Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Мікропроцесорна система безконтактної ідентифікації персоналу з шифруванням даних

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав: студент 2 курсу, групи 1КІ-21м
спеціальності 123 – комп'ютерна інженерія
_____ Лизогуб Д.В.
Керівник к.т.н., доц. каф. ОТ
_____ Крупельницький Л. В.
"15" 12 2022 р.
Опонент к.т.н., доц. каф. ПЗ
_____ Коваленко О.О.
"16" 12 2022 р.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.
_____
"19" 12 2022 р.

ВНТУ 2022

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітній рівень – магістр
Спеціальність – 123 Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
обчислювальної техніки
_____ д.т.н., проф. О.Д. Азаров
"15" 09 2022 р.

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту **Лизогубу Денису Володимировичу**

1 Тема роботи «Мікропроцесорна система безконтактної ідентифікації персоналу з шифруванням даних» керівник роботи __Крупельницький Леонід Віталійович к.т.н. доцент, затверджено наказом вищого навчального закладу від "_15_"___09___2022 року№_205-А_

2 Строк подання студентом роботи __19.12.2022____

3 Вихідні дані до роботи: робоча частота — 13,56МГц; спосіб ідентифікації — карта з контролером; відстань спрацювання до 60мм; діапазон робочих температур від мінус 30°С до 70°С; розміри не більше 80х60х35 мм; конструкція — окремий модуль; живлення напругою від 12 до 24 В та сила струму 0.15А.

4 Зміст розрахунково-пояснювальної записки: (перелік питань, які потрібно вирішити) вступ; аналіз сучасних систем безконтактної ідентифікації; методи захисту авторизації; аналіз підходів побудови мікропроцесорних систем; розробка програмного забезпечення;

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): функціональна схема; алгоритм роботи; схема електрично принципова; перелік елементів, зовнішній вигляд пристрою.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1 – Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-5	Крупельницький Л.В., доц., к.т.н. каф ОТ		
6	Небава М.І. к.е.н., професор кафедри ЕПВМ		

7 Дата видачі завдання 24.09.2022
8 Календарний план наведено в таблиці 2

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі	24.09	вик
2	Аналіз завдання	27.09	вик
3	Розробка технічного завдання	28.09	вик
4	Аналіз аналогів	1.10	вик
5	Систематизація та вибір методів безконтактної ідентифікації	5.10	вик
6	Аналіз вразливостей та методів захисту	10.10	вик
7	Розробка функціональної схеми та алгоритму роботи пристрою керування та ідентифікації	15.10	вик
8	Розробка мікропроцесорної системи	17.10	вик
9	Розробка програмного забезпечення	25.10	вик
10	Аналіз економічної доцільності	26.10	вик
11	Аналіз виконання ТЗ, висновки	2.11	вик
12	Попередній захист ДП	22.11	вик

Студент _____ Лизогуб Д.В.

Керівник роботи _____ к.т.н., доц. каф. ОТ Крупельницький Л.В.

УДК 004.9

Лизогуб Д.В. Мікропроцесорна система безконтактної ідентифікації персоналу з додатковим шифруванням. Магістерська кваліфікаційна робота зі спеціальності 123 — Комп'ютерна Інженерія, Вінниця: ВНТУ, 2022, 95 с.

На укр.мові. Бібліогр.: 29 назв; рис.: 33 ; табл. 6

В роботі проаналізовано способи безконтактної ідентифікації та обрано найбільш оптимальні методи допуску. Розглянуто сучасні системи та на основі аналізу аналогів сформульовано параметри для кращого рішення.

Розглянуто вразливості сучасних систем та запропоновано методу підвищення захищеності.

Обрано мікропроцесорну платформу та розроблено алгоритми роботи. Скомпоновано електронні елементи, створено схему електричну принципову, розроблено друковану плату та програмне забезпечення для пристрою.

Проведено економічний аналіз для підтвердження економічної вигоди та доцільності розробки.

ABSTRACT

Lyzohub D.V. Microprocessor system of non-contact personnel identification with additional encryption. Master's thesis on specialty 123 — Computer Engineering, Vinnytsia: VNTU, 2022, 95 p.

In the Ukrainian language. Bibliography: 29 titles; Fig.: 33; table 6

The paper analyzed methods of contactless identification and selected the most optimal methods of admission. Modern systems are considered and parameters for a better solution are formulated based on the analysis of analogues.

Vulnerabilities of modern systems are considered and a method of increasing security is proposed.

A microprocessor platform was chosen and work algorithms were developed. Electronic elements were assembled, an electrical schematic diagram was created, a printed circuit board and software for the device were developed.

An economic analysis was conducted to confirm the economic benefit and feasibility of the development.

ЗМІСТ

ВСТУП

Важливою частиною організації є безпека персоналу та її інформації. Тому, практично в кожній компаній реалізовано пункти пропуску щоб запобігти доступу сторонніх осіб. З розвитком технологій, такий важливий але досить простий процес стало можливим автоматизувати. Використання комп'ютерів замість людей підвищує надійність та виключає людський фактор. Автоматизована система дозволяє реалізувати надійну та швидку ідентифікацію, зберігати данні про активність користувачів чи повідомляти про помилки або спроби несанкціонованого доступу.

В сучасних системах застосовується або біометрична або радіочастотна ідентифікація з використанням технології RFID. Обидва способи ідентифікації мають свої переваги та недоліки, тому однаково часто зустрічаються в системах обмеження або розмежування доступу.

В процесі розробки було опрацьовано значний теоретичний матеріал в напрямку реалізації мікропроцесорних систем такими закордонними та вітчизняними науковцями, як S. Jeevananthan, N. Senthil Kumar, Cornel Turcu, M. Saravanan, Хунянь Кан, Крупельницький Л. В., Кінзерський В. О., Азаров О. Д., Трояновська Т. І., Цирульник С. М. [1– 4].

Разом зі стрімким розвитком технологій, зловмисники розробляють засоби та вивчають можливості для несанкціонованого доступу. Тому компанії, що встановили більш дешеві системи, є ціллю для зловмисників. Додатковою проблемою є робота при довготривалому вимкненні електрики. Системи, що використовують базу даних на комп'ютерах, стали дуже вразливими, оскільки акумуляторні батареї не здатні забезпечити довготривалу роботу енергоємних пристроїв. Отже, є актуальною розробка системи, яка вирішить всі проблеми сучасних реалізацій та дозволить компаніям підвищити власний захист і автономність на вже встановлених системах.

Метою роботи є створення мікропроцесорної системи безконтактної ідентифікації, що дозволяє ідентифікувати персонал з можливістю працювати

без бази даних на час її відсутності та з використанням RFID-карти із захистом від копіювання.

Щоб досягнути цілі роботи, необхідно вирішити такі **задачі**:

- розглянути існуючі системи безконтактної ідентифікації;
- спроектувати структуру системи безконтактної ідентифікації;
- виготовити плату та схему системи безконтактної ідентифікації;
- розробити програмний код для системи;
- реалізувати метод, що дозволить зробити картку захищеною від копіювання;
- провести тестування розробленого пристрою.

Наукова новизна дослідження – підвищено рівень захисту в методах авторизації персоналу з використанням технології RFID за рахунок додаткового шифрування унікальних даних користувача, що безпосередньо зберігаються на електронній картці.

Практична цінність – реалізація запропонованого способу дозволила підвищити рівень безпеки авторизації без додаткових витрат на оновлення апаратного забезпечення та використання системи без встановлення сервера з базою даних. Це також дозволяє створити енергонезалежний пункт пропуску без підключення до мережі Інтернет.

Об’єктом дослідження є процес реалізації новітніх мікропроцесорних систем для ідентифікації користувачів.

Предметом дослідження є розробка захищеної мікропроцесорної системи для безконтактної ідентифікації персоналу.

Апробацію досліджень виконано на L науково-технічній конференції НТКП ВНТУ (м. Вінниця, 2021).

Публікації. Згідно із результатами досліджень, проведених в МКР, було опубліковано тези доповіді: повний опис [5].

1 ОГЛЯД ТА АНАЛІЗ СУЧАСНИХ СИСТЕМ БЕЗКОНТАКТНОЇ ІДЕНТИФІКАЦІЇ

1.1 Огляд систем безконтактної ідентифікації

Досягнення сучасної науки і техніки призвели до широкого використання багатьох електронних систем. Багато з них призначені для виконання монотонних, рутинних, але важливих операцій авторизації, контролю та збору інформації про отримані результати.

Як відомо, основним завданням функціонування автоматизованих систем є забезпечення абсолютної достовірності інформації. Зрештою, навіть пошук і відсіювання неправильно введеної інформації у великих наборах даних забирає багато часу та грошей, не кажучи вже про можливі негайні збитки, які можуть виникнути внаслідок неправильних рішень на її основі. Технологія безконтактної ідентифікації найкраще відповідає всім вимогам комп’ютеризованих систем управління, де об’єкти та дозволи необхідно ідентифікувати та реєструвати в режимі реального часу. Безконтактне розпізнавання загалом означає можливість достовірної ідентифікації об'єктів за окремими природно або штучно присвоєними ознаками без безпосереднього контакту з об'єктом.

Для захисту будь-якого об'єкта існує кілька рубежів. В кожному з випадків є важливою система управління і контролю доступу. СКУД, що доступні на ринку дають змогу вирішувати ряд актуальних задач, а саме протидіяти розкраданню, промисловому шпигунству та саботажу. Запобігають навмисному пошкодженню матеріальних цінностей, захищають конфіденційну інформацію та регулюють потік відвідувачів

СКУД являє собою згруповані в комплекси електронні, механічні, апаратно-програмні, електротехнічні та інші засоби, що дозволяють доступ конкретних осіб в визначені зони або до певних, технічних засобів і предметів. СКУД контролюють доступ осіб, яким не надано на це права. Дані системи здійснюють контроль переміщення персоналу і транспорту по території, що

охороняється. Також вони забезпечують безпеку персоналу і відвідувачів та матеріальні та інформаційні ресурси компанії

Структура СКУД відображена на рисунку 1.1. Не зважаючи на особливість кожної системи контролю доступу, вона містить три базові елементи: користувацький ідентифікатор, пристрій ідентифікації, керуючий контролер і виконавчі пристрої.

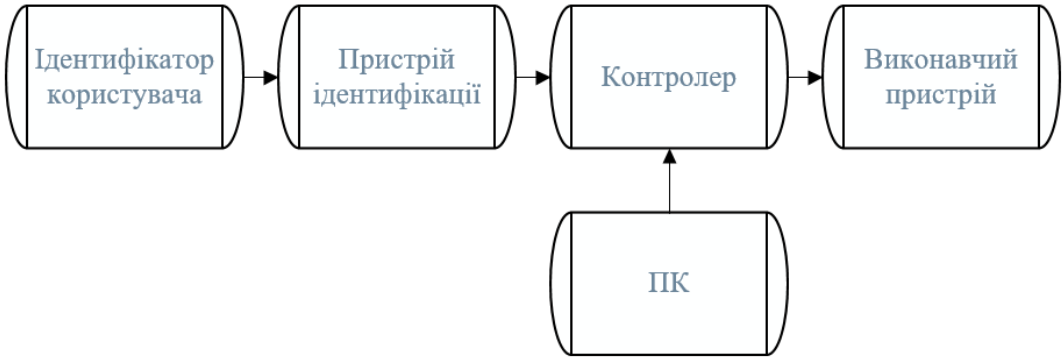


Рисунок 1.1 — Загальна схема систем контролю

Спрощену форму функціональності СКУД можна описати наступним чином. Кожен співробітник або постійний відвідувач організації отримує ідентифікатор — пластикову картку або брелок з персональним кодом. Коди персональної «електронної картки» власника та його «електронного ключа» співвідносяться та вносяться до спеціально організованої комп’ютерної бази даних. На вході в будівлю встановлені картрідери, які зчитують код картки та інформацію про права доступу власника картки та передають цю інформацію системному контролеру. Контролер відкриває або блокує двері, переводить кімнату в безпечний режим і активує сигнал тривоги. Усі факти про видачу картки та відповідні дії записуються в контролер і зберігаються в комп’ютері. Атрибути та біометричні ідентифікатори використовуються для ідентифікації в рамках EMS. В якості ідентифікаторів використовуйте в'їзні знаки, магнітні картки, безконтактні картки, сенсорні брелоки з пам'яттю, різноманітні радіоключі, автономні носії біометричних зображень. Всі ідентифікатори

унікальні та закодовані двійковим кодом. Кожному коду відповідає інформація про права і привілеї користувача [6].

Реалізація автоматизованого розпізнавання об'єктів досить стара. Зустрічаються п’ять основних різновидів ідентифікації, що наведені на рисунку 1.2:

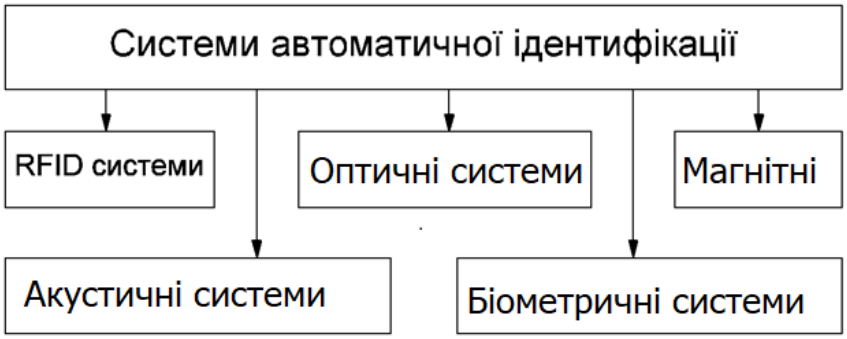


Рисунок 1.2 — Різновиди ідентифікації

Зчитувач RFID — це стаціонарний або мобільний пристрій захоплення даних, який генерує електромагнітне поле для запуску та захоплення відповіді даних із закодованої мітки, присутньої у визначеній зоні опитування. Пасивні мітки, що активуються зчитувачем, використовують потужність, отриману від електромагнітного поля зчитувача RFID, для передачі своїх даних назад на зчитувач. Батарейні або напівпасивні мітки використовують батареї для роботи мікрочіпа та вбудованих датчиків температури, вібрації та інших датчиків. Вони мають довший діапазон читання, ніж пасивні теги. Активні теги, що живляться від батареї, передають дані назад до зчитувачів у їхній мережі під час активації або в заздалегідь визначений час[7].

RFID може бути застосований для автоматизації та ідентифікації в різноманітних системах, наприклад:

— керування доступом;
— відстеження товарів;
— стеження тваринами;
— стягнення та безконтактна оплата;

— електронні проїзні документи;

— smartdust — для масово розподілених сенсорних мереж;

— відстеження товарів для перевірки автентичності;

— логістика відстеження багажу в аеропорту;

Принцип оптичної карти пам'яті такий же, як і CD-ROM і CD-ROM. Для зберігання інформації на карті кріпиться позолочена лазерна панель. Матеріал, який використовується для цієї панелі, складається з кількох шарів, які активуються при попаданні на них лазерного променя. Лазер пропалює невеликий отвір у цьому матеріалі, який потім використовується в процесі зчитування. Наявність або відсутність такої вигорілої точки означає «одиницю» або «нуль». Оптична карта може зберігати від 4 до 6,6 Мб інформації [8].

Біометрія — це ідентифікація людини за її унікальними біологічними характеристиками. Біометрична ідентифікація передбачає використання індивідуальних характеристик людини — біометричних ідентифікаторів: відбитків пальців, геометрії рук, малюнків райдужних оболонок і судин, сітківки очей, теплових зображень облич, динаміки підписів, спектральних параметрів мови. Базові типи біометричної ідентифікації відображені на рисунку 1.3.

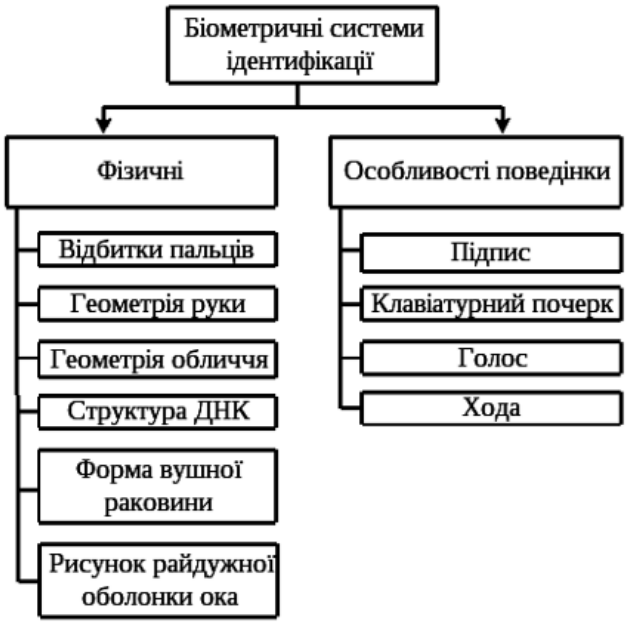


Рисунок 1.3 — Види біометричної ідентифікації

Сучасні системи використовують більше десяти різних біометричних ознак. До того ж для найпоширеніших з них, таких як дактилоскопія і райдужна оболонка ока, реалізовані безліч різноманітних за принципом дії сканерів. Таким чином існує велика різноманітність вибору для реалізації систем контролю з використанням біометричної ідентифікації.

Біометричні технології зарекомендували себе як системи з найвищою надійністю. Проте зловмисники виявили деякі вразливості і оприлюднили декілька способів обману. До прикладу, необхідні відбитки пальців можуть бути скопійовані на плівку або до сканера може бути піднесена велика фотографія пальця зареєстрованого користувача. Однак, під час розробки сучасних пристроїв ці вразливості були виправлені, тому можливість несанкціонованого доступу шляхом обману біометричних сканерів залишається практично неможливою[9].

Головним недоліком біометричної ідентифікації стає коштовність устаткування. Оскільки для кожного комп’ютера, що включений до даної системи, потрібно придбати власний сканер. Необхідно також зазначити, що дешеві сканери мають малий строк роботи. До того ж, вони мають високий відсоток помилок другого роду. Тобто користувач, що зареєстрований, може бути ідентифікований як незареєстрований. Тому, перед компаніями стоїть дилема стосовно вибору пристрою, оскільки на ринку доступні більш дороговартісні з високим ступенем захисту та терміном експлуатації і більш дешевші але з періодичними помилками.

Біометрія стає все більш популярною в корпоративних системах безпеки, смартфонах та інших електронних пристроях. Окрім високого рівня безпеки використання біометричних сканерів, розвиток біометричних технологій також виграв від простоти використання, оскільки не потрібно використовувати багато паролів для різних типів пристроїв, які можна легко забути та розкрити.

Питання пропускної здатності біометричних систем контролю доступу є дуже актуальним. Через дуже велику кількість даних, які аналізуються читачами, навіть простий пошук у базі даних займає значну кількість часу. Щоб скоротити

час аналізу, біометричні зчитувачі зазвичай мають додаткову вбудовану клавіатуру, на якій користувач вводить персональний код доступу перед початком біометричного процесу. Принадність біометричної системи контролю доступу також полягає в тому, що вона не ідентифікує об’єкт, а саму людину[10].

1.2 Огляд систем радіочастотної ідентифікації

Безконтактна ідентифікація — забезпечується технічними засобами, організаційними заходами, серією дій, ідентифікація без використання клавіатури та збір даних безпосередньо в комп'ютер. Ця технологія найбільш повно відповідає всім вимогам комп'ютерних систем управління, які вимагають ідентифікації та реєстрації об'єктів і дозволів в режимі реального часу.

У сучасних системах контролю доступу одним із найпопулярніших методів ідентифікації є доступ через смартфон. Безпека та простота використання — головні переваги мобільного доступу до СКУД. Смартфони мають такі функції, як багатофакторна аутентифікація та розблокування відбитків пальців, що робить цей метод ідентифікації досить надійним. Зі зручністю все під рукою — вам більше не потрібно переносити картки доступу з одного одягу на інший — просто тримайте свій смартфон при собі. Проте мобільна ідентифікація часто використовується як доповнення до традиційного карткового доступу: одні використовують картки, інші — смартфони [11].

RFID — це використання бездротової безконтактної системи, яка використовує радіочастотні електромагнітні поля для передачі даних із мітки, прикріпленої до об’єкта, з метою автоматичної ідентифікації та відстеження. Деякі мітки не потребують батареї та живляться від електромагнітних полів, які використовуються для їх зчитування. Інші використовують локальне джерело живлення та випромінюють радіохвилі. Мітка містить збережену в електронному вигляді інформацію, яку можна зчитувати на відстані до кількох метрів. На відміну від штрих-коду, тег не обов’язково повинен знаходитися в межах прямої видимості зчитувача і може бути вбудований у відстежуваний об’єкт. Тег можна прочитати, якщо пройти поруч із зчитувачем, навіть якщо він закритий об’єктом

або невидимий. Його можна зчитувати в футлярі, коробці чи іншому контейнері, і на відміну від штрих-кодів, RFID-мітки можна зчитувати сотні одночасно.

Система радіочастотної ідентифікації використовує теги або ярлики, прикріплені до об'єктів, які потрібно ідентифікувати. Двосторонні радіопередавачі-приймачі, що являються запитувачами або зчитувачами, посилають сигнал до мітки та зчитують її відповідь. Зчитувачі зазвичай передають свої спостереження в комп’ютерну систему, на якій працює спеціалізоване програмне забезпечення.

Інформація мітки зберігається в електронному вигляді в енергонезалежній пам'яті. Мітка RFID містить невеликий радіочастотний передавач і приймач. Зчитувач RFID передає закодований радіосигнал для опитування мітки. Тег отримує повідомлення та відповідає своєю ідентифікаційною інформацією. Це може бути лише унікальний серійний номер пристрою або може бути пов’язана з продуктом інформація, номер запасу, чи партії, дата виробництва чи інша конкретна інформація[12].

RFID-мітки можуть бути пасивними, активними або пасивними з акумулятором. Активний тег має бортовий акумулятор, який періодично передає свій ідентифікаційний сигнал. Пасивний пристрій має маленьку батарею на борту, яка активується за наявності зчитувача RFID. Пасивний тег дешевший і менший, оскільки не має елемента живлення. Натомість тег використовує радіоенергію, яку передає зчитувач, як джерело енергії. Запитувач має бути близько, щоб радіочастотне поле було достатньо високим, щоб передати достатню потужність до мітки. Оскільки мітки мають індивідуальні серійні номери, конструкція системи RFID може розрізняти кілька міток, які можуть бути в радіусі зчитування RFID, і зчитувати їх одночасно.

Теги можуть бути лише для читання, маючи присвоєний на заводі серійний номер, який використовується як ключ до бази даних, або можуть бути для читання та запису, де дані об’єкта можуть бути записані в тег системним користувачем. Теги, що програмуються полями, можуть бути одноразового

запису, багаторазового читання, а теги без внесеної інформації можуть бути заповнені користувачем з електронним кодом продукту.

Транспондер містить змінну або записувану пам'ять і засіб реагування на переданий запитувальний сигнал для обробки сигналу та вибіркового запису даних у пам'ять або зчитування даних із пам'яті. Мітки RFID містять принаймні дві частини: інтегральну схему для зберігання та обробки інформації, модуляції та демодуляції радіочастотного сигналу, збору живлення постійного струму від сигналу зчитувача, що потрапляє, та інших спеціалізованих функцій і антену для прийому і передачі сигналу.

Стаціонарні зчитувачі налаштовані для створення спеціальної зони опитування, яку можна жорстко контролювати. Це дозволяє чітко окреслити область зчитування, коли мітки входять і виходять із зони опитування. Мобільні зчитувальні пристрої можуть бути ручними або встановленими на візках чи транспортних засобах. Передача сигналів між зчитувачем і тегом здійснюється декількома різними несумісними способами залежно від діапазону частот, який використовує тег. Мітки, що працюють на НЧ і ВЧ, за довжиною радіохвилі знаходяться дуже близько до антени зчитувача, менш ніж на одну довжину хвилі. У цій області ближнього поля тег тісно електрично пов’язаний із передавачем у зчитувальному пристрої. Тег може модулювати поле, яке створює зчитувач, змінюючи електричне навантаження, яке представляє тег. Перемикаючись між нижчими та вищими відносними навантаженнями, тег створює зміни, які читач може виявити. На УВЧ та вищих частотах тег становить більше ніж одну довжину радіохвилі від зчитувача. Активні мітки можуть містити функціонально розділені передавачі та приймачі, і мітка не повинна відповідати на частоті, пов’язаній із сигналом запиту зчитувача. На ринку доступні декілька видів систем для радіочастотної ідентифікації поділених за частотним діапазоном, детальні дані наведені в таблиці 1.1[13].

Електронний код продукту — це один з поширених типів даних, що зберігаються в тегу. Пристрій містить певну кількість біт, що є унікальним серійним номером для певного тегу. Загальний електронний код продукту можна

використовувати як ключ до глобальної бази даних для унікальної ідентифікації конкретного продукту, як URL-адресу.

Таблиця 1.1 — Частотні діапазони RFID

Частотний діапазон	Відстань	Швидкість даних	Примітка
120-150 кГц	10 см	Повільно	Ідентифікація тварин та збір даних на промислових об’єктах
13.56 МГц	1 м	Середня	Розумні електронні картки
433 МГц	1-100 м	Середня	Рішення для захисту з активними тегами
868-870 МГц 902-928 МГц	1-2 м	Між середньою та високою	Має різні стандарти
2450 МГц 5800 МГц	1-2 м	Висока	802.11 WLAN, Bluetooth стандарти
3.1 ГГц -10 ГГц (мікрохвилі)	до 200 м	Висока	Вимагає напівактивні або активні теги

Часто кілька тегів реагують на зчитувач, наприклад, багато окремих продуктів із тегами можуть бути відправлені в загальній коробці або на спільному піддоні. Виявлення колізій є важливим для зчитування даних. Два різних типи протоколів використовуються для відокремлення певного тегу, що дозволяє зчитувати його дані серед багатьох подібних тегів. У системі авторизації зчитувач транслює команду ініціалізації та параметр, який теги окремо використовують для псевдовипадкової затримки своїх відповідей. При використанні протоколу адаптивного бінарного дерева зчитувач надсилає символ ініціалізації, а потім передає по одному біту ідентифікаційних даних, тому лише теги з відповідними наборами бітів відповідають, і зрештою лише один тег відповідає повному рядку ідентифікації.

1.3 Аналіз відомих аналогів

Технічно системи іноді можуть сильно відрізнятися за розпізнаванням обличчя, але всі вони мають приблизно однакові принципи роботи. Продуманий підхід до реалізації безконтактної ідентифікації дозволяє різними способами контролювати доступ зареєстрованих користувачів. Загальною функцією є перевірка наявності прочитаних даних у базі даних, яка була раніше заповнена адміністратором. Оскільки використання окремого сервера з базою даних дуже дороге, біометрія не може бути конкурентом за ціною. Ще одним недоліком біометрії є можливість некоректного та тривалого зчитування та заборона доступу зареєстрованим користувачам. Сканери також потрібно часто підтримувати в чистоті, оскільки це має вирішальне значення для належної роботи пристрою. Для підключення такої системи управління потрібно використовувати багато модулів і заповнювати базу користувачів. Якщо контрольні точки повторюються, на кожній контрольній точці необхідно виконати однакові дії.

RFID-мітки стійкі до впливу навколишнього середовища. Існують деякі RFID-мітки з більшою міцністю та стійкістю до важких умов робочого середовища. У програмах, де один і той же об’єкт можна використовувати необмежену кількість разів, RFID-мітка здається більш прийнятною формою ідентифікації, оскільки її не потрібно розміщувати на видному місці. Пасивні RFID-мітки мають практично необмежений термін служби. Мікросхеми RFID передають інформацію в діапазоні радіочастот на зчитувальний пристрій або сканер, тому при використанні технології RFID навіть чіпи з нейтральним покриттям, наприклад вбудовані в корпус виробу або вшиті в одяг, можуть бути зчитані за допомогою інформації, що кодує сканер.

Контролер із вбудованим зчитувачем Mifare вологостійкий ATIS ACPR-07 MF-W (рис. 1.4) призначений для організації контролю доступу через одну точку доступу. Встановлюється для організації доступу в офіс або житлове приміщення. Контролер взаємодіє з картками, брелоками та браслетами та іншими підтримуваними ідентифікаторами стандарту Mifare.

Пристрій має міцний корпус із захистом від пилу та вологи за стандартом IP66. Діапазон робочих температур: -10°C ~ +60°C. Кріпиться на будь-якій плоскій поверхні та забезпечує легкий доступ до карток або брелоків. Система RFID складається з трьох основних компонентів: зчитувача або сканера, мітки та комп’ютеризованої системи обробки даних. Зчитувач підключається за допомогою радіозв'язку, отримує дані з мітки і відправляє отриману інформацію в базу даних. Зчитувач має трансивер і антену, яка посилає сигнал на тег і отримує відповідь, комп’ютерна система перевіряє та декодує дані та зберігає їх для подальшої передачі, якщо це необхідно. У комплект також входить 2 основні карти і панель управління [14].

Рисунок 1.4 — Зчитувач карт MIFARE

Наступним рішенням є пристрій від компанії Hikvision (рисунок 1.5). Система здатна підтримувати всі операційні системи. Для шифрування картами SAM окремо виділено два роз’єми. Частим рішенням є антена, що вмонтована в разом з приймачем і декодером, що утворює зчитувач, який здатний бути як переносним, так і стаціонарним. Розмір та форма антен можуть бути різні. Вони інтегруються в дверну коробку, для того щоб отримувати дані про користувача, що перетнула рамку сканування. Особливістю є здатність антени одночасно сканувати кілька міток, що перебувають в зоні її дії. Для зручності керування встановлено віддалене оновлення пристрою[15].

Рисунок 1.5 — Hikvision DS-K1F100-D8E

Автономний комплект доступу Tecsar Trek SA-TS22(рисунок 1.6) призначений для організації контролю доступу над однією точкою проходу та оснащений вбудованим зчитувачем. У комплекті контролер даної комплектації, зчитувач та 5 карток типу EM Marine. Налаштування та керування здійснюється за допомогою клавіатури на контролері. Є можливість підключення виносного зумера, що виконує роль дзвінка. Інформація про користувачів зберігається в енергонезалежній пам'яті контролера. Додаткова периферія підбирається індивідуально під масу дверей. Детальні технічні характеристики наведені в додатку [16].

Перевагами RFID-технології є можливість перезапису. Дані з RFID-мітки можуть записуватись і доповнюватися багато разів. Зчитувач RFID не потребує прямої видимості мітки для зчитування даних, а взаємна орієнтація мітки та зчитувача зазвичай не важлива. Теги прочитуються через матеріал, що робить можливим їх приховане розміщення. Для зчитування даних мітці достатньо хоча б ненадовго увійти в зону реєстрації і рухатися, в тому числі з досить високою швидкістю.

Рисунок 1.6 — Комплект доступу Tecsar Trek SA-TS22

Окрім функції носія даних, RFID-мітки також можна використовувати для інших завдань. Унікальний незмінний ідентифікаційний номер, присвоєний етикетці під час виробництва, гарантує високий ступінь захисту від підробок. Крім того, дані на мітці можуть бути зашифровані. Мітки RFID можуть закривати операції запису та зчитування даних за допомогою паролів і шифрувати їх передачу. Відкриті та закриті дані можуть зберігатися в тегу одночасно.

Карта Mifare — це безконтактний контролер в корпусі у вигляді карти. Такі карти є захищеними криптографічним ключем, тому скопіювати або підробити їх досить важко. Дана модифікаціє є більш дорогим аналогом карт EM-Marine, але надійно захищені з можливістю перезапису та використання в складних системах контролю та керування доступом.

Перевагою використання карт Mifare є безпека, можливість перезапису, захист від копіювання та підробки, можливість реалізувати складні сценарії роботи системи контролю та управління доступом. Однак більший ступінь захисту вимагає більше витрат на розробку, тому карти розроблені за новою технологією, є більш дорожчі ніж EM-Marine.

В сучасних системах контролю доступом застосовуються карти декількох типів. Існують наступні карти Mifare:

— MIFARE Classic — одна з найвідоміших карт із крипто-захистом, вона використовує алгоритм шифрування Crypto 1 та захищає дані;

— MIFARE Plus — в даній версії застосовується алгоритм AES який досі не був скомпрометований зловмисниками, ап еревагою карти є безпечний ідентифікатор який не можна скопіювати або ж підробити;

— MIFARE DESFire — дорогі карти захищені складними алгоритмами, якими користуються в системах контролю доступу NASA та інших організаціях з високим ступенем безпеки;

— MIFARE Ultralight — найпростіший тип карт, які бувають без криптографічного захисту або із захистом 3DES, який є досить надійним але повільним.

Високий рівень безпеки карток Mifare базується на тому, що зчитувач розпізнає не серійний номер картки, як це відбувається при використанні карток EM-Marine, а інформацію зі спеціального блоку пам'яті картки, який захищений криптоключем.

Наявність надійної карти не забезпечує відповідний ступінь захисту якщо зчитувач не переналаштувати на зчитування захищеного ідентифікатора, і він зчитує лише серійний номер. Серійний номер картки Mifare можна скопіювати і хоча це досить складно, на відміну від серійного коду карти EM-Marine. Тому, основною задачею є розробка системи яка буде використовувати всі переваги сучасних технологій для захищення даних.

Наступним недоліком систем є зв’язок між зчитувачем та контролером за протоколом Wiegand-26. Інтерфейс Wiegand-26 передає номери розміром 3 байти. Він використовується в СКУД, в яких як ідентифікатор використовуються карти EM-Marine. Оскільки номер картки Mifare займає 4 байти, останні цифри індивідуального номера не передаються. Через це у системі з'являються дублікати номерів, а рівень захисту знижується до карт EM-Marine.

Щоб уникнути цього, потрібно використовувати більш масштабні протоколи та інтерфейси, які дозволять повністю передавати номери, що складаються 4 і більше байт разом з додатковими параметрами.

Захищена карта Mifare — це ідеальний ідентифікатор для тих СКУД, де потрібно забезпечити високий захист від проникнення чужих осіб. Також Mifare використовується для побудови прогресивних систем контролю доступу — все завдяки тому, що ці карти можна адаптувати до складних багатовекторних сценаріїв.

1.4 Формулювання технічних вимог та задач

Можливості радіочастотної ідентифікації дають змогу застосувати її в розробці багатофункціональної системи контролю та управління доступом з можливістю управління, модернізації та інтегрування в інші системи.

В результаті аналізу сучасних систем виявлено ряд недоліків, що роблять систему не захищеною від несанкціонованого доступу, вразливою до відсутності з’єднання із сервером та ускладнюють організацію енергонезалежності. Також велика кількість систем мають обмеження щодо кількості зареєстрованих користувачів тим самим унеможлививши інтегрування в організації з великою кількістю персоналу чи навчальні заклади.

Тому, є актуальним покращення методу безконтактної ідентифікації на існуючій базі загальноприйнятих компонентів та розробка мікропроцесорної системи для допуску персоналу.

Для покращення методу безконтактної ідентифікації необхідно забезпечити додаткове шифрування даних із використанням завадостійкого інтерфейсу з високою пропускною здатністю. Щоб досягти результату необхідно виконати наступні вимоги:

— робоча частота 13,56 МГц;
— відстань зчитування карти до 7 см;
— тип карт Mifare Clasic;
— живлення 12 В;

— інтерфейс зв’язку між модулями CAN;

— протокол ISO 14443;

— мікроконтролер STM32f103;

— протокол шифрування Crypto1.

Запропонований метод повинен мати змогу покращити всі наявні системи контролю доступу, що містять зчитувачі здатні працювати з картами Mifare Clasic.

Розроблене обладнання не повинно обмежуватися кількістю користувачів, а передача даних буде здійснюватися через стабільний і стійкий до перешкод інтерфейс. Треба було розробити прототип зчитувача у вигляді невеликої дошки, яка буде розміщена в точці доступу разом з антеною. Програмування контролера повинно враховувати стандарти та алгоритми використання безконтактних карт Mifare Classic, а також впровадження нових методів. Програмний код має бути оптимізований за допомогою загальної мови C++ для досягнення швидкої та стабільної авторизації користувача. Щоб створити бібліотеку пристроїв, використано підхід об’єктно-орієнтованого програмування.

2 МЕТОДИ ТА СПОСОБИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ АВТОРИЗАЦІЇ

2.1 Аналіз актуальних способів та причин несанкціонованого доступу

Несанкціонований доступ (НСД) слід розуміти як отримання можливості обробляти дані, що зберігаються на різних носіях та накопичувачах, за допомогою самовільної зміни чи фальсифікації відповідних прав та повноважень. Подібне явище має місце, коли якась інформація призначена лише певному колу осіб, але існуюче обмеження порушується. НСД здійснюють за рахунок помилок, допущених контролюючою структурою або системою комп'ютерної безпеки, а також шляхом заміни документів, що засвідчують, або протиправного заволодіння інформацією про іншу особу, якій надано такий доступ.

Причини виникнення несанкціонованого доступу можуть бути такими:

— неправильно налаштована система контролю доступу до певних баз даних;

— прогалини у створенні захисту різних засобів авторизації. Це можуть бути паролі, що легко вгадуються, автоматичне збереження даних, що використовуються для авторизації в конкретній системі;

— використовується застаріле програмне забезпечення, з'являються помилки або конфлікти;

— відбувається зловживання довірою та службовими повноваженнями;

— застосовуються трояни, клавіатурні шпигуни та інші подібні засоби;

— прослуховуються та перехоплюються різними способами канали зв'язку.

В інших варіантах здійснення несанкціонованого доступу відбувається по-різному, кількість способів зростає у міру розвитку віртуального світу загалом. Впливає і поява нових видів пристроїв. Проте існуючі методи можна умовно звести до двох. Перший — обхід системи доступу, другий — незаконне отримання даних ідентифікованого користувача[17].

Усі можливі способи несанкціонованого доступу до інформації в комп'ютерних системах наведено на рисунку 2.1 та можна класифікувати по наступним ознаках:

— за принципом несанкціонованого доступу;
— по положенню джерела несанкціонованого доступу;
— по режиму виконання несанкціонованого доступу;
— за типом використаних уразливих місць інформаційної системи;
— по шляху несанкціонованого доступу;
— по поточному місцю розташуванню кінцевого об'єкта атаки;
— по безпосередньому об'єкту атаки;

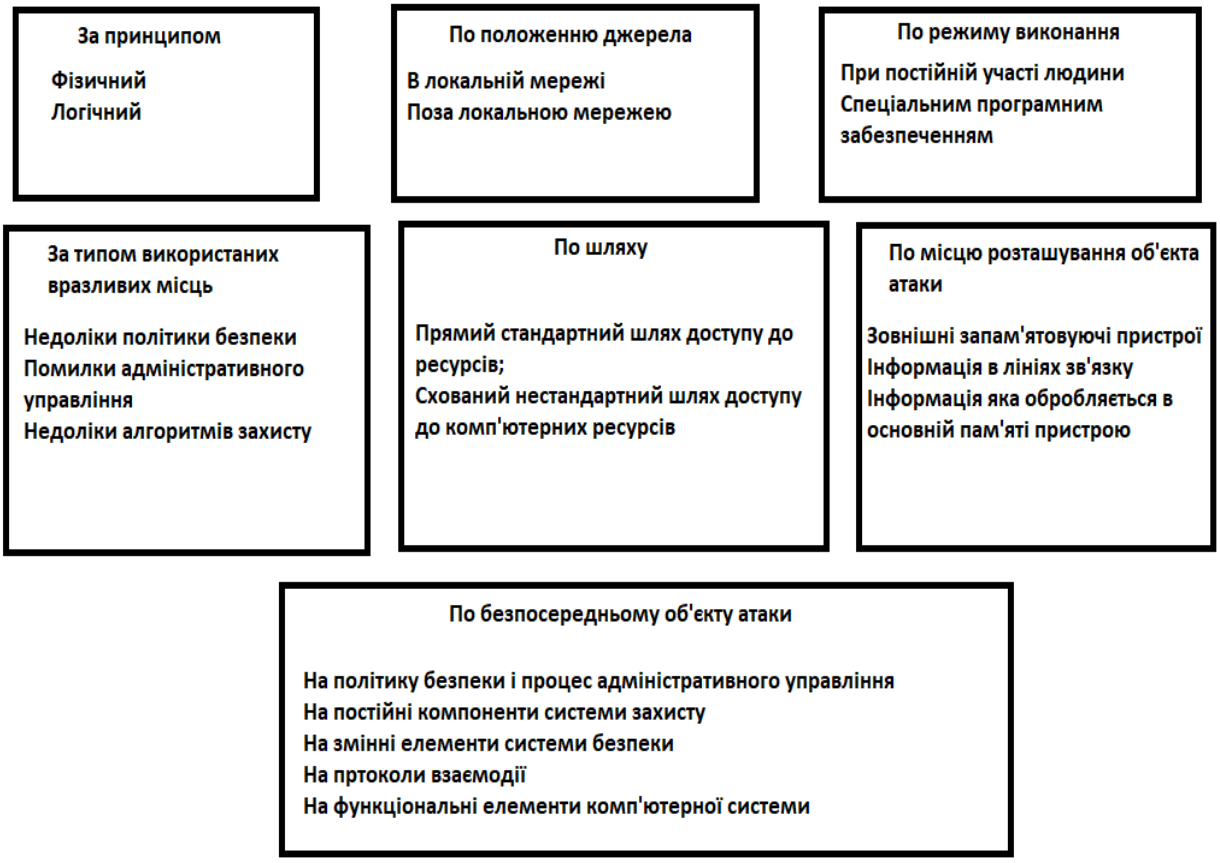


Рисунок 2.1 — Способи несанкціонованого доступу

Кінцевим об'єктом реалізації несанкціонованого доступу завжди є інформація, що захищається, а саме інформаційні ресурси, бази та банки знань. Під безпосереднім же об'єктом атаки розуміється об'єкт, аналіз чи використання

якого дозволяє успішно реалізувати несанкціонований доступ до інформації, що захищається. Наприклад, безпосереднім об'єктом нападу може бути криптосистема, що дозволяє зловмиснику спрогнозувати значення згенерованого секретного ключа. Ознака класифікації способів несанкціонованого доступу по безпосередньому об'єкту атаки є найбільш важливою, тому що точніше всього дозволяє розмежувати застосовувані способи реалізації несанкціонованого доступу.

Приведена система класифікації способів несанкціонованого доступу дозволяє зробити висновок, що ефективний несанкціонований доступ до інформації здійснюється тільки на основі вразливості системи захисту комп'ютерної системи, що атакується.

2.2 Аналіз недоліків сучасних RFID систем

Більшість сучасних систем використовують прості картки та алгоритми, що дозволяє зловмиснику дублювати картку доступу. Дублювання вимагає спеціального обладнання, яке легко здобути та є відносно недорогим. Однак передбачені способи протистояти цьому. Легкий спосіб захистити карту від дублювання — це використовувати екрановані тримачі для карток, які захищають карту тонкою металевою смугою, що запобігає доступу до RFID-чіпів за допомогою бездротової технології злому, що використовується зловмисниками. Серед інших рекомендації є більш надійне шифрування, щоб ідентифікатор не надсилався у вигляді відкритого тексту, а також використання безконтактних смарт-карток, які включають шифрування, взаємну автентифікацію та захист від відтворення повідомлень.

Легко доступні лінії зв’язку можуть бути зіпсовані, що може призвести до несанкціонованого доступу. Така ситуація може статися в тому випадку, якщо кабелі блокування або керування явно розміщені, оголені або доступні.

Використання протоколу Wiegand, що вважається поширеним для захисту зчитувачів, але він вже застарілий і схильний до зловживань. Wiegand є простим текстом, легко перехоплюється, легко відтворюється, включає вихідні дані

біометричних зчитувачів — це означає, що зловмисник може вкрасти дані, що зберігаються на картці, і включає вихідні дані навіть від надійних безконтактних криптографічних інтелектуальних зчитувачів. На жаль, виробники рішень контролю доступу досі виробляють зчитувачі магнітних карт, які використовують протокол Wiegand та обізнані про його вразливість. Єдиний дієвий спосіб захисту від злому Wiegand — це оновити технологію. Відповідним рішенням вважається використання безконтактних карток, здатних виконувати криптографічні з’єднання зі зчитувачем[18].

Аналогічно можуть бути порушені незахищені канали зв'язку між різними частинами СКУД. Наприклад, між зчитувачем та контролером або веб-браузером та сервером. Націлювання на канали зв'язку, ймовірно, вважається частим способом атаки, оскільки засоби зв'язку широко поширені та різноманітні. Тут також застосовні ефективні практики захисту організації від кібератак. Надійні політики паролів, належне керування комп'ютерною мережею, регулярне тестування вразливостей та процедури посилення захисту компонентів.

2.3 Способи захисту інформації від несанкціонованого доступу

Захист інформації — комплекс заходів, направлених на уникнення або стримування порушень цілісності даних або її модифікації. Під захистом розуміється інформація в будь-якому вигляді, формі, типу, об’ємі, які можуть нанести шкоди власнику або будь-якому суб’єкту. Також це розповсюджується на різні галузі в сферах науки, техніки, адміністративних підприємств, державі чи до корпорацій. Сполучення методів з засобами захисту інформації може включати в себе програмні, апаратні, програмно-апаратні комплекси, захисні перетворення разом з організаційними заходами[19].

Апаратні засоби передбачають, що в пристроях та інших технічних засобах опрацювання даних планується наявність спеціальних мікросхем або інтегрованих пристроїв, які можуть забезпечити захист та контроль витоку

інформації чи схеми контролю на відповідність між різним обладнаннями чи пристроями.

Рисунок 2.2 — Методи й засоби захисту інформації

Програмні методи захисту під собою розуміють певну кількість програмних засобів які можуть забезпечити певне розділення ролей доступу та виключення несанкціонованого витоку інформації.

Ідеологія методів захисного перетворення в тому, що дані які зберігаються в якомусь середовищі та передається за допомогою каналів зв’язку передається в певному коді, що обмежує пряме його використання.

Організаційні заходи з захисту інформації являють собою певний набір дій з точковим підбором та перевірки персоналу, які беруть участь та мають доступ до роботи програм чи інформації, його експлуатацію з чітко визначеними правилами розробки процесів та життєдіяльності інформаційної системи.

Керування доступом — спосіб захисту даних шляхом обмежень використання тотальних даних, в тому числі автоматизованих інформаційних

систем корпорації. Керування доступом повинно включати в себе наступні функції захисту:

— ідентифікацію персоналу з ресурсами компанії;

— автентифікацію суб’єкта з об’єктом за допомоги наданого ідентифікатора;

— перевірка компетенцій;

— організація робочих умов в межах встановленого регламенту компанії;

— реєстрація звертань до ресурсів, які знаходяться під захистом;

— реагування під час спроб несанаційного доступу.

Маскування — тип захисту інформації з використанням інженерних технічних засобів, враховуючи криптографічне маскування інформації. Маскувальники, аналогово-цифрово статичні.

Скремблери — програмний чи апаратний пристрій або алгоритм, які виконують функцію скремблювання. Скремблювання це зворотне перетворення цифрового потоку без змін швидкостей передачі з метою отримати властивість випадкової послідовності. Після скремблювання поява “1” з “0” на вихідній послідовності рівноймовірні. Скремблювання це оборотній процес, значить, що вихідне повідомлення може бути відновлене при використанні зворотного алгоритму.

Для захисту від несанкціонованого доступу розділяють два способи. Ідентифікація — процедура розпізнавання системою за допомогою наперед присвоєного ідентифікатора або іншої зазначеної інформації про користувача, яка сприймається системою. Це є першою ступеню в процедурі надання доступу до системи, після чого надається автентифікація з авторизацією. Автентифікація — це процедура відповідності належності ідентифікатора об'єкта, іншими словами встановлення чи підтвердження об’єкта дійсним, і перевірка чи є об'єкт або суб'єкт, що піддається перевірці, насправді тим, за кого він себе видає або намагається видати[20].

На теперішній час є декілька основних методів автентифікації, які відрізняються своєю складністю та надійністю з вартістю. Будь-який метод має свої переваги та недоліки. Використовуються наступні види автентифікації:

— однобічна автентифікація, коли користувач системи для отримання доступу до даних підтверджує свою автентичність;

— двобічна — це метод, коли система повинна підтвердити автентичність, окрім самого користувача;

— трибічна — використання, так званої, “нотаріальної служби автентифікації” для підтвердження дійсності кожного з клієнтів при обміні чи передачі інформації.

2.4 Вибір методу захисту

Стандарт MIFARE Classic компанії NXP — це ціле сімейство карт. До нього входять MIFARE Classic 4K, 1K, EV1 1K, EV1 4K, MIFARE ID, MIFARE Mini. Також цей стандарт може емулюватися іншими, новішими картами NXP. Робота картки із пристроями читання базується на стандарті ISO 14443A, частота 13,56 МГц. Карти MIFARE Classic 1K надають область пам'яті, організовану в секторі по 64 байти. Кожен сектор розбитий на 4 блоки розміром 16 байт (додаток Ж).

Останній блок кожного сектора називається трейлером сектора, у ньому записані ключі та параметри доступу до сектора. Нульовий блок нульового сектора — це спеціальний блок, заблокований на запис, він містить ідентифікатор та інформацію виробника картки.

Перед зверненням до сектора читання або запису необхідно виконати авторизацію за допомогою ключа розміром 6 байт. Авторизація відбувається за триетапним протоколом, близьким до того, що описаний у розділі 5.2.2. стандарту ISO/IEC 9798-2:1999. При цьому використовується пропрієтарний алгоритм потокового шифрування CRYPTO1.

Пристрій читання надсилає запит на авторизацію, вказуючи номер сектора, якого відбувається авторизація. Карта читає з внутрішньої пам'яті ключ доступу,

генерує випадкову послідовність та повертає її пристрою читання. Пристрій читання обчислює відповідь, використовуючи ключ доступу до сектора та алгоритм шифрування CRYPTO1, потім відправляє його з новою випадковою послідовністю, що згенерувала. Карта перевіряє відповідь, обчислену пристроєм читання. Потім обчислює відповідь на виклик пристрою читання та повертає його. Пристрій читання перевіряє відповідь картки. [21]

Диверсифікація — це процес отримання ключів доступу по ключу з використанням деяких унікальних для картки вхідних даних. Процес отримання ключів наведено на рисунку 2.3, може бути реалізований у прикладному ПЗ, що працює з пристроями читання або засобами SAM-модуля. Для прикладу це може працювати так:

— як вхідні дані для диверсифікації використовується ідентифікатор карти та номер сектора, ключ до якого ми хочемо отримати;

— дані шифруються майстер-ключем, результат скорочується до 6 байт і використовується як ключ доступу до відповідного сектора.

Рисунок 2.3 — Диверсифікація ключа

У результаті кожна карта отримує унікальні ключі доступу до секторів. Навіть якщо ключі для якихось конкретних карток будуть скомпрометовані, це не призведе до масового використання цих ключів.

3 МЕТОДИ ПОБУДОВИ МІКРОПРОЦЕСОРНИХ СИСТЕМ РАДІОЧАСТОТНОЇ АВТОРИЗАЦІЇ

3.1 Аналіз мікропроцесорних платформ

Щоб побудувати мікропроцесорну систему було розглянуто та обрано платформу, що має функціональні можливості, які необхідні для функціонування пристрою, що проектується. Серед доступних варіантів є мікропроцесорна платформа Arduino. Дана платформа має декілька модифікацій, що відрізняються за функціональними можливостями, призначенням та вартістю.

Arduino Pro Mini зображена на рисунку 3.1 побудована на мікроконтролері ATmega168. Платформа містить 14 цифрових входів та виходів, 6 аналогових входів, резонатор, кнопку перезавантаження.

Arduino Pro Mini призначена для непостійної установки в об'єкти чи експонати. Платформа поставляється без встановлених виводів, що дозволяє користувачам застосовувати власні виводи та роз'єми. Розміщення контактів сумісне з платформою Arduino Mini.

Рисунок 3.1 — Плата Arduino Pro Mini

Arduino Duemilanove (рис. 3.2) — це плата мікроконтролера на основі ATmega168 або ATmega328 . Контролер містить чотирнадцять цифрових входів та виходів, з яких шість можна використовувати як ШІМ-виходи, 6 аналогових входів, кварцевий генератор 16 МГц, USB-з’єднання, роз’єм живлення, роз’єм

ICSP і кнопку скидання. Містить все необхідне для підтримки мікроконтролера[22].

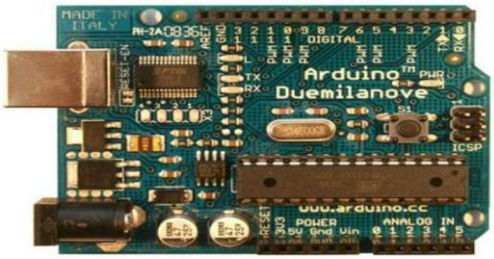


Рисунок 3.2 — Плата Arduino Duemilanove

Платформа Arduino Nano (рис. 3.3), є компактною налагоджувальною платою ядром якої є мікроконтролер ATmega 328p, який являється аналогом Arduino Uno. Ці плати Arduino практично конструктивно ідентичні. Завдяки компактному розміру, плата дає великий заділ для використання в багатьох пристроях. Окремий роз'єм для живлення плати відсутній, тому дана модель отримує енергію 5V через USB Mini-B.

Даний пристрій дозволяє виконати ISP завантаження. Також програмування можливе безпосередньо через блок контактів ICSP, має 8 аналогових вхідних каналів та 14 цифрових вводів-виводів, 6 з яких можуть використовуватися як виходи ШІМ[23].

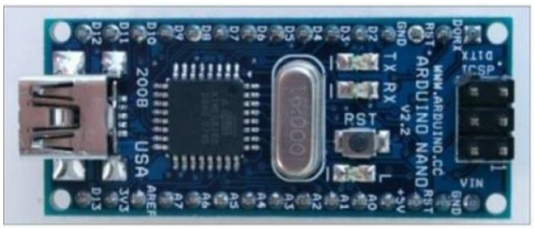


Рисунок 3.3 — Плата Arduino Nano

Arduino Uno (рис. 3.4) виконана на базі мікроконтролера ATmega328P. На відміну від усіх попередніх плат Ардуїно, Uno як перетворювач інтерфейсів USB-UART використовує мікроконтролер ATmega16U2, що дозволяє підвищити

швидкість передачі даних. Після прошивання, ATmega16U2 дозволяє використовувати контролер як клавіатуру, мишу або джойстик[24].

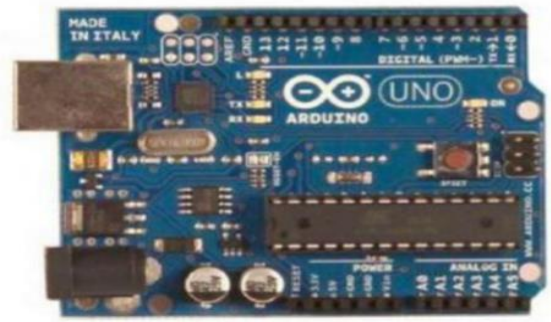


Рисунок 3.4 — Плата Arduino Uno

Arduino Mega (рис. 3.5) реалізована на базі мікроконтролера ATmega2560. Його перевагою являється 54 цифрових входів і виходів та пам’ять великого об’єму 256 Кбайт.

Arduino Mega — це покращена версія Arduino Uno. Ця плата призначена для більш масштабних проектів. Arduino Mega має безліч пінів для складних проектів, таких як 3D-принтери і різноманітна робототехніка. Arduino Mega 2560 — це сучасна плата, робота якої побудована на потужному мікроконтролері ATmega2560. Він містить на собі 54 контакти вводу та виводу інформації. Arduino Mega містить всі необхідні компоненти для мікроконтролера. Для того щоб розпочати роботу вам необхідне просте під’єднання плати до комп'ютера, яке відбувається через USB роз’єм. Arduino Mega має сумісність з більшістю сучасних платформ призначених для Arduino Duemilanove або Uno[25].

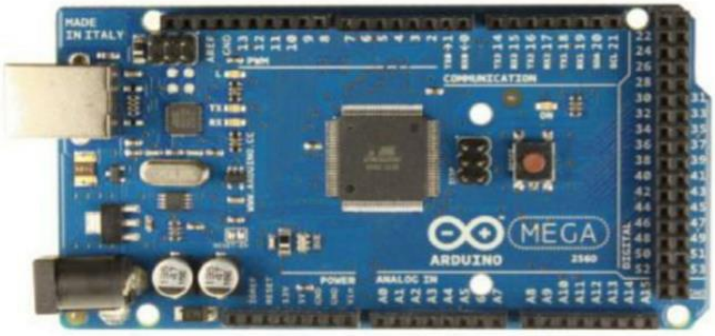


Рисунок 3.5 — Плата Arduino Mega

Конкурентами для платформи Arduino є мікроконтролери від STMicroelectronics. Мікроконтролери STM32 — популярна і широко використовувана платформа, яка дозволяє створювати професійні рішення для автоматизації в різних галузях. Враховуючи доступність Arduino, STM32 вимагає більш глибоких деталей завантаження, що складніше для початківців, а навчальної літератури українською мовою менше.

За технічними параметрами Arduino програє STM32. Тактова частота мікроконтролера Arduino становить 16 МГц, що нижче, ніж 72 МГц у STM32. У STM32 є більше контактів GRIO. STM32 також має більший обсяг пам'яті. Важливо відзначити pin-to-pin сумісність STM32 — можна замінити один продукт на інший, не змінюючи плату. Але конкуренти не можуть повністю замінити Arduino. Перш за все, це пов’язано з високим входовим бар’єром — щоб використовувати STM32, потрібно мати певну базу знань та досвіду. Плати Arduino є відносно поширеними, і якщо у користувачів виникають проблеми, рішення можна знайти на форумах. Для розширення функціональності Arduino також створено різні модулі. За співвідношенням ціна та якість виграє STM32.

Що відрізняє мікроконтролери серії STM32 від конкурентів, так це їх чудова стабільність в діапазоні температур від -40C до +80C, і, на відміну від Arduino, немає втрати високої продуктивності. Також можна знайти продукти, які працюють при температурах до 105C. На малюнку 3.6 показано приклад плати з мікроконтролером STM32.

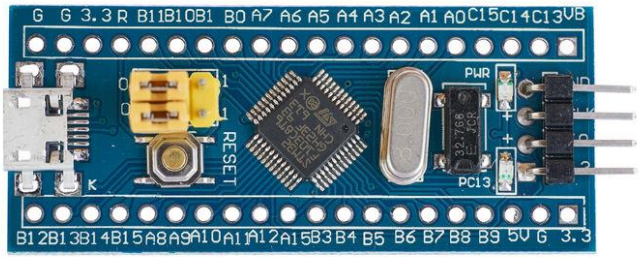


Рисунок 3.6 — STM32 blue pill

Для архітектури ARM розроблено ряд середовищ розробки. Системні інструменти Keil і IAR є найвідомішими і найдорожчими. Програми цих компаній пропонують найпростіші інструменти оптимізації коду. Також існують різні системи — стеки USB, стеки TCP/IP тощо. Використовуючи систему Keil, користувачі можуть отримати хороший рівень технічної підтримки. Таким чином, STM32 є надійною платформою, на якій можна створити систему, що забезпечує стабільну та точну роботу розробленого пристрою.

3.2 Розробка структурної та функціональної схеми

Для реалізації обраного обладнання згідно технічного завдання розроблено структурні схеми. Схема пристрою складається з блоку керування та виконавчого блоку (рис. 3.7). Блок управління, в свою чергу, містить друковану плату з мікроконтролером і читач карт RC522, який обробляє карти на частоті 13,56 МГц. Обмін даними про результати обробки даних здійснюється між блоком керування та блоком виконання через інтерфейс CAN. Виконавчий блок також виконаний у вигляді мікроконтролера і містить набір комутаційних пристроїв, які керують пропускним елементом.

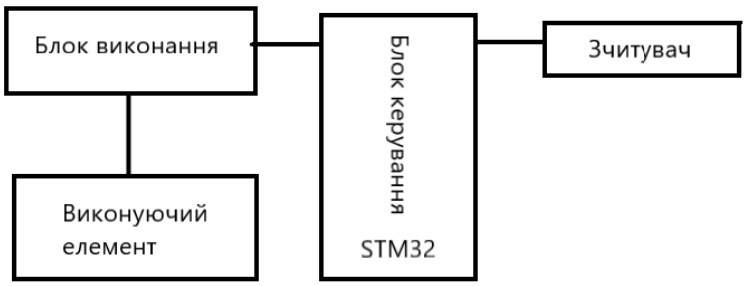


Рисунок 3.7 — Структурна схема системи

Система працює за наступним алгоритмом: спершу електронна карта записується данними про параметри доступу, після чого доступ до зчитування та запису захищається надійним ключем. Карти загальний об’єм пам’яті яких складає 1КБ містять 16 секторів і в кожному 4 блоки по 16 байт. Така структура Забезпечує розміщення різних даних в окремих блоках та за допомогою

налаштувальних запобігти несанкціонованому доступу. Система забезпечує антиколізійний алгоритм і працює за наявності декількох карт в зоні досяжності зчитувача. Коли карта активується в зоні дії зчитувача, реалізується авторизація і зчитування захищених даних. В разі успішної авторизації, блок контролю формує відповідний пакет для блоку виконання. Після отримання пакету, блок виконання реалізує запрограмований алгоритм для організації сценарію що дозволяє або забороняє доступ. Функціональна схема зображена на рисунку 3.8.

Коли програмний код розпочинає роботу, виконується ініціалізація периферії та бібліотек. Система розроблена з використанням інтерфейсів SPI, USART та CAN, тому для всіх блоків периферії реалізовано функції, які налаштовують їх згідно з технічних вимог. Додатково налаштовані контакти, що керують світловим та акустичним відтворенням.

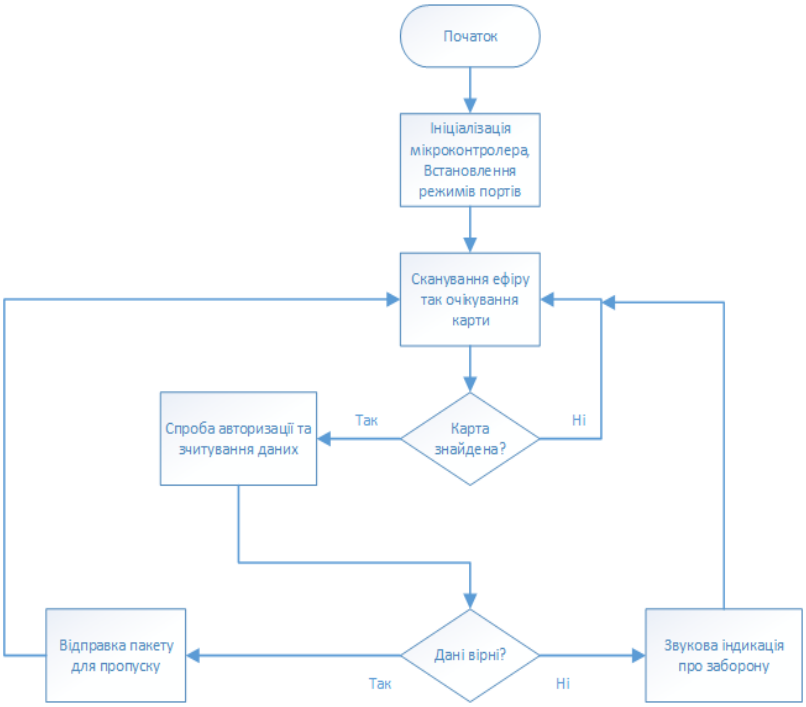


Рисунок 3.8 — Функціональна схема

Отже, реалізовано синтез структурної і функціональної схеми системи безконтактної ідентифікації. Повний перелік елементів і принципова схема наведена в додатку Д.

3.3 Вибір мікропроцесорної платформи

Враховуючи переваги та недоліки різних платформ, для реалізації пристрою обрано мікропроцесорну платформу STM. STM32 — це мікроконтролер на основі ядра ARM Cortex-M3. Це ядро має багато переваг, які будуть перераховані нижче, але універсальність сьогодні є головною його перевагою. Це представлено кількістю виробників, підключених до цієї архітектури. ST була однією з перших компаній, яка випустила свій мікроконтролер Cortex-M3 і швидко стала лідером ринку.

Однією з причин всесвітньої популярності серії STM32 є максимальний комфорт для розробників. Якщо універсальність ядра STM32 дозволяє мінімізувати вартість програмного коду, сумісність між контактами всередині серії STM32 дозволяє змінювати пам’ять і периферійні пристрої (Ethernet, USB, CAN) без заміни плати. Сумісність між контактами передбачає, що для однакового розміру корпусу всі сигнали залишаються на тих самих контактах для різних варіантів мікроконтролерів сімейства.

Як і всі мікроконтролери серії STM32, STM32F100 має вбудований контролер DMA, який дозволяє розвантажити ядро від роботи з обробкою, прийомом та передачею інформації. Його відсутність у поточній реалізації Cortex-M0 є значним недоліком у всьому виробництві мікроконтролерів. Чи присутні в серії STM32 передові аналогові периферійні пристрої, не уточнюється. Зокрема, STM32F100 має 12-розрядний 16-канальний АЦП із часом вимірювання 1,2 мкс. В інших сімействах і сімействах АЦП набагато швидше. Цей АЦП має багато переваг: можливість встановлювати пакетні зміни, можливість варіювати тривалість вимірювання на кожному каналі, можливість роботи в режимі аналогового блоку, вбудований датчик температури та зовнішній тригер. На додаток до першого, в серії мікроконтролерів STM32 є кілька АЦП, і швидкість перетворення можна збільшити в кілька разів, використовуючи декілька АЦП разом. Наприклад, лінія STM32F-1 може досягати швидкості 0,5 мкс.

STM32F100 також має багато входів і виходів загального призначення (GPIO). Серія STM32 відрізняється від конкурентів на ринку тим, що на GPIO припадає значна частка загальної кількості контактів пакета: до прикладу, в серії STM32F100 корпус LQFP48 складає 37 GPIO, пакет LQFP64 має 51 GPIO, а пакет LQFP100 має 80 GPIO. Ці GPIO дуже гнучкі в тому, що їх можна налаштувати не тільки в різних стандартних режимах (двосторонній, відкритий колектор, підтягування тощо), але також як входи або виходи для периферійних пристроїв. Швидкість GPIO регулюється для зменшення електромагнітних перешкод: для STM32F100 вона може становити 2 МГц, 10 МГц і 50 МГц. У випадку серії STM32F-2 робоча швидкість GPIO може досягати 100 МГц. Це відкриває нові можливості для управління та передачі даних. Ви можете створювати власні інтерфейси програмно. Серія STM32 має вбудований контролер CAN 2.0, ліцензія на який купується безпосередньо у Bosch, творця стандарту.

У деяких серіях STM32 є корисні периферійні пристрої SDIO і FSMC (в серіях STM32F103, STM32F101). FSMC — це інтерфейс, який використовує зовнішні пам’яті, такі як SRAM, NOR Flash і NAND Flash. SDIO —це інтерфейс, який працює з картами пам'яті SD, mini SD, micro SD, MMC. Єдиний тип пам’яті, який не охоплює серія STM32, — DRAM, але більшості розробників вона не потрібна. Усі мікроконтролери STM32 STM32W мають набір універсальних 16-розрядних таймерів (STM32F-2 має 32-розрядні таймери) і один або більше 12-розрядних ЦАП. Серія STM32F-2 містить цікаву нову функцію —інтерфейс DCMI для підключення камер, який може працювати зі швидкістю до 54 МБ/с, таким чином підтримуючи камери з матрицями приблизно до 1 мегапікселя. Цей інтерфейс також може отримувати дані у форматі JPEG з камери. Інтерфейси FSMC і SDIO дозволяють динамічно зберігати потокові дані з камери у зовнішній пам'яті. Усі продукти серій STM32L, STM32F-2 і STM32F-1 з пам’яттю понад 512 Кбайт мають вбудований модуль захисту пам’яті MPU, який може додатково підвищити безпеку системи. MPU дозволяє розширювати пам'ять на сегменти, встановлюючи до них різні рівні доступу (читання, запис, виконання). Це дозволяє блокувати доступ до окремих областей пам’яті для

програмного коду та встановлювати повний привілейований і непривілейований режими. MPU також генерує попередження, якщо програма намагається отримати доступ до захищеної області пам’яті. Мікроконтролери серії STM32 з флеш-пам'яттю понад 512 Кбайт мають корисну функцію —пам'ять розділена на два банки. Це дозволяє розмістити дві окремі мікропрограми мікроконтролера в кожній групі та вибрати ту чи іншу під час запуску мікроконтролера, що означає радикальну зміну всієї функціональності пристрою.

Серед розглянутих мікроконтролерів найбільш кращий виявився STM32F103C8T6. Мікроконтролер потребує живлення номіналом 3В, при чому високі рівні вхідних та вихідних дискретних сигналів також 3В. Частину контактів дозволено використовувати як входи для сигналів з рівнями 5 В, тобто вони є толерантними до 5В. Інші входи не розраховані для підключення напруги більше напруги живлення, тобто, 3 В. В разі підвищення вказаного рівня вище 4В може статися пошкодження мікроконтролера. Струм що проходить через мікроконтролер не може перевищувати 20 мА. Найбільш рекомендованим значенням є не більше 8мА[26].

3.4 Вибір електронних компонентів

Оскільки система повинна використовувати безконтактні картки, був обраний модуль на основі мікросхеми RC522 (рис. 3.9) та інтерфейсу SPI. Він повинен забезпечитись джерелом живлення 3,3 В і струмом 13 мА — 26 мА під час роботи. У режимі очікування пристрій споживає 10 — 13 мА, а в режимі сну споживає менше 80 мкА. Використано карти, що працюють на частоті 13,56 МГц, на відстані до 60 мм. Розміри дошки 40 мм х 60 мм [27].

Використання модулів MFRC522 вимагає спеціальних роз'ємів для підключення і компактного розміщення. Модуль містить 8 контактів, через які передається живлення та дані.

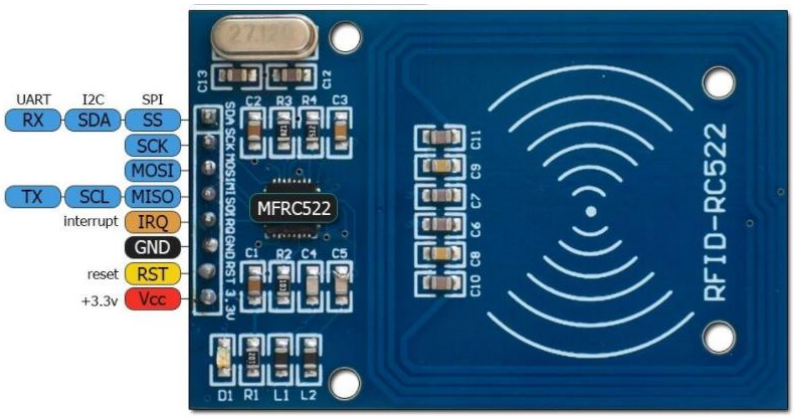


Рисунок 3.9 — Модуль MFRC522

Ядром системи являється мікроконтролер STM32F103C8T6 (рис. 3.10). Корпус виготовлений за стандартом LQFP-48. Перевага такого корпусу в тому, що його можна встановити без додаткового дорогого обладнання. Функціонал кожного виводу наведена в додатку Б.

Рисунок 3.10 — Мікроконтролер

Для правильної роботи пристрою використовується стабілізатор напруги RT7272, який усуває відхилення і забезпечує 5В. RT7272A — це високоефективний понижуючий перетворювач постійного струму в режимі синхронного струму, який може забезпечити вихідний струм до 3 А в діапазоні широких значень вхідної напруги від 4,5 В до 36 В. Мікросхема інтегрує МОП-транзистори 150 мОм з високим опором і 80 мОм з низьким опором. Досягнуто високої ефективності перетворення до 95%. Архітектура керування поточним режимом підтримує швидку перехідну реакцію та прості схеми компенсації.

Покрокове обмеження струму дозволяє захиститись від короткого замикання, а стрибки вхідного струму під час запуску усуваються внутрішнім плавним пуском. RT7272A реалізує повні функції захисту, а саме захист від перенапруги, обмеження струму та термовідключення. RT7272A доступний у стійкому до високих температур корпусі SOP-8. Усі розміри наведені в Додатку В [28].

Потім підключіть лінійний регулятор AMS1117, щоб генерувати 3,3 В, які можуть безпосередньо використовуватися мікроконтролером. Сімейство регульованих і фіксованих стабілізаторів напруги AMS1117 розроблено для забезпечення вихідного струму 800 мА (максимальний короткочасний струм 1,5 А). Напруга відсічення пристрою гарантовано становить до 1,3 В при максимальній потужності струму і знижується при менших струмах навантаження. Межі мікросхеми регулюють опорну напругу до 1%. Обмеження струму також обмежене, мінімізуючи умови перевантаження напругою на регуляторі та ланцюгах живлення.

Пристрій AMS1117 сумісний з іншими контролерами SCSI з трьома контактами і доступний у низькопрофільних корпусах для поверхневого монтажу в корпусі SOT-223 і пластиковому корпусі TO-252 (DPAK). У цьому проекті корпус SOT-223 був обраний через його компактні розміри та тому, що пристрій розроблений для споживання дуже малого струму. Розміри мікросхем наведені в додатку Г. Основний корпус пристрою показаний на малюнку 3.11.

Рисунок 3.11 — Габарити AMS1117

Інтерфейс CAN (Controller Area Network — Controller Network) — це промисловий мережевий стандарт, орієнтований на об’єднання різних приводів

і датчиків в одну мережу, розроблений Robert Bosch GmbH для автомобільної автоматизації в середині 1980-х років. В даний час стандарт широко використовується в промисловій автоматизації, технології розумного будинку, автомобільній промисловості, бортових мережах, системах управління кондиціонуванням повітря, ліфтах, медичних і промислових установках.

CAN-стандарт Bosch визначає передачу безпосередньо, без прив'язки до фізичного способу передачі даних, тобто це може бути що завгодно, наприклад радіоканал або оптоволокно. Але на практиці мережа CAN зазвичай відноситься до мережі з фізичним рівнем у формі загальної та однієї диференціальної пари (ISO 11898). При визначеній стандартом максимальної швидкості передачі (1 Мбіт/с) довжина шини може досягати 30 м. На менших швидкостях даний показник можливо збільшити до кількох кілометрів, приміром на швидкості 10 кбіт / с — довжина шини до 5 км. В разі необхідності великої довжини, в систему додають мости або повторювачі. Теоретично кількість приєднаних до шини пристроїв не обмежена жодним правилом, але на практиці не перевищує 64.

Врахувавши переваги вище наведеного інтерфейсу, було додано мікросхему, що дозволяє інтеграцію його в пристрої що проектується. Для реалізації взаємозв'язку між модулями використано конвертер TJA1050 розроблений компанією NXP. Серед його переваг є режим роботи в діапазоні напруги від 3,3 до 5 В, та низьке енергоспоживання, що складає 75мА. Робота модуля забезпечується мінімальною кількістю електронних компонентів в схемі. Пристрій не є вибагливим до невеликих змін напруги та забезпечує доставку даних без втрат. Корпус модуля виготовлений в стандарті SOP-8. Габарити мікросхеми наведені в додатку Г.

3.5 Розробка плати та схемотехніки

Розробка електричної схеми відбувається на підставі технічної документації вищевказаних пристроїв (Додаток Г). Проектування виконується в програмному середовищі Proteus. Результати див. у Додатку Д.

Proteus — програмний засіб для налагодження та проектування електронних пристроїв, у тому числі на основі різних сімейств мікроконтролерів. Надає можливість вводити схеми в графічний редактор, моделювати їх роботу та розробляти друковані плати, включаючи 3D візуалізацію їх складання. Унікальною особливістю середовища Proteus є можливість ефективної імітації роботи та налагодження вбудованого програмного забезпечення для різних мікроконтролерів .

PROTEUS має велику бібліотеку електронних компонентів, і дозволяє виготовити ті, яких бракує, самостійно. Забезпечує підтримку моделей SPICE, які зазвичай надаються виробниками електронних компонентів.

Програмне забезпечення PROTEUS сумісне з популярними середовищами розробки вбудованого програмного забезпечення, включаючи:

— IAR (МК);
— HiTECH (МК 8051 і PIC);
— ICC (МК AVR, ARM7);
— CodeVisionAVR (тільки МК AVR);
— Keil (МК 8051 і ARM).

Трасування друкованої плати було реалізовано в програмному середовищі Sprint layout, оскільки воно має більш зручний інтерфейс на відміну від попереднього рішення. Важливою перевагою Sprint-Layout є інтуїтивно зрозумілий інтерфейс, який містить в собі лише найнеобхідніші інструменти для підготовки друкованих плат невеликих розмірів 300 на 300 мм. Програма дає змогу працювати з двома шарами, тобто, провідників і маркування, для кожної сторони плати. Додатковими можливостями є шар для паяльної маски, металізація та SMD-маска. Недоліком вбудованого трасувальника є можливість тільки розміщувати провідники, і лише в ручному режимі. У додатковій бібліотеці розташовані найчастіше використовувані електронні компоненти. В Sprint-Layout організована можливість генерувати результати роботи в поширені формати Excellon і Gerber, а також зберегти у файл HPGL для обробки проекту на програмно-керованому фрезерному верстаті. Пакет часто застосовується для

виготовлення плат, що розробляють в домашніх умовах. Результат моделювання наведено на рисунку 3.12.

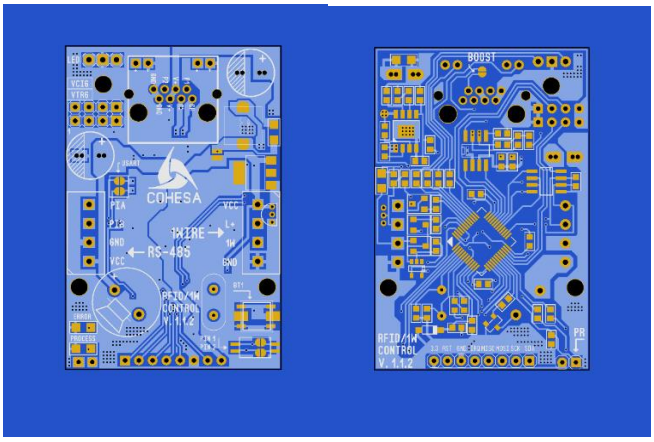


Рисунок 3.12 — Зовнішній вигляд друкованої плати

Під час розробки було розділено шари на окремі трафарети із розміщенням електронних компонентів, що дозволило полегшити монтаж та зекономило місце на платі (рисунок 3.13). Таким чином стає можливим відмовитись від маркування елементів на друкованій платі та виготовити її більш компактною.

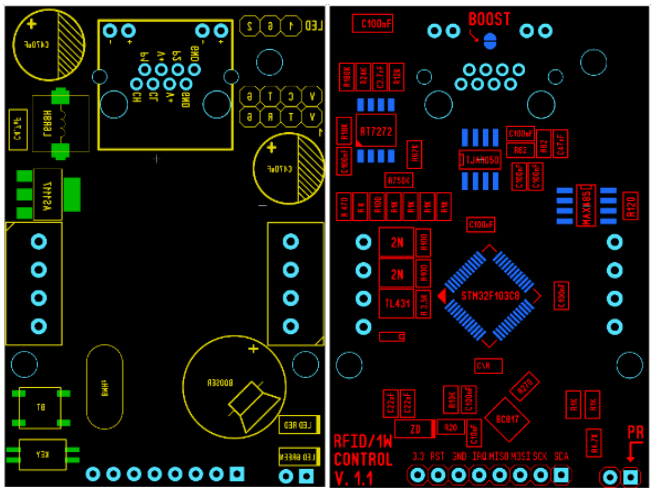


Рисунок 3.13 — Трафарет плати

Розробку готової друкованої плати було покладене на закордонне підприємство JLC PCB. Це дало змогу виготовити плату товщиною 1,6 мм та шириною провідників 0.3 мм. Після виконання замовлення, надіслані файли на

JLCPCB, були перевірені інженерами перед початком виробництва. Інженерами було підтверджено, що конструкція змодельована вірною щодо виконання отворів і відстані між контактними майданчиками, доріжок та обмежень допусків для зазору між границями плати.

На готову плату було змонтовано відповідні елементи. По закінченню монтажу проведено перевірку на відсутність проблем, короткого замикання та відповідність всіх значень напруги у вузлових точках. Щоб запобігти корозії та захистити від вологи пристрій було покрито захисним шаром лаку. Готовий пристрій зображено на рисунку 3.14.

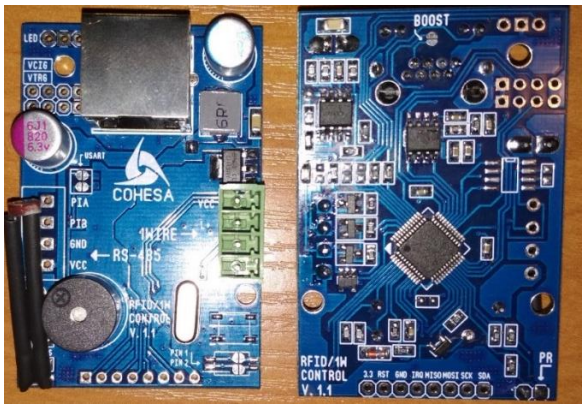


Рисунок 3.14 — Готова плата з елементами

Рисунок 3.15 — Готовий пристрій

Заключним етапом було змонтовано модуль MFRC522. Готова конструкція має невеликі розміри та може поміститись в компактний корпус. Результат розробки зображено на рисунку 3.15

Отже, виготовлено апаратну частину мікропроцесорної системи безконтактної ідентифікації на базі мікроконтролера STM32F103C8T6 та модуля, що здатен працювати на радіочастоті 13.56 МГц. Модуль MFRC522 дозволяє обмінюватись інформацією без дотику з картами Mifare та реалізувати систему з підвищеним захистом для авторизації.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1 Аналіз алгоритму роботи карти MIFARE

В розробленій системі використано безконтактні карти MIFARE classic 1k. Перевагою цих карт є наявність пам’яті в розмірі 1024 байти. Пам’ять організована таким чином що утворено 16 секторів доступ до кожного з яких можна окремо налаштувати в залежності від потреб. Кожен сектор розмежований на 4 менші частини — блоки по 16 байт. Четвертим блоком кожного сектору є сектор-трейлер, який зображений на рисунок 4.1, він містить особливу інформацію.

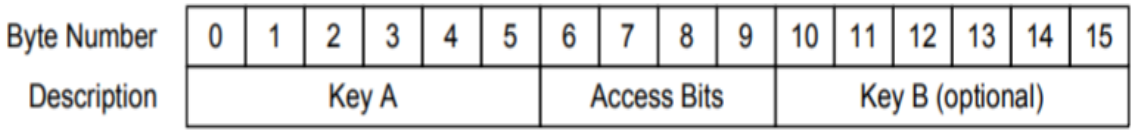


Рисунок 4.1 — Структура сектор-трейлера

Трейлер блоку містить 2 ключі та біти для налаштувань доступу. Ключ B можна використовувати як дані, збільшуючи розмір сектора на 6 байт. Біти доступу можна використовувати для встановлення обмежень для кожного з чотирьох блоків. За замовчуванням дозволи на читання та редагування налаштовано для перших трьох блоків з використанням ключів A або B. Доступ до трейлера можна отримати лише за допомогою ключа A, інший ключ використовується як дані. Метод формування набору бітів наведено в Додатку E, а структура відображення наведена в Додатку G.

Для активації карти, зчитувач транслює комбінацію на 1,56 МГц. У зоні дії карта живить внутрішній контролер і готова обробляти команди. Інтелектуальна функція запобігання зіткненням дозволяє працювати з кількома картками одночасно. Алгоритм запобігання зіткненням вибирає кожну картку окремо та гарантує, що транзакції з вибраною карткою виконуються правильно без втручання в іншу картку в полі. Схематично зв’язок з картою наведена на рисунку 4.2.

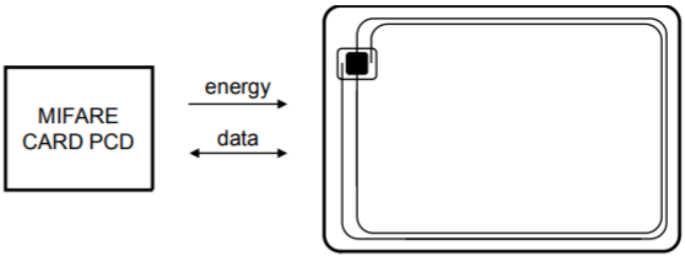


Рисунок 4.2 — Схема роботи з картою

На фізичному рівні команди повинні надсилатися в певному порядку, щоб використовувати карту. Після увімкнення пристрою та виконання жорсткого скидання потрібно просканувати зону дії зчитувача на наявність карти та очікувати відповідь від карти. У відповідь карта посилає два байти даних, в яких закодована інформація про тип і обсяг пам'яті. Основні коди команд показані на рисунку 4.3.

Command	ISO/IEC 14443	Command code (hexadecimal)
Request	REQA	26h (7 bit)
Wake-up	WUPA	52h (7 bit)
Anticollision CL1	Anticollision CL1	93h 20h
Select CL1	Select CL1	93h 70h
Anticollision CL2	Anticollision CL2	95h 20h
Select CL2	Select CL2	95h 70h
Halt	Halt	50h 00h
Authentication with Key A	-	60h
Authentication with Key B	-	61h
Personalize UID Usage	-	40h
SET_MOD_TYPE	-	43h
MIFARE Read	-	30h

Рисунок 4.3 — Основні команди для зв’язку з картою

Після визначення типу картки запускається процес антиколізії, в результаті картка надсилає власний унікальний ідентифікатор, що може формуватися з 4 або 7 байт, в залежності з типом карти. Наступним кроком за допомогою отриманого ідентифікатора відбувається авторизація, після якої стає доступним проводити операції в секторі картки. Дані на картці можна зчитувати, перезаписувати, збільшувати, зменшувати та переносити[29]. Повна схема алгоритму наведена в Додатку І.

4.2 Ініціалізація периферії

Для початку роботи системи налаштовано виводи мікроконтролера у відповідні режими. На платі змонтовано дзвінок, два світлодіоди, інтерфейс SPI для зв'язку із модулем MFRC522, CAN для передачі сигналу до модуля виконання та USART для відлагодження та перегляду даних на комп'ютері.

Налаштування виводів реалізовано за допомогою регістрів CRL та CRH які відповідають за перших 8 виводів на наступних 8 відповідно. Для налаштування доступні такі параметри:

Для зручності керування та налаштування було розроблено універсальний список макросів, що є масками із бітами налаштувань. Це підвищило зручність при налаштуванні виходу чи входу мікроконтролера, оскільки використовується макросова заміна відразу із трьома параметри. Налаштування потребує ім'я порту до якого підключений вивід, номер цього виводу від 0 до 16 та режим який потрібно встановити. Макроси режимів для заміни зображено на рисунку 4.4

```
#define MODE_IN_AN          0x0
#define MODE_IN_IF          0x4
#define MODE_IN_PU_PD       0x8
#define MODE_OUT_PP_10MHZ   0x1
#define MODE_OUT_PP_2MHZ    0x2
#define MODE_OUT_PP_50MHZ   0x3
#define MODE_OUT_AF_PP_10MHZ 0x9
#define MODE_OUT_AF_PP_2MHZ  0xA
#define MODE_OUT_AF_PP_50MHZ 0xB
#define MODE_OUT_AF_OD_10MHZ 0xD
#define MODE_OUT_AF_OD_2MHZ  0xE
#define MODE_OUT_AF_OD_50MHZ 0xF
```

Рисунок 4.4 — Макросові підміни режимів

Ввімкнення та вимкнення світлодіодів реалізовано з використанням регістра ODR. Алгоритм його роботи досить простий. Для активації піна необхідне встановлення одиниці у його відповідний біт і світлодіод засвічується, деактивація відбувається після очищення одиниці. Макроси для маніпуляції виходами до яких підключені світлодіоди наведені на рисунку 4.5.

```
#define RC522_PROCESS_LED_ON  GPIOB->ODR|=0x2000
#define RC522_PROCESS_LED_OFF  GPIOB->ODR&=~0x2000

#define RC522_ERROR_LED_OFF  GPIOB->ODR&=~0x0004
#define RC522_ERROR_LED_ON  GPIOB->ODR|=0x0004
```

Рисунок 3.5 — Макроси для роботи з виводами

Наведений вище список макросів використовується для налаштування інтерфейсу, оскільки контакти, до яких підключено пристрій, у свою чергу підключені до блоку інтерфейсу. У параметрах конфігурації USART вказано двопровідний режим роботи зі швидкістю 9600 байт в секунду. Передача, прийом і сам блок включені.

Інтерфейс SPI забезпечує налаштування 5 контактів для роботи пристрою. У регістрах налаштувань цього блоку дозволені швидкість, режим роботи супервізора або веденого, активація периферійних пристроїв. Налаштування контактів показано на малюнку 4.6.

Налаштування CAN виконується подібно до попереднього налаштування, але з деякими відмінностями. Спочатку налаштуйте вихід, а потім налаштуйте швидкість і режим передачі даних. Особливістю є можливість встановити ідентифікатор, що передається в посилці, як адресу відправника, і відповідно додати адресу одержувача. Наступна функція — це можливість налаштовувати фільтри та блокувати проходження пакетів із заборонених пристроїв у фізичній мережі тим самим розвантаживши ресурси мікроконтролера.

```
SETUP_GPIO(GPIOA, 5, MODE_OUT_AF_PP_50MHZ);          ///SCK
SETUP_GPIO(GPIOA, 6,  MODE_IN_PU_PD);                ///MISO
SETUP_GPIO(GPIOA, 7,  MODE_OUT_AF_PP_50MHZ);        ////MOSI
SETUP_GPIO(GPIOA, 4,   MODE_OUT_PP_50MHZ);    ///SDA CS
SETUP_GPIO(GPIOA, 1,   MODE_OUT_PP_50MHZ);       // RST
```

Рисунок 4.6 — Налаштування інтерфесу SPI

Робота програми забезпечується циклічним викликом функцій тому, було налаштовано таймер. В функцію, що обробляє переривання додано методи, що будуть викликатись при кожному перериванні. Для оперативності системи,

швидкість таймера налаштована на частоту, що дозволяє генерувати переривання 1000 разів за секунду.

4.3 Створення бібліотеки для роботи з модулем MFRC522

Стабільна робота пристрою забезпечена розробленою власною бібліотекою, оскільки загальнодоступні рішення є застарілими, мають малу швидкодію, відсутню оптимізацію та порушену послідовність алгоритму. Використавши офіційну документацією виробника та запропонований ним алгоритм, розроблено сучасну версію бібліотеки яка не містить вище згаданих недоліків, що знижують швидкодію мікроконтролера. Розроблена бібліотека містить файли заголовків та файли з методами. Для зручності подальшої імплементації, файли названі в честь мікросхеми для якої були написані, тобто — RC522. Назви наявних файлів відображено на рисунку 4.7.

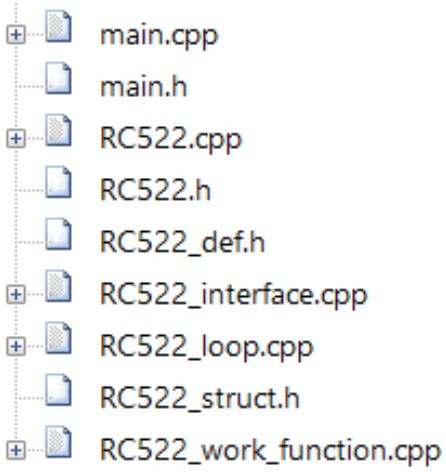


Рисунок 4.7 — Структура файлів проекту

Файл RC522.h містить оголошення класів, методів і полів. Створення методів для ініціалізації відкритих класів і модулів. Також доступні функції для перевизначення ключів у певних блоках, встановлення ключів для доступу до секторів, перевизначення цілих секторів, перевірка того, чи можна отримати доступ до певного сектора за допомогою вказаного ключа, читання всієї карти, сектора або окремого блоку, функція запису єдиний блок.

Щоб відстежувати різні стани, створено набір змінних, які вказують на те, що картку було піднято або замінено. Реалізовано лічильник помилок який збільшується коли карта зникає з робочої області, а також увімкнено виконання всього алгоритму або вимкнено. Код програми наведено в Додатку К.

Приватна частина класу реалізує функції низького рівня для сканування ефіру, надсилання та отримання даних, запобігання зіткненням, читання ідентифікаторів, виведення даних на COM-порти, обчислення контрольних сум, а також запису та читання блоків і секторів. Серед полів створено масиви, що зберігають коди паролів доступу та комбінації для виконання входу щоб читати та записувати вміст.

Метод loop викликається в перериванні таймера 1000 разів за секунду і реалізує наступні дії:

— сканує ефір на наявність активних пристроїв;

— в разі відповіді карти своїм типом, запускається алгоритм антиколізії;

— алгоритм отримує унікальний ідентифікатор карти з яким звертається до конкретної карти для авторизації;

— в результаті успішної авторизації відбувається обмін даними і перевірка на коректність;

— у випадку успішного виконання всіх перевірок активується відповідний сценарій що інформує решту системи про успіх.

Використано програмне середовище Keil для компіляції та запису написаної бібліотеки в розроблений пристрій. Запис у внутрішню пам'ять контролера організовано за допомогою окремого пристрою ST-Link V2. Програматор ST-Link V2 у форм-факторі флешки сумісний з лінійними контролерами STM32 і STM8. Підтримка інтерфейсу SWD, SWIM. ST-LINK дозволяє виконувати програму MCU крок за кроком і контролювати значення всіх регістрів, що значно полегшує проект. Програмісти можуть писати в пам'ять мікроконтролера і сам завантажувач, за допомогою якого можна прошити МК через USB/UART, відновивши контролер.

Рисунок 4.8 — Програматор ST-LINK V2

STLINK V2 (див. рис. 4.8) — програматор і відладчик для мікроконтролерів серій STM8 і STM32, є недорогим аналогом оригінального програматора STLINK від STM. За допомогою ST-LINK MINI дозволено програмувати та налагоджувати через інтерфейси SWIM (для мікроконтролерів STM8), SWD та JTAG (для мікроконтролерів STM32). Всі інтерфейси для комунікації програм (SWIM, SWD, JTAG) виведені на 10-ти контактний роз'єм і доступні для використання і програмування.

5 ТЕСТУВАННЯ ЗАПРОПОНОВАНОГО МЕТОДУ

5.1 Аналіз способу авторизації

Процес обміну починається з так званого POR стану картки, Power-on Reset, або скидання при включенні живлення, що означає, що карта видаватиме сигнал Reset до тих пір, поки напруга не стабілізується. Далі від зчитувача надходить команда REQA — запит картки, або WUPA — запит усіх карток. Карта повинна відповісти кодом ATQA. Цей код залежить від моделі картки та виробника. Механізм антиколізії (команда ANTICOLLISION, код 0x93) використовується для визначення унікального номера картки, UID, з якою зчитувач продовжуватиме роботу при одночасному знаходженні в полі зчитувача кількох карт. UID, отриманий зчитувачем у процесі обміну інформацією складається з 4-х байт і контрольного байта BCC, обчисленого з допомогою операції XOR побітово над цими байтами. 4 байти UID та контрольний байт BCC знаходяться у нульовому блоці нульового сектора пам'яті карти.

У основі механізму антиколізії лежить принцип виявлення біт, одержуваних зчитувачем від карти. При наявності в полі зчитувача одночасно декількох карток вони синхронно відповідають зчитувачу своїми UID-кодами.

Оскільки кожна карта має свій, відмінний від інших UID, то в деякому біту під час передачі UID відбудеться накладання "1" на "0". Зчитувач визначить цю ситуацію як колізію і за певним алгоритмом, встановить значення біта рівним «1» і повторною командою антиколізії надішле частину UID, що закінчується цим бітом, і тільки ті карти, у яких збігається передана зчитувачем частина UID, повинні відповісти частиною своїх UID, що залишилася. За кілька циклів антиколізії зчитувач знатиме UID карти, з якою він продовжить роботу.

Після того, як зчитувачу стає відомий UID карти, він посилає команду SELECT (код 0x93, такий же, як і у команди ANTICOLLISION). Далі слідує байт NVB, рівний розміру команди, що посилається, тобто. 7 повних байт, далі UID карти (4 байти), байт BCC. Формат команди наведено на рис. 5.1.

1 byte	1 byte	4 bytes	1 byte
SELECT	NVB	UID	BCC
0x93	0x7	0xabcdef00	0x1d

Рисунок 5.1 — Команда SELECT

Команда SELECT завершується двома байтами CRC (CRC, або Cyclic Redundancy Check — алгоритм знаходження контрольної сума, призначена для перевірки цілісності даних, що породжує поліном для обчислення CRC MIFARE), обчисленого по семи попереднім байтам.

Щоб отримати доступ до даних на карті, зчитувач повинен пройти процедуру автентифікації. Ця процедура складається з трьох етапів, заснованих на припущенні, що і карта, і зчитувач знають секретний ключ, виходячи з чого кожен із трьох етапів завершиться успішно і стан шифру карти та зчитувача буде однаковим, що у свою чергу уможливить шифрування та дешифрування даних.

Коли зчитувач надсилає запит тегу на проведення будь-якої операції з пам'яттю, він повинен довести, що має право її проведення. Доказом є знання секретного ключа блоку або сектора, операцію з даними якого зчитувач хоче провести. У процесі автентифікації стан шифру зчитувача та тега буде змінюватися послідовно, і в результаті буде однаковим, що дозволить передавати дані вже у зашифрованому вигляді. Після того, як зчитувач надсилає запит на проведення операції тегу, стан шифру зчитувача та тега ініціалізується секретним ключем. У разі успіху весь подальший обмін даними між тегом та зчитувачем буде проводитись у зашифрованому вигляді.

5.2 Огляд протоколу шифрування Crypto1

Більшість систем використовують карти сімейства MIFARE виробництва компанії NXP Semiconductors. Найбільш популярним типом карт є Classic.

Реалізація MIFARE є секретною, і надійність чіпа підтверджена лише його творцями. Більше того, алгоритм шифрування Crypto1, що використовується для захисту даних на картах MIFARE Classic, був винайдений NXP. Документації до цього шифру немає, шифр є пропрієтарним. Надійність шифру, як і надійність чіпу, підтверджується лише компанією NXP.

Crypto1 — пропрієтарний алгоритм шифрування, створений NXP Semiconductors для використання MIFARE Classic карти. Crypto1 є потоковим шифром, дуже схожим на попередній Hitag2. Crypto1 складається з:

— одного 48-бітного LFSR для зберігання секретного стану лінійної функції;

— дворівневої нелінійної функції;

— 16-бітний LFSR, який використовується при аутентифікації.

Початковий стан 48-бітного LFSR визначається секретним ключем, відомим карті та зчитувачу. Кожен новий біт ключового потоку генерується на підставі 18 біт стану LFSR у певний момент часу. Після чого регістр зсувається вліво на один біт, а новий біт, що згенерував, зсувається праворуч .

16-бітний LFSR використовується картою як ГПСЧ. Варто зазначити, що значення, що генеруються, повинні бути 32-бітними, це необхідно для коректної роботи шифру.

Стан LFSR у кожен момент часу визначається поточним значенням, зрушеним вліво на 1 біт, та згенерованим бітом, який зсувається в регістр праворуч.

5.3 Результати перевірки вразливостей

Проаналізовано безпеку смарт-карток на прикладі MIFARE Classic і стійкості шифру Crypto1, що використовується для захисту даних на карті, перевірка здійсненності та ефективності атак, можливість злому ключа та зняття дампу з карти. Варто також зазначити, що аналіз безпеки смарт-карток це аналіз комплексу факторів, які сприяють їх використанню. Сюди входить використання шифру Crypto1 для захисту даних на карті, використання певної інфраструктури,

де використовуються смарт-картки; таким чином, безпека даних на карті прямо залежить від стійкості шифру до злому, яка в свою чергу може виявитися марною, якщо інфраструктура реалізована з помилками і дозволить зловмиснику обійти шифрування. Безпека всієї системи є безпека її найслабшої ланки, тому є важливим унеможливити різні методи, що так чи інакше дозволяють отримати доступ до даних на карті, незалежно від локалізації вразливості.

Вразливості шифру Crypto1 ще не оприлюднені компанією NXP і не є дуже критичними оскільки для авторизації зменшено відстань дії зчитувача до 5 см, а це унеможливлює зловмисникам застосувати пристрої для прослуховування радіосигналів.

Запропонований метод передбачає використання ключа розміром 6 байт, що в свою чергу створює ключ розрядністю 48 біт та передбачає 281 474 976 710 656 можливих комбінацій. Оскільки, час авторизації складає 50 мс, для перебору та злому секретного ключа необхідно близько 450 тисяч років. Натомість сучасні системи пропуску не здатні стати конкурентами з такими показниками та відповідною ціновою категорією.

6 ЕКОНОМІЧНА ЧАСТИНА

6.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку мікропроцесорної системи безконтактної ідентифікація персоналу з додатковим шифруванням. Особливістю програми є підвищено рівень захисту в методах авторизації персоналу з використанням технології RFID за рахунок додаткового шифрування унікальних даних користувача, що безпосередньо зберігаються на електронній картці.

Аналогом може бути Hikvision DS-K1F100-D8E ціною 20 000 грн. (500$).

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п’ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 6.1.

Таблиця 6.1 — Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
2	Багато аналогів на малому ринку	Ринкові п Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
Ринкові переваги					
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів

Усі дані по кожному параметру занесено в таблиці 6.2

Таблиця 6.2 — Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	4	4	4
Наявність аналогів на ринку	4	4	4
Цінова політика	4	4	4
Технічні та споживчі властивості виробу	4	3	4
Експлуатаційні витрати	3	4	4
Ринок збуту	4	3	4
Конкурентоспроможність	3	4	4
Фахівці з комерційної реалізації	4	3	4
Фінансування	4	4	3
Матеріально-технічна база	4	4	3
Термін реалізації ідеї	4	4	4
Супровідна документація	4	3	3
Сума	46	44	45
Середньоарифметична сума балів	(46+44+45) / 3 = 45		

За даними таблиці 6.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 6.3.

Таблиця 6.3 —Рівні комерційного потенціалу розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок того, що в мікропроцесорній системі безконтактної ідентифікація персоналу з додатковим шифруванням підвищено рівень захисту в методах авторизації персоналу з

використанням технології RFID за рахунок додаткового шифрування унікальних даних користувача, що безпосередньо зберігаються на електронній картці.

6.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

6.2.1 Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t \,, \tag{6.1}$$

де М — місячний посадовий оклад конкретного розробника (дослідника), грн.;

$Т_р$ — число робочих днів в місяці, 20 днів;

t — число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 6.4.

Таблиця 6.4 — Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	35000	1750,00	40	70000,000
Програміст	30000	1500,00	40	60000,000
Всього				130000,00

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

6.2.2 Додаткова заробітна плата розробників, які приймали участь в розробці обладнання.

Додаткова заробітна плата прийнято розраховувати як 10 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 10\ \% / 100\ \% \quad (6.2)$$

$З_д = (130000{,}00 \cdot 10\ \% / 100\ \%) = 13000{,}00$ (грн.)

6.2.3 Нарахування на заробітну плату розробників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \quad (6.3)$$

$Н_з = (130000{,}00 + 13000{,}00) \cdot 22\ \% / 100\ \% = 31460{,}00$ (грн.)

6.2.4. Оскільки для розроблювального пристрою було потрібно витрачати обладнення вартість якого не перевищує 20000 грн. (Паяльник QUICKO T12-942 MINI — 1500 грн.) та комплектуючи (Мікроконтролер STM32F103C8T6 — 500 грн., RFID набір з тегами — 100 грн., замовлення розробки друкованої плати через сервіс JLC PCB — 400 грн.), то витрати на них занесемо в повному обсязі в вартість розробки: В = 1500 + 500 + 100 + 400 = 2400 грн.

6.2.5 Амортизація обладнання, яке використовувалось для проведення розробки.

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді амортизація обладнання, що використовувалась для розробки розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (6.4)$$

де Ц — балансова вартість обладнання, грн.;

Т — термін корисного використання обладнання згідно податкового законодавства, років

$t_{вик}$ — термін використання під час розробки, місяців

Розрахуємо, для прикладу, амортизаційні витрати на комп'ютер балансова вартість якого становить 33000 грн., термін його корисного використання згідно податкового законодавства — 2 роки, а термін його фактичного використання — 2,00 міс.

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до таблиці 6.5.

Таблиця 6.5 — Амортизаційні відрахування матеріальних і нематеріальних ресурсів для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія (Ноутбук — hp — pavilion gaming 15)	33000	2	2,00	2750,000
Офісне обладнення (меблі)	25000	4	2,00	1041,667
Приміщення	800000	20	2,00	6666,667
Ліцензійна ОС, та спеціалізовані ліцензійні нематеріальні ресурси (Keil MDK Essential, Proteus PCB design)	23000	2	2,00	1916,667
Всього				12375,00

6.2.6 Тарифи на електроенергію для непобутових споживачів відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників, будуть різними. Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (6.6)$$

де В — вартість 1 кВт-години електроенергії для 1 класу підприємства, В = 6,2 грн./кВт;

П — встановлена потужність обладнання, кВт. П = 0,4 кВт;

Ф — фактична кількість годин роботи обладнання, годин.

$К_п$ — коефіцієнт використання потужності, $К_п$ = 0,9.

6.2.7 Інші витрати та загальновиробничі витрати.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (6.7)$$

де $Н_{ів}$ — норма нарахування за статтею «Інші витрати».

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (6.8)$$

де $Н_{нзв}$ — норма нарахування за статтею «Накладні (загальновиробничі) витрати».

6.2.9 Витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи: $B_{заг}$ = 130000,00 + 13000,00 + 31460,00 + 2400,00 + 12375,00 +231,55+71500+175500 = 436466,55 грн.

6.2.10 Розрахунок загальних витрат на науково-дослідну (науково-технічну) роботу та оформлення її результатів.

Загальні витрати на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються *ЗВ*, визначається за формулою:

$$ЗВ = \frac{B_{заг}}{\eta} \text{ (грн)}, \qquad (5.9)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка: *ЗВ* = 436466,55 / 0,5 = 623524 грн.

6.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

6.3.1 Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (6.10)$$

де $\pm \Delta Ц_o$ — зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N — кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_o$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_o = Ц_б \pm \Delta Ц_o$;

$Цб$ — вартість програмного продукту у році до впровадження результатів розробки;

ΔN — збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

ρ — коефіцієнт, який враховує рентабельність продукту;

ϑ — ставка податку на прибуток, у 2022 році ϑ =18%.

До моменту впровадження результатів наукової розробки реалізації продукту не було. Отже, комерційний ефект від реалізації результатів розробки за три роки складе 86099996,56 грн.

6.3.2 Розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Розраховуємо приведену вартість збільшення всіх чистих прибутків $ПП$, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (6.11)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т – період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t — період часу (в роках).

Збільшення прибутку ми отримаємо починаючи з першого року: 69566770,32 грн.

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (6.12)$$

де $k_{інв}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \quad (6.13)$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{6.14}$$

$T_ж -$ життєвий цикл наукової розробки, роки.

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{6.15}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{6.16}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,35 роки, то фінансування даної наукової розробки є доцільним.

ВИСНОВКИ

У першому розділі роботи виконано аналіз сучасних систем безконтактної ідентифікації, розглянуто найефективніші системи, способи їхньої дії та переваги. Описано недоліки систем, що встановлені на контрольних пунктах пропуску. Продемонстровано зразки пристроїв, що доступні на ринку та їхню вартість. В результаті сформульовано вимоги для системи що буде конкурентом та матиме вищий ступінь захисту ніж запропоновані.

Другим розділом є огляд способів та методів підвищення захищеності авторизації. Розглянуто можливі варіанти несанкціонованого доступу та їх характер та варіанти захисту від них. Проаналізовано відомі недоліки сучасних RFID систем та запропоновано методи для підвищення їх захищеності.

Третій розділ містить в собі огляд способів побудови мікропроцесорних систем та розглянуто платформи, що є найбільш популярними та зручними. Для проектування власної системи розглядались мікроконтролер STM32 та платформа ARDUINO. Виконано порівняння переваг та недоліків та обрано найбільш кращий пристрій. Відображено обрані електронні компоненти, їхні характеристики та параметри. Спроектовано принципову схему, описано алгоритм моделювання друкованої плати, описано процес монтажу елементів та виготовлення готового пристрою.

В четвертому розділі розглянуто технічну документацію для безконтактної роботи з картками. Описано кроки написання бібліотеки та налаштування периферії з використанням програмного середовища Keil. Реалізовано стабільну версію драйвера для роботи з модулем MFRC522.

У п'ятому розділі розглянуто застосований метод, алгоритм роботи та виявлено ряд переваг, що забезпечують захищеність системи.

Шостий розділ містить розрахунок витрат на розробку нового програмного продукту, сума яких складає 623524 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення,

розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,35 роки.

Отже, результатом даної роботи є виконання поставлених завдань і відповідно досягнення мети.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Senthil K., Saravanan M., Jeevananthan S. Microprocessors and microcontrollers: monograph. New York, 2013.

2. Cornel Turcu, Current trends and challenges in RFID: monograph. Croatia: InTech, 2011. 540 с.

3. Хунянь Кан, Анализ и реализация протокола обмена сигналов радиочастотной идентификации на основе эллиптической криптографии: монографія. Хэцзэ, 2016. 102 с.

4. Програмування мікроконтролерів AVR: навчальний посібник/ Цирульник С. М., Азаров О. Д., Крупельницький, Л. В., Трояновська Т. І. Вінниця : ВНТУ, 2018. 111 с.

5. Лизогуб Д. В. Крупельницький Л. В. Особливості безконтактної ідентифікації та допуску персоналу організації. Тези на L конференції НТКП ВНТУ. URL : https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/12021. Дата звернення: Вер. 9, 2022.

6. Структура і переваги систем управління доступу в офісах. [Електронний ресурс]. — Режим доступу: https://protocol.ua/struktura-i-preimushchestva-sistem-upravleniya-dostupa-v-ofisah

7. Маниш Бхуптани, та Шахрам Морадпур, RFID field guide deploying radio frequency identification system. Prentice Hall, 2007.

8. Оптична пам’ять[Електронний ресурс]. — Режим доступу: https://studfile.net/preview/5259889/page:15/ Дата звернення: Вер. 20, 2022.

9. Х.А.Лисенко та О.С.Мельник, Застосування біометричних систем для ідентифікаціїй особи, Юридичні науки 2004

10. Що таке біометрія? [Електронний ресурс]. — Режим доступу: http://www.biometria.org.ua/what-is-biometrics.html. Дата звернення: Вер. 20, 2022.

11. Технології безконтактної ідентифікації [Електронний ресурс]. — Режим доступу: https://stud.com.ua/172354/logistika/ Дата звернення: Вер. 22, 2022.

12. ЩО ТАКЕ СИСТЕМА RFID? [Електронний ресурс]. — Режим доступу: https://idcard.com.ua/ua/blog/ Дата звернення: Вер. 23, 2022.

13. RFID Frequency Bands & Spectrum [Електронний ресурс]. — Режим доступу:https://www.electronics-notes.com/articles/connectivity/rfid-radio-frequency-identification Дата звернення: Вер. 24, 2022.

14. Радіочастотний термінал ATIS [Електронний ресурс]. — Режим доступу: https://atis-security.com/ Дата звернення: Квіт. 27, 2021.

15. Зчитувач безконтактних ідентифікаційних карт Hikvision DS-K1F100-D8E [Електронний ресурс]. — Режим доступу: https://hikvision.co.ua/hikvision-ds-k1f100-d8e Дата звернення: Трав. 1, 2021.

16. Комплект автономной Tecsar Trek SA-TS22/FLASH EM [Електронний ресурс]. — Режим доступу: https://nadzor.ua/product/komplekt-avtonomnoj-tecsar-trek-sa-ts22flash-em Дата звернення: Жовт. 1, 2022.

17. Несанкціонований доступ [Електронний ресурс]. — Режим доступу: https://jak.bono.odessa.ua/articles/nesankcionovanij-dostup-nsd.php Дата звернення: Жовт. 3, 2022.

18. Ідентифікація по захищеним картам Mifare [Електронний ресурс]. — Режим доступу: https://targcontrol.com/vozmozhnosti/identifikaciya-po-zashhishhennym-kartam-mifare/ Дата звернення: Жовт. 3, 2022.

19. Методи автентифікації [Електронний ресурс]. — Режим доступу: http://www.panasenko.ru/Articles/69/69.html Дата звернення: Жовт. 5, 2022.

20. Автентифікація. [Електронний ресурс]. — Режим доступу: https://uk/wikipedia.org/wiki/Автентифікація Дата звернення: Жовт. 5, 2022.

21 Вразливості RFID систем [Електронний ресурс]. — Режим доступу: https://habr.com/ru/company/ppr/blog/437414/ Дата звернення: Жовт. 7 2022.

22. Arduino Duemilanove [Електронний ресурс]. — Режим доступу: https://docs.arduino.cc/retired/boards/arduino-duemilanove Дата звернення: Жовт. 7 2022.

23. Arduino Nano [Електронний ресурс]. — Режим доступу: https://foton.ua/catalog/arduino/plata-arduino-nano.html Дата звернення: Жовт. 10 2022.

24. Arduino Uno [Електронний ресурс]. — Режим доступу: https://arduino.ua/prod32-arduino-uno-rev3-a000066 Дата звернення: Жовт. 10 2022.

25. Arduino Mega [Електронний ресурс]. — Режим доступу: https://uamper.com/Arduino-Mega-2560-R3-оригинал Дата звернення: Жовт. 10 2022.

26. Datasheet — production data [Електронний ресурс]. — Режим доступу: https://www.st.com/resource/en/datasheet/stm32f103c8.pdf Дата звернення: Лист. 5, 2022.

27. MFRC522 Standard performance MIFARE and NTAG frontend [Електронний ресурс]. — Режим доступу: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf Дата звернення: Лист. 5, 2022.

28. RT7272A [Електронний ресурс]. — Режим доступу: https://www.richtek.com/Products/Switching%20Regulators/DC_DC%20Step Down%20Convertor/RT7272A?sc_lang=en&specid=RT7272A Дата звернення: Лист. 7, 2022.

29. MF1S50YYX_V1 Product data sheet COMPANY PUBLIC [Електронний ресурс]. — Режим доступу: http://cache.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf Дата звернення: Лист. 15, 2022.

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

проф.,д.т.н. Азаров О.Д.

"___"_____2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

«Мікропроцесорна система безконтактної ідентифікації персоналу з шифруванням даних»

08-23.МКР.008.00.000 ТЗ

Науковий керівник:

к.т.н., доц. кафедри ОТ ВНТУ

_____Л. В. Крупельницький

Виконав ст. гр. 1КІ-21м

_____Д. В. Лизогуб

ВНТУ 2022

1. Підстава для виконання магістерської кваліфікаційної роботи (МКР**)**

1.1 Підставою для виконання МКР є розкриття поточної проблеми мікропроцесорних систем безконтактної ідентифікації, оскільки кожна система ідентифікації має свої переваги та недоліки, і є важливим пошук найбільш ефективного, стабільного та недорогого рішення;

1.2 Наказ про затвердження теми МКР.

2. Мета МКР і призначення розробки

2.1 Метою роботи є створення мікропроцесорної системи безконтактної ідентифікації, яка дозволяє ідентифікувати персонал та контролювати допуск.

2.2 Розробка призначена для безконтактної ідентифікації та допуску персоналу організації.

3. Вихідні дані для виконання МКР

3.1 Аналіз існуючих систем безконтактної ідентифікації і методи їх побудови;

3.2 Огляд вразливостей та методів захисту авторизації;

3.3 Розглянуто способи побудови мікропроцесорних систем;

3.4 Виготовлення друкованої плати;

3.5 Розробка програмного забезпечення з використанням технічної документації;

3.6 Виконання розрахунків для доведення доцільності нової розробки з економічної точки зору;

4. Вимоги до виконання МКР

- відстань спрацювання до 60мм;
- діапазон робочих температур від мінус 30^{o}C до 70^{o}C;
- розміри не більше 80х60х35 мм;
- конструкція — окремий модуль;
- живлення напругою від 12 до 24 В.

5. Етапи МКР та очікувані результати

Робота виконується в 6 етапів, таблиця А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз сучасних систем безконтактної ідентифікації	27.09	30.09	Аналітичний огляд літературних джерел, задачі досліджень
2	Огляд методів та способів підвищення захищеності авторизації	1.10	5.10	Аналіз вразливостей та пошук методів захисту
3	Аналіз підходів побудови мікропроцесорних систем	10.10	17.10	Розділ 3
4	Розробка програмного забезпечення	19.10	25.10	Розділ 4
5	Тестування запропонованого методу	26.10	1.11	Розділ 5
6	Економічне обгрунтування	5.11	15.11	Економічні розрахунки
	Оформлення пояснювальної записки, графічного матеріалу і презентації	4.12	10.12	Пояснювальна записка, графічний матеріал і презентація
	Підготовка супроводжуючих документів, їх підписування, проходження нормоконтролю та тесту на плагіат	15.12	16.12	Оформлені документи

6. Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, довідка про відповідність оформлення МКР діючим вимогам.

7. Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженою наказом ректора.

8. Вимоги до оформлення ДП

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Едина система конструкторської документації. Основні написи»;

— Методичні вказівки. Кафедра обчислювальної техніки 2022;

— Документами на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21».

ДОДАТОК Б

Призначення виводів мікроконтролера

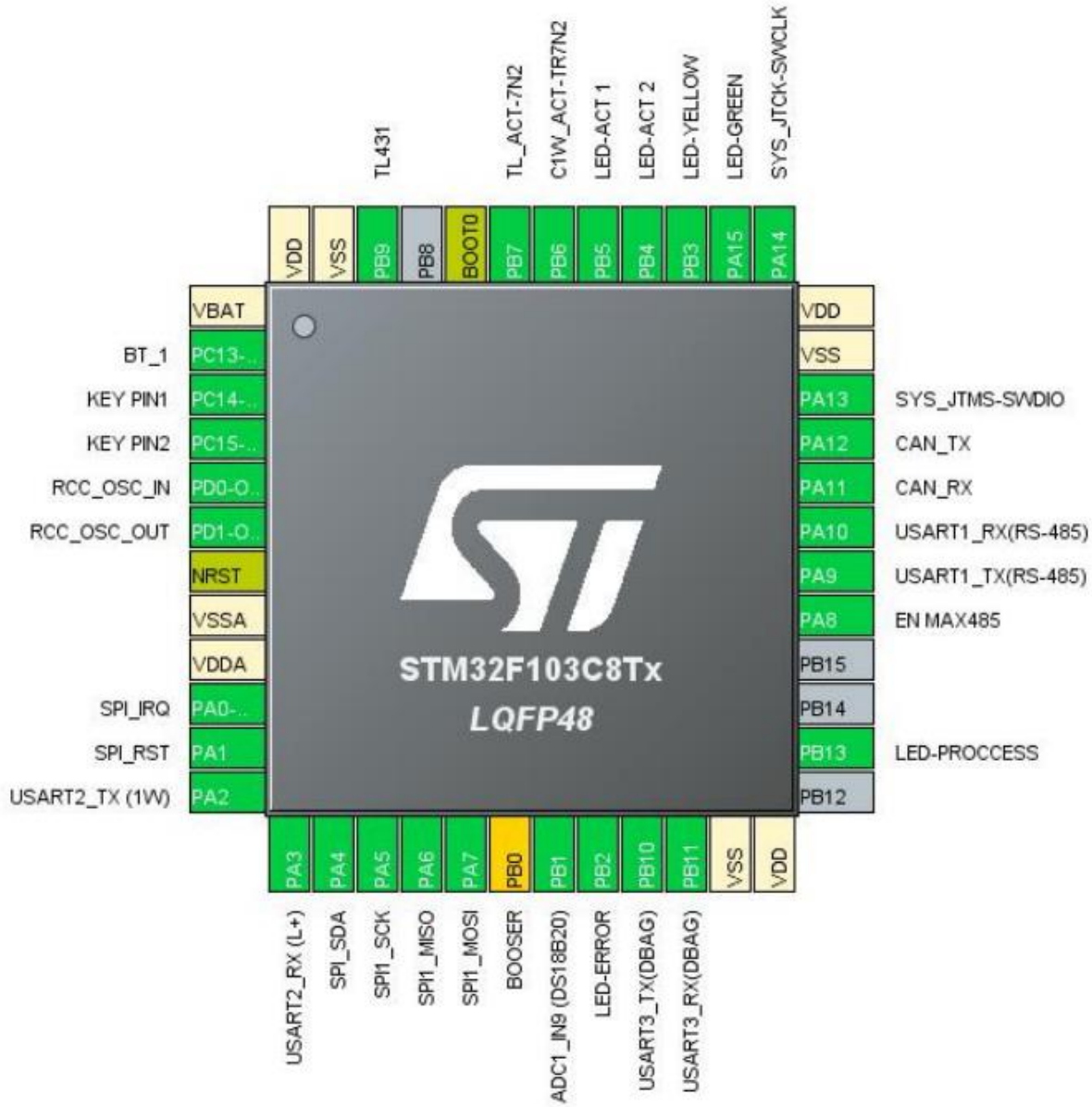


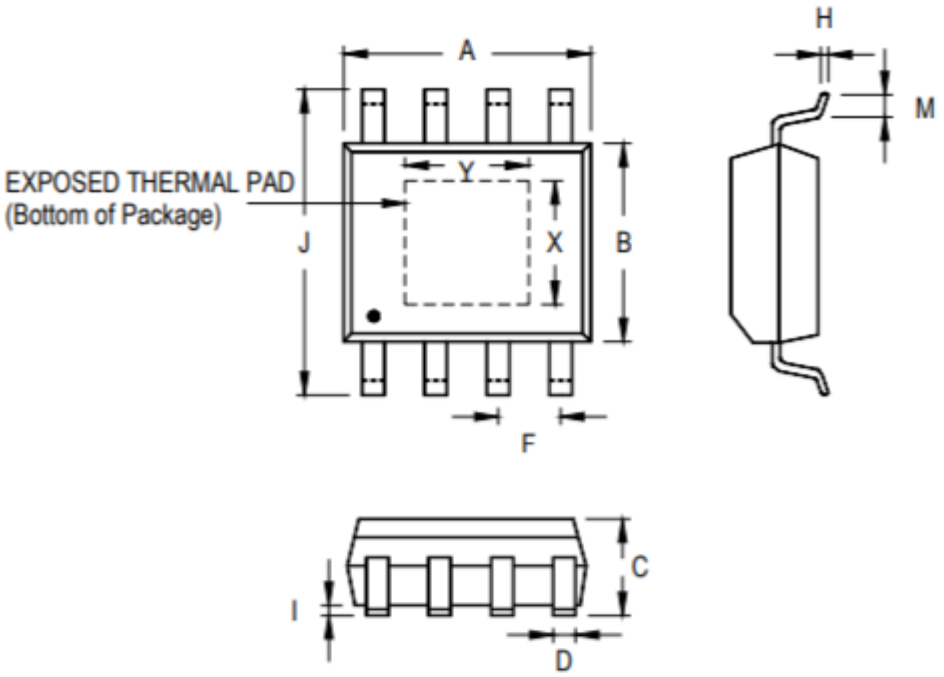
Рисунок 2.1 — Розміщення виводів мікроконтролера

Таблиця 2.1 — Призначення виводів

Pin Number LQFP48	Pin Name (function after reset)	Pin Type	Alternate Function(s)	Label
1	VBAT	Power		
2	PC13-TAMPER-RTC *	I/O	GPIO_Output	BT_1
3	PC14-OSC32_IN *	I/O	GPIO_Output	KEY PIN1
4	PC15-OSC32_OUT *	I/O	GPIO_Output	KEY PIN2
5	PD0-OSC_IN	I/O	RCC_OSC_IN	
6	PD1-OSC_OUT	I/O	RCC_OSC_OUT	
7	NRST	Reset		
8	VSSA	Power		
9	VDDA	Power		
10	PA0-WKUP *	I/O	GPIO_Input	SPI_IRQ
11	PA1 *	I/O	GPIO_Input	SPI_RST
12	PA2	I/O	USART2_TX	USART2_TX (1W)
13	PA3	I/O	USART2_RX	USART2_RX (L+)
14	PA4 *	I/O	GPIO_Input	SPI_SDA
15	PA5	I/O	SPI1_SCK	
16	PA6	I/O	SPI1_MISO	
17	PA7	I/O	SPI1_MOSI	
18	PB0 **	I/O	TIM3_CH3	BOOSER
19	PB1	I/O	ADC1_IN9	ADC1_IN9 (DS18B20)
20	PB2 *	I/O	GPIO_Output	LED-ERROR
21	PB10	I/O	USART3_TX	USART3_TX(DBAG)
22	PB11	I/O	USART3_RX	USART3_RX(DBAG)
23	VSS	Power		
24	VDD	Power		
26	PB13 *	I/O	GPIO_Output	LED-PROCCESS
29	PA8 *	I/O	GPIO_Output	EN MAX485
30	PA9	I/O	USART1_TX	USART1_TX(RS-485)
31	PA10	I/O	USART1_RX	USART1_RX(RS-485)
32	PA11	I/O	CAN_RX	
33	PA12	I/O	CAN_TX	
34	PA13	I/O	SYS_JTMS-SWDIO	
35	VSS	Power		
36	VDD	Power		
37	PA14	I/O	SYS_JTCK-SWCLK	
38	PA15 *	I/O	GPIO_Output	LED-GREEN
39	PB3 *	I/O	GPIO_Output	LED-YELLOW
40	PB4 *	I/O	GPIO_Output	LED-ACT 2
41	PB5 *	I/O	GPIO_Output	LED-ACT 1
42	PB6 *	I/O	GPIO_Output	C1W_ACT-TR7N2
43	PB7 *	I/O	GPIO_Output	TL_ACT-7N2
44	BOOT0	Boot		
46	PB9 *	I/O	GPIO_Output	TL431
47	VSS	Power		
48	VDD	Power		

ДОДАТОК В

Габарити rt7272



Symbol		Dimensions In Millimeters		Dimensions In Inches	
		Min	Max	Min	Max
A		4.801	5.004	0.189	0.197
B		3.810	4.000	0.150	0.157
C		1.346	1.753	0.053	0.069
D		0.330	0.510	0.013	0.020
F		1.194	1.346	0.047	0.053
H		0.170	0.254	0.007	0.010
I		0.000	0.152	0.000	0.006
J		5.791	6.200	0.228	0.244
M		0.406	1.270	0.016	0.050
Option 1	X	2.000	2.300	0.079	0.091
	Y	2.000	2.300	0.079	0.091
Option 2	X	2.100	2.500	0.083	0.098
	Y	3.000	3.500	0.118	0.138

Рисунок 3.1 — Габарити RT7272

ДОДАТОК Г

Габарити ams1117

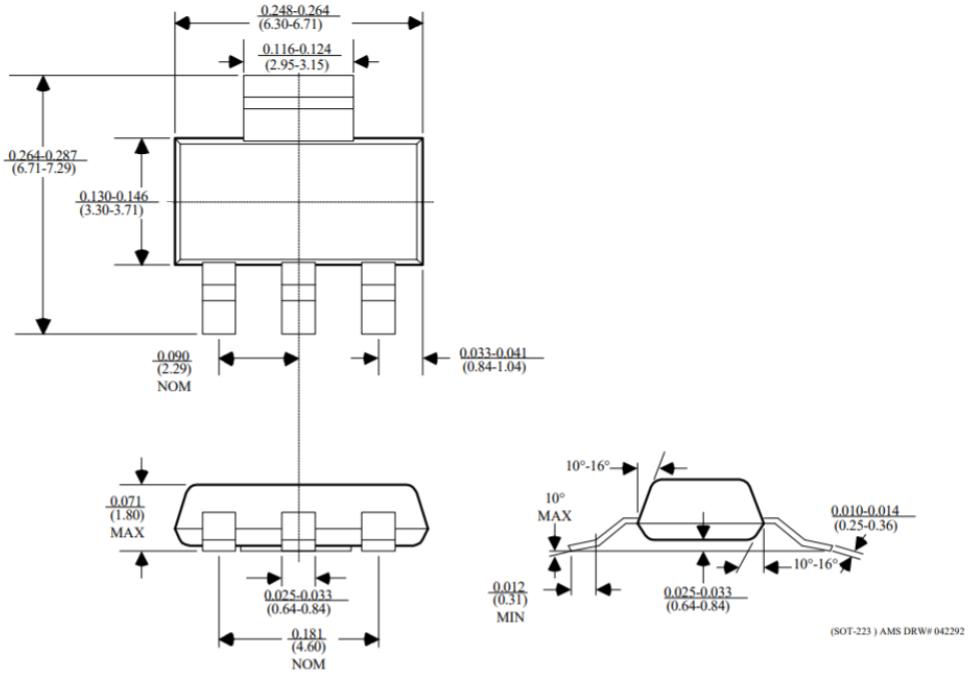
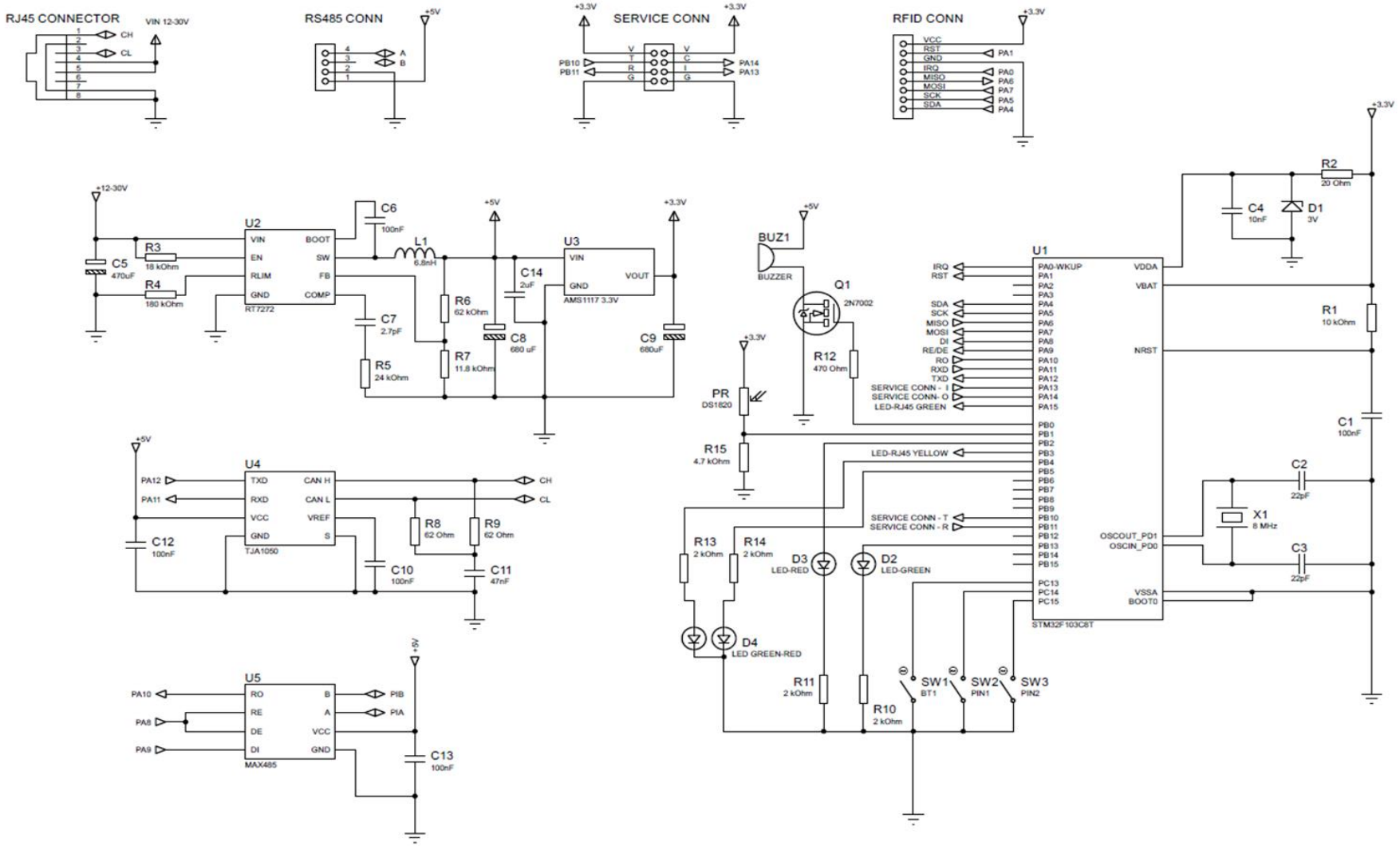


Рисунок 4.1 — Габарити ams1117

ДОДАТОК Д

Схема електрична принципова



					08-23.МКР.008.00.000 Е3			
Зм	Лист	№ докум.	Підпис	Дата				
Розробив		Лизогуб Д.В.			Мікропроцесорна система	Літ	Маса	Масштаб
Перевірив		Крупельницький Л.В.						
Реценз.		Коваленко О.О.			Схема електрична принципова	Аркуш 1	Аркушів 1	
Н. контр.		Швець С.І.				1КІ-21м		
Затверд.		Азаров О. Д.						

Позн.	Найменування	Кіл.	Примітка
A1	Модуль MFRC522	1	
	Конденсатори		
C1	SMD-1812 — 100 нФ ±10%	1	
C2,C3	SMD-1812 — 22 пФ ±10%	2	
C4	SMD-1206 — 10 нФ ±10%	1	
C5	SMD-D — 470 мФ ±10%	1	
C6	SMD-0805 — 100 нФ ±10%	1	
C7	SMD-1206 — 2.7 пФ ±10%	1	
C8, C9	SMD-1812 — 660 мФ ±10%	2	
C10,C12,C13	SMD-1812 —100 нФ ±10%	3	
C11	SMD-1812 — 47 нФ ±10%	1	
C14	SMD-1812 — 2 мФ ±10%	1	
	Мікросхеми		
U1	STM32F103C8T6	1	
U2	RT7272	1	
U3	AMS1117	1	
U4	TJA1050	1	
U5	MAX485	1	
	Резистори		
R1	SMD-1206, 10 кОм ± 5%	1	
R2	SMD-1206, 20 Ом±5%	1	
R3	SMD-1206, 18 кОм±5%	1	
R4	SMD-1206, 180 Ом±5%	1	
R5	SMD-1206, 24 кОм±5%	1	
R6	SMD-1206, 62 кОм±5%	1	

					08-23.МКР.008.00.000 ПЗ
Змн.	Арк.	№ докум.	Підпис	Дата	
Розроб.		Лизогуб Д.В.			Мікропроцесорна система Перелік елементів
Перевір.		Крупельницький Л.В			
Реценз.		Коваленко О.О.			
Н. Контр.		Швець С.І.			
Затверд.		Азаров О.Д.			

Літ.	Арк.	Акрушів
	85	94

1КІ-21М

Позн.	Найменування	Кіл.	Примітка
R7	*SMD-1206, 8 кОм±5%*	*1*	
R8,R9	*SMD-1206, 62 Ом±5%*	*2*	
R10,R11	*SMD-1206, 2 кОм±5%*	*2*	
R12	*SMD-1206, 470 Ом±5%*	*1*	
R13,R14	*SMD-1206, 2 кОм±5%*	*2*	
R15	*SMD-1206, 4.7 кОм±5%*	*1*	
D1	*Стабілітрон 3,3 В*	*1*	
D2,D4	*Світлодіоди*	*2*	
Q1	*Транзистор 2N7002*	*1*	
BUZ1	*Дзвінок*	*1*	
X1	*Кварцовий генератор*	*1*	

ДОДАТОК Е

Алгоритм комбінації бітів доступу

Table 6. Access conditions

Access Bits	Valid Commands		Block	Description
$C1_3$, $C2_3$, $C3_3$	read, write	→	3	sector trailer
$C1_2$, $C2_2$, $C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1$, $C2_1$, $C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0$,$C2_0$, $C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

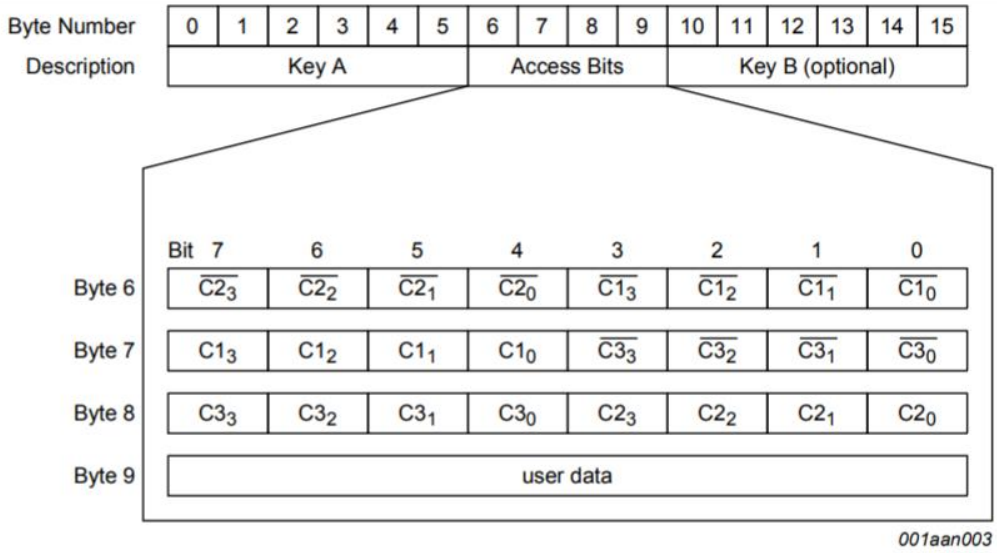
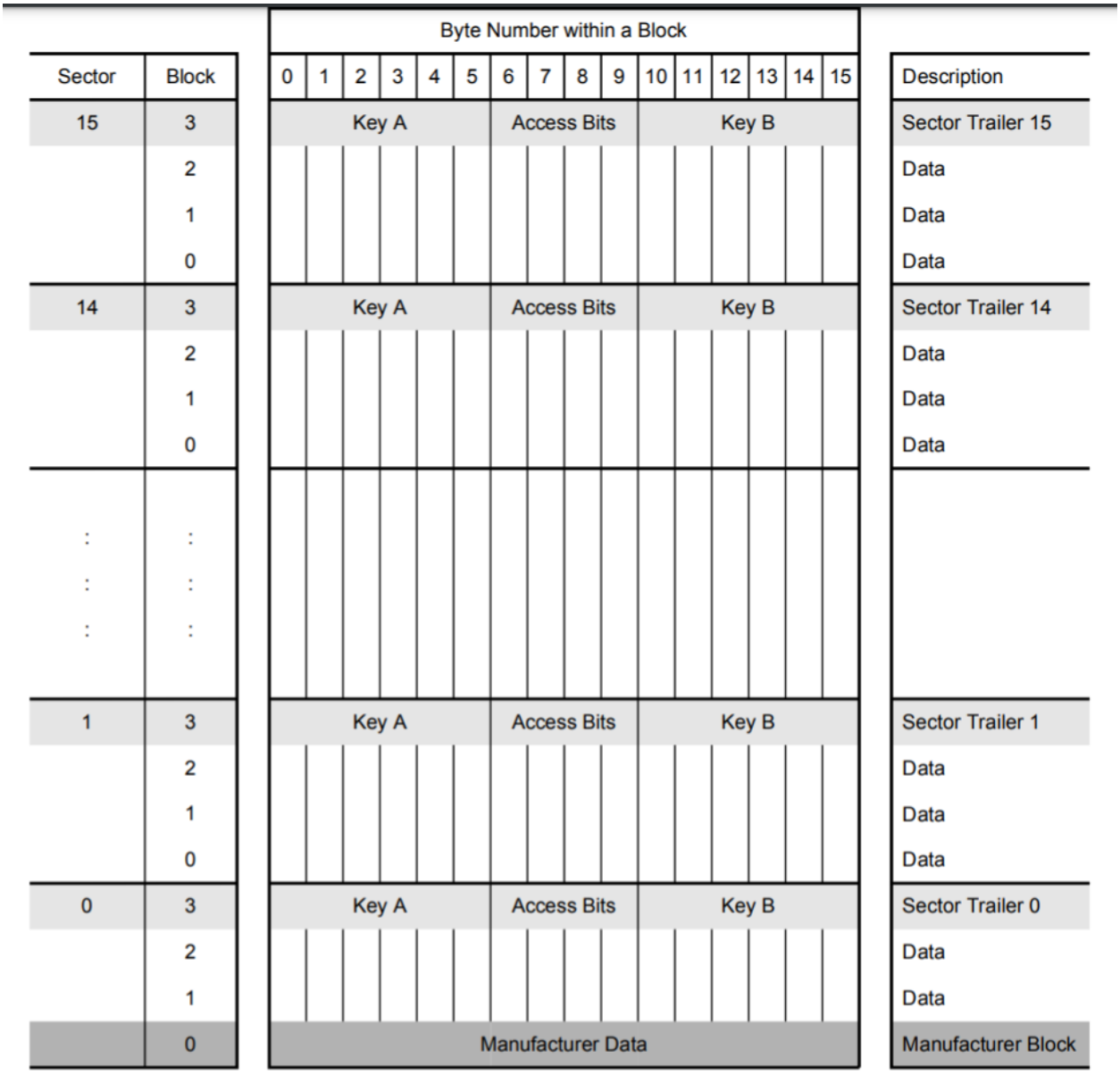


Figure 10. Access conditions

Рисунок 7.1 — Комбінації бітів доступу

ДОДАТОК Ж

Структура карти



Sector	Block	Byte Number within a Block															Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0	Manufacturer Data																Manufacturer Block

Рисунок 8.1 — Структура карти

ДОДАТОК И

Алгоритм роботи з картою

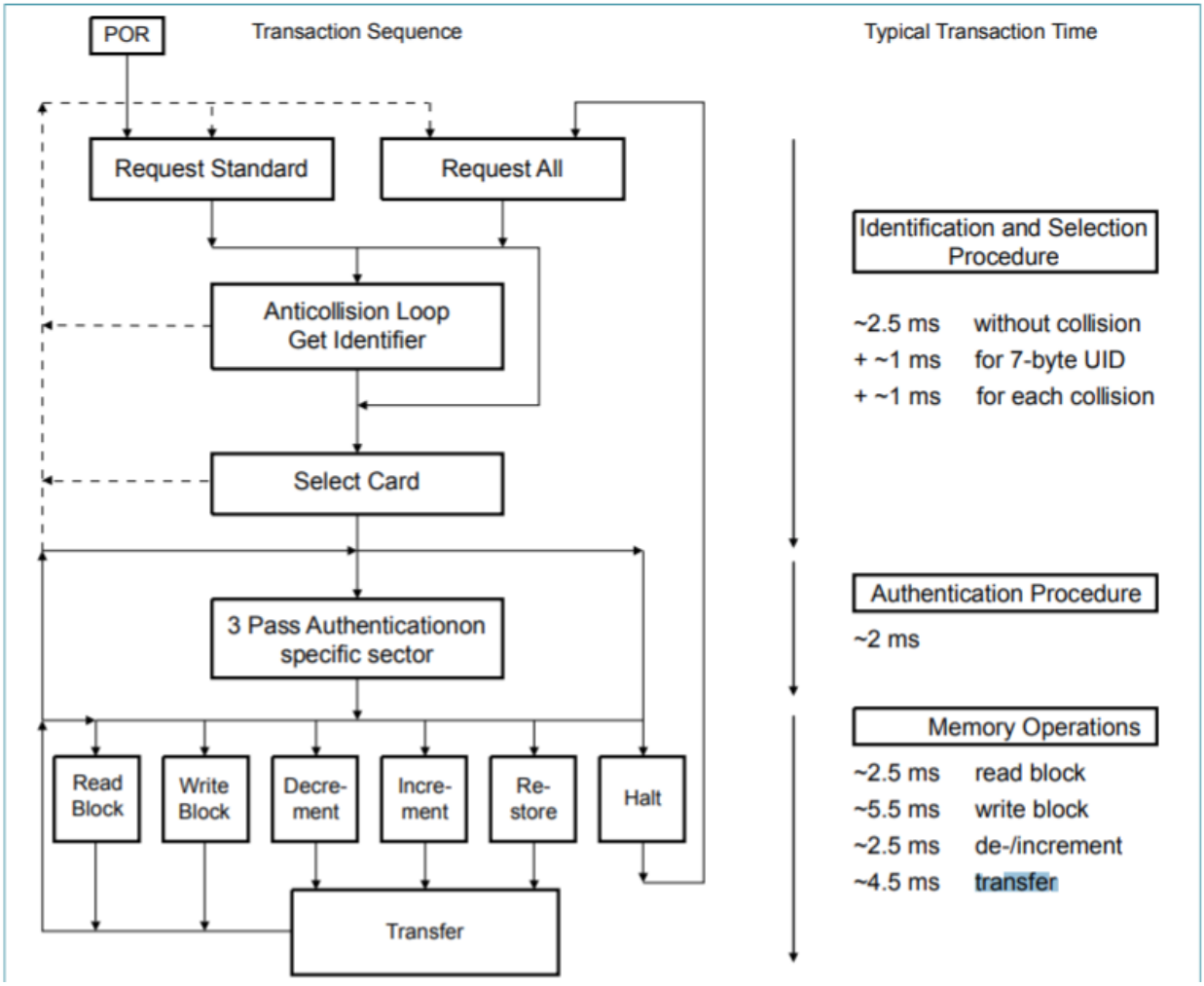


Рисунок 9.1 — Алгоритм роботи з картою

ДОДАТОК К

Лістинг програми

```
class RC522_class
{
public:
        void Init(void);
        void Init_MFRC522(void);
        void loop();
        void Set_Curent_Key(uint32_t __key_MSB,uint32_t __key_LSB);
        uint8_t Set_New_Key(uint8_t __num_block, uint32_t __key_MSB,uint32_t
__key_LSB);
  uint8_t Write_Sector(uint8_t __num_sector, uint8_t *__data);
        uint8_t Check_Key(uint8_t __num_block, uint32_t __key_MSB,uint32_t
__key_LSB);                  // Check key/ return 1 if Key access is true
        uint16_t Read_Card(u8 *__bufer);
                                ////45 blocks * 16 byte
        uint16_t Read_Block(u8 __num_Block, u8 *__bufer);          /// num Block
0-45  bufer = 16 byte
        uint16_t Read_Sector(u8 __num_Sector, u8 *__bufer);        /// num Sector
0-15  bufer = 16 byte*3
        uint8_t Write_Block(uint8_t __num_block, uint8_t *__data); ////16 byte

        u8 flag_card_include;
        u8 flag_error;
        u8 flag_new_card;
        u16 cnt_no_card;
        uint8_t version;
        uint8_t uid[7];
        u8 control_on;

        void Debug(char* __data, uint32_t __num = 0, uint8_t __count_system =
0);
private:

        uint8_t Scan_Efir();
        uint8_t Read_Version(void);
        void Send_Byte(uint8_t __data);
        uint8_t Get_Byte(void);
        uint8_t Read_Data(uint8_t __cmd);
        void Write_Data(uint8_t __cmd, uint8_t __data );
        void Send_REQA(void);
        void Anticolision(void);
```

```
        uint16_t Read_REQA(void);
        uint16_t Read_UID(void);
        uint16_t Calculate_CRC(uint8_t *__arr = 0, uint8_t __size = 0);
        uint16_t Authenticate(uint8_t __num_sector, uint8_t *__key);
        uint16_t R_Card();
        uint16_t R_Block(uint8_t __num_block, u8 __key = 0);
        uint16_t R_Sector(uint8_t __num_sector);
        uint8_t W_Block(uint8_t __num_block, uint8_t *__data);
        void HEX_Table(uint8_t* __data, uint8_t __size);
        uint8_t Check_is_corect_UID();
        void Calculate_Accses_Bits (uint8_t *__ac_b );

        uint8_t busy;
        uint8_t crc[2];
                uint8_t KEY_A[6], KEY_B[6], AccsesBits[4], Acces_Key[6];    ////
block 4 //// secktor trailer
        u8 sector_trailer[16];
        Sector_struct sector[16];  /// strucct for data from card
                //Access_conditions_struct access_conditions;   /// arr 12 byte,   4
block * 3/////// ( C1 C2 C3)
        uint8_t init_combinations[18];
        uint8_t reqa_combinations[8] ;
        uint8_t auth_combinations[24];
        uint8_t read_combinations[12];
        uint8_t anticol_combinations[8];
        uint8_t prep_write_combinations[12] ;
        uint8_t write_combinations[40];
};


//=== Transmite information to SPI
void RC522_class::Send_Byte(uint8_t __data)
{
        while(!(RC522_INTERFACE_SPI->SR & SPI_SR_TXE));
        RC522_INTERFACE_SPI->DR = __data;
        while(!(RC522_INTERFACE_SPI->SR & SPI_SR_TXE));
}
uint8_t RC522_class::Get_Byte()
{
        u8 m = RC522_INTERFACE_SPI->DR;
        RC522_INTERFACE_SPI->DR = 0xFF;
        while(!(RC522_INTERFACE_SPI->SR & SPI_SR_TXE)){};
        while(!(RC522_INTERFACE_SPI->SR & SPI_SR_RXNE)){};
        return (RC522_INTERFACE_SPI->DR);
}
```

```
uint8_t RC522_class::Check_Key(uint8_t __num_block, uint32_t
__key_MSB,uint32_t __key_LSB)
{
		u8 k = (__num_block/3 ) * 4;

		Acces_Key[0]  =    (__key_MSB &0x00FF0000)>>16;
		Acces_Key[1]  =  (__key_MSB &0x0000FF00)>>8;
		Acces_Key[2]  =  (__key_MSB &0x000000FF);
		Acces_Key[3]  =  (__key_LSB &0x00FF0000)>>16;
		Acces_Key[4]  =  (__key_LSB &0x0000FF00)>>8;
		Acces_Key[5]  =  (__key_LSB &0x000000FF);

		if (Authenticate(k,Acces_Key) == 1)
		{
			return 1;
		}

		return 0;
}

uint16_t RC522_class::Calculate_CRC( uint8_t *__arr, uint8_t __size )
{
	if (__size == 0)
	{
		return 0;
	}
else
{
		for (uint8_t i = 0; i < __size-1 ;i+=2 )
		{
			for(int j =0; j < RC522_SPEED/50; j ++){}
			Write_Data(__arr[i], __arr[i+1]);
		}
		Write_Data(RC522_REG_CMD, 0x03);
		Write_Data(RC522_REG_CMD, 0x00);

		crc[0] = Read_Data(RC522_GET_CRC_FSB);
		crc[1] = Read_Data(RC522_GET_CRC_LSB);
//		Debug((char*)"CRC 1 = ", crc[0], 16 );
//		Debug((char*)"CRC 2 = ", crc[1], 16 );
		return 1;
}
}
```

```
uint8_t RC522_class::Read_Data(uint8_t __cmd)
{
	u8 buff;
	RC522_CS_LOW;
	for(int i =0; i < RC522_SPEED/50; i ++){}
	RC522.Send_Byte(((__cmd<<1)|0x80));
	buff = RC522.Get_Byte();

	RC522_CS_HIGH;
	return buff;
}

void RC522_class::Write_Data(uint8_t __cmd, uint8_t __data )
{
		RC522_CS_LOW; for(int j =0; j < RC522_SPEED/50; j ++){}
		Send_Byte((__cmd<<1)&0x7E);
		Send_Byte(__data);
		RC522_CS_HIGH;

		for(int j =0; j < RC522_SPEED/10; j ++){}
}
```

ДОДАТОК Л

Протокол перевірки кваліфікаційної роботи

Назва роботи: Мікропрцесорна система безконтактної ідентифікаї персоналу з шифруванням даних

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра обчислювальної техніки

Показники звіту подібності Unicheck

Оригінальність 98,1% Схожість 1,9%

Аналіз звіту подібності (відмітити потрібне):

+ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.

□ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Лизогуб Д.В.

Керівник роботи _____ Крупельницький Л.В.