. Підтримка введення відбитків, інтелектуальна обробка зображень, порівняння відбитків пальців, режим пошуку. Висока чутливість до вологого та сухого розпізнавання.

Ціна: 43 долари США

Рисунок 3.6 — Сканер SENSOR FPM10A

— **Waveshare.** Ємнісний сканер працює на мікроконтролері STM32. Роздільна здатність 508 точок на дюйм. Пристрій підтверджує або відхиляє доступ за 1 секунду. Модуль може підключатися до Arduino через інтерфейс UART. Можливе підключення до комп'ютера через порт USB або за допомогою конвертеру USB-UART.

Ціна: 85,75 доларів США

Рисунок 3.7 — Сканер Waveshare

— **ZKTeco SLK20R.** Біометричний зчитувач відбитків пальців із застосуванням передової оптичної схемотехніки. Підтримує функції детектування підроблених відбитків. Стабільно працює при високомурівні освітлення, підтримує інтерфейс USB.
Ціна: 146 доларів США

Риссунок 3.8 Сканер ZKTeco SLK20R

— **ZFM-20**. 512-байтовий датчик відбитків пальців із зеленим підсвічуванням для Arduino UART виконаний на мікроконтролері STM32. Швидкість сканування: не більше пів секунди, здатенза-пам’ятовувати 1000 різних відбитків.
Ціна: 68 доларів США

Рисунок 3.9 — Сканер ZFM-20

У ході проведеного аналізу було обрано сканери що працюють на основі ідентифікації відбитків пальців. Вони забезпечують усі необхідні функції нашої системи доступу, та набагато дешевшими за своїх конкурентів – сканерів відбитків райдужки.

У якості моделі вибір пав на ZFM-20. Переваги: відносно невисока ціна, наявність на ринку в Україні, легке підключення до пристрою Arduino завдяки підтримці інтерфейсу UART.

4 ЗАГАЛЬНІ ВІДОМОСТІ ПРО БІОМЕТРІЮ ВІДБИТКІВ ПАЛЬЦІВ

Основою ідентифікації користувача є сканування його пальця, трансформація зображення у цифровий набір даних та подальше порівняння з оригіналом, заздалегідь занесеним у базу даних (рис. 4.1)

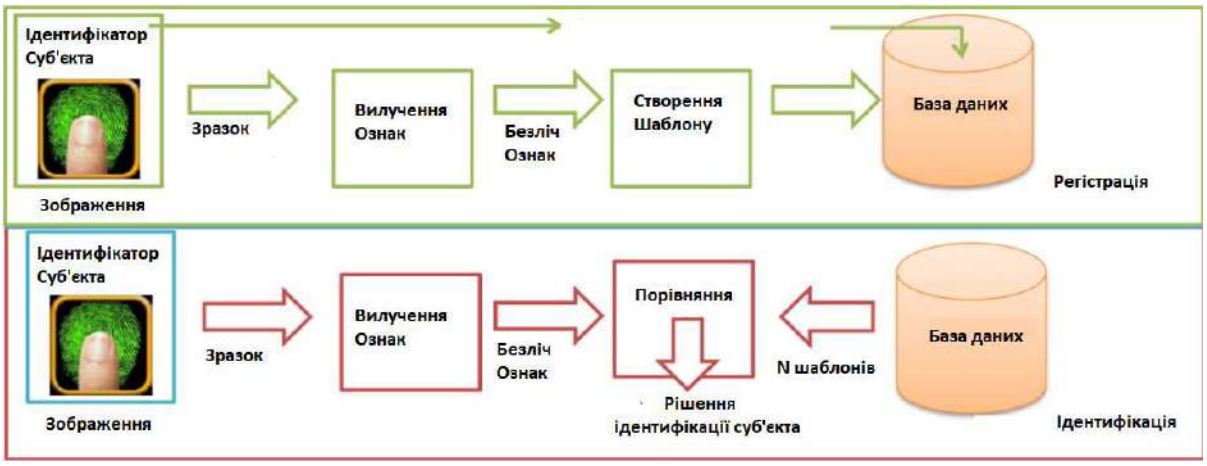


Рисунок 4.1 — Алгоритм реєстрації та ідентифікації відбитків

4.1 Деталі що використовуються при ідентифікації

Кожний палець на верхньому шарі шкіри (дерма) має папілярний візерунок – певний рельєф який являє собою набір пагорбів і западин. Усього існує 3 типи папілярних візерунків, (рис. 4.2): завитковий, дуговий та петльовий, і всі вони мають відмінні деталі.

Рисунок 4.2 — Типи папілярних візерунків

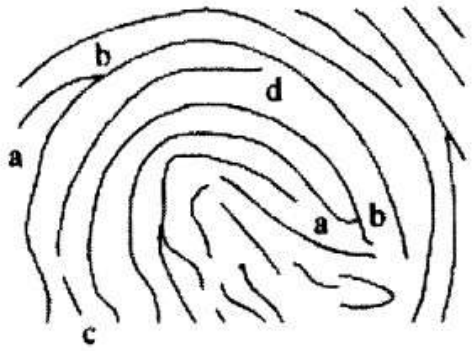


Рисунок 4.3 — Спрощена структура відбитка пальця

Експерти використовують велику кількість деталей папілярних візерунків для визначення того що різні відбитки належать одному пальцю. На (рис. 4.3) демонструється зпрощена структура відбитка, що має такі ознаки як a) кінець борозни, b) роздвоєння борозни, c) незалежна борозна. На (рис. 4.4) Зображений повний список другорядних деталей. Автоматичні алгоритми зіставлення відбитків пальців працюють схожим чином. В них частіше за все використовується роздвоєння та кінець борозни – деталі що виділяються з оцифрованого відбитку. Багато алгоритмів розпізнавання навіть не розрізняють роздвоєння та кінець борозни, тому що під час зняття відбитків та обробки, вони можуть мати обернений один одному вигляд. Все це відбувається в залежності від сили тиску на сенсор. Приклад можна побачити на (рис. 3.2), d) невизначена деталь, кінець борозни/роздвоєння.

Рисунок 4.4 — Другорядні деталі папілярного візерунка

4.2 FRR та FAR

Двома основними показниками якості розпізнавання та надійності біометричної системи є 2 параметри:

FRR (False Rejection Rate) – вирогідність помилкових відмов зареєстрованого користувача. Допустиме значення: <1%

FAR (Ralse Acceptance Rate) – вирогідність помилкового доступу незареєстрованого користувача. Допустиме значення: <0,001%

Стандартизація шаблонів відбитків пальців

4.3 Стандартизація шаблонів

INCITS 378-2009 – стандарт, що визначає концепцію та формат даних для представлення відбитків пальців з використанням основного поняття дрібниць. Формат даних є загальним і його можна застосовувати в широкому діапазоні областей де використовується автоматичне розпізнавання відбитків пальців. У цьому стандарті не розглядаються вимоги чи функції, що стосуються конкретної програми. Стандарт містить визначення відповідних термінів [10].

4.4 Методі розпізнавання відбитків

Виділяють три основних типи алгоритмів по розпізнаванню відбитків пальців:

Кореляційне порівняння. Суть методу полягає у тому що зображення відбитку, отримане зі сканеру та збережені шаблони накладаються, потім розраховується кореляція (за рівнем інтенсивності) між відповідними пікселями. Розпізнавання проводяться шляхом розрахунку для різноманітних вирівнювань зображень відносно один одного (зсув, обертання і т. ін.) [9]. Згідно відповідного коефіцієнту відбувається подальше рішення стосовно збігу відбитків.

Розпізнавання по особливим точкам. По одному або декільком зображенням проводиться процес виділення особливих точок на відбитку, як приклад ними можуть бути закінчення, розходження папілярної лінії. Отримані виділені фрагменти конвертуються у двомірний цифровий масив. Після цього проводиться порівняння з шаблоном і на основі кількості подібних точок, відбувається ідентифікація чи відхил операції.

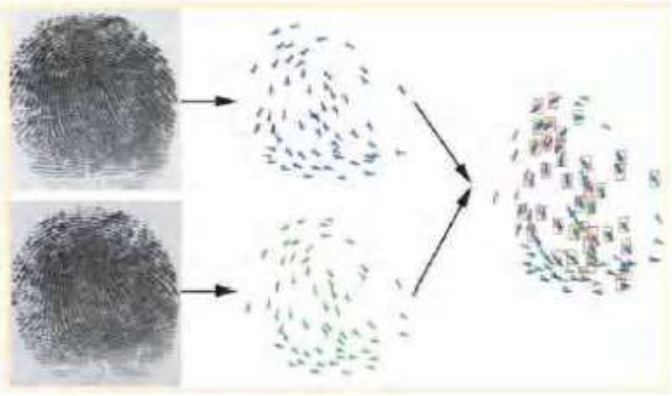


Рисунок 4.5 — Другорядні деталі папілярного візерунка

Розпізнавання по шаблону. У ході цього методу порівняння відбитків відбувається шляхом зіставлення повного зображення папілярного візерунку. Отримане зі сканера зображення розбивається на велику кількість малих фрагментів, (рис. 4.6), вони оцифровуються, та потім отриманий масив даних порівнюється з шаблоном [9].

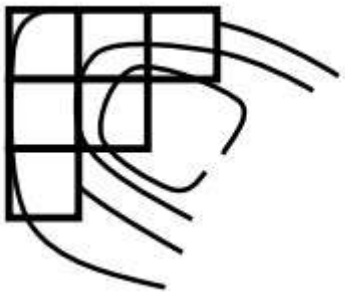


Рисунок 4.6 — Розбиття папілярного візерунка на фрагменти

4.5 Архітектури систем біометричного доступу

Архітектура Match-on-Host. Сьогодні практично кожна реалізація біометричного доступу через розпізнавання відбитків пальців: смартфон, комп'ютер, чи окремий модуль, виконує процес зіставлення безпосередньо за принципом Match-on-Host. Його робота полягає в тому, що сканер зчитує дані відбитків пальців і надсилає їх на обробку хост-процесором або іншим зовнішнім процесором [11]. В той час, коли як датчик фіксує дані відбитків пальців, вся робота з обробки та узгодження виконується на хост-платформі (рис. 4.7).

Основна вимога до визначення відбитків пальців передбачає позитивну ідентифікацію користувача шляхом збігу з відомим і захищеним «шаблоном» або записом відбитка пальця користувача.

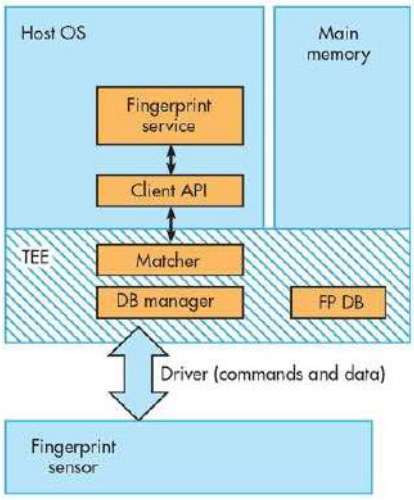


Рисунок 4.7 — Архітектура технології Match-on-Host

Датчик спочатку використовується для збору даних, які створюють запис користувача в процесі «реєстрації», а потім використовується під час кожної наступної спроби доступу для захоплення даних відбитків пальців для порівняння із збереженим шаблоном [11].

В результаті архітектура Match-on-Host розділяє функціональні вимоги між сенсорною інтегральною схемою, яка фіксує дані, і окремою інтегральною

схемою контролера (часто це процесор додатків на мобільному пристрої), що використовується для запуску програмного забезпечення.

Функції, що виконуються в програмному забезпеченні (Host OS), включають ідентифікацію характеристик відбитків пальців, створення захищеного шаблону відбитків пальців, зберігання та узгодження щойно створеного шаблону відбитків пальців із тим, що вже знаходиться у пам'яті пристрою. Головна система також забезпечує безпеку, необхідну для захисту цілісності та конфіденційності даних відбитків пальців. Крім того, хост-система відповідає за виявлення біометричних підробок [11].

Дві основні переваги архітектури Match-on-Host полягають в її низькій вартості та відностно простій інтеграції у систему основного пристрою [11].

Архітектура Match-in-Sensor. Match-in-Sensor інтегрує процеси управління біометричними функціями безпосередньо в мікросхему датчика. У свою чергу, мікросхема містить високошвидкісний мікропроцесор, сховище для інструкцій і даних, безпечний зв'язок і високопродуктивні криптографічні можливості. ізолюють операції відбитків пальців від основної (Host OS) у самому сенсорі (рис. 4.8).

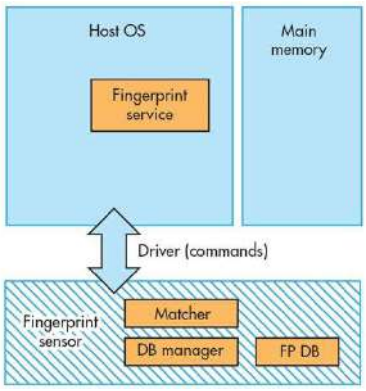


Рисунок 4.8 — Архітектура технології Match-in-Sensor

Дані відбитків пальців, створені шаблони, обробляються лише всередині вбудованого ЦП і сховища датчика. Жоден з цих файлів ніколи не передається та не оброблюється для хост-пристрою.

Реєстраційна база даних розташована у флеш-пам’яті, яка є системно ізольованою і фізично доступна лише датчику. Крім того, шаблони реєстрації шифруються та підписуються датчиком за допомогою власних надійних криптографічних ключів перед тим, як зберігатися в приватній флеш-пам’яті [11].

Великою перевагою цієї архітектури є високий рівень захищеності. Навіть якщо зловмисник отримає доступ до самого хосту, він не зможе заволодіти біометричною інформацією власника.

5 МАКЕТУВАННЯ СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ARDUINO

5.1 Вибір компонентів та комплектуючих

Керуючись даними, наведеними в попередніх розділах даної роботи, система повинна виконувати наступні функції:

- реєстрація відбитків пальця;

- обробка зображення згідно заданого алгоритму у заданому форматі;

- створення шаблону та його порівняння з наявними в бібліотеці (з можливістю запису та видалення шаблонів з бібліотеки);

- за результатом аналізу відпрацювання команд ТАК/НІ, які подаються на виконавчі пристрої;

- контроль виконання команди виконавчим пристроєм та фіксація події;

- управління, логін та статистика подій а також та їх контроль можуть здійснюватися віддалено з використанням технологій віддаленого доступу, хмарних технологій та відповідного ступіню захисту інформації (***В даній роботі функціонал щодо захисту інформації розглядається тільки як опис. Формат обміну даними, характеристики каналів зв'язку, ступіні захисту інформації, інші вимоги надаються замовником системи згідно технічних умов га кожний об'єкт телекомунікацій окремо).***

Враховуючи наведене вище, а також керуючись умовами щодо наявності елементів системи, що вже знаходяться в експлуатації та відповідають затвердженим нормам ТЗІ, обираємо елементи системи.

Зауважимо, що важливим є необхідність обміну інформацією між елементами системи для обробки та отримання команди на виконавчий елемент. Також приймаємо до уваги, що у пристроях систем контролю та управління доступом (СКУД) з метою уніфікації використовується інтерфейс Wiegand.

Wiegand – провідний інтерфейс зв'язку між пристроєм зчитуванні ідентифікатору (зчитувачам) та контролером та призначений для передачі в контролер СКУД унікального коду карти або pin-коду з клавіатури.

Однією із вимог є необхідність використати сканер відбитків пальців, що використовуються на діючих об’єктах. Одним із таких сканерів є ZFM-20.

Ефективним з точки зору роботи з бібліотеками зображень, підключення сканеру відбитків пальців з подальшою можливістю з інтерфейсом Wiegand є Arduino у виконанні UNO R3. Також цей пристрій має можливість підключення і управління різноманітними датчиками, модулями, т.і.

Відповідно до вимог щодо функціоналу системи перелік елементів системи буде складатися з наступних пристроїв:

— сканер відбитків пальців ZFM-20 - 1 шт. ;

— Arduino UNO R3 - 1 шт.;

— LCD дисплей LCD1602 з модулями IIC/I2C (зелений) - 1шт.;

— модуль зуммер – 1 шт.;

— модуль кнопка – 2 шт.;

— світлодіодний модуль - 2шт.;

— силовий ключ - 1шт.;

— контролер віддаленого доступу PAL-ES SG314GI-WR – 1 шт.;

— модуль Shield – 1 шт.;

— Електромагнітний замок

— Шина живлення постійного струму

— з’єднувачі [12]

Для реалізації функціонування системи на програмному рівні необхідно забезпечити використання бібліотек, які надають можливість підключення периферійних пристроїв до Arduino:

— LiquidCrystal_I2C_V112 (для роботи з дисплеями LCD1602 з підключенням до Arduino через шину I2C);

— Adafruit_Fingerprint (для роботи зі сканером відбитків пальців);

— Стандартні бібліотеки Wire та SoftwareSerial, що входять до складу інтегрованої середи розробки Arduino IDE [12].

— Wiegand.h Стандартна бібліотека для роботи з протоколом Wiegand

5.2 Сканер відбитків пальців ZFM-20

ZFM-20 – сканер відбитків пальців, що підключається до контролеру через UART протокол. Технічні параметри наведено в таблиці.

Таблиця 5.1 — Характеристики сканеру ZFM-20

Напруга живлення	DC 3,8 – 7,0 V 3,3 V
Вхідний та піковий струми	<65 мА, <95 мА,
Час вводу зображення відбитка пальця	<0,5 мА
Зберігання шаблонів	1000 шт
Коефіцієнт помилкового прийняття (FAR)	<0,001%
Коефіцієнт помилкового відхилення (FAR)	<1%
Робоча середа	Діапазон робочих температур: від -20 до +50 градусів Цельсія Рівень відносної вологи: <85%

Сканер відбитків пальців ZFM-20 має 4 порти:

— VCC живлення;

— GND земля;

— RXD приймання даних;

— TXD передача даних.

5.3 Arduino Uno R3

Arduino Uno R3 – пристрій, виконаний на основі мікроконтролера ATmega 16U2. До складу 14 цифрових портів IN/OUT (серед них 6 можуть використовуватися у якості ШІМ-виходів), 6 аналогових портів IN, кварцевий резонатор 16 МГц .

У складі плати Arduino наявний інтерфейс USB, який виконує роль роз’єму живлення та роз’єму для внутрішньо-схемного програмування [13].

Живлення плати можливе через спеціальний роз’єм за допомогою AC/DC-адаптера чи акумуляторної батареї. В Arduino Uno також є запобіжники для захисту USB-порта комп'ютера від коротких замикань та перевантажень.

Максимальна довжина та ширина друкованої плати Uno R3 становить 6,9 см і 54 см відповідно, з урахуванням роз'єму USB та роз'єму живлення, що виступають за межі плати. Чотири отвори для кріплення дозволяють прикріплювати плату до поверхні або корпусу.

Рисунок 5.1 — Плата Arduino Uno R3

Переваги виконання Arduino Uno R3:

— програмне забезпечення від виробника безкоштовне. ПЗ має простий інтерфейс та має можливість використання бібліотек;

— низька ціна;

— компактні габаритні розміри. Різноманітні порти підключення;

5.4 Дисплей LCD1602

LCD QC1602 IIC/ - дисплей для підключення до Arduino. Має два рядки по 16 символів у кожному. Працює зі стандартною бібліотекою LiquidCrystal яка наявна у програмному забезпеченні Arduino IDE.

Таблиця 5.2 — Технічні параметри дисплею LCD1602

Напруга живлення	DC 3,8 – 7,0 V 3,3 V
Вхідний та піковий струми	<65 мА, <95 мА,
Час вводу зображення відбитка пальця	<0,5 мА
Зберігання шаблонів	1000 шт
Коефіцієнт помилкового прийняття (FAR)	<0,001%
Коефіцієнт помилкового відхилення (FAR)	<1%
Робоча середа	-20…+50 С, рівень відносної вологості: <85%

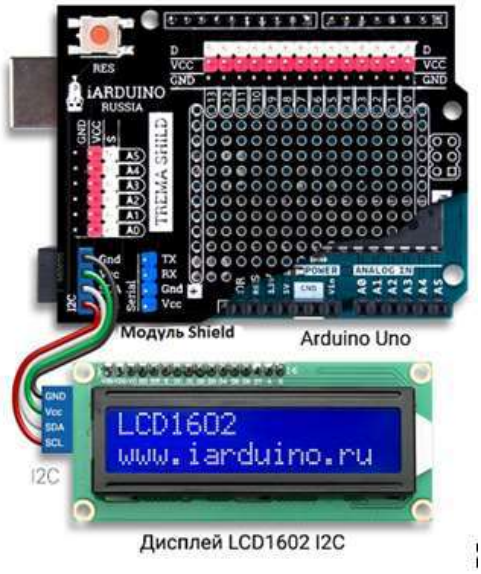


Рисунок 5.2 — Схема підкюченуя дисплею до плати Shield

Плюсом цього дисплею є те що у ньому також наявна шина I2C, і це значно спрощує підключення дисплею до плати.

Порти шини I2C:

— SCL, послідовна лінія тактування (Serial Clock);

— SDA, послідовна лінія даних (Serial Data);

— VCC, живлення ;

— GND, земля.

5.5 Зумер

Зумер виконано з генератора прямокутних імпульсів (меандра) 5 Вольт з частотою 2,3 кГц та електромагнітного випромінювача в одному корпусі. Сигнал з генератора подається на електромагнітний випромінювач і перетворюється на звукові хвилі тієї ж частоти [14].

Таблиця 5.3 — Технічні параметри зумеру

Напруга живлення	5 В
Споживаний струм	30 мА
Інтенсивність звуку	>= 85 дБ
Резонансна частота	2048 Гц
Робоча температура	-20 … +70 С
Габарити (мм)	30 х 30 х 9 (без урахування виводів)

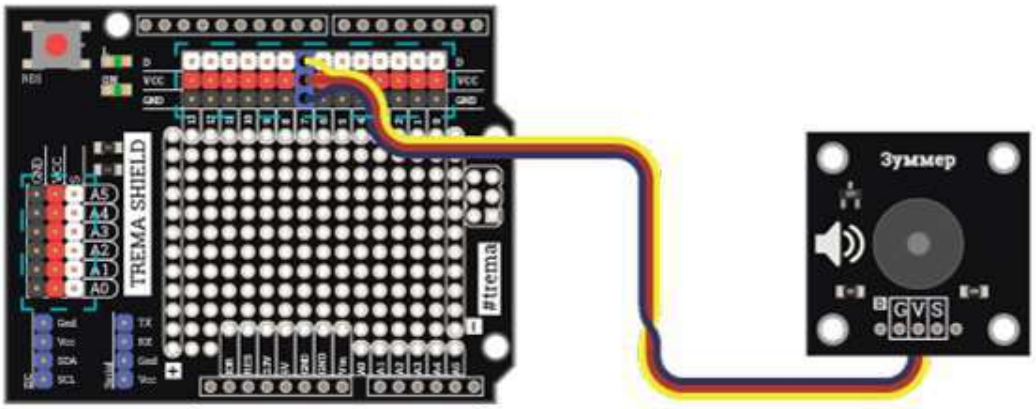


Рисунок 5.3 — Схема підкючення зумеру

Цей модуль підключається до нашого пристрою конекторами через порти GND та VCC. S - порт інформаційного сигналу.

5.6 Кнопка

Тактова кнопка є одним з елементів управління системи аутентифікації. Може підключатися до цифрового та аналогового виводів Arduino.

Таблиця 5.4 — Технічні параметри кнопки

Робоча напруга	до 5,5 В
Комутуючий струм	до 50 мА
Час брязкіту при натисканні	< 3 мкс
Час брязкіту при відпусканні	< 4 мкс
Робоча температура	-20 … +70 С
Габарити (мм)	30 х 30 х 15 (без урахування виводів)

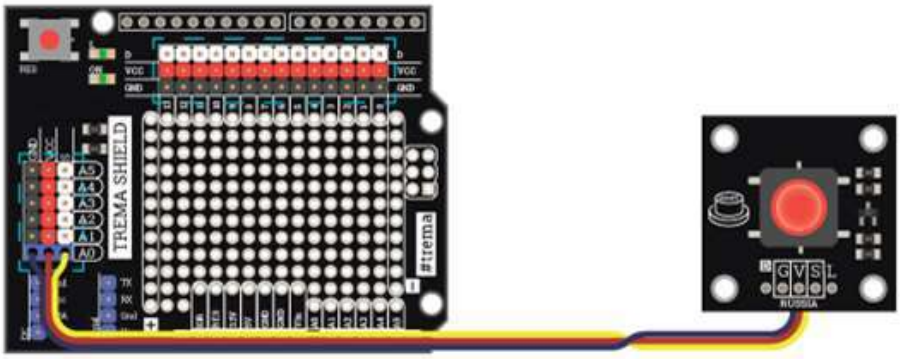


Рисунок 5.4 — Схема підкючення кнопки

Модуль має 3 порти:

— GND;

— VCC;

— S - порт інформаційного сигналу. В положенні «ненатиснута» на виході S логічний нуль, вихід через резистор пад'єднаний до GND. При натисканні S з'єднується з виходом VCC та змінює свій стан на логічну одиницю.

5.7 Світлодіод

Світлодіод необхідний для візуалізації підтвердження або відхилення аутентифікації. Плата модулю світлодіоду має чотири виходи: VCC, GND, S (сигнальний вихід). При подачі сигналу (логічної одиниці) на порт S світлодіод світиться.

Таблиця 5.4 — Технічні параметри світлодіоду

Напруга живлення	Від 3 В до 5,5 В
Габарити	30×30 мм
Робоча температура	від -10 до +70 градусів Цельсія

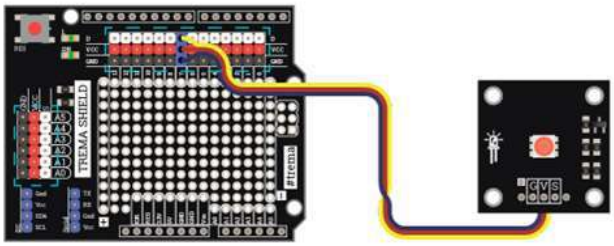


Рисунок 5.5 — Схема підкючення світлодіоду

5.8 Силовий ключ

Силовий ключ являє собою модуль, який за допомогою низької напруги Arduino (та інших платформ) може керувати більш високим навантаженням високого струму, що є зручним для управління пристроями, які споживають значно більший струм, на відміну від того, що може видати на виході контролер. У нашому випадку таким пристроєм є контролер віддаленого доступу Pal-Es SG314GI-WR.

Характеристики силового ключа:

— комутація можлива лише через постійну напругу;

— максимальний струм комутації: 10А (від 6А рекомендовано використання радіаторів);

— максимальна напруга комутації: 30 В;

— напруга живлення: від 3 В до 5,5 В;

— виконання на базі польового транзистору LR8113;

— підтримка ШІМ;

— габарити: 31 × 31 мм

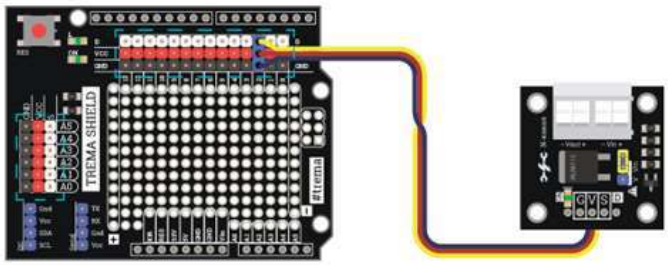


Рисунок 5.6 — Схема підключення силового ключа

Виводи:

— G – мінус (GND), живлення пристрою;

— V – плюс (Vcc), живлення пристрою;

— S – сигнал (Signal), керуючий сигнал.

При поданні позитивного рівня сигналу (логічна одиниця) на вивід S відбудеться увімкнення ключа, а при поданні логічного нуля - відключення.

5.9 Модуль Shield

Shield – плата розширення для Arduino, що спрощує процес підключення модулів до пристрою та кріпиться до тильної сторони Arduino.

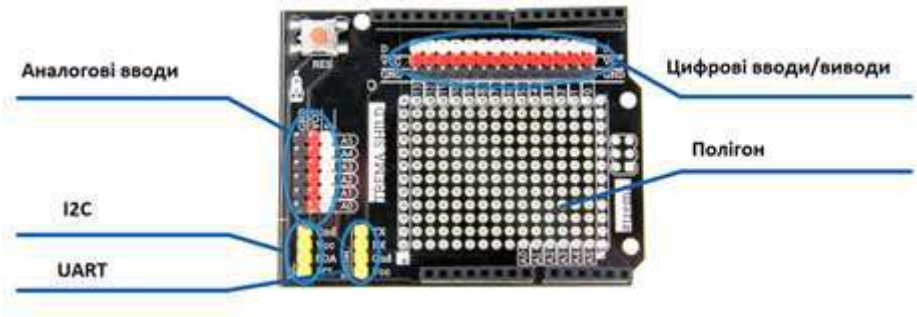


Рисунок 5.7 — Плата Shield

Плата містить:

— колодку з 14 виводами (D), з виводами шини живлення (Vcc та GND) для підключення цифрових модулів;

— колодку з 6 аналоговими виводами (S) з виводами шини живлення (Vcc та GND) для підключення аналогових та цифрових модулів;

— колодку апаратної шини UART (Serial), що складається з 4 виводів (TX, RX, GND, Vcc), для підключення UART модулів;

— колодку апаратної шини I2C, що складається з 4 виводів (SDA, SCL, GND, Vcc), для підключення I2C модулів;

— кнопка Reset для перезавантаження Arduino;

— два світлодіоди, «ON» – інформує про наявність живлення, «L» – інформує про наявність високого логічного рівня на виводі D13 [15];

— макетна область (сітка контактних отворів).

5.10 Електромагнітний замок

При подачі напруги на замок, ригель переміщується всередину корпус. При відсутності напруги ригель приймає вихідне положення.

Характеристики:

— Робоча напруга: 12 В;

— Максимальний струм до 0.8;

— Максимальний час роботи не повинен перевищувати 10 секунд;

5.11 Контролер віддаленого доступу Pal-Es

Обрано модель SG314GI-WR, призначену для роботи з інтерфейсом Wiegand.

Пристрій призначений для правління доступом до приміщень, територій т.і., з можливістю створення алгоритму за датою, часом, статусом, групами користувачів з використанням технологій передачі даних.

Контролер є функціонально автономним радіопристроєм, основними складовими якого є радіомодуль, центральний процесор, блок комутації з виконавчими пристроями, слот для встановлення SIM-карти.

В залежності від призначення використовуються один або два радіомодулі.

Налаштування та управління контролером здійснюється через додаток IOS/Android або WEB інтерфейс в особистому кабінеті. Алгоритм подій за декількома параметрами, права доступу, кількість користувачів задаються адміністратором з можливістю формування журналу подій імпорту/експорту даних у форматі EXCEL.

Команда на виконавчий пристрій може бути сформована після телефонного дзвінка з дозволеного номера або адміністратором віддалено.

У випадку використання контролерів з двома радіомодулями, додатково управління здійснюється за допомогою анти-клон пульту. Захист від клонування здійснюється за рахунок використання ключа шифрування довжиною 128 біт. Кожен пульт (у разі використання) має унікальний ідентифікатор, що дозволяє формувати персоналізований журнал подій, та може бути активований (деактивований) віддалено. Пульт може використовуватись для однієї або декількох груп користувачів з різними заданими параметрами.

Живлення в межах 12 - 24 В DC розширює можливості використання.

Переваги контролерів PAL-ES:

- низька ціна та можливість використання на всій території України (наявний Сертифікат відповідності);
- формування алгоритму доступу за різними параметрами і рівнями та мінімізація вірогідності доступу у приміщення (зони) з підвищеним ризиком для осіб, що не мають права на доступ;
- віддалене адміністрування особистого кабінету з будь-якого місцезнаходження;
- можливість подати команду на відкриття простим телефонним дзвінком;
- використання пульту дистанційного управління для одного або декількох контролерів (Наприклад, відповідальна особа охорони. За

необхідності, команда на відкриття також може подаватися за допомогою кнопки з пульту охорони. В цьому випадку інформація в журналі подій не фіксується);

— зберігання журналу подій в особистому кабінеті та формування файлів з даними про події для подальшого використання;
— можливість використання пульту дистанційного управління для декількох об’єктів;
— захист від клонування пульту дистанційного управління та неможливість зчитування коду (шифрування ключем 128 біт);
— наявність нормально-розімкнутого (односмугового) реле (60 В / 900 мА);
— можливість використання інтерфейсу Wiegand;
— некритичні технічні характеристики (живлення пристрою від 12 до 24 В);
— кількість користувачів необмежена.

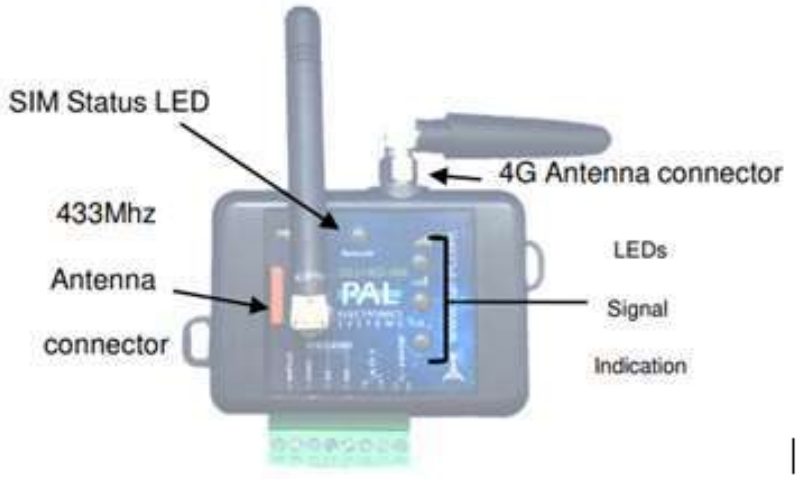


Рисунок 5.8 — Контролер SG314GI-WR

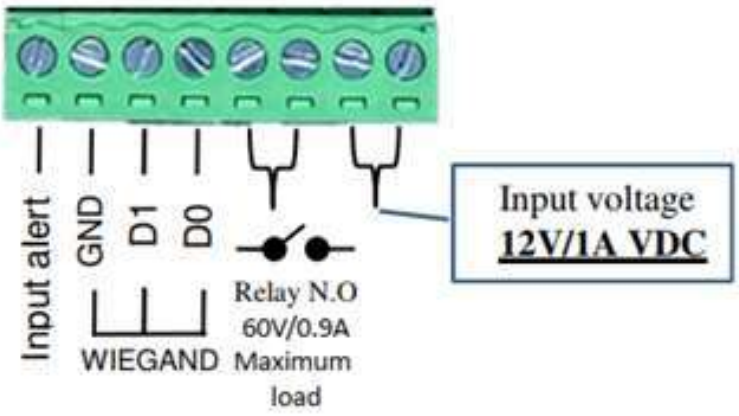


Рисунок 5.9 — Реле контролеру SG314GI-WR

5.12 Схема підключення

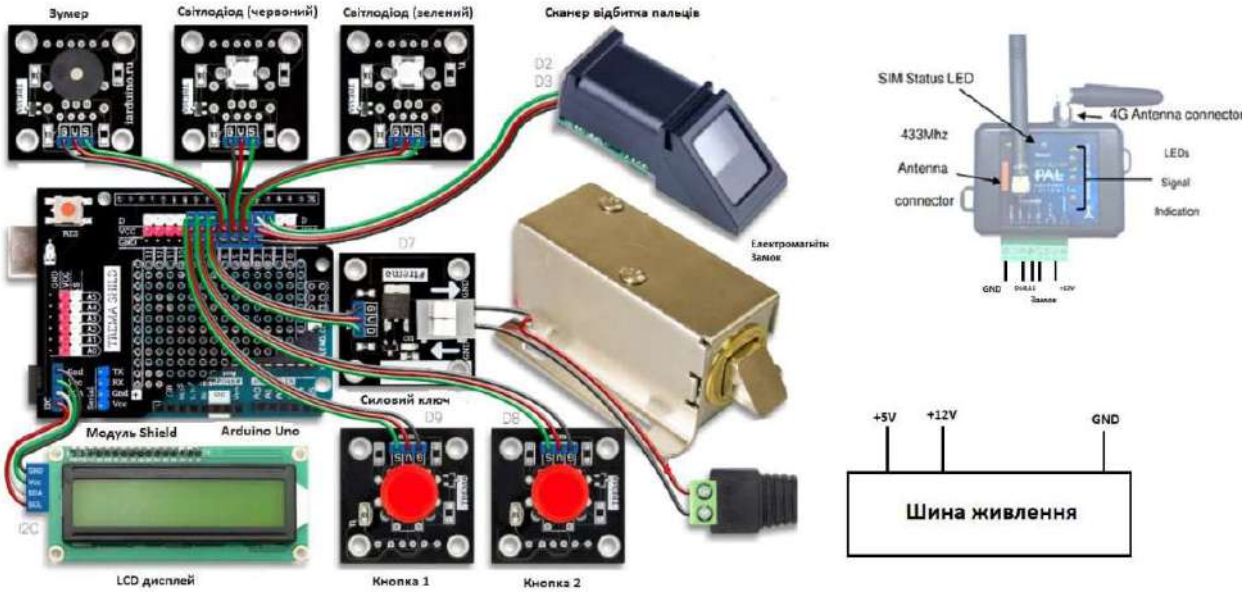


Рисунок 5.10 — Схема повної збірки

Таблиця 5.5 — Таблиця комутації

Arduino (порти)	Модулі
2 (RX - ввід програмного UART)	T – вивід сенсора відбитків пальців
3 (TX - вивід програмного UART)	R – ввід сенсора відбитків пальців
4	Світлодіод зелений
5	Світлодіод червоний
6	Зуммер
7	Силовий ключ
8	Кнопка 1
9	Кнопка 2

Таблиця 5.5 — Таблиця комутації

10	SG314GI-WR
11	SG314GI-WR
Шина I2C	LCD дисплей

Таблиця 5.6 — Функції індикаторів

Індикатори	**Значення**
Швидке блимання SIM індикатора	Система завантажується
Повільне блимання SIM індикатора	Пошук мережі
Два блимання і пауза	Процес підключення до мережі інтернет
Чотири коротких блимання SIM індикатора	Підключення до PAL інтерфейсу
Постійне світіння	Система готова
Увімкнено світловий індикатор № 1	Поганий сигнал
Увімкнено світловий індикатор № 2	Хороший сигнал
Увімкнено світловий індикатор № 3	Дуже хороший сигнал

Таблиця 5.7 — Перелік елементів системи біометричного доступу

н/п	**Назва**	**Кількість, шт.**
1	Сканер відбитків пальців ZFM-20	1
2	Arduino UNO R3 - 1 шт.	1
3	LCD дисплей LCD1602 з модулями IIC/I2C (зелений)	1
4	Модуль зуммер	1
5	Модуль кнопка	2
6	Світлодіодний модуль	2
7	Силовий ключ	1
8	Контролер віддаленого доступу PAL-ES SG314GI-WR	1
9	модуль Shield	1
10	Електромагнітний замок (12 В)	1
12	Шина живлення постійного струму та елементи комутацій	1

5.13 Опис роботи системи та функціональне призначення елементів

Система призначена для роботи на об’єктах зв’язку, що введені в експлуатацію, мають затверджену проектну та дозвільну документацію та які потребують модернізації щодо доступу на об’єкт та віддаленого контролю доступу. Це об’єкти, де розташоване серверне обладнання операторів зв’язку (дата-центри, приміщення з правами обмеженого доступу), базові станції мобільних операторів, т.і. При проведенні модернізації об’єкту вимоги щодо технічного захисту інформації а на деяких об’єктах комплексної системи захисту інформації потребують внесення змін до документації з відповідним погодженням документації. Також можливість посилення заходів безпеки при доступі на об’єкт та віддаленого контролю доступу суттєво підвищує надійність мережі взагалі та дає можливість оптимізації витрат на технічну підтримку мережі.

Біометрична система контролю доступу може бути використана як тимчасова заміна елементів існуючих систем доступу на об’єкт з можливістю фіксації самої події доступу віддалено.

Важливим є можливість модернізації процедури доступу та переходу на діючі протоколи обміну інформацією між елементами СКВД. В нашому випадку основним є використання інтерфейсу Wiegand.

Зважаючи на появу на ринку СКВД нових технологічних систем, які дозволяють набагато розширити функціонал та забезпечити надійний контроль з використанням мереж операторів мобільного та фіксованого зв’язку, а також можливість віддаленого адміністрування, контролю, легування подій може суттєво скоротити витрати операторів на обслуговування мереж. Використання хмарних технологій з необхідним рівнем захисту дає можливість оптимізувати витрати на обладнання.

В даній дипломній роботі розглянуто можливість отримати принципове рішення, тому комплектуючі обираються з розрахунку найнижчої ціни, мінімуму функціоналу та відносної надійності для роботи в умовах приміщення.

Основними вимогами є можливість ідентифікації особи, гарантія неможливості несанкціонованої зміни інформації в бібліотеці, де зберігається інформація для ідентифікації, обмін інформацією для подальшої ідентифікації в протоколах СКУД, команда на виконавчий пристрій та фіксація події.

Найкращим пристроєм для відпрацювання можливості побудови системи є Arduino UBO R3. Перевагами є наявність дуже простих периферійних пристроїв, що використовуються в системах контролю, як LCD дисплей LCD1602 з модулями IIC/I2C, модуль зумер, модуль кнопка, світлодіодний модуль, модуль Shield. Крім того, цей пристрій дозволяє записати стандартне програмне забезпечення, сформувати бібліотеку, здійснити обмін інформацією з контролером через інтерфейс Wiegand.

Таким чином забезпечується наступний алгоритм роботи системи:

Попередньо, після інсталяції стандартного програмного забезпечення, яке, в свою чергу після доопрацювання кодів (додаток В), дає можливість отримання обміну даними між сканером та Arduino, безпосередньо Arduino записується сформований на біометричному сканері файл з відбитком пальця особи. Фіксація запису здійснюється за допомогою однієї із кнопок. Подальше видалення з бібліотеки можливе тільки за допомогою другої кнопки. Згідно з запрограмованим алгоритмом відбувається порівняння, результатом якого є візуальна (світлодіоди) та звукова команди. У разі підтвердження повноважень особи, команда дозволу передається на виконавчий пристрій (замок). Одночасно команда з Arduino подається на контролер, який також під’єднується до замка. Контролер знаходиться в мережі 3G/4G через слот з SIM-картою, або через Ethernet. Подія фіксується в особистому кабінеті на контролер, доступ до якого через додаток має адміністратор. Для можливості управління замком використовується модуль Shield. Живлення активних елементів системи стандартне : +5В та +12…24 В та наявне на будь-якому об’єкті зв’язку.

6 РОЗРОБКА АЛГОРИТМУ ВЗАЄМОДІЇ КОНТРОЛЕРУ ARDUINO З ВИКОНАВЧИМ ПРИСТРОЄМ ПО ПРОТОКОЛУ WIEGAND.

Wiegand — простий інтерфейс зв'язку між датчиками або пристроями мережі охоронної системи з контролерами та широко використовується в нинішніх системах контролю та управління доступом СКУД). В нашому випадку відбувається передача даних з контролера Arduino на виконавчий пристрій - електронний замок.

Опис протоколу розпочинаємо зі структури посилки, яка повинна бути передана по Wiegand-26. Структуру посилки наведено на (рис. 6.1)

В кожному кадрі передається 3 (B2, B1, B0) байти та + 2 біти парності ($b_{\text{старш}}, b_{\text{молодш}}$). Від цього й походить назва стандарту "Wiegand-26".

Причому код самої команди в двох молодших байтах даних B1 и B0. Старший байт може бути використаний або не використаний розробником на його вибір. Він називається "фасіліті" та присутній для сумісності з ранніми версіями стандарту. В нашому випадку він може бути довільним числом. Контролер виконавчого пристрою його ігнорує.

Розташовані послідовно, від старшого до молодшого, 3 байти можна умовно розділити навпіл. Отримуємо дві частини по 12 бітів кожна. Стандарт передбачає використання по одному додатковому біту парності для кожних 12 бітів. Загалом два біти парності.

Причому саме значення (парність/непарність) для бітів парності стандартом не оговорюється та вибір на рішення розробника. Але регламентується послідовність передачі бітів у посилці.

Посилка, яка повинна бути сформована (рис. 6.1) складається з:

— біту $b_{\text{старш}}$ парності для старших 12 бітів;

— старших 12 бітів, що передаються від старшого біту до молодшого;

— молодших 12 бітів, що передаються від старшого біту до молодшого;

— біта $b_{\text{молодш}}$ парності для молодших 12 бітів.

Стандартом також регламентуються:

— ширина імпульсу передачі біта $t_{\text{імп}}$;

— період слідування імпульсів передачі біта $T_{\text{слід}}$ (звідси можна вирахувати $\tau_{\text{імп}}$);

— інтервал часу між двома сусідніми імпульсами $= T_{\text{слід}} - t_{\text{імп}}$;

— період слідування кадрів $T_{\text{кадра}}$;

Ширина імпульсів та їх період сильно варіюються в залежності від виробника зчитувача. Ширина імпульсів в діапазоні 20…200 мкс. Період слідування імпульсів — 300…3000 мкс. Розділення кадрів відбувається по тайм-ауту. Реально мінімальний час між кадрами 0,5 сек., рекомендований тайм-аут для контролера СКУД — 50…250мс.

Загальний алгоритм формування посилки Wiegand-26 наведено на (рис 6.2)

Першочергово необхідно задати параметри:

- байти B0 та B1 -код команди;

- байт B2 - фасіліті;

- константа для ініціалізації таймера імпульса передачі біта tімп.;

- константа для ініціалізації таймера інтервалу часу між бітами $\tau_{\text{імп}}$.

- константа для ініціалізації таймера інтервалу часу між кадрами $T_{\text{кадра}}$.

Константи вибираються як добуток тактової частоти таймера на тривалість часу спрацювання таймера.

Далі йде цикл очікування команди передачі коду на виконавчий пристрій (умовно зазначений на структурній схемі "Wait").

Потім відбуваються перевірки на дотримання заданого інтервалу між кадрами. Якщо час, який пройшов з початку передачі попереднього кадру, менший ніж заданий період між кадрами, програма повинна зайти в цикл очікування до того моменту, поки час між двома сусідніми кадрами не стане більшим чи рівним заданому.

Після цього запускається алгоритм бітів парності (рис 6.3) та опис роботи наведено нижче).

Далі йде ланцюг алгоритмів побітової передачі, при виконанні яких послідовно йде передача:

- біта $b_{\text{старш}}$ парності для старших 12 бітів;

- старших 12 бітів, що передаються від старшого до молодшого;

- молодших 12 бітів, що передаються від старшого біта до молодшого;

- біта $b_{\text{молодш}}$ парності для молодших 12 бітів.

Структура алгоритму побітової передачі наведено на (рис. 6.4)

Після закінчення передачі кадру скидається таймер контролю періоду слідування кадрів, що необхідно для дотримання заданого періоду слідування кадрів. Алгоритм переходить в режим очікування команди на передачі наступних трьох байтів.

Алгоритм розрахунку бітів парності представлено на Рис 6.3

В загальному випадку Assembler контролеру містить команди визначення парності бітів. Для визначення парності посилки з 12 бітів парність байту B2 або B0 необхідно "зшивати" з парністю старшої або молодшої частин байту B1 відповідно.

При цьому для виділення старшої частини байту B1 використовується маска F0h. А для виділення молодшої частини байту B1 використовується маска 0Fh. Маска накладається командою логічного множення на B1.

Перша частина алгоритму (рис 6.3) представляє собою послідовний пошук спочатку біта парності $b_{\text{старш}}$ для старших 12 бітів. А друга – пошук біта $b_{\text{молодш}}$ парності для молодших 12 бітів. Причому в обох частинах біт парності формується на підставі визначення комбінацій стану біта парності:

- байту B2 та чотирьох старших байтів B1 у верхній частині алгоритму;

- байту B0 та чотирьох молодших байтів B1 в нижній частині алгоритму.

В результаті на виході ми маємо $b_{\text{старш}}$, $b_{\text{молодш}}$, що дозволяє передати їх алгоритму на (Рис 6.2)

На (рис 6.4) представлений алгоритм формування імпульсів передачі з порту P0 Arduino на виконавчий пристрій.

В загальному випадку протокол "Wiegand" передбачає два сигнали (два дроти або дві виті пари) для передачі сигналів логічного нуля «Data0» та логічної одиниці «Data1». Схемотехнічно це вирішується управлінням бітом P0.0 та бітом P0.1 порту 0 відповідно.

Завданням алгоритму є формування:

- заданої тривалості імпульсу передачі біта $t_{\text{імп}}$;

- заданого періоду слідування імпульсів $T_{\text{слід}}$.

Суть алгоритму в тому, щоб в залежності від того, що нам необхідно передавати, логічний нуль або логічну одиницю, відкрити біт P0.0 або біт P0.1 порту 0 відповідно.

Причому при відкритті цього порту запускається таймер, який контролює період часу $t_{\text{імп}}$, на який цей порт повинен бути відкритий.

Після спрацювання таймера в порт P0 записується байт, який скидає біти P0.0 та P0.1 в похідний стан. І запускається новий таймер, який обліковує заданий інтервал $\tau_{\text{імп}}$, по закінченні якого відбувається вихід з цієї підпрограми для переходу на передачу наступного біта.

При написанні коду для спрощення використовуються відповідні бібліотеки, що є одним з елементів програмування.

Оформлена у вигляді бібліотечної функція передачі управляючого слова outwieg26 може виглядати наступним чином. Реалізована структурна схема послідовної передачі старшого і молодшого слова. При цьому outwiegbit – це виклик підпрограми передачі біта.

Оскільки мова "C" дозволяє використовувати конструкції більш високого рівня, ніж ті, що допускає Assembler самого мікроконтролера, то розрахунок старшого і молодшого бітів парності p_odd та p_even, як варіант, можна реалізувати через програмну реалізацію 12-тирозрядного здвигового регістру, що спрощує код програми.

```
// outputs ONE Wiegand bit
void outwiegbit(unsigned int b)
{
 int sel = b == 0 ? W_D0 : W_D1;
 digitalWrite(sel, 0);
 delayMicroseconds(80);
 digitalWrite(sel, 1);
 delayMicroseconds(240);
}


// outputs a 26 bit Wiegand code
// u32 is actually the 24-bit numeric code
void outwieg26(uint32_t u32)
{
 uint32_t tmp = u32;
 unsigned int p_even = 0;
 unsigned int p_odd = 1;
 // compute parity on trailing group of bits
 for (int n=0; n<12; ++n)
 {
 p_odd ^= (tmp & 1);
 tmp >>= 1;
 }
 // compute parity on heading group of bits
 for (int n=12; n<24; ++n)
 {
 p_even ^= (tmp & 1);
 tmp >>= 1;
 }
 // now output data bits framed by parity ones
 outwiegbit(p_even);
 for (int n=0; n<24; ++n)
 {
 outwiegbit((u32 >> (23-n)) & 1);
 }
 outwiegbit(p_odd);
}
```

Опис структурної схеми алгоритму по своїй суті не залежить від специфічного набору команд будь-якого контролеру.

Алгоритм повністю відповідає стандарту "Wiegand-26" та дозволяє управляти практично будь-яким пристроєм, який використовує цей протокол, а також з будь-якого з існуючих контролерів, не тільки Arduino.

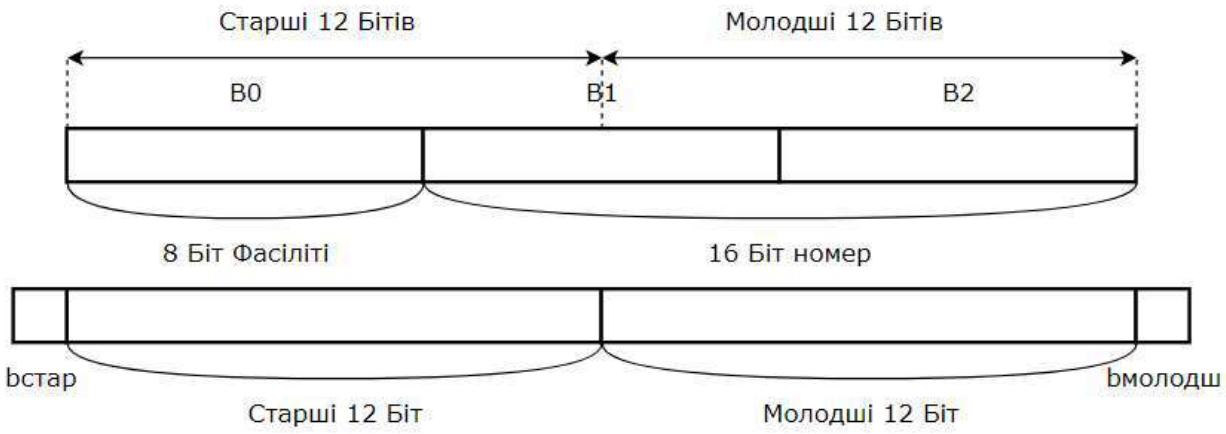


Рисунок 6.1 — Структура кадра

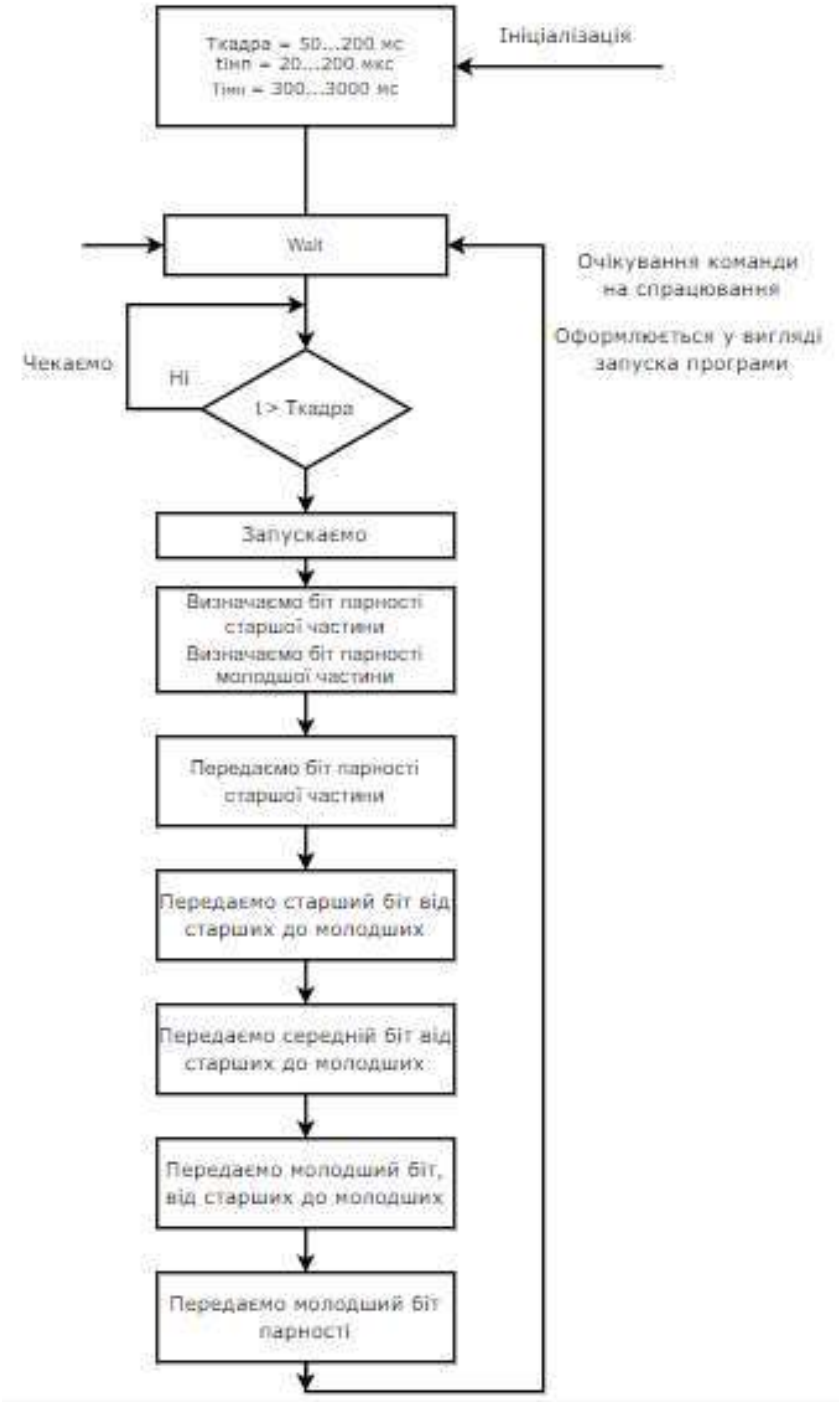


Рисунок 6.2 — Загальний алгоритм

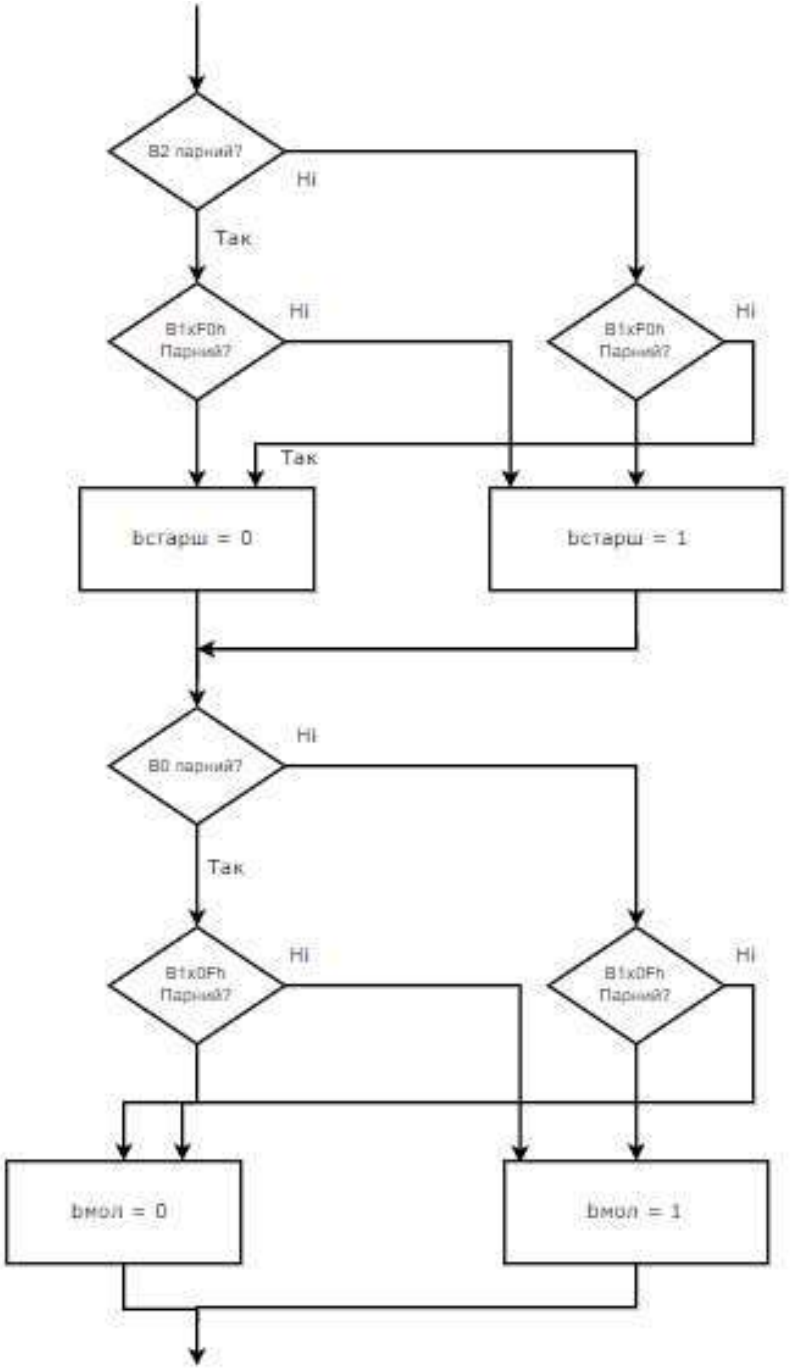


Рисунок 6.3 — Алгоритм визначення бітів парності

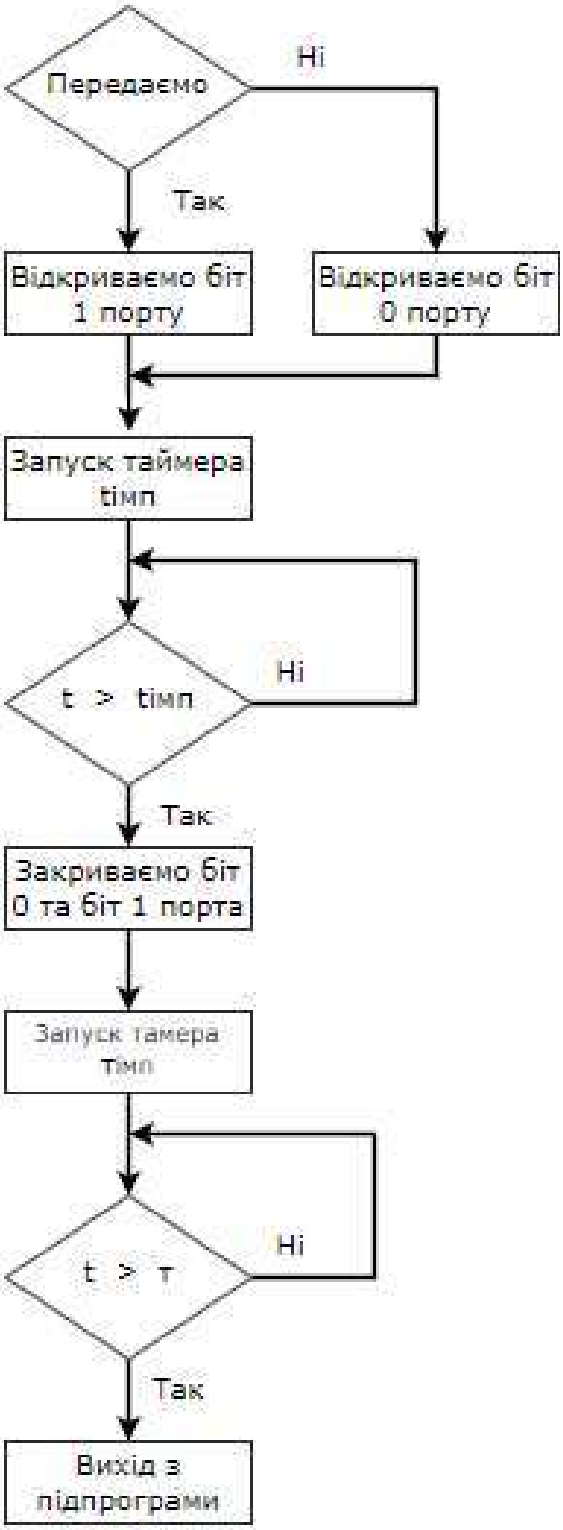


Рисунок 6.4 — Алгоритм підпрограми передачі байта

ВИСНОВКИ

В роботі проведено аналіз можливості використання біометричних сканерів як виконавчих елементів систем контроля доступу для вже введених в експлуатацію об’єктів, їх подальша експлуатація в системі разом з новітніми пристроями, зокрема з контролерами віддаленого доступу, в яких використовується новий інтерфейс обміну даними Wiegand, розроблено новий алгоритм, за допомогою якого формуються та в подальшому програмуються параметри цифрового потоку.

Для різних пристроїв коди можуть відрізнятися. Підхід, який реалізовано в алгоритмі, завдяки заміні параметрів цифрового потоку, дозволить управляти будь-яким пристроєм.

Для реалізації вимог технічного завдання в дипломній роботі були задані параметри, що відповідають інтерфейсу обміну даними Wiegand.

Зважаючи на те, що інтерфейс обміну достатньо новий, стандартних апаратних рішень немає, реалізація можлива з використанням програмно-апаратних засобів.

Система може бути впроваджена на об’єктах зв’язку для розширення функціоналу та зменшення витрат на технічну підтримку роботоздатності мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Посібник з біометрії / Р. М. Болл, Дж. Х. Коннел [та ін.]. — Москва : Техносфера, 2007. — 15 - 70 с.
2. Повне внутрішнє відбиття [Електронний ресурс]. — Режим доступу: https://en.wikipedia.org/wiki/Total_internal_reflection
3. Сканери відбитків пальців. Класифікація та реалізація [Електронний ресурс]. — Режим доступу: https://habr.com/ru/post/116458/
4. Сканери відбитків пальців. Класифікація та реалізація [Електронний ресурс]. — Режим доступу: https://www.argov.com/en/research-and-events/article/new-fingerprint-sensors-work
5. Офтальмология: Учебник для студ. мед. вузов / Е. А. Егоров. — Москва: ГЭОТАР-Медиа, 2008. — 240 с
6. Anil Jain, Arun A. Ross, Karthik Nandakumar/ Chapter 4 Iris Recognition. Introduction to Biometrics. — Springer Science & Business Media, 2011. — P. 141 - 175. — 276 p.
7. Аутентифікація по сітківці ока [Електронний ресурс]. — Режим доступу: https://en.wikipedia.org/wiki/Retinal_scan
8. Сучасні методи біометричної ідентифікації [Електронний ресурс]. — Режим доступу: https://www.azone-it.ru/sovremennye-metody-biometricheskoy-identifikacii
9. ANSI INCITS 378-2004 [Електронний ресурс]. — Режим доступу: https://webstore.ansi.org/Standards/INCITS/ansiincits3782004
10. Построение алгоритма распознавание отпечатков пальцев для системы контроля доступа / Омри Карим. [Електронний ресурс]. — Режим доступу: https://cyberleninka.ru/article/n/postroenme-algoritma-raspoznavaniya-otpechatkov-paltsev-dlya-sistemy-kontrolya-dostupa
11. What’s the Difference Between Match-on-Host and Match-in-Sensor Fingerprint Authentication? [Електронний ресурс]. — Режим доступу: https://www.electronicdesign.com/technologies/embedded-

revolution/article/21801072/whats-the-difference-between-matchonhost-and-matchinsensor-fingerprint-authentication

12. Контроль доступа по отпечатку пальца [Електронний ресурс]. — Режим доступу: https://lesson.iarduino.ru/page/urok-28-kontrol-dostupa-po-otpechatku-palca/
13. Arduino Uno R3. [Електронний ресурс]. — Режим доступу: https://iarduino.ru/shop/boards/dccduino-uno-r3.html
14. Зумер. [Електронний ресурс]. — Режим доступу: https://iarduino.ru/shop/Expansion-payments/zummer-trema-modul.html
15. Shield. [Електронний ресурс]. — Режим доступу: https://iarduino.ru/shop/Expansion-payments/trema-shield.html

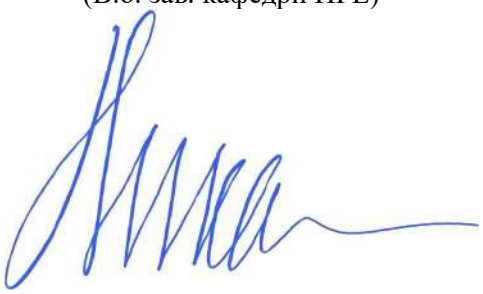
ДОДАТОК А. ТЕХНІЧНЕ ЗАВДАННЯ

ПОГОДЖЕНО

Доц.к.т.н. Сушко І. О.
(керівник)

ЗАТВЕРДЖЕНО

д.т.н., проф. Степанов М. М.
(В.о. зав. кафедри ПРЕ)



ТЕХНІЧНЕ ЗАВДАННЯ

НА ДИПЛОМНИЙ ПРОЄКТ

«Біометрична система контролю доступу»

Київ – 2022 року

1. НАЗВА І ПІДСТАВА ДЛЯ ВИКОНАННЯ

Назва дипломного проєкту «Біометрична система контролю доступу»

Підставою для виконання є завдання, видане кафедрою прикладної радіоелектроніки від «01» травня 2022 року

2 ВИКОНАВЕЦЬ

Виконавець — студент групи РА-81 Кириленко Олександр Анатолійович.

3 МЕТА ВИКОНАННЯ ДР І ПРИЗНАЧЕННЯ СИСТЕМИ

Метою дипломної роботи є аналіз існуючих практичних рішень контролю доступу на об’єкти, можливість застосування біометричних сканерів для підвищення рівня контролю та інтерфейсу Weagand для можливості підключення контролеру віддаленого доступу; розробка алгоритму обміну даними між виконавчими елементами Систем контролю та управління доступом та контролерами віддаленого боступу з інтерфейсом Wiegand.

4 ТЕХНІЧНІ ВИМОГИ

Система повинна :

Забезпечити роботу з біометричними датчиками, іншими пристроями різних елементів сигналізації.

Забезпечити можливість обміну даними між кінцевими виконавчими пристроями та контролером віддаленого доступу з використанням інтерфейсу Wiegand 26.

Забезпечити надійність системи та оптимальний рівень витрат.

Використати існуючу елементну базу.

Забезпечити можливість підключення контролерів віддаленого доступу.

5 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація оформлюється згідно ДСТУ 3008:2005.

Документація має містити:

технічне завдання, Пояснювальну записку, структурну схему, приклад програмних кодів.

6 ОРІЄНТОВНИЙ ЗМІСТ ДИПЛОМНОЇ РОБОТИ

- Титульний лист
- Завдання на дипломну роботу
- Зміст
- Актуальність проблеми
- Вступ

1. Огляд існуючих методів біометричної аутентифікації.
2. Огляд аналогів пристроїв біометричної ідентифікації
3. Загальні відомості про біомерію відбитків пальців
4. Вибір та опис елементів збірки
5. Розробка системи
6. Розробка алгоритму

- Висновки
- Перелік посилань
- Додаток А Технічне завдання
- Додаток Б Структурна схема
- Додаток В Код програми

7 ЕТАПИ ВИКОНАННЯ ДИПЛОМНОЇ РОБОТИ

Дипломна робота виконується в 5 етапів.

Таблиця 1 – етапи Дипломної роботи

№	Назві етапу	Термін виконання	Форма звітності
1	Актуальність тематики	2.05.22 – 13.05.22	Розділ 1
2	Огляд існуючих рішень	14.05.22 – 18.05.22	Розділ 2
3	Загальні відомості про біометрію відбитків пальців	19.05.22 – 29.05.22	Розділ 3
4	Вибір та обгрунтування елементів системи	30.05.22 – 6.06.22	Розділ 4

Таблиця 1 – етапи Дипломної роботи

5	Розробка системи	7.06.22 – 10.06.22	Розділ 5
6	Розробка алгоритму управління	11.06.22 – 12.06.22	Розділ 6

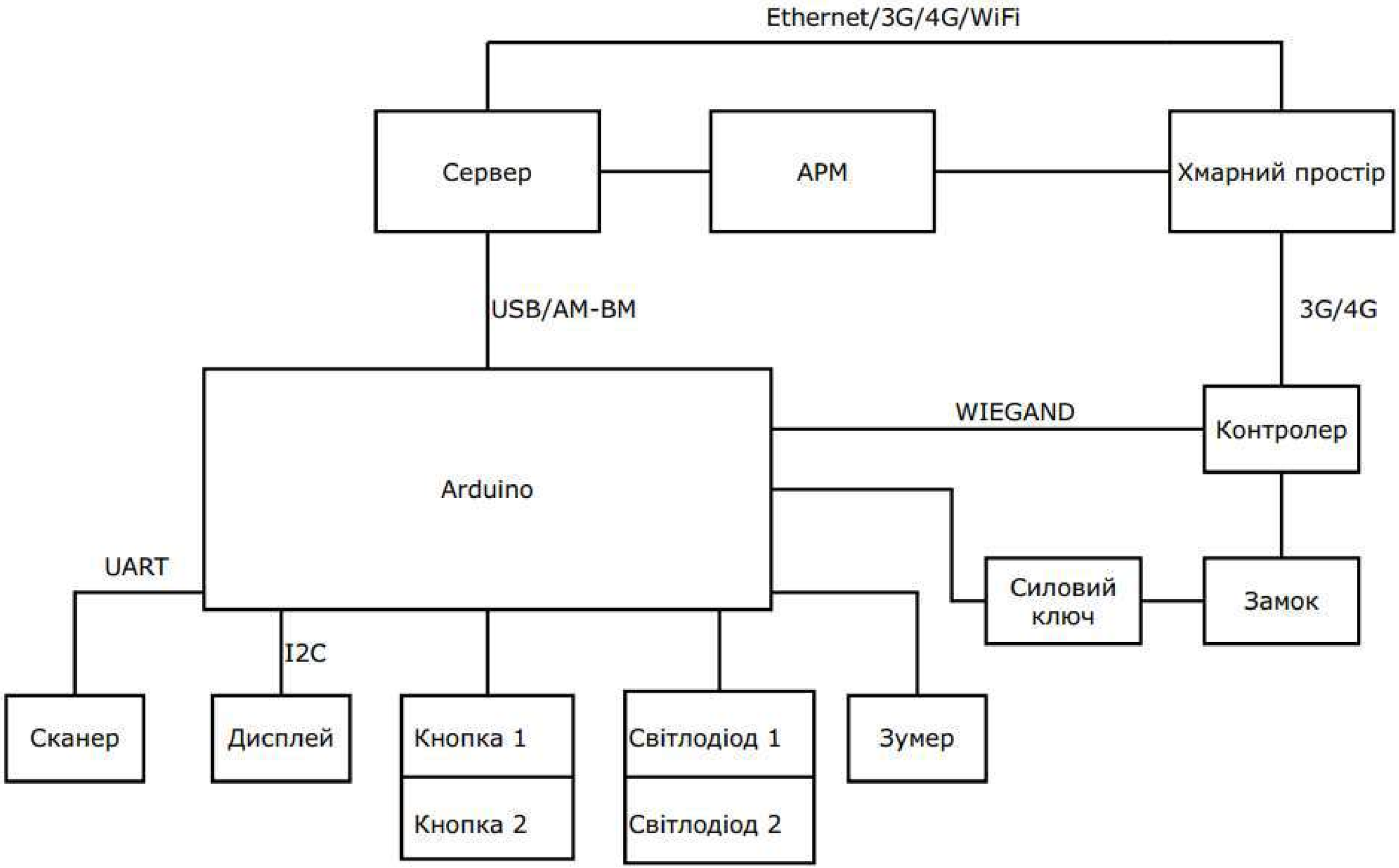
8. ПОРЯДОК ПРИЙМАННЯ ДИПЛОМНОЇ РОБОТИ І МАТЕРІАЛИ, ЯКІ ПОДАЮТЬСЯ ПІД ЧАС ЗАКІНЧЕННЯ ЕТАПІВ І ДИПЛОМНОЇ РОБОТИ ВЦІЛОМУ

Матеріали, які є проміжними, подаються у вигляді розділів дипломної роботи на перевірку в зазначені терміни. Після закінчення виконання дипломна робота представляється та захищається комісії.

Виконавець — Кириленко О.А.

Керівник — доц.к.т.н. Сушко І.О.

ДОДАТОК Б. СТРУКТУРНА СХЕМА ПИСТРОЮ


Ethernet/3G/4G/WiFi
Сервер
APM
Хмарний простір
USB/AM-BM
3G/4G
Arduino
WIEGAND
Контролер
UART
I2C
Силовий ключ
Замок
Сканер
Дисплей
Кнопка 1
Кнопка 2
Світлодіод 1
Світлодіод 2
Зумер