

РОЗРОБЛЕННЯ ПІДСИСТЕМИ АВТОМАТИЗОВАНОГО ДОСТУПУ ТА ОБЛІКУ РОБОЧОГО ЧАСУ

Гурін Д.В., Грижак В.М.

Харківський національний університет радіоелектроніки,

Україна, 61166, Харків, пр. Науки 14

E-mail: dmytro.gurin@nure.ua, valeriia.hryzhak@nure.ua

Анотація: розглянуто розроблення підсистеми автоматизованого доступу та обліку робочого часу на основі двофакторної ідентифікації користувачів. Запропонована структура підсистеми передбачає послідовне використання RFID-ідентифікації та розпізнавання обличчя, що дає змогу підвищити достовірність встановлення особи перед наданням доступу до об'єкта.

Ключові слова: автоматизована підсистема, контроль доступу, облік робочого часу, двофакторна ідентифікація, RFID, розпізнавання обличчя, ESP32-S3.

DEVELOPMENT OF AN AUTOMATED ACCESS AND TIME AND ATTENDANCE SUBSYSTEM

Gurin D.V., Hryzhak V.M.

Kharkiv National University of Radio Electronics

Ukraine, 61166, Kharkiv, Nauky av., 14

E-mail: dmytro.gurin@nure.ua, valeriia.hryzhak@nure.ua

Abstract: The development of a subsystem for automated access control and time tracking based on two-factor user identification is examined. The proposed subsystem structure involves the sequential use of RFID identification and facial recognition, which enhances the reliability of identity verification prior to granting access to the facility.

Keywords: automated subsystem, access control, time and attendance tracking, two-factor authentication, RFID, facial recognition, ESP32-S3.

Автоматизація процесів контролю доступу та обліку робочого часу є одним із напрямів удосконалення організації роботи підприємств. Використання автоматизованих систем дає можливість поєднати ідентифікацію працівника, керування виконавчим пристроєм та реєстрацію подій доступу в єдиній інформаційній системі.

Одним із важливих аспектів таких систем є достовірність ідентифікації користувача. Використання лише одного ідентифікаційного фактора не завжди забезпечує необхідний рівень захисту. У зв'язку з цим доцільним є застосування двофакторного підходу, у якому використовуються різні способи підтвердження особи.

У розробленій підсистемі як перший фактор використовується RFID-карта, яка забезпечує швидку ідентифікацію користувача. Другим фактором є розпізнавання обличчя, за допомогою якого виконується додаткова перевірка відповідності користувача зареєстрованому ідентифікатору.

Основою запропонованої системи є двофакторна ідентифікація. На першому етапі користувач прикладає RFID-карту до зчитувача. Контролер отримує унікальний ідентифікатор карти та передає його через Wi-Fi до хмарного сервера. Сервер виконує перевірку отриманого ідентифікатора у базі даних.

У разі наявності відповідного ідентифікатора система переходить до другого етапу. Активується камера, яка здійснює захоплення зображення обличчя. Отримане зображення порівнюється з еталонним шаблоном, пов'язаним із відповідним RFID-ідентифікатором.

Якщо обидва фактори успішно пройшли перевірку, контролер формує керуючий сигнал для виконавчого пристрою. Електромагнітний замок переходить у стан, що забезпечує доступ

користувача. Одночасно формується повідомлення про успішну ідентифікацію, а подія передається на сервер для подальшої реєстрації.

У разі невідповідності хоча б одного з факторів доступ не надається. Система активує відповідну світлову та звукову індикацію, а інформація про невдалу спробу також реєструється у журналі подій.

Таблиця 1 – Зведена таблиця апаратних модулів підсистеми

Модуль	Призначення	Інтерфейс	Напруга
ESP32-S3 Freenove	Центральний контролер	-	3,3 В
PN532	RFID-зчитувач	I2C	3,3 В
OV2640	Камера розпізнавання обличчя	DVP	3,3 В
Електромагнітний замок	Виконавчий пристрій	MOSFET	12 В
Перетворювач напруги	Перетворення напруги	DC Barrel Jack	12 В - 5 В
Світлодіоди (×2)	Візуальна індикація	GPIO	3,3 В
П'єзосуммер	Звукова індикація	GPIO (ШИМ)	3,3 В
SD-картка	Конфігурація	I2C	3.3 В

Структурно підсистема містить такі основні функціональні блоки:

- центральний мікроконтролер;
- модуль RFID-ідентифікації;
- модуль відеокамери;
- виконавчий пристрій;
- блок світлової та звукової індикації;
- модуль живлення;
- хмарний сервер.

Центральний мікроконтролер виконує функції локального обчислювального вузла, отримує інформацію від периферійних модулів, здійснює її оброблення та формує керуючі сигнали.

RFID-модуль використовується для реалізації першого етапу ідентифікації. Камера забезпечує отримання зображення для другого етапу. Виконавчий пристрій забезпечує фізичне обмеження доступу, а блок індикації інформує користувача про поточний стан підсистеми.

Хмарний сервер є верхнім рівнем архітектури. На ньому передбачається централізоване зберігання інформації про персонал, журналу подій доступу з часовими мітками та функціонування веб-інтерфейсу адміністратора.

У початковому стані підсистема перебуває в режимі очікування. Мікроконтролер постійно контролює стан RFID-зчитувача, очікуючи появи карти в зоні зчитування. У цьому стані активується зелений світлодіод, що відповідає режиму готовності.

Після виявлення RFID-карти зчитується її унікальний ідентифікатор. Отримані дані передаються на сервер для перевірки.

Якщо ідентифікатор не зареєстрований у базі даних, доступ не надається та система формує сигнал про невдалу спробу ідентифікації.

Якщо карта зареєстрована, система переходить до другого етапу. Активується камера та виконується захоплення зображення обличчя. Результат розпізнавання порівнюється з еталонним шаблоном, пов'язаним із відповідним RFID-ідентифікатором.

При успішному проходженні обох етапів мікроконтролер формує керуючий сигнал на виконавчий пристрій, активує зелену світлову та звукову індикацію. Подія успішного доступу передається на сервер і записується до журналу із часовою міткою.

У разі невідповідності RFID-ідентифікатора або результату розпізнавання обличчя активується червоний світлодіод та тривожний звуковий сигнал. Відповідна подія також передається на сервер та фіксується як невдала спроба доступу.

Таким чином, алгоритм забезпечує послідовне проходження двох незалежних етапів ідентифікації перед формуванням команди на відкриття замка.

Схема підключення елементів наведених у таблиці 1 представлена на рисунку 2.

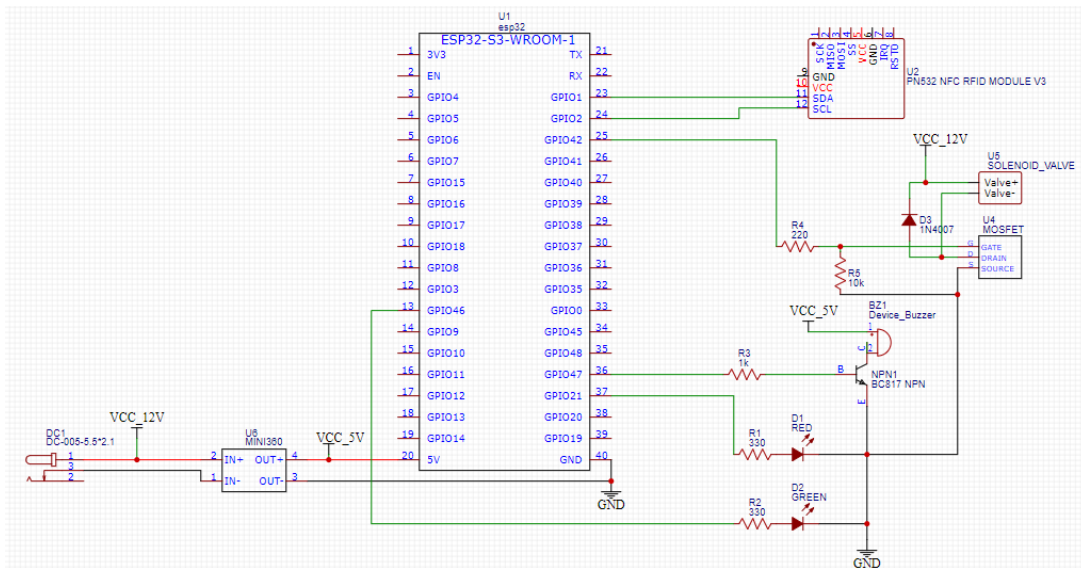


Рисунок 2 – Схема підключення компонентів

Зведена структура апаратної частини підсистеми включає центральний контролер ESP32-S3 Freenove, RFID-зчитувач PN532, камеру OV2640, електромагнітний замок, перетворювач напруги, світлодіодні індикатори, п'єзозуммер та SD-карту.

У макеті живлення здійснюється від USB-порту комп'ютера через вбудований стабілізатор плати Freenove ESP32-S3. Вхідна напруга становить 5 В, після чого стабілізатор формує 3,3 В для живлення мікроконтролера та периферійних модулів.

Оскільки в макеті електромагнітний замок замінено світлодіодом-імітатором, окреме силове коло 12 В для виконавчого пристрою не використовується.

Модуль PN532 працює через інтерфейс I²C. Лінія SDA підключається до GPIO2, а SCL — до GPIO1. Живлення здійснюється від напруги 3,3 В.

Камера OV2640 підключається через спеціалізований CAM-роз'єм плати ESP32-S3. Це забезпечує передавання сигналів DVP без додаткового розведення окремих сигнальних ліній.

Зелений світлодіод підключається через резистор 330 Ом до GPIO46, червоний — через резистор 330 Ом до GPIO21.

П'єзозуммер керується через NPN-транзистор із GPIO47. Синій світлодіод, що імітує електромагнітний замок, керується через NPN-транзистор із GPIO42.

Для ліній керування транзисторами передбачено стягувальні резистори, призначені для зменшення впливу перешкод та забезпечення швидкого закривання транзисторів.

Таким чином, сформована схема забезпечує взаємодію всіх основних компонентів підсистеми та дає можливість реалізувати функції ідентифікації, індикації та керування виконавчим пристроєм.

ВИСНОВКИ. Розроблено структуру підсистеми автоматизованого доступу та обліку робочого часу, побудовану на принципі двофакторної ідентифікації користувачів.

Як центральний обчислювальний вузол обрано ESP32-S3 Freenove, який забезпечує необхідні обчислювальні ресурси, бездротовий зв'язок та підключення периферійних пристроїв. Для першого фактора ідентифікації використано RFID-модуль PN532, а для другого — камеру OV2640.

Як виконавчий пристрій обрано електромагнітний замок YLI YM-280. Для прототипування його функції реалізовано за допомогою світлодіода-імітатора. Для забезпечення зворотного зв'язку передбачено два світлодіоди та п'єзоелектричний зуммер.

Розроблений алгоритм передбачає послідовну перевірку RFID-ідентифікатора та обличчя користувача. Надання доступу здійснюється лише за умови успішного проходження обох етапів ідентифікації. Результати успішних та невдалих спроб передаються на хмарний сервер для подальшого зберігання та аналізу.

Для підсистеми живлення обрано понижувальний перетворювач Mini-360 на базі MP2307. Проведене математичне моделювання показало, що сформована система автоматичного регулювання є стійкою. Єдиний корінь характеристичного рівняння становить ($\lambda_1 = -1185$), а постійна часу замкненої системи — приблизно (0,000844) с.

Розроблена апаратна структура забезпечує основу для створення макету підсистеми автоматизованого контролю доступу та обліку робочого часу і дозволяє реалізувати взаємодію засобів ідентифікації, керування виконавчим пристроєм, індикації та передавання інформації на сервер.

ЛІТЕРАТУРА

1. Гурін Д. В. Ідентифікація оператора в робочій зоні колаборативного робота / Д. В. Гурін, Ю. М. Мірошніченко // Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт 2026 : матеріали I-ої Всеукраїнської конфер. 12-13 лютого 2026 р. - Харків: [електронний друк], 2026. – С. 148-153.
2. Yevsieiev, V., & Gurin, D. (2023). COMPARATIVE ANALYSIS OF THE BASIC METHODS USED IN INDUSTRY 4.0 AND INDUSTRY 5.0. *Collection of Scientific Papers «ΛΟΓΟΣ»*, (September 29, 2023; Bologna, Italy), 113–115. <https://doi.org/10.36074/logos-29.09.2023.31>
3. Yevsieiev, V., & Gurin, D. (2024). Study of Methods of Dynamic Description of The Environment for Collaborative Robots-Manipulators in the Concepts of Industry 5.0 (Doctoral dissertation, Collection of scientific papers «SCIENTIA»).
4. Molozhanov L. Analysis of operator identification methods in the working area of a collaborative manipulator robot / L. Molozhanov, D. Gurin // Manufacturing & Mechatronic Systems 2025 : Theses of Reports of IX-st International Conference, October 25-26, 2025. - Kharkiv, 2025. - P. 34-37.
5. Nevliudov, I., Yevsieiev, V., & Sotnik, S. (2026). PREDICTIVE ANALYTICS AND ARTIFICIAL INTELLIGENCE IN EMERGENCY WARNING SYSTEMS. *Collection of Scientific Papers «SCIENTIA»*, (August 7, 2026; Marseille, France), 108–111. Retrieved from <https://previous.scientia.report/index.php/archive/article/view/4634>
6. Yevsieiev, V., & Holod, I. (2026). HARDWARE-SOFTWARE MODULE FOR INTELLIGENT MICROCLIMATE CONTROL IN INDUSTRIAL FACILITIES. *Scientific Papers of Donetsk National Technical University. Series: "Computer Engineering and Automation"*, 4(6(38), 7–17. [https://doi.org/10.32782/2786-9024/v4i6\(38\).359113](https://doi.org/10.32782/2786-9024/v4i6(38).359113)