

КОМП'ЮТЕРНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДО СПОРТИВНОГО КОМПЛЕКСУ З ВИКОРИСТАННЯМ МЕРЕЖЕВИХ СЕРВІСІВ

Вінницький національний технічний університет;

Анотація

Проведено аналіз сучасних технологій та підходів до побудови комп'ютерних систем контролю доступу на основі мережесервісів. Визначено вимоги до системи керування доступом для спортивного комплексу, розроблено архітектуру веборієнтованого рішення, що забезпечує взаємодію локальних пристроїв контролю з центральним сервером через веб-сервіси.

Ключові слова: контроль доступу, мережесервіси, веб-додаток, сервер, інфраструктура, спортивний комплекс.

Abstract

An analysis of modern technologies and approaches to building access control systems based on network services was conducted. System requirements for managing access within a sports complex were defined, and the architecture of a web-based solution enabling interaction between local control devices and a central server via web services was developed.

Keywords: access control, network services, web application, server, infrastructure, sports complex.

Вступ

У сучасних умовах цифровізації та зростання вимог до безпеки об'єктів спортивної інфраструктури особливого значення набувають системи контролю доступу, здатні забезпечити оперативне управління потоками користувачів та моніторинг стану обладнання в реальному часі. Традиційні системи контролю доступу, що працюють автономно, мають низку обмежень, таких як відсутність централізованого адміністрування, складність оновлення даних, обмежена інтеграція з іншими сервісами та недостатня гнучкість при масштабуванні. Використання мережесервісів у поєднанні з вебтехнологіями дозволяє усунути ці недоліки та забезпечити єдиний інформаційний простір для керування всією системою. Такі рішення відкривають можливість централізованого зберігання даних, швидкого доступу до журналів подій, віддаленої діагностики та автоматизованого обліку користувачів спортивного комплексу [1-3].

Розробка комп'ютерної системи контролю доступу з інтеграцією локальних пристроїв контролю до центрального серверу через веб-сервіси забезпечує підвищений рівень надійності, розширює аналітичні можливості та покращує ефективність управління інфраструктурою.

Основна частина

Контроль доступу є ключовим елементом забезпечення безпеки у спортивних комплексах, де щоденно відбувається значна кількість потоків відвідувачів, тренерів та технічного персоналу. На відміну від адміністративних або виробничих будівель, спортивні заклади мають ускладнену логістику доступу: різні зони мають різний рівень відкритості, частина приміщень є загальнодоступними, а інші – призначені лише для персоналу або власників абонементів. Це вимагає використання адаптивних і гнучких систем доступу, здатних оперативно змінювати правила та реагувати на динамічні ситуації [4].

Специфіка контролю доступу в спортивних комплексах обумовлена також розгалуженою інфраструктурою, що включає тренажерні зали, басейни, зони SPA, адміністративні приміщення, склади інвентарю та додаткові сервісні майданчики. Кожен з цих секторів вимагає індивідуальних політик доступу, що ускладнює роботу класичних автономних систем. Саме тому актуальним стає

перехід до мережесих рішень, які дозволяють управляти всіма контролерами з єдиного центру та забезпечують актуальність даних у реальному часі.

Існуючі на ринку комп'ютерні системи контролю доступу зазвичай орієнтовані на промислові або корпоративні об'єкти, де правила доступу більш статичні. У спортивних закладах ситуація змінюється частіше: клієнти можуть купувати різні типи абонементів, отримувати разові пропуски, користуватися знижками або тимчасовими акціями. Тому типові рішення не завжди забезпечують достатню гнучкість у налаштуванні сценаріїв та часто не містять засобів інтеграції з вебінтерфейсами чи мобільними додатками.

На сьогодні використовуються різні технології ідентифікації користувачів: RFID-карти, магнітні ключі, QR-коди, біометричні системи, мобільні додатки з NFC. Кожен метод має власні переваги та недоліки: RFID-карти зручні та недорогі, але можуть бути легко передані іншій людині; біометричні дані забезпечують високий рівень безпеки, але вимагають дорогого обладнання; мобільні ідентифікатори є універсальними, але залежать від стану смартфона користувача. Саме тому сучасні системи створюють комбіновані рішення, які поєднують кілька методів для досягнення оптимального балансу між безпекою, ціною та зручністю [6-7].

Аналіз вимог до системи контролю доступу у спортивному комплексі показує, що вона повинна забезпечувати не лише технічний контроль проходу, але й розширені інформаційні функції: ведення журналів відвідувань, статистику навантаження залів, відстеження пікових годин, автоматичне блокування порушників правил, а також інтеграцію з CRM чи системами оплати. Всі ці функції потребують централізованого серверного компонента і продуманого вебінтерфейсу адміністратора.

Вибір технологій для розробки мережесих сервісів базувався на необхідності забезпечити стабільну багатокористувацьку роботу, підтримку асинхронної обробки запитів та можливість швидкого масштабування [8-9]. Серверна частина реалізується на Node.js, що дозволяє обробляти високочастотні HTTP- та WebSocket-запити від контролерів доступу. Клієнтська частина розробляється з використанням React, який забезпечує швидке оновлення інтерфейсу без перезавантаження сторінки та зручну побудову компонентної структури.

Веб-інтерфейс адміністратора створюється відповідно до вимог до сучасних систем моніторингу: модульність, інтерактивність, доступність з будь-якого пристрою, можливість інтеграції з API та зовнішніми системами. Використання React також дозволяє впровадити логіку маршрутизації між сторінками, авторизацію, а також динамічне відображення даних через REST API.

Багаторівнева архітектура системи контролю доступу забезпечує чітке розділення відповідальностей між компонентами (рисунок 1). На рівні обладнання знаходяться локальні контролери (наприклад, турнікети або електронні замки), що виконують миттєві рішення про дозвіл чи заборону доступу. Наступний рівень — мережесих сервіси, які надають централізоване зберігання правил доступу та обробку подій. Найвищий рівень — вебінтерфейс адміністратора, який дозволяє управляти системою, аналізувати статистику та отримувати інформацію у реальному часі.

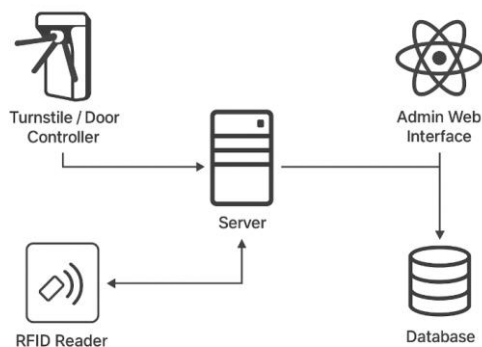


Рисунок 1 – Схема взаємодії між апаратним забезпеченням та мережесих сервісами

Схема взаємодії між апаратним забезпеченням та мережесих сервісами побудована таким чином, щоб мінімізувати затримки та забезпечити високу достовірність даних. Контролери надсилають інформацію про кожну подію (ідентифікацію користувача, спробу проходу, помилки обладнання) на

центральний сервер. Сервер обробляє запит, звіряє правила доступу у базі даних та повертає рішення. Усі події додатково записуються до журналу, який доступний адміністраторам у вебінтерфейсі.

Проектування структури бази даних передбачало створення оптимальної моделі для зберігання великої кількості подій, інформації про користувачів, їхні припустимі зони доступу, статуси контролерів та налаштування системи. Основні сутності включають: Користувачі, Ролі, Контролери, Події, Правила доступу, Абонементи. Особлива увага приділена індексації таблиць подій для забезпечення швидкого пошуку у великих журналах.

REST API забезпечує стандартизований спосіб комунікації між клієнтом та сервером. Він включає маршрути для авторизації, керування користувачами, отримання журналів подій, конфігурації контролерів, зміни правил доступу та генерації статистики. API розроблено з дотриманням принципів REST: чітка структура URL, використання методів GET/POST/PUT/DELETE, передачі даних у форматі JSON та захист запитів через JWT.

Реалізація серверної частини охоплює налаштування маршрутизатора запитів, модулів обробки подій та підсистеми авторизації. Сервер виконує функції центрального ядра, приймаючи запити від контролерів та користувачів, перевіряючи їхню валідність і повертаючи відповідь згідно з правилами доступу. Логіка обробки подій побудована таким чином, щоб система коректно працювала навіть за умови високого навантаження.

Для забезпечення інформаційної безпеки система має підтримувати гнучкий модуль авторизації та ролей. Адміністратор повинен мати можливість визначати категорії користувачів (наприклад, відвідувач, тренер, персонал) та призначати їм відповідні привілеї. Доступ до адміністративного інтерфейсу має бути захищений токенами або іншими безпечними механізмами автентифікації.

Підсистема обробки запитів від контролерів повинна забезпечувати визначення прав доступу користувача до певної зони. Валідація ідентифікатора, перевірка чинності абонемента, статусу облікового запису та відповідності правилам доступу мають виконуватися у реальному часі, а рішення – негайно передаватися локальному контролеру.

Клієнтська частина веб-інтерфейсу адміністратора повинна містити базовий набір функціональних модулів: панель управління, модуль керування користувачами, інтерфейс роботи з контролерами, статистичний розділ та журнал подій. Веб-інтерфейс має бути структурованим, модульним та зручним для перегляду. Особливе місце відводиться журналу подій, який повинен відображати проходи, спроби доступу, технічні несправності та інші системні події з можливістю фільтрації за датою, користувачами та зонами.

Функціонал контролю доступу має забезпечувати створення правил і шаблонів для різних категорій користувачів, прив'язку контролерів до зон та оперативне оновлення їхнього статусу. Система повинна дозволити додавання нових користувачів, зміну параметрів їх доступу та блокування у випадку порушення правил.

Статистична й аналітична підсистема повинна надавати можливість отримання даних щодо відвідуваності, пікових періодів навантаження та активності в окремих зонах спортивного комплексу. Інформація має відображатися у зручному вигляді – графіки, таблиці, діаграми – для підтримки управлінських рішень та планування роботи комплексу.

Вимоги до якості системи включають забезпечення стабільності роботи, швидкого реагування на події, захищеності даних та коректної взаємодії між серверною частиною, веб-інтерфейсом і локальними контролерами. Система повинна підтримувати можливість подальшого масштабування, модернізації та інтеграції з додатковими сервісами або обладнанням.

Висновки

Отже, можна зазначити, що впровадження архітектур, заснованих на інтеграції локальних пристроїв контролю з центральним сервером через веб-сервіси, відкриває можливість суттєвого підвищення ефективності систем контролю доступу. Такий підхід забезпечує уніфікований механізм взаємодії між апаратними модулями та серверною частиною, дозволяє централізовано керувати політиками доступу, оптимізувати обробку подій та значно спростити масштабування системи в умовах зростання інфраструктури. Використання веб-орієнтованих протоколів та стандартних API сприяє гнучкості, модульності та адаптивності архітектури, що є критично важливим у сучасних

безпекових рішеннях. Таким чином, теоретичні засади побудови таких систем формують фундамент для подальшого розвитку технологій контролю доступу, забезпечуючи узгодженість, надійність та можливість інтеграції з іншими інформаційними сервісами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- 1 Indoor Positioning Technologies — Overview and Comparison [Електронний ресурс]. – Режим доступу: <https://www.pozyx.io/blog/indoor-positioning-technologies>
- 2 Wi-Fi Location-Based Services Design Guide – Cisco Documentation [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/200527>
- 3 Bluetooth Low Energy (BLE) Positioning: How It Works [Електронний ресурс]. – Режим доступу: <https://www.bluetooth.com/learn-about-bluetooth/key-attributes/low-energy/>
- 4 Indoor Positioning Systems Explained: Wi-Fi, BLE, UWB and More [Електронний ресурс]. – Режим доступу: <https://www.infsoft.com/technology/indoor-positioning>
- 5 Zafari F., Gkelias A., Leung K. A Survey of Indoor Localization Systems and Technologies [Електронний ресурс]. – Режим доступу: <https://arxiv.org/abs/1709.01015>
- 6 Fingerprinting Wi-Fi Technologies for Indoor Localization [Електронний ресурс]. – Режим доступу: <https://iotbyhvm.ooo/wifi-fingerprinting-indoor-positioning/>
- 7 Martyniuk, T., Kozhemiako, A., Katashynskyi, D., & Bulyga I. (2024). Structural peculiarities of neurolike object classifier . Scientific Works of Vinnytsia National Technical University, (4). <https://doi.org/10.31649/2307-5392-2023-4-1-7>
- 8 Real-Time Location Systems (RTLS): Principles and Applications [Електронний ресурс]. – Режим доступу: <https://www.rfidjournal.com/rtls-real-time-location-systems>
- 9 Benantar M. Access Control Systems: Security, Identity Management and Trust Models. – Springer, 2006. – 300 p.

Доманський Антон Францович - студент групи 2KI-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Науковий керівник: *Кожем'яко Андрій Вікторович* — к.т.н. доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця, e-mail: kvantron@vntu.edu.ua

Domanskyi Anton Frantsovych — a student of group 2KI-24m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Scientific supervisor: Kozhemiako Andrii Viktorovich — Ph.D. in Technical Sciences, Associate Professor of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kvantron@vntu.edu.ua