

СИСТЕМА КЕРУВАННЯ ДОСТУПОМ НА БАЗІ RFID TA SPRING BOOT

Тези представляють аналіз актуальності та перспектив розробки системи керування доступом(СКД) на основі технології радіочастотної ідентифікації (англ. Radio Frequency Identification, RFID) та фреймворку Spring Boot. У роботі розглянуто принцип роботи RFID, досліджено сучасні СКД, проведено порівняльний аналіз RFID з альтернативними технологіями, з оцінкою їхньої безпеки, зручності та вартості. Визначено вимоги до СКД, що забезпечує автоматизовану ідентифікацію користувачів, централізоване управління доступом та інтеграцію з IoT.

Ключові слова: система керування доступом(СКД), RFID(Radio Frequency Identification), безпека, тайм-менеджмент.

У нашій час системи керування доступом (СКД) є важливою складовою в забезпеченні надійного захисту об'єктів, що потребують обмеженого доступу, таких як офіси, склади, навчальні заклади чи житлові комплекси, вимагає розробки ефективних, надійних і доступних СКД. Поряд із цим, важливим аспектом є оптимізація тайм-менеджменту, оскільки швидке й зручне адміністрування доступу сприяє економії часу, що в сучасних економічних умовах трансформується у фінансові вигоди. Традиційні методи, такі як механічні замки чи паролі, мають обмеження, пов'язані з безпекою, зручністю використання та можливістю масштабування. Отже, розробка інноваційних підходів у цій галузі є актуальною для підвищення рівня безпеки та вдосконалення операційної ефективності організацій.

Актуальність теми кваліфікаційної бакалаврської роботи визначається необхідністю розробки економічно доступних і високоефективних рішень для керування доступом, які поєднують апаратне забезпечення з програмними засобами, забезпечуючи не лише безпеку, а й оптимізацію часу адміністрування.

Метою дослідження є створення СКД, яка забезпечує автоматизовану ідентифікацію користувачів і керування механізмом доступу шляхом розробки апаратно-програмного забезпечення (АПЗ) на основі RFID з вебзастосунком на базі Spring Boot

Технологія радіочастотної ідентифікації RFID являє собою сучасний метод безконтактної ідентифікації об'єктів, що ґрунтується на використанні радіохвиль. RFID-системи набули широкого застосування у сферах логістики, роздрібно́ї торгівлі, охорони здоров'я, транспортній інфраструктурі та інших галузях завдяки їхнім можливостям забезпечення оперативного, автоматизованого та надійного зчитування даних.

Основні складові RFID-систем:

- RFID-мітка: ідентифікаційна мітка, будучи первинним носієм інформації в RFID-системі, конструктивно включає інтегральну мікросхему для зберігання унікального ідентифікаційного коду та, за потреби, додаткових даних, а також антену, що забезпечує комунікацію зі зчитувачем; залежно від джерела енергії, мітки поділяються на пасивні, які не мають власного живлення та активуються електромагнітним полем зчитувача, характеризуючись компактністю, низькою вартістю та обмеженим радіусом дії (до 10 м); активні мітки, що містять автономне джерело живлення, забезпечуючи функціонування на значних відстанях (до 100 м і більше) та можливість ініціювання передачі даних; і напівпасивні мітки, які використовують батарею для живлення мікросхеми, але для передачі сигналу залежать від електромагнітного поля зчитувача;

- зчитувальний пристрій: зчитувач являє собою пристрій, що генерує електромагнітне поле для активації мітки та здійснює прийом радіосигналів, що нею транслюються. Зчитувачі можуть бути стаціонарними (наприклад, інсталльованими на контрольно-пропускних пунктах складських приміщень) або мобільними (портативні сканери). Їхня конструкція включає антени для передачі та прийому сигналів, а також модулі для первинної обробки даних та їхньої подальшої передачі до інформаційної системи;

- інформаційна система: дані, отримані від мітки за посередництвом зчитувача, надходять до комп'ютеризованої системи для подальшої обробки, зберігання та аналізу. Зазначена система може бути інтегрована з базами даних, системами управління складськими запасами (англ. Warehouse Management System) або іншими програмними платформами з метою автоматизації бізнес-процесів.

Схематичне зображення складових RFID-системи (рис. 1).



Рис. 1. Схематичне зображення складових RFID та їх взаємодія

У тому числі, конструкція БПЛА дозволяє здійснити оснащення його, як платформи, необхідними датчиками для виконання збору цифрових даних з метою їх подальшої обробки, аналізу та визначення наявності порушень в конструкціях або їх елементах.

Функціонування RFID-систем ґрунтується на принципі обміну радіосигналами між ідентифікаційною міткою та зчитувальним пристроєм у визначеному частотному діапазоні.

Процес ідентифікації включає наступні етапи:

- генерація електромагнітного поля: зчитувач за допомогою власної антени створює електромагнітне поле в межах операційної зони. Частота даного поля визначається типом використовуваної RFID-системи (низькочастотна, високочастотна або ультрависокочастотна);
- активація мітки: при потраплянні RFID-мітки в зону дії електромагнітного поля, її антена абсорбує енергію. У пасивних мітках отримана енергія використовується для живлення мікросхеми, що ініціює перехід мітки в активний стан. Активні мітки, маючи автономне джерело енергії, здатні самостійно ініціювати процес передачі даних;
- трансляція даних: активована мітка передає збережені дані (наприклад, унікальний ідентифікатор) назад до зчитувача за допомогою радіосигналу. Даний процес отримав назву модуляції сигналу. У більшості систем застосовується принцип зворотного розсіювання (англ. backscatter), при якому мітка здійснює модуляцію відбитого сигналу зчитувача, накладаючи на нього власну інформацію;
- обробка даних: зчитувач здійснює декодування отриманого сигналу, трансформуючи його в цифровий формат, та передає отримані дані до інформаційної системи. Система, у свою чергу, обробляє отриману інформацію, співставляючи її з даними, що зберігаються в базі даних, та ініціює відповідні дії, такі як актуалізація даних про інвентар, верифікація доступу або моніторинг переміщення об'єкта.

Блок-схема принципу роботи RFID-систем (рис. 2).

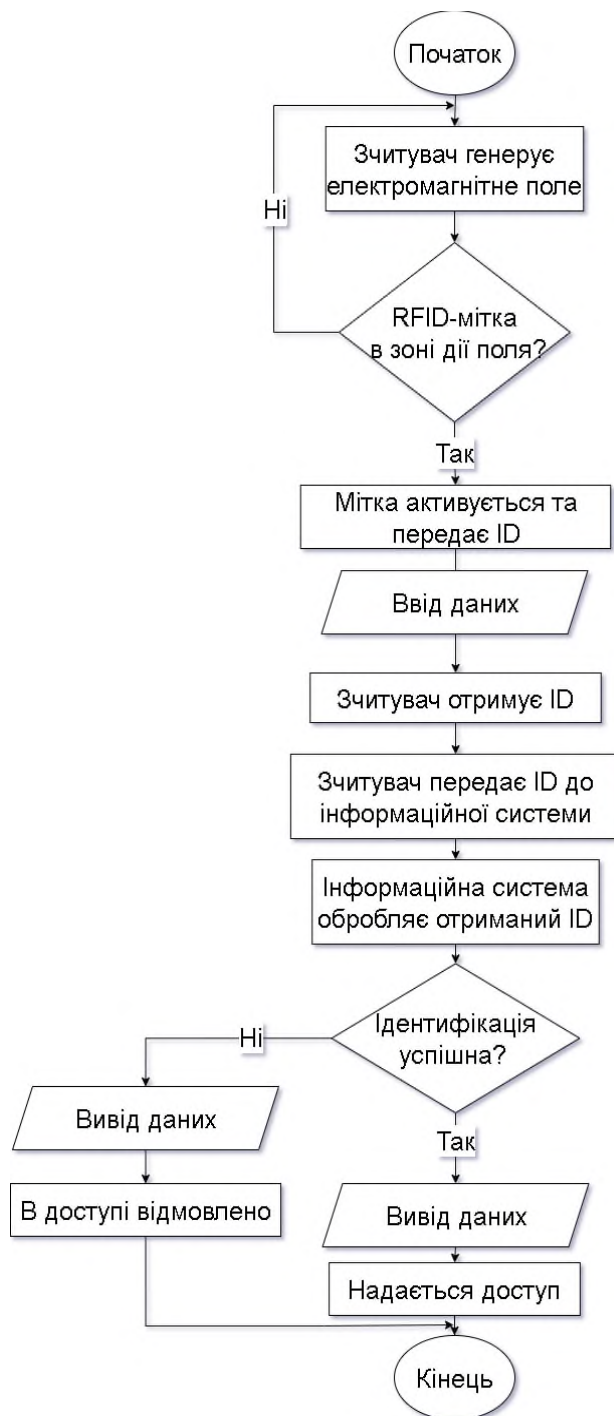


Рис. 2. Блок-схема, що ілюструє принцип роботи RFID-системи

Аналізуючи доступну інформацію, можна виділити кілька ключових типів систем, які конкурують із RFID, і зрозуміти, чому вони є поширеними. СКД класифікуються залежно від архітектури, способу ідентифікації, рівня безпеки та сфери застосування.

Вибір конкретної СКД визначається комплексом факторів, серед яких ключову роль відіграє контекст її застосування (табл. 1). Біометричні системи набули поширення завдяки високому рівню безпеки, що забезпечується унікальністю та невідчужуваністю біологічних ідентифікаторів, що є критично важливим для об'єктів з високим рівнем ризику. Мобільні системи демонструють зростаючу популярність завдяки зручності використання та можливості оперативного керування правами доступу через програмні інтерфейси, що є значною перевагою для великих організацій. Кодові замки приваблюють своєю простотою експлуатації та відсутністю потреби у додаткових фізичних носіях, що знижує операційні витрати. Системи з магнітними картками, незважаючи на певні обмеження в безпеці, залишаються затребуваними завдяки їхній економічності та сумісності з існуючою інфраструктурою, особливо в об'єктах старої забудови. Фізичні ключі зберігають свою актуальність у низькотехнологічних середовищах, де простота та автономність є визначальними факторами.

Порівняння основних СКД

№ з/п	Система	Рівень безпеки	Зручність	Вартість	Приклади використання
1	Біометричні системи	Високий	Середній	Висока	Банки, урядові установи
2	Мобільні системи	Середній-Високий	Висока	Середня	Офіси, житлові комплекси
3	Кодові замки	Низький-Середній	Висока	Низька	Малі офіси, гаражі
4	Магнітні картки	Низький	Середній	Низька	Старий офіс, готелі
5	Фізичні ключі	Низький	Низька	Дуже низька	Приватні будинки, малі об'єкти

Нефункціональні вимоги є основою для забезпечення стабільності, безпеки та зручності використання СКД. Вони сприяють створенню гнучкої та масштабованої платформи, що відкриває можливості для подальшого розвитку функціоналу (табл. 2).

Таблиця 2.

Нефункціональні вимоги

№ з/п	Вимога	Опис
1	Продуктивність	Система має обробляти запити на доступ протягом 1 секунди
2	Вартість	Компоненти в сумі не мають бути дорожчими 2'000–3'000 грн
3	Надійність	СКД забезпечує доступність на рівні 99,9 % часу завдяки резервному копіюванню даних і механізмам відновлення після збоїв
4	Безпека	СКД використовує шифрування даних, безпечну автентифікацію, ролевий контроль доступу через Spring Security

Функціонування системи ґрунтується на наступному алгоритмі: RFID-модуль ініціює процес зчитування ідентифікаційної інформації з безконтактної картки. Отримані дані обробляються мікроконтролером, який формує відповідний запит та передає його на сервер через бездротову мережу Wi-Fi. Серверний застосунок на базі Spring Boot здійснює верифікацію прав доступу на основі отриманих ідентифікаційних даних та повертає результат авторизації. На основі отриманої відповіді, мікроконтролер активує сервопривід для забезпечення фізичного розблокування (або підтримує його в заблокованому стані). Локальний дисплей та клавіатура використовуються для конфігурації параметрів мережевого з'єднання з сервером, зокрема для введення IP-адреси. Таким чином, апаратна та програмна складові системи функціонують в режимі реального часу, забезпечуючи централізоване управління доступом до контрольованих зон.

References

1. Zhang Z., Yan C. Research on data sharing access control based on blockchain technology. *Autom Control Intell Syst.* 2022. Vol. 10, Is. 1. P 8–13. DOI: 10.11648/j.acis.20221001.12.
2. Hassan S., Shibli A. R., Raza R. Ubiquitous computing with Radio Frequency IDentification tags. *Math Comput Sci.* 2023. Vol. 8, Is. 3. P 73–86. DOI: 10.11648/j.mcs.20230803.12.
3. Aliyu M. B., Suru H., Gabi D., Garba M., Argungu M. The need for adaptive access control system at the network edge. *American Journal of Information Science and Technology.* 2024. Vol. 8, Is. 2. P. 45–55. DOI: 10.11648/j.ajist.20240802.13.
4. RFID teknolojiiia dlia avtomatyzatsii obliku. Retrieved from: <https://remonline.ua/blog/rfid-technology/> (data zvernennia: 10.05.2025).
5. Shcho take systema RFID, v chomu yii osoblyvosti vykorystannia. Retrieved from: https://idcard.com.ua/ua/blog/chto-takoe-sistema-rfid-v-chem-ee-osobennosti-ispolzovaniya/?srsltid=afmbooptmjvbpzudevvj7uwvfhapvaoh1zk_voamfcodjsmtc9u1i1b (data zvernennia: 10.05.2025).

DOI 10.34132/mspc2025.01.06.39

Andrii Shylik,
Serhii Puzyrov

ACCESS CONTROL SYSTEM BASED ON RFID AND SPRING BOOT

The abstract presents an analysis of the relevance and prospects of developing an access control system (ACS) based on Radio Frequency Identification (RFID) technology and the Spring Boot framework. The study examines

the operating principles of RFID, investigates modern ACS, and conducts a comparative analysis of RFID with alternative technologies, evaluating their security, convenience, and cost. Requirements for the ACS are defined, ensuring automated user identification, centralized access management, and integration with IoT.

Key words: *access control system (ACS), Radio Frequency IDentification (RFID), security, time management.*

Відомості про авторів / Information about the Authors

Андрій Шилік, бакалаврант кафедри комп'ютерної інженерії, Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна. E-mail: andreishulik@gmail.com, orcid: <https://orcid.org/0009-0007-2318-1245>.

Andrii Shylik, BSc Student of the Computer Engineering Department, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: andreishulik@gmail.com, orcid: <https://orcid.org/0009-0007-2318-1245>.

Сергій Пузирьов, кандидат фізико-математичних наук, доцент кафедри комп'ютерної інженерії факультету комп'ютерних наук Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: svpuzyrev@gmail.com, orcid: <https://orcid.org/0000-0003-0520-1496>.

Serhii Puzyrov, Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Computer Engineering Department, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: svpuzyrev@gmail.com, orcid: <https://orcid.org/0000-0003-0520-1496>.

© А. Шилік, С. Пузирьов
20.05.2025.

Стаття отримана редакцією