

СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ

Тарновський А.М., Коляда К.В.

Факультет прикладної математики КПІ ім. Ігоря Сікорського, Україна

E-mail: tarnovskiyo211@gmail.com

REMOTE ACCESS CONTROL SYSTEM

An approach to building a system for remote access control for the hotel is proposed. The identifier for access is a QR code sent to the customer's mobile phone. The interaction between the administrator application and the access controller is carried out through the cloud server

Запропоновано підхід до побудови системи для віддаленого керування доступом для готелю. Ідентифікатором для доступу є QR-код, що надсилається на мобільний телефон клієнта. Взаємодія між додатком адміністратора та контролером доступу здійснюється через хмарний сервер.

Однією з перспективних сфер застосування систем контролю і управління доступом є готельний бізнес. Система контролю і управління доступом для готелів є сучасним інструментом, що дозволяє суттєво підвищити рівень безпеки і сервісу, зробити перебування гостя максимально комфортним, забезпечити режим енергоефективності та енергозбереження, тощо [1]. Як правило, сьогодні в готельних системах керування доступом використовуються електронні замки з доступом за безконтактною картою Em Marin або Mifare [2].

Розвиток та широке застосування Інтернет технологій у сфері готельного бізнесу характеризується впровадженням і поширенням Інтернет-бронювання. Багато готелів розміщують на своїх веб-сайтах (а також на сайтах туристичних компаній або фірм-посередників) модуль онлайн-бронювання, за допомогою якого відвідувач може самостійно вибрати номер і замовити його. У зв'язку з цим для повноцінної зручності бажано мати можливість отримувати права доступу до заброньованого номеру на визначений період також дистанційно. Особливо це актуально для малих готелів, в яких стійка реєстрації відсутня або працює не цілодобово.

Підходи до реалізації системи віддаленого керування доступом.

Сучасним трендом інформатизації в різних областях стало широке використання смартфонів. За допомогою смартфона можна отримати доступ до Інтернету, електронної пошти, банківських рахунків і багато чому іншому. Смартфон також може використовуватися і як засіб ідентифікації.

На теперішній час більшість систем контролю та управління доступом, що використовують технології мобільної ідентифікації, як правило містять чотири структурні компоненти [3]:

1. Мобільний ідентифікатор – цифровий код, що передається бездротовим зв'язком від смартфона до зчитувача; його можна розглядати як віртуальну

карту, що зберігається на смартфоні;

2. Мобільний зчитувач – пристрій для зчитування мобільного ідентифікатора і передачі його номера в контролер системах контролю та управління доступом;

3. Мобільний додаток – засіб для отримання і зберігання мобільного ідентифікатора, а також для здійснення взаємодії з мобільним зчитувачем;

4. Портал адміністратора – «хмарний» сервіс або додаток для персонального комп'ютера, що служить для видачі / відкликання мобільного ідентифікатора на смартфон.

У більшості випадків мобільна ідентифікація реалізується за допомогою інтерфейсу NFC. Проте такий підхід вносить суттєві обмеження щодо використання через відсутність підтримки NFC поки ще у більшості смартфонів. Тому отримання доступу за технологією NFC на теперішній час для багатьох клієнтів буде технічно не здійсненою.

З іншого боку, передачу коду між смартфоном та контролером доступу можна здійснити через Bluetooth. Не зважаючи на наявність Bluetooth майже в усіх мобільних телефонах такий підхід теж не можна вважати вдалим. По-перше, перше підключення мобільного телефону до контролера вимагає від користувача виконання певних дій для авторизації. Це потребує хоча і доволі незначного, але все ж таки певного рівня розуміння процесу та досвіду в здійсненні підключення через Bluetooth. По-друге, мобільний телефон за версією підтримуваного Bluetooth може виявитися не сумісним з тим, що підтримується контролером, а підтримка усіх можливих версій не є доцільною.

З врахуванням викладеного вище для отримання прав доступу пропонується здійснювати ідентифікацію за QR-кодом, що відображається на екрані смартфона. Такий підхід не висуває ніяких особливих вимог до характеристик мобільного телефону та технічної обізнаності користувача. Єдине що потрібно зробити, то це лише відкрити зображення коду на телефоні та піднести його до контролера.

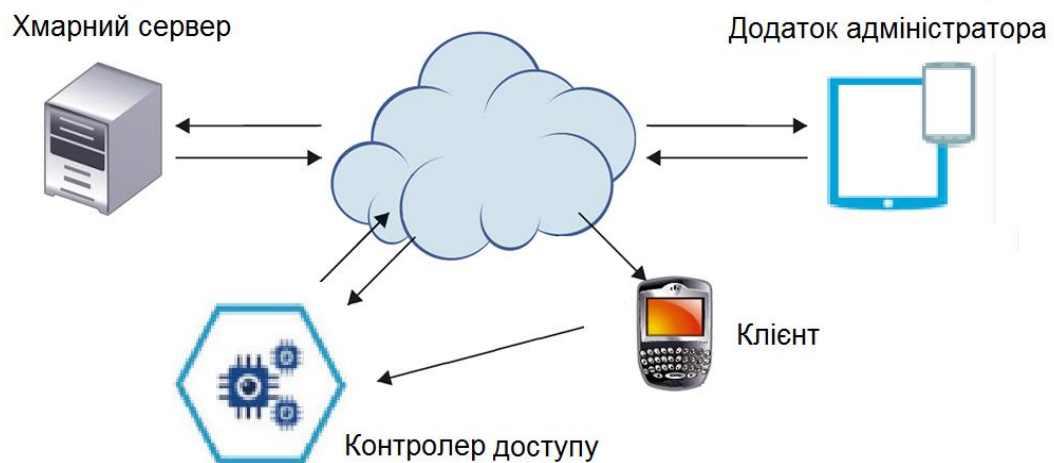


Рис. 1. Система віддаленого керування доступом.

Структурно система віддаленого керування доступом складається з чотирьох компонентів: хмарного сервера, контролера доступу, додатка адміністратора та мобільного телефону клієнта (рис. 1).

Контролер доступу є мікроконтролерним засобом зі зчитувачем QR-кодом та Wi-Fi модулем. Обмін даними між контролером та додатком адміністратора, що задає ідентифікатор доступу у вигляді QR-коду, здійснюється за моделлю клієнт-сервер через хмарний сервер та точку доступу до бездротової мережі Wi-Fi відповідно до протоколу TCP/IP. Для побудови контролера може бути використаний мікроконтролері середньої продуктивності та модуль зчитувача QR-коду типу EM2028 [4] та Wi-Fi модуль типу ESP-07 [5].

Клієнт завантажує картинку з QR-кодом за URL посиланням, що надсилається йому адміністратором. Альтернативно код клієнту може бути надісланий через будь-який месенджер, наприклад, Viber або Telegram.

Висновки. Застосування Інтернет технологій популяризує Інтернет-бронювання, що робить бажаним отримання прав доступу віддалено. Це особливо актуально для малих готелів, в яких стійка реєстрації відсутня або працює не цілодобово.

Віддалене надання прав доступу може бути забезпечене за допомогою ідентифікатора, що надсилається на мобільний телефон. Простим рішенням ідентифікації з використанням мобільного телефону є ідентифікація за QR-кодом, яка, на відміну від ідентифікації через Bluetooth або NFC, може бути реалізована на будь-якому телефоні і вимагає від користувача лише елементарних навичок користування смартфоном.

Література

1. Система контроля и управления доступом для гостиниц. [Електронний ресурс]. Режим доступу: <https://avectis.by/solutions/integrirovannye-sistemy-bezopasnosti/sistema-kontrolya-i-upravleniya-dostupom-dlya-gostinic>.
2. Быков О. Системы контроля доступа на бесконтактных смарт-картах Mifare // Алгоритм Безопасности. 2011. № 3. С. 78 –79.
3. Умнов А. В. Системы мобильного доступа. Как сделать правильный выбор? // Алгоритм Безопасности. 2019. № 1. С. 32 –34.
4. Сканирующий модуль Newland EM2028. [Електронний ресурс]. Режим доступу: <https://agrovesy.com.ua/p1243145426-skaniroyuschij-modul-newland.html>.
5. Wi-Fi модуль ESP8266 версія ESP-07. [Електронний ресурс]. Режим доступу: <https://arduino.ua/prod1444-wi-fi-modul-esp8266-versiya-esp-07>.