УДК 004.89.658.5
DOI 10.36910/10.36910/6775-2313-5352-2024-25-04
**Грудецький Р. Я., Маркіна Л. М., Пльотка Б. С., Сацик В. О.**
Луцький національний технічний університет, м. Луцьк, Україна

# ВИКОРИСТАННЯ МОДУЛЯ ПРИЙНЯТТЯ РІШЕНЬ СМАРТ-СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ПІДРОЗДІЛІВ ОРГАНІЗАЦІЇ

*У статті представлено розробку web-додатку, основною частиною якого є модуль прийняття рішень у смарт-системі. На основі проведено огляду та порівняння існуючих технологій, на яких базуються системи контролю доступу; зокрема систем на основі механічних замків, магнітних карток, біометричних систем та систем з використанням RFID-технології, було сформовано архітектуру web-додатку та розроблено алгоритм, на якому базується модуль прийняття рішень. Даний алгоритм роботи розробленого нами додатку базується на запропонованих рішеннях та передбачає використання динамічно генерованих ключів доступу у форматі штрих-кодів, що забезпечує зручність, ефективність і простоту поетапної схеми розробки та впровадження смарт-системи контролю доступу, яка забезпечує напівавтономний, а в разі необхідності і автономний контроль доступу до окремих локацій і ресурсів організації.*

*Апробацію та тестування результатів дослідження проведено на базі підрозділів Луцького національного технічного університет. Запропоноване рішення також може знайти застосування в організаціях різних форм власності які мають ряд своїх структурних підрозділів, в кампусах, на локаціях масових подій, де виникає потреба в управлінні доступом для співробітників, відвідувачів та учасників.*

***Ключові слова:*** *контроль доступу, web-додаток, контроль в режимі реального часу.*

**Постановка проблеми.** Сучасні складноструктуровані організації різних форм власності, кампуси, локації масових подій і т.п. стикаються з необхідністю забезпечення високого рівня безпеки, зокрема контролю доступу до окремо взятих підрозділів. Традиційні механічні замки та пропускні системи вже не відповідають вимогам сучасності, як безпековим, так і пропускним можливостям. Ця стаття описує розробку та впровадження смарт-системи контролю доступу до різних підрозділів тої чи іншої організації.

Одним із ключових аспектів системи контролю доступу є забезпечення контролю доступу сторонніх осіб як на регулярній основі, так і на основі одноразових та багаторазових пропусків і абонементів. Організації різних форм власності доволі часто стикаються з необхідністю надання доступу до окремих підрозділів не тільки своїм співробітникам та студентам, а й запрошеним лекторам, відвідувачам, обслуговуючому персоналу та учасникам різних заходів. Такий доступ має бути ретельно контрольованим, щоб запобігти несанкціонованому проникненню та забезпечити безпеку всіх учасників того чи іншого заходу.

**Аналіз існуючих рішень.** Сучасні системи контролю доступу можуть базуватися на різних технологіях, кожна з яких має свої переваги та недоліки. Традиційні методи контролю доступу, такі як механічні замки та магнітні картки, вже не задовольняють вимог сучасних складноструктурованих організацій, оскільки вони не забезпечують достатнього рівня безпеки, зручності, адаптивності. Механічні замки можуть бути легко зламані, а магнітні картки часто губляться або підробляються. Це спонукає до пошуку кардинально нових підходів, або інтеграції існуючих сучасних та надійних технологій [1].

Технології контролю доступу включають різноманітні рішення, які відрізняються за рівнем безпеки, вартістю впровадження, зручністю та комфортом використання. Традиційні механічні замки залишаються найпростішим і найдешевшим способом забезпечення доступу, однак вони не забезпечують гнучкості та високого рівня захисту.

Біометричні системи, такі як розпізнавання відбитків пальців чи обличчя, пропонують найвищий рівень безпеки завдяки унікальним фізіологічним характеристикам користувачів. Вони ефективно виключають ризик передачі доступу іншим особам, проте впровадження таких систем потребує значних фінансових витрат на обладнання і може викликати питання конфіденційності серед користувачів. В той же час, варто відмітити, що біометричні системи контролю доступу набирають популярності завдяки їхній високій точності та надійності.

Сучасні дослідження вказують на широке використання відбитків пальців, розпізнавання обличчя та ідентифікації за райдужною оболонкою ока. Ці методи забезпечують унікальну ідентифікацію користувачів, що робить їх важко доступними для зломів.

Не дивлячись на перелічені переваги, біометричні системи, як показує практика, потребують високих витрат на впровадження та сервісне обслуговування, а також викликають питання щодо конфіденційності та захисту персональних даних [2].

RFID-технології (Radio Frequency Identification (радіочастотна ідентифікація)) є ще одним популярним рішенням для контролю доступу, які надають зручність безконтактного зчитування і більш високий рівень безпеки порівняно з механічними замками. Варто відмітити зручність та комфорт RFID-карток у практичному застосуванні, так як вони забезпечують оперативність зчитування та досить високий пропускний потік, що пояснює їх використання у різних організаціях і не тільки в закладах вищої освіти для контролю доступу до бібліотек, лабораторій та адміністративних приміщень [2]. Ряд авторів, таких як Swedberg C. [3], Байдюк А. В, [4] вказують на досить широкий спектр застосування технології радіочастотної ідентифікації починаючи з безконтактної картки проїзду до автоматизації виробничих процесів на потужних підприємствах.

Ще однією перевагою RFID є можливість інтеграції з іншими системами управління, такими як системи відвідуваності та моніторингу.

Проте, ці системи вимагають інвестицій у зчитувачі та обслуговування, а також залишаються вразливими до ризиків втрати або передачі картки іншим особам, що знижує рівень безпеки.

На противагу біометрії, QR-коди та штрих-коди є економічно ефективними рішеннями, які не вимагають складного обладнання. Вони забезпечують швидкий доступ для відвідувачів завдяки зручності використання смартфонів або простих сканерів, при чому забезпечують достатній рівень захисту та високу пропускну здатність.

**Вибір рішення.** Перспективи використання QR-кодів та штрих-кодів у системах контролю доступу є привабливими завдяки їх простоті розповсюдження та низькій вартості впровадження і експлуатації. Ці технології дозволяють створювати динамічно генеровані ключі доступу, які легко поширювати за допомогою електронної пошти, мобільних додатків або друкувати на папері. Це робить їх ідеальним рішенням для ситуацій, де потрібен тимчасовий або разовий доступ, наприклад, для гостей закладів освіти чи учасників конференцій.

QR-коди були вперше розроблені в 1994 році японською компанією як метод відстеження виробничих процесів в автомобільній промисловості. Найпоширенішими QR-кодами є 2D-штрих-коди, які можуть зберігати інформацію як горизонтально, так і вертикально. Це дозволяє їм кодувати більше інформації, ніж лінійні штрих-коди, які кодують інформацію горизонтально. QR-коди можна сканувати за допомогою додатків для сканування штрих-кодів на смартфонах. Користувачеві потрібно лише навести камеру на QR-код, щоб отримати доступ до інформації, яка в ньому закодована.

Основні елементи структури QR-коду включають:

– заголовок та область пошуку-спеціальні маркери, які дозволяють сканеру знайти QR-код та визначити його розмір та орієнтацію;

– тайм-маркери знаходяться в кутах QR-коду і вказують на його розмір та напрям;

– область даних, містить саму інформацію ( може бути текст, числа, посилання на вебсайт, або інші дані);

– розмітка версії вказує на версію QR-коду, що визначає кількість елементів у структурі даних;

– контрольна сума додається для перевірки правильності декодування інформації.

Код швидкого реагування, який можна скорочено назвати "QR-код", використовується для доступу та зчитування інформації за допомогою простого використання двомірних штрихкодів. QR-код був предметом багатьох систематичних досліджень щодо того, як інформація впорядковується і зберігається шляхом організації QR-кодів у 2D-матриці, разом зі стовпчиками і рядками цієї матриці. QR-коди використовуються в областях, які передбачають передачу текстової інформації, а це поштові повідомлення, номери телефонів, гіперпосилання або інші текстові файли. Це відбувається шляхом захоплення зображення QR-коду, яке потім інтерпретується за допомогою зчитувача QR-кодів або додатків для смартфонів, які підготовлені для цієї мети. QR-код також містить різні шаблони: шаблони пошуку, шаблони вирівнювання, шаблони синхронізації та інші типи, такі як інформація про форматування та часові інтервали, а

також інші змінні. Вони роблять QR-код більш сприйнятливим до розшифрування та виявлення, що дозволяє використовувати QR-коди у простий та ефективний спосіб [5].

Штрих-код – це графічне представлення даних у вигляді послідовності чорних смуг і пробілів, які розташовані у певній комбінації для кодування інформації. Основна мета штрих-коду –забезпечити швидкий і точний доступ до даних за допомогою автоматизованого зчитування. Серед переваг штрих-кодів:

– простота реалізації: штрих-коди мають лінійну структуру, що спрощує їх генерацію та інтеграцію в документи.

– мінімальні вимоги до обладнання: для зчитування штрих-кодів використовується недороге та широко доступне обладнання, що знижує витрати на впровадження.

– ефективність для малих обсягів даних: штрих-коди ідеально підходять для задач, де потрібно закодувати невеликий обсяг інформації, наприклад, унікальний ідентифікатор документа.

– компактність для друку: штрих-коди займають мінімум місця на документі, що особливо важливо для друкованих форм.

– швидкість зчитування: завдяки простій структурі штрих-коди швидко зчитуються сканерами, що прискорює обробку документів.

– відсутність потреби у складній обробці: на відміну від QR-кодів, штрих-коди не вимагають складного алгоритму декодування, що знижує навантаження на систему.

Штрих-коди є оптимальним вибором для простої ідентифікації документів, забезпечуючи високу швидкість, економічність та легкість впровадження [6].

QR-коди та штрих-коди забезпечують швидке і зручне сканування за допомогою доступних пристроїв, таких як смартфони або спеціальні сканери, без значних фінансових витрат на обладнання. Незважаючи на дещо нижчий рівень безпеки порівняно з біометричними системами або RFID-картками, вони можуть слугувати ефективним додатковим рівнем захисту, якщо поєднуються з іншими методами автентифікації. Зокрема, такі методи включають біометричні дані — відбитки пальців чи розпізнавання обличчя, що забезпечують високий рівень захищеності, або RFID-картки, які є зручними для постійних користувачів і дозволяють швидко ідентифікувати особу. Завдяки простоті та економічній ефективності, QR-коди та штрих-коди мають значний потенціал для впровадження в системах контролю доступу закладів освіти, ефективно керуючи потоками відвідувачів та забезпечуючи належний рівень безпеки без значних витрат.

Для забезпечення ефективного контролю доступу сторонніх осіб була розроблена смарт-система, яка передбачає програмну реалізацію для видачі, перевірки та контролю можливості доступу до підрозділів різних організацій. Представлена нами смарт-система вирізняється простотою впровадження та інтеграції в структуру то чи іншої організації.

З метою запобігання підробок, для формування ключів доступу використовуються динамічно генеровані, (змінні з часом) які можуть бути представлені у подвійному форматі: лінійний (штрих-код), та двомірний (QR-код), що переноситься на фізичний носій.

Запровадження таких інтегрованих механізмів дозволяє ефективно контролювати потоки відвідувачів та забезпечувати необхідний рівень безпеки, не утворюючи при цьому зайвих труднощів для легітимних користувачів. У цій статті розглянуто архітектуру та розроблено смарт-систему контролю доступу, методи автентифікації користувачів та можливі напрями її вдосконалення.

**Реалізація рішення.** Для вирішення поставленої проблеми було реалізовано систему у вигляді web-додатку, що забезпечує управління локаціями, видами та тривалістю доступу; видавати документи, що дозволяють доступ та містять штрих-коди; перевіряти права доступу на основі представлених документів; отримувати звітність завантаженості та потоку відвідувачів в режимі реального часу [7].

Архітектура системи включає кілька основних компонентів: інтерфейс оператора, інтерфейс адміністратора, модуль видачі документів доступу, модуль перевірки документів, сервіс автентифікації користувачів та модуль звітності. Таке розділення дозволяє гнучко розширювати смарт-систему чи окремі її частини.

Інтерфейс оператора забезпечує можливість видачі та перевірки документів доступу шляхом інтеграції з відповідними модулями. Інтерфейс адміністратора включає налаштування підрозділів, правил доступу та управління користувачами, що дозволяє зручно керувати параметрами системи.

Модуль видачі документів доступу відповідає за формування документів відповідно до заданих налаштувань, а модуль перевірки документів забезпечує перевірку прав доступу з логуванням дій для забезпечення прозорості процесів. Базова блок-схема алгоритму перевірки доступів на основі штрих-коду показана на рисунку 1. Сервіс автентифікації визначає доступні користувачам дії та інтерфейси, з прикладом блок-схеми перевірки прав доступу на рисунку 2.

Модуль звітності формує інтерфейси для зручного перегляду та аналізу даних на основі збережених логів, що дозволяє відстежувати й оптимізувати використання системи. Для візуального представлення даних було проаналізовано загальноприйнятті підходи до їх зображення. Серед варіантів візуалізації даних оптимальними формати є таблиці та гістограми [8].

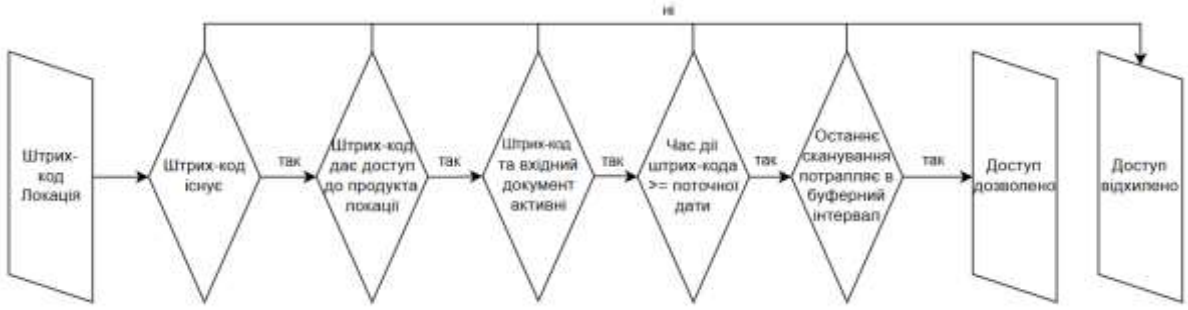


Рисунок 1 - Блок-схема алгоритму перевірки доступу на основі штрих-коду

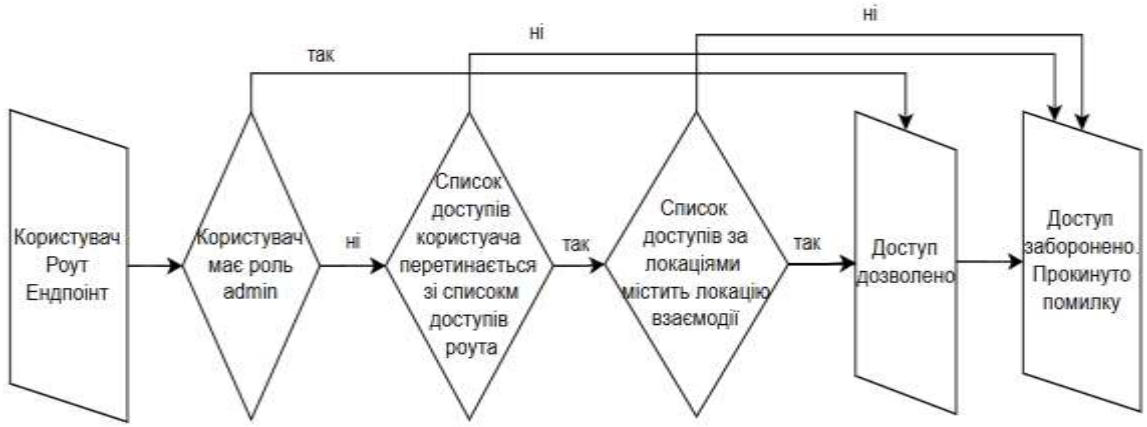


Рисунок 2 - Блок-схема алгоритму перевірки прав доступу до окремих функцій web-додатку

Звіти, що показують результати роботи в як в режимі реального часу так і за певний період, можуть бути представлені у вигляді графіків чи таблиць. На рисунку 3 зображено приклад звіту, що сформовано в системі з використанням демонстраційних даних, потоку відвідувачів за період з 2024.04.01 по 2024.04.05, який візуалізований у вигляді гістограми. Та на рисунку 4 представлено загальний звіт за вищевказаний період на основі аналогічних даних, що реалізований у виді таблиці.

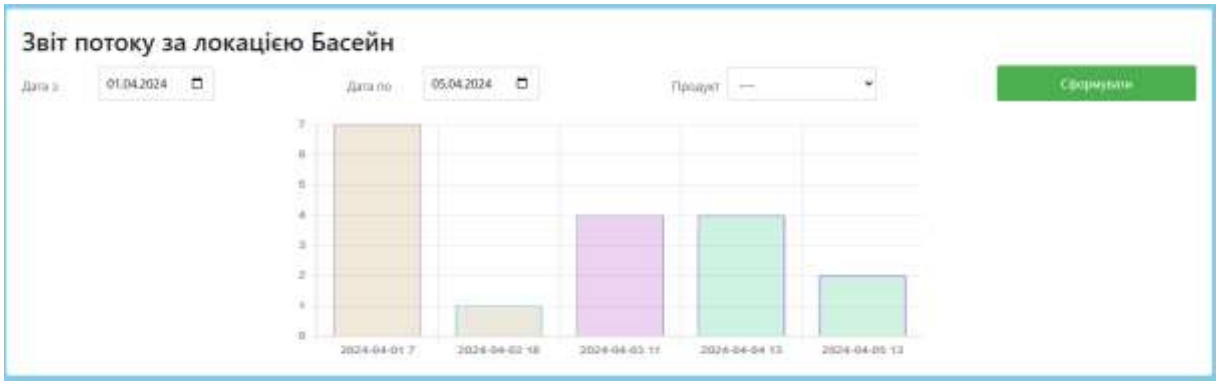


Рисунок 3 - Звіт потоку відвідувачів за період з 2024.04.01 по 2024.04.05


Рисунок 4 - Загальний звіт роботи web-додатку

Смарт-система розроблена для роботи під значним навантаженням і підтримує вертикальне масштабування без ускладнень. Для забезпечення можливостей горизонтального масштабування передбачено розподіл монолітного рішення на мікросервіси, що дозволяє оптимально розподіляти навантаження залежно від ключових компонентів. У випадку підвищеного навантаження на базу даних горизонтальне масштабування може бути досягнуто шляхом кластеризації, що розподіляє операції між кількома вузлами в кластері, забезпечуючи надійність і швидкість обробки даних [9].

Реалізація представленої системи може стати модулями для автономної або напівавтономної смарт-системи контролю доступу. Основні напрями для подальшого розширення включають підтримку додаткових носіїв документів доступу, автоматизацію периферійного обладнання, що може доповнити або замінити інтерфейс оператора, а також автоматизовану видачу документів доступу через персональні кабінети для підтверджених відвідувачів. Крім того, передбачено можливість створення публічного інтерфейсу дистрибуції для організації вільного або платного доступу. Подальше вдосконалення системи буде йти шляхом розширення переліку допустимих способів представлення інформації, таких як QR-коди, впровадження додаткових можливостей ідентифікації користувачів та загального покращення безпеки системи з однієї сторони, і підвищення надійності та масштабованості системи з іншої сторони.

**Висновки.** У роботі проаналізовано різні технології контролю доступу до локацій та підрозділів організацій та методи автентифікації відвідувачів, що дозволило визначити оптимальний варіант для реалізації поставлених завдань та розробити смарт-систему контролю доступу.

У розробленій смарт-системі контролю доступу реалізовано інтеграцію елементів різних існуючих технологій для досягнення балансу між зручністю, комфортом, безпекою та економічною ефективністю. Система використовує динамічні штрих-коди для разових і тимчасових пропусків, що робить її ідеальною для керування доступом гостей і відвідувачів на короткий час.

Розглянута архітектура включає інтерфейс оператора, інтерфейс адміністратора, модуль видачі документів доступу, модуль перевірки документів, сервіс автентифікації користувачів та модуль звітності.

Сформульовано вимоги до web-додатку, на основі яких розроблено рішення, що дозволяє оптимально вирішити поставлені задачі, підвищує ефективність управління доступом і забезпечує належний рівень безпеки.

Модуль прийняття рішень розташований на серверній стороні, що забезпечує централізоване управління всіма процесами автентифікації та доступу, а також дозволяє системі оперативно обробляти запити, зберігаючи записи про відвідування та оптимізувати процеси доступу в режимі реального часу.

Розроблена нами смарт-система дозволяє гнучко реагувати на зміну навантаження та забезпечує можливість без значних ресурсів розширюватися відповідно до динамічних вимог організації, при цьому залишаючи можливість та перспективи подальшого розвитку та вдосконалення відповідно до потреб та викликів організації, одним з напрямків вдосконалення системи є розширення варіантів носіїв для документів ідентифікації користувачів.

**Інформаційні джерела**

1. Chapple M., Implementing Access Control Systems, Indiana, USA, 2020, pp. 110-135.

2. Dwivedi R., Touchless Fingerprint Recognition Basedi on Hierarchical Clustering, Brinston, UK, 2021, pp. 78-94.

3. Swedberg C., "CribMaster Updates Its RFID Units' Real-Time Tool Management," [Електронний ресурс]. Available: https://www.rfidjournal.com/cribmaster-updates-its-rfid-units-real-time-toolmanagement. (дата звернення: 07.10.2024).

4.. Байдюк А. В, Система контролю промислового підприємства на основі технології радіочастотної ідентифікації: Магістерська робота, Київ, Ukraine, 2021, 102 р.

5.. Андреєв А. С, "QR-коди в науці та техніці," [Електронний ресурс]. https://openarchive.nure.ua/server/api/core/bitstreams/8a25bd76-cdd1-47b9-90a0-466e2a55b246/content. (дата звернення: 07.10.2024).

6. Chaudhary A., Sharma A., and Gupta N., "Digital Data Protection Using Barcode & Steganographic Approach," 2022. pp. 11-16.

7. Benantar M., Access Control Systems: Security, Identity Management and Trust Models, Brinston, UK, 2019, pp. 200-230.

8. Healy K., Data Visualization: A Practical Introduction, Princeton University Press, New Delhi, India, 2019, pp. 30-58.

9. Pansara R., Navigating Data Management in the Cloud: Exploring Limitations and Opportunities, Taxes, USA, 2023, pp. 1-9.

**Grudetsky R., Markina L., Plotka B., Satsyk V.**
Lutsk national technical university, Lutsk, Ukraine

## USING THE DECISION-MAKING MODULE OF THE SMART ACCESS CONTROL SYSTEM FOR ORGANIZATION

*The article presents the development of a web application, with its core component being a decision-making module within a smart system.*

*Based on a review and comparison of existing technologies underpinning access control systems specifically those based on mechanical locks, magnetic cards, biometric systems, and RFID technology the architecture of the web application was designed, and an algorithm for the decision-making module was developed. This algorithm is built on the proposed solutions and incorporates dynamically generated access keys in the form of barcodes. This approach ensures convenience, efficiency, and simplicity in the step-by-step design and implementation of a smart access control system that provides semi-autonomous, and if necessary, fully autonomous access control to specific locations and resources of an organization.*

*The testing and validation of the research results were carried out within the units of Lutsk National Technical University. The proposed solution is also applicable to organizations of various forms of ownership with multiple structural divisions, campuses, and venues for mass events where managing access for employees, visitors, and participants is essential.*

***Keywords**: access control, web application, real-time control.*