БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ В СИСТЕМІ КОНТРОЛЮ ДОСТУПУ З ВИКОРИСТАННЯМ СЕНСОРНОЇ МЕРЕЖІ

Афанасьев Ю.В.
Науковий керівник – д.т.н., проф. Лемешко О.В.
Харківський національний університет радіоелектроніки
(61166, Харьков, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-13-20)

Ensuring access control to facilities based on the use of telecommunication systems and networks is an urgent task. This problem is solved by finding effective ways to build access control systems. The paper studies the possibility of building an access control system based on one-factor and multi-factor authentication. A version of the hardware and software system implementation is proposed. For various system configuration options, the system availability time has been experimentally determined.

Аналіз публікацій з питань рішення задачі контролю доступу показує, що питання безпеки доступу до інформації є актуальним [1]. Існуючі методи автентифікації, такі як паролі, картки, різноманітні електронні ключі, не забезпечують в повній мірі захист від несанкціонованого доступу. Одним з ефективних методів забезпечення захисту інформації є застосування біометричних методів автентифікації.

За результатами дослідження питань реалізації технологій автентифікації визначено, що вартість апаратних засобів залежить від методу автентифікації, інформація про користувача зберігається в базі даних на сервері, що при певних умовах не забезпечує захист від доступу до неї. Удосконалення методів несанкціонованого доступу обумовлює розробку нових та удосконалення існуючих методів автентифікації. До них відносяться динамічні і статичні методи, методіи багатокритеріального аналізу показників та інше [2].

В загальному випадку методи автентифікації повинні забезпечувати найменше значення частот помилкових спрацювань та відмов в обслуговані. Підвищення рівня безпеки в системах контролю доступу (СКД) можливе за рахунок застосування методу двофакторної автентифікації (two-factor authentication). Прикладами реалізації даного методу є способи автентифікації в соціальних мережах, банківській сфері де використовуються: SMS-автентифікація, одноразовий пароль, Google Authenticator та ін. [3]. Структура СКД залежить від наступних характеристик: кількості персоналу, для якого необхідно визначити заданий рівень доступу до певної інформації (об'єкту); просторових показників, які визначаються розмірами об'єкта, взаємному розташуванню окремих складових на місцевості; особливостями топології інформаційної

системи. Таким чином, зазначені системи представляють собою мережі, які поєднують в собі комплекс розподілених приладів автентифікації. Тому, такі мережі можна розглядати як сенсорні мережі.

В основу програмно-апаратної реалізації варіантів СКД покладено застосування наступних елементів: зчитувач відбитків пальців FPM10A; мікроконтролер ESP32 з інтегрованими Wi-Fi та Bluetooth контролерами та антенами; модуль RFID модуль RC522; мікроконтролер ESP8266; сервер одноплатний компьютер Raspberry Pi 3; Bluetooth-пристрої.

Розроблено алгоритм з автентифікацією по Bluetooth-пристрою. Він включає етап внесення даних користувача для автентифікації в базу даних та етап автентифікації користувача. В загальному випадку алгоритми роботи з автентифікацією по відбитку пальця та з використанням модуля RFID аналогічні. Загальними рисами реалізованих варіантів є наступне: необхідність наявності серверу, в якому зберігається база даних користувачів; використання мікроконтролеру ESP32 забезпечує реалізацію розглянутих методів; використання мікроконтролеру ESP8266 забезпечує реалізацію методів автентифікації без використання Bluetooth.

З метою визначення особливостей побудови мережі з використанням мікроконтролерів типу ESP32, в роботі проведено експериментальне дослідження часової характеристики мережі - часу готовності мережі. Розглянуто два варіанта налаштування мережі. Перший – один модуль ESP32 роздає свою WI-FI мережу а другий модуль підключається до неї за умови введення параметрів налаштування мережі вручну. Другий – один модуль ESP32 роздає свою WI-FI мережу, а другий модуль підключається до неї за умови передачі параметрів налаштування мережі автоматично по каналу WI-FI. В результаті аналізу отриманих даних визначено, що при налаштуванні мережі вручну, час підключення має більш стабільний характер і складає 1,35 сек. При автоматичному налаштуванні час готовності знаходиться в межах 1,3 – 44,3 сек.

ЛІТЕРАТУРА

1. Афанасьєв Ю.В. Шляхи забезпечення функціональної стійкості системи конролю та управління доступом до режимних обєктів / Ю.В. Афанасьєв, Д.В. Сумцов // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 23-24 березня 2017 р.; Київський національний університет імені Тараса Шевченка. - К.: ВПЦ «Київський університет», 2017.- С. 8–13.

2. Кравченко Ю. В. Визначення проблематики теорії функціональної стійкості щодо застосування в комп'ютерних системах / Ю. В. Кравченко, С. В. Нікіфоров // Телекомунікаційні та інформаційні технології. – 2014. – № 1. – С. 12–18.

3. Кикина А.Л., Когельман Л.Г., Мишиев А.И. Вопросы безопасности беспроводных сенсорных сетей / Труды международной научно-технической конференции – Пенза, ПензГТУ, 2017, Вып. 25, с. 70.