УДК 62-526

Д. Г. Писаренко

Ю. Ю. Нестюк

А. С. Васюра

СУЧАСНА СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Вінницький Національний Технічний Університет

Анотація

Проведено аналіз сучасних систем контролю та управління доступом. Досліджено методи автентифікації по відбиткам пальців для застосування в засобах ідентифікації. Запропоновано реалізацію системи контролю та управління доступом на базі платформи Arduino з використанням оптичного сканера відбитків пальців в якості зчитувального пристрою біометричних даних, що ідентифікують особу.

Ключові слова: безпека, контроль, ідентифікація, біометрія, відбитки пальців, Arduino, Wi-Fi, підвищення ефективності.

Abstract

The analysis of modern systems of access control and management is carried out. Fingerprint authentication methods for use in identification tools are explored. An implementation of an Arduino platform based access control and control system is proposed using an optical fingerprint scanner as a biometric identity reader.

Keywords: security, control, identification, biometric authentication, fingerprints, Arduino, Wi-Fi, improving efficiency.

Вступ

Сучасні системи контролю та управління доступом (СКУД) – це об'єднанні в комплексі електронні, механічні, електротехнічні, апаратно-програмні та інші засоби, що забезпечують можливість доступу визначеного персоналу в певні зони або до певної апаратури, технічних засобів, та обмежують доступ суб'єктам, які не мають таких прав, що надзвичайно важливо для інформаційної безпеки об’єктів. СКУД можуть здійснювати контроль пересування співробітників та транспорту по території, що охороняється, забезпечувати безпеку персоналу і відвідувачів, та збереження матеріальних і інформаційних ресурсів підприємства. СКУД є також засобом автоматизації відслідковування виконання завдань, що пов’язані з безпекою та контролем осіб.

Системи контролю та управління доступом можуть мати різні конфігурації: від найпростіших, розрахованих на поодинокі двері, до надзвичайно складних, розрахованих на забезпечення контролю та управління доступом до важливих, стратегічних об’єктів (заводів, підприємств, банків тощо).

Кожна система доступу, якою б складною вона не була, обов'язково поєднує в собі наступне: контролери, зчитувачі (пристрої ідентифікації) та технічні засоби обмеження доступу - виконавчі пристрої (електромагнітні замки, засувки, турнікети тощо).

Контролери - це головна частина системи контролю доступу. Саме контролери приймають рішення про дозвіл або заборону доступу на об’єкт. Коли співробітник або відвідувач пред'являє ідентифікатор (електронний ключ) - proximity карту чи особисті біометричні дані, зчитаний індивідуальний код

порівнюється з кодом, який зберігається в пам'яті контролера. На підставі порівняння охоронна система дозволяє або, відповідно, забороняє доступ на охоронний об’єкт.

Метою даної роботи є підвищення ефективності контролю та управління доступом на режимному об’єкті.

Результати дослідження

Об'єктом дослідження є процес розробки СКУД на базі платформи Arduino в якості контролера, що дозволить ефективно забезпечувати контроль та обмеження кола персоналу, шляхом ідентифікації осіб за їх біометричними показниками.

Предметом дослідження є методи, засоби та інструменти контролю і управління, розробленого апаратно-програмного продукту на основі використання біометричних особливостей суб’єктів.

Якісно організована з використанням сучасних технічних засобів СКУД дозволяє вирішувати цілий ряд питань. До найбільш важливих слід віднести:

- протидія промисловому шпигунству, крадіжкам, саботажу, навмисному пошкодженню матеріальних цінностей;
- облік робочого часу;
- регулювання потоку відвідувачів;
- реєстрація і повідомлення про випадки спроб проникнення в приміщення, що охороняються;
- контроль в'їзду та виїзду транспорту.

Окрім того, системи контролю та управляння доступом – це перепона для "допитливих". На сьогоднішній день існує велика кількість різновидів СКУД від різних виробників, а також її складових. Не зважаючи на унікальність кожної системи, вони складається з чотирьох головних елементів:

- ідентифікатор користувача;
- прилад ідентифікації;
- керуючий контролер;
- виконавчі пристрої.

Користувацькі права для доступу та ідентифікації можуть бути реалізовані різними методами і засобами, наприклад, використанням паролів, особистих PIN-кодів, радіочастотних технологій, біометрії. Для підтвердження своїх прав особа може пред'явити ті, чи інші ідентифікатори, такі як електронні картки, радіочастотні ідентифікатори, особисті біометричні дані для зчитування системою.

В даній роботі для ідентифікації суб’єкта пропонується використання біометричні даних. Найпоширенішою біометричною технологією автентифікації користувача є ідентифікація за відбитком пальця. Основою методу цієї ідентифікації є використання унікального малюнка папілярних візерунків на пальцях людей. Відбиток можна отримати застосовуючи сканер відбитків пальців. Сканер зчитує папілярний візерунок, перетворює його в цифрову модель і потім проводить порівняння з раніше введеним малюнком, який прийнято вважати еталонним.

Основні види папілярних візерунків (рис. 1):

- арка;
- петля;
- завиток.

Рис. 1 - Основні види папілярних візерунків

В зв’язку з тим, що відбиток досить малий, необхідне застосування вузько направлених методів. Алгоритм розпізнавання відбитків пальців реалізується наступним чином: після отримання рисунка відбитка за допомогою сканера, він перетворюється в цифрову модель. З графічного зображення виділяються ключові характерні точки з яких формується цифрова модель відбитка. У сучасних системах береться від 12- 24 ключових точок. При виборі більшої кількості ключових точок, сучасних обчислювальних ресурсів не вистачає для нормальної експлуатації системи в зв'язку з низькою швидкістю ідентифікації. При виборі меншої кількості точок, існує велика ймовірність допуску чужого відбитку пальця. Тому необхідно брати певне середнє значення для задоволення обох вимог.

Для реалізації функції зчитування біометричних даних використовується оптичний сканер відбитків FPM10A(ZFM60XSA) (рис. 2).

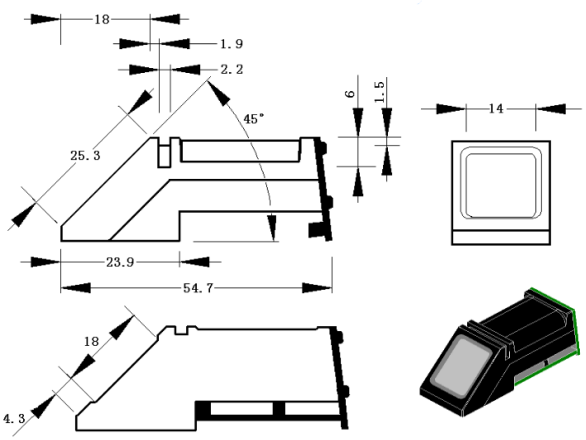

Рис. 2 - Оптичний сканер відбитків FPM10A

Модуль побудовано на процесорі ARM Cortex M 32-bit - Synochip AS608, завдяки якому забезпечується підтримка алгоритмів шифрування даних, створюється база відбитків у внутрішній пам'яті та порівняння по шаблону. Сканер може керуватися, як комп'ютером так і самою платформою Arduino. Останній варіант дозволяє використовувати сканер в автономних пристроях. Живлення модулю складає 3,6-6 В, споживання струму 120 мА. Час, який необхідний для опрацювання відбитку, менше 1 секунди.

Взаємодія з модулем відбувається за допомогою пакетів, які мають в собі контрольну суму. Модуль складається з камери, кількох буферів та флеш пам’яті де зберігаються шаблони (рис. 3).

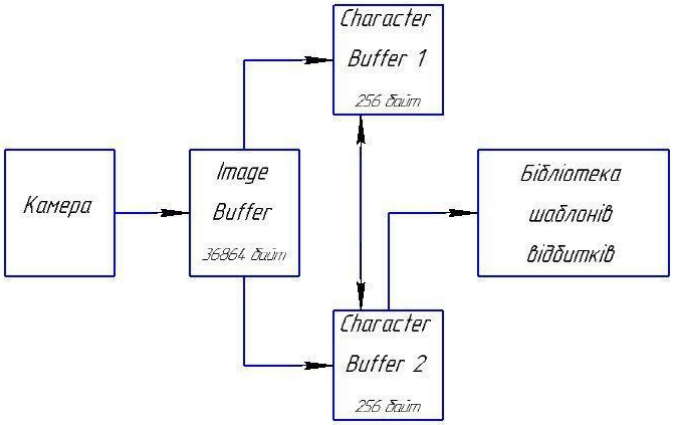

Рис. 3 - Схема роботи модуля

При способі авторизації від сенсору циклічно надсилається команда Genimg, до моменту фіксації відбитку, в буфер обміну, що має роздільну здатність 256 на 288 точок з 16 градаціями сірого. До буферу надсилається команда img2TZ, яка виконує функцію згортання – алгоритм, який перетворює вхідні 35 кБайт в зображення розміром 256 байт із збереженням унікальних рис відбитку. Після цього виконується команда search – пошук та порівняння з шаблонами бібліотеки або з певним діапазоном бібліотеки. Як результат порівняння повертається номер шаблону, результат операції авторизації та коефіцієнт співпадіння. Рівень співпадіння залежить від характеристики порогу співпадіння. Поріг може бути відредаговано за допомогою програмного забезпечення шляхом встановлення одного з п’яти рівнів безпеки. Перший рівень – найменший рівень безпеки, п’ятий – найвищий.

При внесені відбитків у базу шаблонів, фіксація відбитків відбувається двічі. Перше зображення зберігається в першому буфері обміну, другий результат сканування - в другому. Зображення згортаються та відбувається операція RegModel, що дозволяє отримати усереднене значення з двох результатів. Кінцевий результат зберігається у вигляді шаблону в бібліотеці.

В якості модулю бездротового зв’язку використовується мікроконтролер ESP8266 з підтримкою Wi-Fi інтерфейсу. Мікроконтролер, в даному випадку хоч і використовується лише як модуль бездротового зв’язку, може також використовуватися як окремий контролер для реалізації проектів в системах автоматизації побуту та IoT. На сьогодні існує велика кількість різновидів моделей даного контролеру, від ESP-01 до ESP-12. Моделі мають відмінності головним чином в роз’ємах та кількості флеш пам’яті.

Модель мікроконтролеру ESP-01S має 8 контактів та PCB-антену (друкований передавач на самій платі) (рис. 4). В модельному ряду ESP8266 використовується 32 бітний процесор Tensilica L106, що може бути «розігнаний» до частоти 160 МГц. Споживання енергоживлення в режимі передавання даних складає 220 мА. Модуль потребує живлення в межах 2,5-3,6 В, для забезпечення стабільної напруги використовується мікросхема AMS1117-3,3, тобто, лінійний стабілізатор з малим падінням напруги. Модуль ESP8266 працює за протоколом IPv4, TCP/UDP, HTTP, та підтримує протоколи передавання 802.11 b/g/n, протоколи WPA/WPA2 та шифрування WEP/TKIP/AES.

Для керування контролером використовуються, як браузери, так і програмне забезпечення для Android/iOS/Desktop.

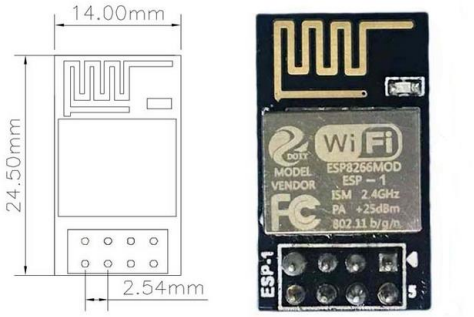

Рис. 4 - Мікроконтролер ESP8266-01S

В якості контролера системи пропонується застосувати платформу Arduino - відкриту програмовану апаратну платформу для роботи з різними фізичними об'єктами. Платформа являє собою просту плату з мікроконтролером та спеціальне середовище розробки для створення програмного забезпечення мікроконтролера.

Arduino може використовуватися для розробки інтерактивних систем, керованих різними датчиками і перемикачами. Такі системи, в свою чергу, можуть управляти роботою різних індикаторів, двигунів та інших пристроїв. Проекти Arduino можуть бути як самостійними, так і взаємодіючими з програмним забезпеченням, що встановлене на персональному комп'ютері (наприклад, додатками Flash, Processing,

MaxMSP). Середовище розробки для програмування такої плати має відкритий вихідний код. Плата Arduino складається з мікроконтролеру Atmel AVR та елементів обв'язки для програмування та інтеграції з іншими схемами.

Реалізація системи контролю та управління доступом

Принципову схему системи контролю та керування доступом зображено на рис. 5.

До складу системи входять:

- L1 – соленоїд з живленням 12 В;
- R1 – джерело живлення соленоїду 12 В;
- R2-R10 – резистори;
- SW1 – кнопка для переведення в стан програмування ESP8266;
- SW2 – кнопка відкриття дверей з середини приміщення;
- SW3 – кнопка перезавантаження мікроконтролера ESP8266;
- P1 – платформа Arduino Uno з мікроконтролером ATmega328;
- U1 – модуль реле SDR-05VDC;
- U2 - мікроконтролер ESP8266;
- U3 – зчитувач відбитків пальців FPM10A;
- U4 – стабілізатор напруги AMS 117 3.3V;
- LED1 (2) – світлодіоди індикації результату зчитування відбитків.

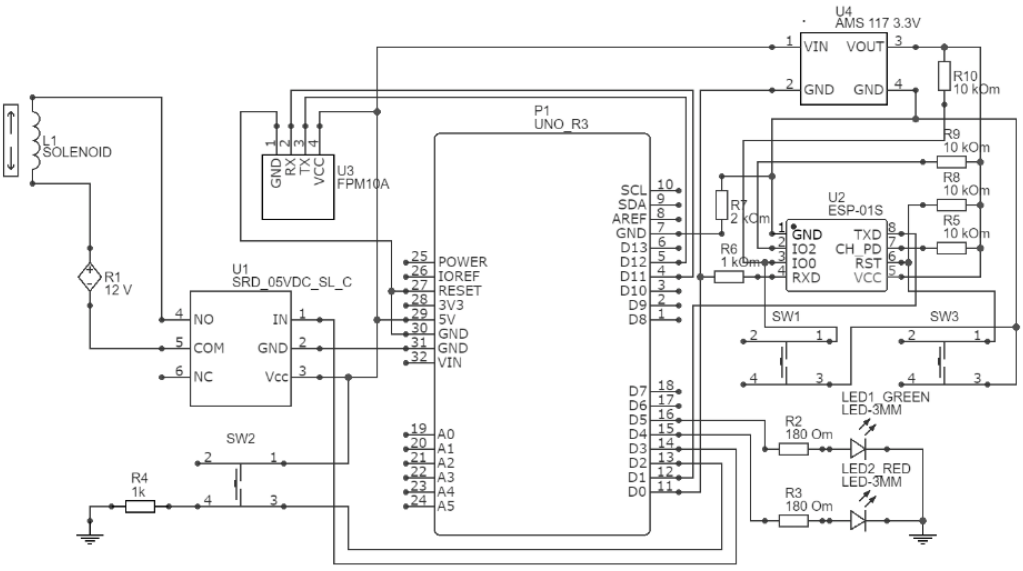

Рис. 5 - Принципова схема системи

Принцип дії системи – при зчитуванні біометричних даних модулем FPM10A відбувається порівняння зчитаного з тим, що зберігається в пам'яті FPM10A. При відсутності співпадінь біометричних даних передається імпульс на Arduino та вмикається індикація за допомогою червоного світлодіоду, що свідчить про невдалу спробу автентифікації. При вдалій спробі автентифікації, по-перше, вмикається індикація, що засвідчує про співпадіння відсканованого відбитку з тим, що був збережений в пам'яті, по-друге, подається імпульс певної тривалості на модуль реле, що керує тими чи іншими засобами автоматичного надання доступу на режимну територію (додатково цю функцію реалізовано за допомогою натиснення кнопки), по-трете, за допомогою модулю бездротового зв'язку відправляється ідентифікатор особи, що пройшла автентифікацію для реєстрування наявності суб'єкта на об'єкті.

Висновки

Запропонована і досліджена система контролю та управління доступом із застосуванням платформи Arduino і актуальних сучасних засобів захисту, дозволяє ефективно здійснити надійний контроль та управління доступом до важливих стратегічних об'єктів. Перевагою застосування платформи Arduino є цілком реальні можливості використання за помірні кошти різноманітних давачів, сенсорів та інших засобів, що є органічно сумісними з цією платформою. Застосування біометричної ідентифікації суттєво сприяє значному підвищенню рівня надійного контролю та безпеки, оскільки біометричні параметри є унікальними для кожної людини. Слід зазначити також, що ефективність функціонування системи контролю та управління доступом, помітно зростає при інтеграції з системами відеоспостереження та сигналізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Биняковский А. А., Петин В. А. Практическая энциклопедия Arduino. –Москва : ДМК Пресс. 2017. – 152 с.
2. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. Телеком. – Москва : 2010. – 272 с.
3. Даутов А. Л., Пуряев А. С. Внедрение и развитие систем контроля и управления доступом на предприятии //Инновационная наука. – 2016. – №. 5-1 (17)
4. Петин В. А. Arduino и Raspberry Pi в проектах Intemet of Things. – Санкт-Петербург : БХВ-Петербург. 2016. – 320 с.
5. Системы контроля и управления доступом. [Електронний ресурс] : [Веб-сайт] http://infoteclab.ru/skud.html .(дата звернення 05.03.2020) – назва з екрану
6. FPM10A [Електронний ресурс] : [Веб-сайт] https://cdn-shop.adafruit.com/datasheets/ZFM+user+manualV15.pdf .(дата звернення 05.03.2020) – назва з екрану
7. ESP8266EX Datasheet [Електронний ресурс] : [Веб-сайт] www.espressif.com .(дата звернення 05.03.2020) – назва з екрану

Писаренко Дмитро Георгійович – студент групи АКІТ-19мс, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця, e-mail : pisarenkomit@gmail.com

Нестюк Юлія Юріївна – студентка групи 2АКІТ-17б, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця, e-mail : yynestiuk@gmail.com

Науковий керівник: **Васюра Анатолій Степанович —** професор кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця.

Pysarenko Dmytro G. – Department of Computer System and Automation, Vinnytsia National Technical University, Vinnytsia, email : pisarenkomit@gmail.com

Nestiuk Yuliia Y. - student of 2AKIT-17b group, Faculty of Computer Systems and Automation, Vinnitsa National Technical University, Vinnytsia, e-mail : yynestiuk@gmail.com

Supervisor: **Vasyura Anatoly S. —** Professor, academician of Ukrainian Technological Academy, Professor of automation and intelligent information technologies department, Vinnytsia National Technical University, Vinnytsia, email: vasanat@i.ua.