

*Мурашова Валерия Вячеславовна,
обучающаяся 5 курса,
ФГАОУ ВО «Мурманский арктический университет»,
г. Мурманск, Россия*

АППАРАТНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА С ДВУХФАКТОРНОЙ ИДЕНТИФИКАЦИЕЙ

***Аннотация:** Статья посвящена разработке и экспериментальному исследованию системы контроля доступа с двухфакторной идентификацией на основе RFID карты и отпечатка пальца. Обоснован выбор элементной базы (Arduino Uno, RC522, FPM10A), представлена математическая модель в виде конечного автомата, описана программная реализация на C++. Приведены результаты тестирования макета: частота ложного допуска 0%, полный цикл идентификации $\approx 0,7$ с. Показана возможность использования макета в учебном процессе по радиотехническим дисциплинам.*

***Ключевые слова:** двухфакторная идентификация, СКУД, RFID, биометрия, отпечаток пальца, Arduino, конечный автомат, система контроля доступа.*

***Murashova Valeria Vyacheslavovna,
5th year student,
Murmansk Arctic University,
Murmansk, Russia***

HARDWARE IMPLEMENTATION OF A TWOFACTOR AUTHENTICATION ACCESS CONTROL SYSTEM PROTOTYPE

Abstract: *The article is devoted to the development and experimental study of an access control system prototype with twofactor authentication based on an RFID card and fingerprint. The choice of components (Arduino Uno, RC522, FPM10A) is justified, a mathematical model in the form of a finite state machine is presented, and the software implementation in C++ is described. The testing results are presented: false acceptance rate 0%, full identification cycle ≈ 0.7 s. The possibility of using the prototype in the educational process for radio engineering disciplines is shown.*

Keywords: *twofactor authentication, ACS, RFID, biometrics, fingerprint, Arduino, finite state machine, access control system.*

Введение

Обеспечение безопасности объектов различного назначения является одной из приоритетных задач. Классические системы контроля доступа (СКУД), основанные на механических ключах, электронных картах или PIN кодах, имеют существенные недостатки: ключи и карты могут быть утрачены или потеряны, PIN коды – подобраны или подсмотрены. Это делает однофакторные методы аутентификации недостаточно надёжными для защиты важных объектов. Повысить уровень безопасности позволяет двухфакторная идентификация, которая требует предъявления двух различных факторов аутентификации. Наиболее перспективным является сочетание RFID карты (фактор владения) и биометрического параметра – отпечатка пальца (фактор свойства) [1]. Цель работы – разработать версию аппаратной реализации и провести экспериментальное исследование макета СКУД с двухфакторной идентификацией на основе RFID и биометрии.

Результаты исследования

Обоснование выбора элементной базы

Для реализации макета был выбран микроконтроллер Arduino Uno [2] ввиду его доступности, наличия встроенного источника питания (возможность

работы от 9В) и большого количества готовых библиотек[2]. В качестве RFID считывателя предлагается использование модуля RC522 (частота 13,56 МГц, интерфейс SPI), позволяющего считывать UID карты стандарта MIFARE. Для биометрической идентификации более оптимальным является оптический сканер отпечатков пальцев FPM10A (интерфейс UART, память до 162 отпечатков). В макетном исполнении применён сервопривод SG90, имитирующий открытие двери. Для информирования оператора используется LCD дисплей 16×2 с I2C модулем, светодиодная (красный, жёлтый, зелёный) и звуковой зуммер. Для снижения взаимных помех цифровые компоненты (RFID, сервопривод, светодиоды) подключены к цифровой земле (DGND), а сканер отпечатков – к аналоговой земле (AGND) с соединением в одной точке у источника питания.

Математическая модель в виде конечного автомата

Логика работы системы реализована в виде конечного автомата, содержащего семь состояний (таблица 1). Переходы между состояниями осуществляются под действием входных событий: приложение карты администратора («card_admin»), карты пользователя («card_user»), неизвестной карты («card_unknown»), корректного/некорректного отпечатка («finger_correct»/«finger_incorrect»), истечение таймаута («timeout») и др. Взаимно однозначное соответствие между RFID картой и отпечатком задаётся структурой «User { byte uid; uint8_t fingerprintID; bool valid; }, хранящейся в EEPROM (до 10 пользователей). Мастеркарта администратора имеет фиксированный UID, её отпечатку присвоен ID=100.

Таблица 1.

Состояния системы контроля доступа

Обозначение	Наименование	Описание
S ₀	STATE_IDLE	Ожидание карты, горит красный светодиод
S ₁	STATE_WAIT_FINGER	Карта считана, мигает жёлтый светодиод

S ₂	STATE_ACCESS_GRANTED	Доступ разрешён, дверь открыта (3 с)
S ₃	STATE_ADMIN_MODE	Режим администратора (таймаут 15 с)
S ₄	STATE_ADD_WAIT_CARD	Ожидание новой карты для добавления
S ₅	STATE_ADD_WAIT_FINGER	Ожидание отпечатка для добавления
S ₆	STATE_DELETE_WAIT_CARD	Ожидание карты для удаления

Программная реализация

Программное обеспечение разработано на языке C++ в среде Arduino IDE [2]. Код разделён на две независимые части: для точки доступа (управление RFID, сканером отпечатков, сервоприводом, индикацией) и для пульта охраны (отображение информации на LCD дисплее). Связь между платами организована по проводному UART (пины A0, A1, скорость 57600 бод). Конечный автомат реализован через перечисление «enum State» и оператор «switchcase» в основном цикле. Основные функции:

«grantAccess()» – поворот сервопривода на 90°, зелёный LED, звуковой сигнал;

«denyAccess()» – красный LED, длинный звуковой сигнал;

«enrollFingerprint(id)» – запись нового отпечатка (два прикладывания);

«findUserByUID(uid)» – поиск пользователя в EEPROM.

Временные характеристики: таймаут ожидания отпечатка – 15 с, время открытия двери – 3 с. Полный цикл идентификации составляет $\approx 0,7$ с (считывание карты 50 мс, сканирование отпечатка 300 мс, поиск 75 мс, обработка 50 мс, поворот сервопривода 200 мс).

Исследование работы предлагаемой системы на базе макета

Реализация системы выполнена на двух макетных платах методом навесного монтажа. Проведено тестирование по следующим сценариям (всего 150 попыток):

1. Успешная идентификация – зарегистрированная карта + соответствующий отпечаток: дверь открывается, на пульте «DOSTUP RAZRESHEN!».

2. Неизвестная карта – доступ запрещён, на пульте «Unknown card Access denied».

3. Неверный отпечаток – карта распознана, отпечаток не совпадает: доступ запрещён, «Wrong finger Access denied».

4. Режим администратора – мастеркарта + отпечаток администратора: вход в админрежим, возможность добавления (однократное прикладывание новой карты + два прикладывания пальца) и удаления (двойное быстрое прикладывание карты пользователя) пользователей без перепрошивки.

Результаты тестирования показали: частота ложного допуска (FAR) – 0%, частота ложного отказа (FRR) – менее 5% (при сухом или загрязнённом пальце). Все заявленные функции работают корректно. На рисунке 1 представлен общий вид собранного макета.

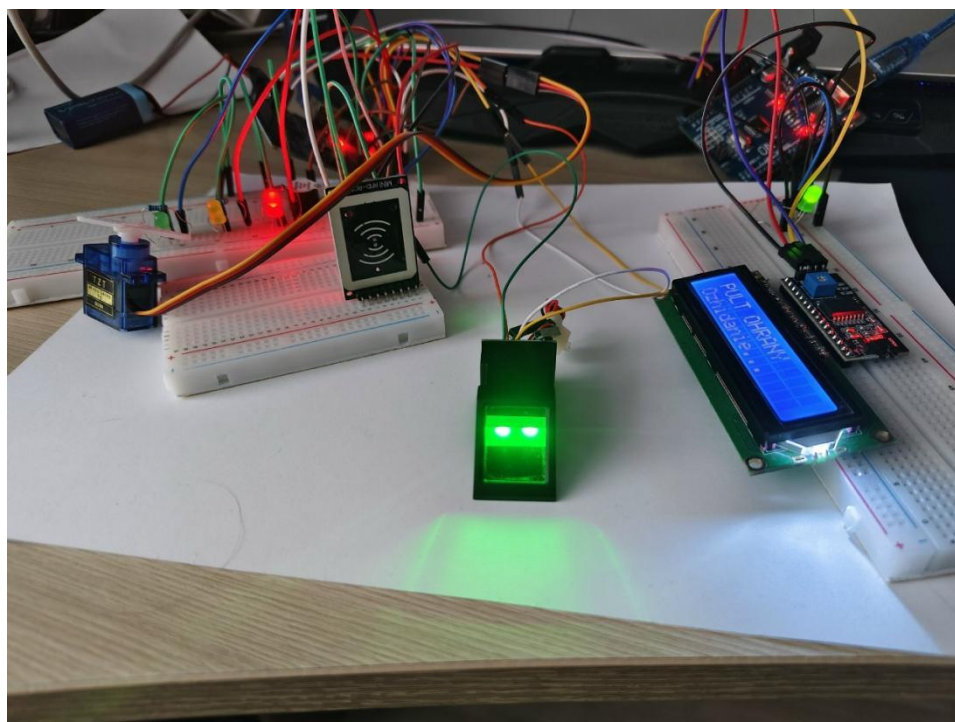


Рисунок 1. Общий вид макета: точка доступа

Заключение

Цель реализации версии аппаратной разработки и экспериментальных исследований СКУД с двухфакторной идентификацией на основе RFID и биометрии достигнута.

Разработан и экспериментально исследована работа системы контроля доступа с двухфакторной идентификацией (RFID карта + отпечаток пальца) на базе действующего макета. Подтверждён правильный выбор элементной базы (Arduino Uno, RC522, FPM10A). Выполненная математическая модель в виде конечного автомата позволила формализовать логику системы и упростить отладку программного обеспечения. Экспериментальные исследования показали: полный цикл идентификации $\approx 0,7$ с, FAR = 0%, FRR < 5%. Система поддерживает добавление и удаление пользователей без перепрошивки (до 10 пользователей, EEPROM). Разработка может быть рекомендована для использования в учебном процессе по дисциплинам «Охранные радиоэлектронные системы», «Цифровые устройства и микропроцессоры», «Схемотехника аналоговых электронных устройств» для демонстрации принципов построения современных СКУД.

Литература:

1. Петин В. А. Проекты с использованием контроллера Arduino. – 2е изд. – СПб. : БХВПетербург, 2015. – 464 с.
2. Соммер У. Программирование микроконтроллерных плат Arduino/Freeduino. – СПб. : БХВПетербург, 2012. – 256 с.
3. ГОСТ 2.7012019. Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению. – М. : Стандартинформ, 2019. – 28 с.