УДК 004.77

**А. М. Тарновський,**
**Л. В. Крупельницький**

# СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ З ІДЕНТИФІКАЦІЄЮ ЧЕРЕЗ BLUETOOTH

Вінницький національний технічний університет

***Анотація***

*Запропоновано підхід до побудови системи віддаленого керування доступом з використанням технології мобільної ідентифікації, при якій ідентифікатором є MAC-адрес (UUID) Bluetooth модуля, яким обладнаний смартфон. Взаємодія між додатком адміністратора та контролером доступу здійснюється через хмарний сервер*

**Ключові слова:** управління доступом, контролер управління доступом, мобільна ідентифікація, Bluetooth з'єднання, хмарний сервер, веб-додаток.

***Abstract***

An approach to building a remote access control system using mobile identification technology is proposed, in which the identifier is the MAC address (UUID) of the Bluetooth module equipped with the smartphone. The interaction between the administrator application and the access controller is carried out through a cloud server

**Keywords**: access control, access control controller, mobile identification, Bluetooth connection, cloud server, web application..

## Вступ

Одним із найефективніших і цивілізованих підходів до вирішення завдання комплексної безпеки об'єктів різних форм власності є використання систем контролю та управління доступом. Такі системи дозволяють закрити несанкціонований доступ на територію, у будівлю, окремі поверхи та приміщення. Останні тенденції розвитку у цій галузі пов'язані з впровадженням IP-технологій. Майже усі провідні виробники закладають у своєму обладнанні можливість прямого підключення до мережі Ethernet. Завдяки цьому отримуються нові додаткові можливості, основними з яких є зручність використання обладнання, простота та мала вартість впровадження подібних систем на об'єктах з розвиненою IT-інфраструктурою [1].

## Підходи до реалізації віддаленого керування доступом

Основним принципом роботи будь-якої системи управління доступом є порівняння ознак ідентифікації з характеристиками, що зберігаються у пам'яті системи. Для ідентифікації при наданні доступу можуть використовуватися різні технології. В сучасних системах управління доступом найбільше поширення отримали радіочастотна, мобільна та біометрична ідентифікації [1], [2].

Мобільна ідентифікація останнім часом набуває усе більшого поширення, що обумовлено високою популяризацією смартфонів, їх універсальністю та багатозадачністю. Особливостями мобільної ідентифікації є використання безкоштовного або майже безкоштовного віртуального ідентифікатора, на одному смартфоні можна зберігати кілька ідентифікаторів, смартфони підтримують багатофакторну аутентифікацію, біометричну ідентифікацію та інші функції безпеки [3]. Поряд з цим, лише мобільна ідентифікація дозволяє здійснити віддалене керування доступом, що надає високу гнучкість системі, робить легким її масштабування, дозволяє змінювати права доступу та контролювати роботу системи і переміщення користувачів у режимі реального часу. Головними недоліками віддаленого керуваня є необхідність постійного надійного Інтернет зв′язку як з боку смартфона, так і з боку контролера, можливі значні затримки у реакції системи, збільшений ризик несанкціонованого втручання в її роботу, тощо.

Підвищити автономність дозволяє застосування мобільного телефону як носія ідентифікатора, що напряму передається від смартфона до контролера керування за допомогою мобільного додатку. Передача ідентифікатора у смартфон та запис його до бази даних у контролері доступу здійснюється адміністратором через хмарний сервер за допомогою Веб-додатку. Таким чином отримується

можливість управляти правами доступу віддалено. Однак при цьому необхідність у наявності Інтернет зв′язку потрібна лише на час взаємодії віддаленого сервера з мобільним додатком та контролером доступу.

Передачу ідентифікатора від смартфону до контролера керування можна здійснити з використанням технологій NFC (Near field communication) — технології близької ідентифікації або BLE (Bluetooth Low Energy) — технології низького енергоспоживання Bluetooth. Технологія NFC надає набагато меншу швидкість передачі, проте забезпечує менший час встановлення з'єднання та має менший радіус дії, що ускладнює перехоплення даних, а тому гарантує високий рівень безпеки. Проте з використанням NFC можуть виникнути проблеми у пристроях від Apple, оскільки в iOS доступ до NFC забезпечується лише в режимі Read Only, що не дозволяє забезпечити повноцінну взаємодію між мобільним додатком та зчитувачем [4]. Поряд з цим NFC не дає ніяких реальних практичних сценаріїв використання, на відміну від Bluetooth, профілі якого чітко описують як передати файл, як підключити гарнітуру або як забезпечити мережевий доступ,. Тому для передачі ідентифікатора від мобільного пристрою до контролера доступу запропоновано використовувати з′єднання за Bluethooth. Описані принципи побудови системи віддаленого керування доступом схематично представлені на рис. 1. Як ідентифікатор пропонується використовувати MAC-адрес (UUID) Bluetooth модуля, яким обладнаний смартфон.

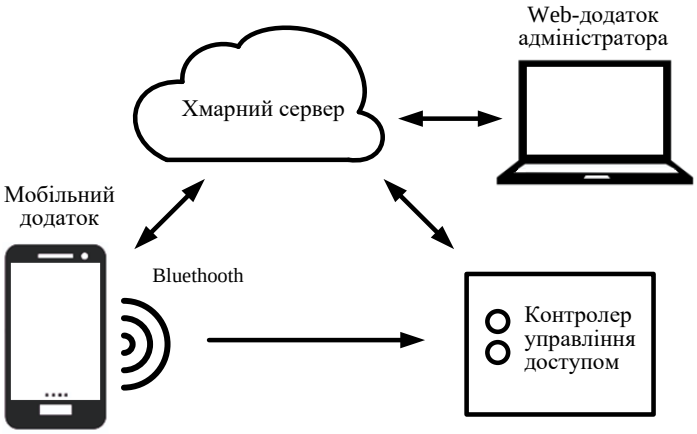


Рис. 1. Система віддаленого керування доступом

Під час розгортання системи на об′єкті адміністратор робить «прив′язування» контролера управління доступом до панелі адміністратора, яке здійснюється за ID контролера, наданому йому виробником. Далі створюється список користувачів, яким будуть надані права доступу. У подальшому цей список може змінюватися. Користувач з використанням мобільного додатку створює акаунт, через який отримує від адміністратора код доступу для реєстрації в системі. Під час реєстрації відбувається запис UUID Bluetooth модуля смартфона користувача до відповідного поля у базі даних на хмарному сервері. Одночасно цей UUID передається у контролер управління доступом і зберігається у ньому, поки користувач зберігає права доступу. У подальшому у мобільному додатку користувача буде відображатися перелік об′єктів з дозволеним доступом. З точки зору системи це ID контролерів, що у своїх базах даних містять UUID Bluetooth модуля смартфона користувача.

Список користувачів, яким надані права доступу, отримується контролером шляхом відправлення періодичних запитів до веб-серверу на оновлення ідентифікаторів. Поряд із цим контролер постійно перебуває у режимі очікування на Bluetooth підключення. При надходженні запиту на встановлення Bluetooth з′єднання контролер вилучає з нього UUID пристрою, що робить цей запит, та перевіряє чи збігається він з одним із тих, що зберігаються в його базі даних. Встановлення повноцінного Bluetooth з’єднання між смартфоном та контролером не відбувається. Після отримання запиту на встановлення з′єднання та прийняття рішення надавати чи не надавати доступ, контролер відмовляє у з’єднанні.

Для отримання доступу користувач у мобільному додатку вибирає потрібний об’єкт, після чого активізується екран керування і у смартфоні автоматично вмикається Bluetooth. Якщо у зоні покриття є інший активний Bluetooth, елемент управління для запиту на отримання доступу стає активним, що надає можливість надіслати запит до контролера.

## Висновки

Запропонований підхід до побудови системи керування доступом дозволяє реалізувати віддалене надання прав доступу в онлайн режимі та забезпечення фізичного доступу в режимі офлайн за допомогою Bluetooth з′єднання.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Системи контролю і управління доступом від А до Я. [Електронний ресурс]. Режим доступу: https://deps.ua/ua/knowegable-base/reference-information/7824.html.
2. Омельченко М.О. Характеристика та загальні вимоги до системи контролю і управління доступом // Сучасний захист інформації №4(44), 2020, С. 46 — 50.
3. Gean Davis Breda New Era of Mobile Access Control System / Gean Davis Breda, Raul Mariano Cardoso, Felipe André Cordeiro Pirotta // International Journal of Computer Science and Network Security, VOL.15, No.8, 2015, P. 6 – 15.
4. Технология NFC в смартфонах и ее практическое использование. [Електронний ресурс]. Режим доступу: https://www.ixbt.com/mobile/nfc-2018.shtml.



***Тарновський Артем Миколайович*** — студент групи 2КІ-21м, факультет інформаційних технологій та комп′ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: tarnovskiy0211@gmail.com

***Крупельницький Леонід Віталійович*** — канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет

***Tarnovskiy Artem M.*** — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : tarnovskiy0211@gmail.com

***Krupelnitskyi Leonid V.*** **—** Cand. Sc. (Eng), Assistant Professor of Department of Computer Engineering , Vinnytsia National Technical University, Vinnytsia.