УДК 004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ RFID-СИСТЕМ ТА АНАЛОГІЧНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Вініцький М.А.
email: mykola.vinitskyi@nure.ua
Харківський національний університет радіоелектроніки, каф. РТІКС
м. Харків, Україна

This study provides an in-depth comparison between RFID-based and biometric access control systems, focusing on security, authentication speed, cost efficiency, and user experience. RFID offers rapid authentication and flexibility, while biometric technologies provide enhanced security by eliminating the risks of credential duplication and unauthorized access. The paper explores key vulnerabilities of both approaches, assesses their suitability for different security levels, and suggests an optimal hybrid model for secure access management.

Системи контролю доступу (СКУД) є невід'ємною частиною безпеки підприємств, урядових установ, навчальних закладів та житлових комплексів. Вони забезпечують ідентифікацію користувачів і визначають їхні права доступу до приміщень. Серед найбільш популярних методів аутентифікації виділяються кодові зчитувачі, які використовують таємний код для автентифікації RFID (Radio Frequency Identification), що використовує радіочастотні мітки, та біометричні технології, які аналізують унікальні фізіологічні особливості людини [1].

Вибір між цими технологіями залежить від таких ключових факторів, як рівень безпеки, зручність використання, швидкість аутентифікації, можливість шахрайства та витрати на впровадження. У цьому дослідженні розглядаються переваги та недоліки всіх підходів, а також їхня доцільність у різних сценаріях використання.

Кодові зчитувачі – найпростіший спосіб обмеження доступу до приміщень. Принцип роботи банальний: до зони мають доступ усі, хто знає код, якщо введений людиною код на вході правильний – двері відчиняються, якщо ж ні, то прохід залишається блокованим. Ця СКУД має певні переваги:

- простота встановлення та використання – інтуітивно зрозуміле використання та весь склад системи – це замок з’єднаний з циферблатом;
- вартість – відсутня потреба у додаткових носіях, складних системах.

Недоліки цієї системи також вкрай очевидні:

- висока вразливість системи – будь-хто може підгледіти код і отримати доступ та передати його.
- необхідність регулярної зміни коду, для підтримки безпеки, адже запобігти потраплянню кода у користування третім особистостям неможливо.

RFID-системи працюють за принципом зчитування унікального іден-

тифікаційного номера з мітки (карти або брелока), який передається на зчитувач за допомогою радіохвиль. Основні стандарти включають Low Frequency (LF, 125 kHz), High Frequency (HF, 13.56 MHz, наприклад, MIFARE DESFire EV1) та Ultra-High Frequency (UHF, 860-960 MHz) [2].

Переваги RFID:

- висока швидкість аутентифікації – ідентифікація користувача займає менше 1 секунди;
- можливість використання безконтактного доступу – забезпечує зручність та зменшує знос карток;
- гнучкість у налаштуванні – адміністратори можуть змінювати права доступу віддалено;
- інтеграція з іншими системами – можливість поєднання з відеоспостереженням та реєстрацією робочого часу.

Недоліки RFID:

- ризик клонування міток – зловмисники можуть використовувати спеціальні пристрої для копіювання даних карток, особливо без захищеного шифрування;
- атаки ретрансляції (relay attack) – зчитування та передача сигналу на відстані можуть використовуватися для злому;
- потреба у фізичних носіях – користувач може загубити картку, що потребує її заміни.

Біометричні системи контролю доступу аналізують унікальні фізіологічні або поведінкові характеристики користувачів, такі як відбитки пальців, геометрія обличчя, сітківка ока, голос чи динаміка друку на клавіатурі. Переваги біометричних методів:

- неможливість передачі ідентифікатора – на відміну від карток RFID, користувач не може "поділитися" своїм відбитком пальця чи обличчям;
- високий рівень безпеки – унеможливлення клонування та крадіжки даних у традиційному вигляді;
- зручність використання – відсутність потреби носити картки чи вводити коди.

Недоліки біометрії:

- чутливість до зовнішніх факторів – мокрі, пошкоджені або забруднені пальці можуть не розпізнаватися системою;
- повільніший процес ідентифікації – біометричне сканування може займати 2-3 секунди, що сповільнює потік людей;
- конфіденційність та правові питання – збереження біометричних даних вимагає високого рівня захисту та може викликати етичні запитання;
- висока вартість впровадження – порівняно з RFID, біометричні системи дорожчі в установці та обслуговуванні;
- неможливість передачі ідентифікатора – на відміну від карток RFID, користувач не може "поділитися" своїм відбитком пальця чи обличчям. І це є також недоліком для розміщення біометричних систем всемісно, адже

виникає незручність короткочасного доступу;

- важка процедура внесення нового користувача у систему – якщо виникає потреба надати доступ новій людині, то ця процедура набагато довша ніж у RFID-системах [3].

Для забезпечення високого рівня безпеки та зручності багато організацій впроваджують гібридні рішення, які комбінують RFID і біометричні методи. Наприклад:

- RFID-картка + біометрія – спочатку користувач підносить картку до зчитувача, а потім підтверджує особу відбитком пальця або розпізнаванням обличчя;

- мобільна RFID-ідентифікація + розпізнавання обличчя – використання смартфона як RFID-мітки у поєднанні з біометричним підтвердженням.

Такі підходи значно зменшують ризики злому та клонування, забезпечуючи багаторівневу автентифікацію.

RFID-системи залишаються ефективним рішенням для швидкого та зручного контролю доступу, проте їхні недоліки, такі як ризик клонування та ретрансляційні атаки, вимагають додаткових заходів захисту. Біометричні методи забезпечують значно вищий рівень безпеки, але мають недоліки у вартості, швидкості роботи та конфіденційності даних.

Оптимальним рішенням є комбіноване використання RFID та біометрії: RFID може виконувати роль швидкої ідентифікації, тоді як біометрія забезпечує остаточне підтвердження особи у критичних зонах доступу. Подальший розвиток технологій, зокрема шифровані RFID-мітки та вдосконалені алгоритми розпізнавання обличчя, дозволять підвищити ефективність систем контролю доступу у майбутньому.

Список використаних джерел:

1. Зчитувачі системи контролю та управління доступом: порівняння функціоналу // Pipl.ua. URL: https://pipl.ua/article/zchituvachi-sistemi-kontrolyu-ta-upravlinnya-dostupom-porivnyannya-funkcionalu (дата звернення: 03.03.2025).

2. RFID зчитувачі – RFID Технотрейд // uarfid.kiev.ua URL: http://uarfid.kiev.ua/ua/category/rfid-readers/ (дата звернення: 03.03.2025).

3. Роговий М.І. Дослідження особливостей використання охоронних СКУД / Роговий М.І. – Харків: Національний університет радіоелектроніки, 2019. – 59 р. – Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/48abe020-383e-43d5-b9f3-c9f340746aab/content, вільний. – Дата звернення: 03.03.2025.

4. Системи контролю доступу до дверей: їх типи та виробники // Superdveri.ua. URL: https://superdveri.ua/door-access-control-systems-types-brands/ (дата звернення: 03.03.2025).