ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

**№ 2 (2), 2021** https://doi.org/10.23939/ictee2021.02.045

# СИСТЕМА АВТЕНТИФІКАЦІЇ НА ОСНОВІ АНАЛІЗУ АКУСТИЧНИХ СИГНАЛІВ

**С. Отрох[1], О. Андрійчук[2], Р. Гусейнов[1], К. Олєнєва[1]**

*[1] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", проспект Перемоги, 37, Київ, 03056, Україна*
*[2] Інститут проблем реєстрації інформації Національної академії наук України, вул. Миколи Шпака, 2, Київ, 03113, Україна*

Відповідальний за рукопис: С. Отрох (e-mail: 2411197@ukr.net)

*(Подано 25 грудня 2021)*

Досліджено питання автентифікації та авторизації користувачів у системах, які працюють в мережі інтернет, розглянуто проблему надійності отримання доступу та варіанти покращення і підвищення рівня безпеки та збереження даних користувачів. В статті запропоновано вирішення проблеми підвищення надійності за рахунок розробленої системи автентифікації із використанням аналізу звукових сигналів. Доведено, що проблема захисту облікових засобів користувачів стає дедалі важливішою із поширенням інтернет-технологій у житті пересічних людей.

**Ключові слова:** *автентифікація; авторизація; MFA.*
**УДК 004.42**

## 1. Вступ

Інтернет давно перестав бути тільки засобом комунікації для технічно просунутих користувачів. Сьогодні майже в усіх країнах світу життя населення не обходиться без інтернету. За допомогою інтернету дізнаються новини, обмінюються інформацією з друзями та даними з колегами, оплачують рахунки, купують валюту та цінні папери, отримують доступ до банківських послуг та роблять безліч інших речей, отримання яких за допомогою мережі інтернет для більшості вже стало рутинною справою. Згідно з даними інтернет-досліджень за 2019 р., 74 % [1] населення України є користувачами інтернету, з яких 85 % користуються ним кожен день. І в той час, як все більше користувацьких даних передаються через інтернет та стають доступними в мережі, виникає потенційний ризик втрати, несанкціонованого доступу, модифікації чи пошкодження даних, що для користувачів і власників цих даних потенційно загрожує значною фінансовою та репутаційною шкодою. В таких випадках одним із ключових механізмів захисту даних є автентифікація користувача й авторизація доступу до його даних. Водночас механізм автентифікації нині реалізований зазвичай за допомогою простого запам'ятовування власних ідентифікатора (логіна) та пароля.

Автентифікація – це процес перевірки особистості користувача [2]. Користувачі ідентифікуються, використовуючи різні механізми автентифікації. У мережах, які підтримують безпечну автентифікацію, реалізовують цей процес, перевіряючи інформацію, яку надав користувач під час входу, з даними, збереженими у базі даних. В умовах швидкого розвитку та поширення мережевих технологій з'являється велика кількість різних методів автентифікації в мережах. Уже існує багато різних типових методів автентифікації, серед них, наприклад: паролі, двофакторна автентифікація,

технологія єдиного входу, біометрична ідентифікація та комп'ютерне розпізнавання даних, а також різноманітні засоби протокольного рівня.

У захищених системах, в яких реалізована можливість двофакторної автентифікації, вхід до системи здійснюється тільки із довірених пристроїв. Під час першого входу до такої системи з нового пристрою користувачеві потрібно надати системі два види інформації: свій пароль і цифровий код підтвердження, який автоматично відображається на вже внесених до цієї системи раніше довірених пристроях. Після реєстрації нового пристрою – його верифікації він автоматично додається до системи та зберігається в ній як довірений для майбутніх повторних входів.

Використання для автентифікації лише одного фактора робить системи вразливими до спроб несанкціонованого доступу, тобто до атак, таких як атаки перебором чи перебором за словником. Такі атаки та несанкціонований доступ до даних користувачів можливі й тому, що самі користувачі часто використовують короткі паролі, дуже прості паролі без додаткових і складних символів, однакові паролі одразу в декількох системах, якими вони користуються. Для того, щоб посилити захист від атак, зазвичай у системах формуються вимоги до пароля, такі як: обмеження мінімальної довжини, використання спеціальних символів і чисел тощо.

З розвитком механізмів автентифікації входу до систем з'явилась можливість багатофакторної автентифікації. Інтернет-ресурси та системи, які підтримують багатофакторну автентифікацію, реалізовують, окрім звичайного входу користувача за логіном і паролем, додатковий захист. У таких системах злочинцям недостатньо для автентифікації заволодіти тільки логіном і паролем користувача.

Для реалізації технологій багатофакторної автентифікації як другий фактор захисту використовують володіння пристроєм, який є зареєстрованим і довіреним у системі, до якої намагаються отримати доступ.

Зазвичай використовують такі фактори автентифікації [3]:

- знання – користувач має ввести певну інформацію до того, як отримають до неї доступ;
- фактор володіння – користувач повинен володіти певною інформацією або приладом перед тим, як отримає доступ;
- фактор локації – перевірка геолокації користувача перед наданням йому доступу;
- фактор властивості – надають доступ за допомогою перевірки факторів, які унікальні для користувача, такі як відбитки пальців, рук, розпізнавання обличчя або голосу;
- фактор поведінки – вимагають від користувача виконати певні дії, наприклад, це система автентифікації за допомогою повторення жестів.

## 2. Формулювання завдання розроблення методу автентифікації

Для забезпечення безпечної авторизації користувачів проблеми несанкціонованого доступу потрібно розглядати з двох сторін: передусім із погляду безпеки інформації, з іншого боку – з погляду зручності для користувачів й операторів систем автентифікації. У системах і на інтернет-порталах, де реалізовують допоміжні засоби забезпечення безпеки користувачів, окрім запиту логіна та пароля під час входу (та першої реєстрації), використовують додавання додаткових факторів автентифікації (складність паролів, підключення авторизованих пристроїв), стійкі алгоритми шифрування та безпечні канали зв'язку.

Будь-який несанкціонований доступ до приватних чи публічних систем, комп'ютерних мереж і ресурсів у мережі інтернет є порушенням прав власників акаунтів і потенційно здатний спричинити значну шкоду не тільки їм, але й операторам систем, в яких зареєстровані ці користувачі, а також організаціям, даними яких можуть заволодіти злочинці. Отримання зловмисником даних для автентифікації – це найпростіший спосіб здобуття контролю над певною системою або заволодіння приватною інформацією. Тому під час розроблення інформаційних систем процесу автентифікації варто приділяти увагу насамперед.

Отже, максимально знизити можливості зловмисника отримати несанкціонований доступ до систем, ресурсів і даних користувачів можна за допомогою розроблення безпечних і впровадження надійних методів автентифікації, що в умовах сьогодення є невід'ємною і однією з найважливіших умов упровадження безпечних інформаційних систем. Такі методи унеможливили б здобуття зловмисниками доступу до ресурсів та надавали б час для проведення дій, спрямованих на нейтралізацію потенційних загроз.

Усі частіше як засіб покращення захисту користувачів та їх ідентифікації використовують саме двофакторну та багатофакторну автентифікації (MFA, TFA) [4]. Суть таких методів полягає у використанні додаткових кроків і засобів для ідентифікації особи, яка намагається отримати доступ до даних за допомогою авторизації, та надання такій особі доступу до ресурсів за умови проходження автентифікації. Двофакторна автентифікація на етапах реєстрації та подальших входів користувача до інформаційних систем або інтернет-ресурсів – це додатковий крок у процесі ідентифікації користувача, додатковий рівень безпеки, який надає можливість відрізнити авторизованого користувача від зловмисника та слугує додатковим шаром безпеки.

Оскільки автентифікацію з використанням статичних ідентифікаторів доступу легко імплементувати, вона є найпоширенішим методом. Але у системах, в яких використовується ідентифікація користувача тільки за паролем, безпека кожного користувача може забезпечуватись на суттєво різних рівнях. Оскільки захист тільки паролем можна зламати звичайним методом перебору, короткі та прості паролі є ненадійними, а користувачі наражаються на більшу небезпеку. Багатосимвольні паролі безпечніші, ніж короткі, тому що їх визначення методом перебору може займати багато часу та не завершитись успіхом. Але існують бібліотеки частовживаних паролів, які складаються з коротких типових паролів. Збільшення довжини пароля підвищує захищеність даних, та водночас призводить до незручностей для користувачів, оскільки довгі паролі важко запам'ятовувати.

Автентифікація користувачів на рівні апаратного забезпечення може бути організована або додатково посилена за допомогою апаратних ключів і приладів, які блокують пристрої та інтерфейси введення – виведення інформації. Апаратні засоби автентифікації – це спеціальні засоби, які використовуються для створення одноразових паролів або виступають ключами доступу.

До технологій, які дають змогу генерувати одноразові паролі, зараховують, наприклад, технології із використанням HMAC алгоритму. Технологія реалізації HMAC алгоритму та роботи з ним полягає в тому, що користувач отримує шестизначний код, який він має використовувати під час входу до системи як другий фактор автентифікації. За алгоритмом, використовуючи поточний час або спеціальний лічильник, перевіряють правильність даних, які надав користувач, за допомогою отримання пароля та обміну спільним ключем між пристроєм і системою.

У системах з двофакторною автентифікацією також використовується RSA SecurID – довірений протокол двофакторної автентифікації. Цей протокол часто застосовують для автентифікації VPN клієнтів, дозволяючи користувачам отримувати доступ до захищених серверів. Кожен фізичний RSA SecurID (рис. 1) прилад має унікальний серійний номер і випадковий 128-бітний секретний ключ, який встановлюється для нього під час виробництва. База даних, в якій містяться всі серійні номери приладів і відповідні їм секретні ключі, зберігається у виробника.


*Рис. 1. Генератор паролів RSA SecureID*

Процесор генератора паролів RSA SecureID кожні 60 секунд отримує поточний час у 64-бітному форматі та 128-бітний шифрувальний запис. За допомогою цих даних і за алгоритмом симетричного шифрування, побудованим, зазвичай, на AES-128 стандарті, генерується велике число, яке хешується для отримання шести- або восьмизначної цифри, яка виводиться користувачеві. Код, який згенерував користувач, надається системі, а далі RSA серверу (рис. 2). Після того,

як користувач ввів свій логін, RSA сервер здійснює пошук у базі даних, для того щоб знайти відповідний йому секретний ключ; після того як ключ знайдено, запускається пошук і перевірка наявності та збігу одноразового ключа в базі за тим самим алгоритмом.

Якщо одноразовий пароль не збігається, то сервер спробує згенерувати пароль, використовуючи інший часовий проміжок. І якщо пароль збігається у допустимому інтервалі, то для підтвердження ідентифікації сервер запитає користувача про надання наступного одноразового пароля. Запит другого пароля реалізовано на випадок, коли зловмисникам вдається підібрати один з ключів.

Програмні токени – це програмні додатки, що виступають ключем для доступу до систем та інтернет-ресурсів. Програмні токени надаються користувачам після авторизації та призначені для електронного підтвердження особистості користувача. Зазвичай токени зберігаються на фізичних пристроях, можуть бути скопійовані або перенесені з одного пристрою на інший.

Широкого застосування програмні токени набули у сучасних мобільних операційних системах, тому що дають змогу швидко та просто, без використання додаткових пристроїв, створити особистий електронний ключ для автентифікації. А у непередбачених ситуаціях використання таких токенів для отримання доступу до даних дає змогу легко згенерувати резервну копію ключа.

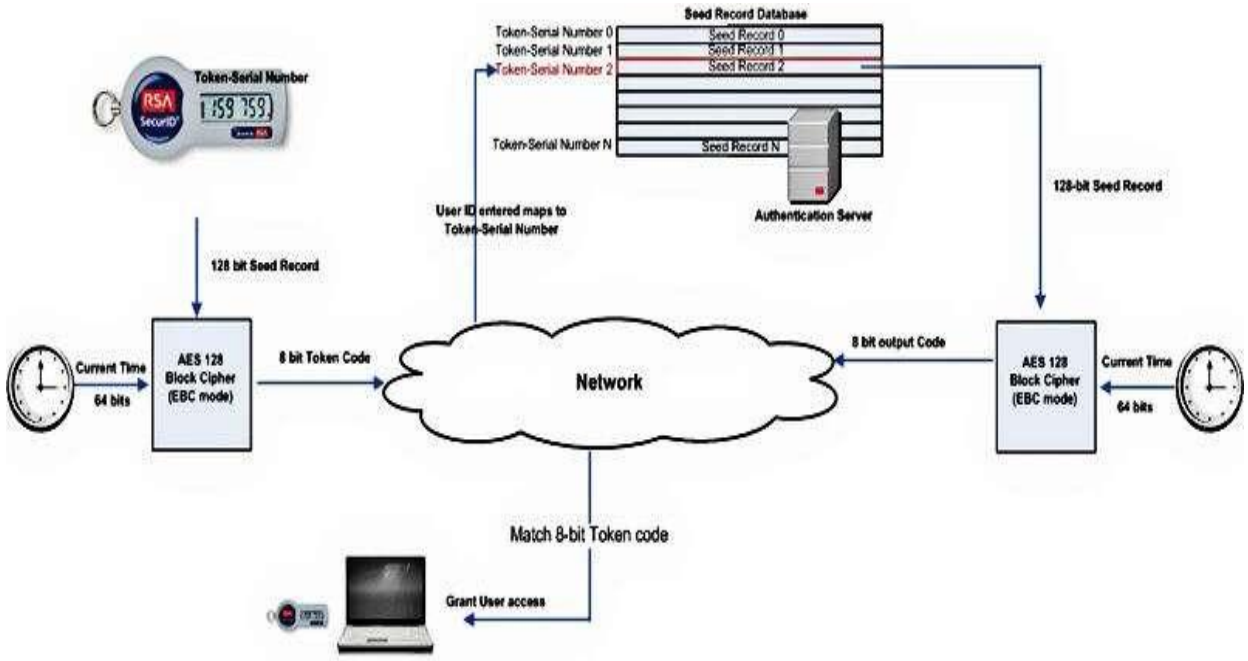


*Рис. 2. Алгоритм роботи RSA Securid*

Завдання розроблення системи автентифікації на основі аналізу акустичних сигналів полягало в побудові надійної системи автентифікації, яка реалізовувала б порівняння звукових доріжок із даними в системі, яка виступає сервером та на основі отриманих даних здійснює автентифікацію залежно від отриманого результату порівняння. Запропонована система розроблена у вигляді системи додатків – сервера автентифікації, який здійснюватиме порівняння аудіотреків та видання секретних ключів додаткам-користувачам системи та мобільному додатку, який зберігає секретний ключ і, на вимогу сервера автентифікації, здійснює запис аудіотреку. Система працює, перевіряючи факт присутності носія ключа щодо термінала системи, до якої відбувається вхід, порівнюючи аудіосигнал із пристрою з аудіосигналом, одержаним терміналом системи. Програмний продукт забезпечує надійну та швидку автентифікацію користувачів.

## 3. Система автентифікації на основі аналізу акустичних сигналів

Для реалізації додатків, розроблених у ході виконання завдання, використано платформу з відкритим кодом NodeJS, зважаючи на її зручність і великий набір інструментів для розроблення користувацьких інтерфейсів. Хоча платформа була розроблена для використання як HTTP вебсерверів, нині її широко використовують у багатьох сферах розроблення програмного забезпечення, адже вона містить набори бібліотек для отримання доступу та роботи з великою кількістю баз даних, а для створення масштабованих серверних застосунків розробникам надається можливість використання різних фреймворків. Також платформа NodeJS надає можливості запуску високопродуктивних мережевих додатків, написаних на мові програмування JavaScript, виконання JavaScript-скриптів на сервері, а їх результат відправляється користувачеві. Платформа доволі зручна за рахунок використання спільної екосистеми для побудови як серверних, так і клієнтських додатків із використанням суміжної бібліотеки засобів розроблення та відлагодження коду.

Сучасні системи, додатки та застосунки в багатьох випадках зобов'язані надавати користувачеві можливості збереження даних і доступу до них у будь-який момент часу та з будь-якої точки планети, незалежно від обставин. Тому процес доступу до даних розробники намагаються робити незалежним від працездатності самих застосунків, а збереження та доступ до даних організовують, використовуючи різноманітні бази даних.

Для розроблення системи автентифікації на основі аналізу акустичних сигналів застосовано систему керування базами даних (СКБД) MongoDB, тому що ця база є документоорієнтованою, надає можливості для розроблення та легкого масштабування застосунків, а також у MongoDB реалізовано зручний інтерфейс та наявна інтеграція з JavaScript.

Кожен запис у MongoDB є структурою даних, яка складається із пар ключ – значення, та являє собою документ [6]. Значеннями полів можуть бути інші документи, масиви та масиви документів.

Для реалізації можливості автентифікації користувачів із використанням аналізу акустичних сигналів потрібно було уможливити передавання акустичного аудіосигналу всередині системи, між її складовими та у взаємодії із зовнішніми пристроями. Для цього вибрано формат WAV [7], який використовується для передавання нестиснутих аудіосигналів. Цей формат – реалізація формату RIFF (рис. 3), який зберігає дані невеликими частинами. Цей формат нативно підтримується для зберігання цифрових аудіоданих. Розроблений компанією Microsoft, завдяки значному поширенню операційної системи Windows цей формат став одним із найчастіше використовуваних аудіоформатів для персональних комп'ютерів. Нині майже неможливо знайти сучасний застосунок або програму, що має змогу відтворювати аудіоформати, та не підтримує WAV формат.

| Offset | Size | Description |
|---|---|---|
| 0x00 | 4 | Chunk ID |
| 0x04 | 4 | Chunk Data Size |
| 0x08 | Chunk Data Bytes | |

*Рис. 3. Формат RIFF*

Використовуючи структуру RIFF, яка розподіляє зміст файла на частини, в результаті аудіофайл становить групу окремих частин, кожна з яких містить свій заголовок (із зазначенням його типу та розміру в байтах) і бітові дані. Водночас певні частини файла можуть поділятись на ще

менші. Методи організації доступу до даних для прискорення їх оброблення дають змогу додаткам не використовувати або не розпізнавати певні частини цілого файла. Одним із недоліків такого підходу з використанням RIFF структури є те, що усі найменші частини повинні вирівнюватись за словами, тобто загальний розмір файла має бути кратний двом байтам. І якщо певна найменша частина даних не має достатнього розміру, доводиться використовувати відступи, які не рахують як розмір частини, в яку складаються найменші поділені частинки, тому застосунки повинні виконувати вирівнювання блока за словами, щоб підрахувати відступи наступної частини даних.

Для зручності роботи користувачів з цією системою та можливості роботи з різних фізичних електронних пристроїв створено вебдодаток, що зберігає приватний ключ користувача. Під час реєстрації у системі користувачеві необхідно за допомогою зчитувача QR кодів отримати секретний пароль, який зберігається у системі та який користувач використовуватиме для автентифікації під час наступного входу. У додатку реалізовано можливість збереження одночасно декількох паролів від декількох різних систем. Також вебдодаток дає змогу здійснити аудіозапис у будь-який момент.

Щоб уможливити тестування та подальшу роботу системи автентифікації на основі акустичних сигналів, було розроблено систему двофакторної автентифікації та Angular-додаток на Nodejs сервері, який надає дані для відображення користувацького інтерфейсу (рис. 4). Необхідність використання саме такої архітектури пов'язана з тим, що додаток містить лише логіку реєстрації користувачів, а перевірка автентифікації реалізована окремою системою, що підключається до додатка та на запит здійснює запис аудіотреку. Як додаток для реєстрації не обов'язково розробляти вебдодаток, HTTP інтерфейс доволі гнучкий і його можна використовувати в користувацьких інтерфейсах різного походження.

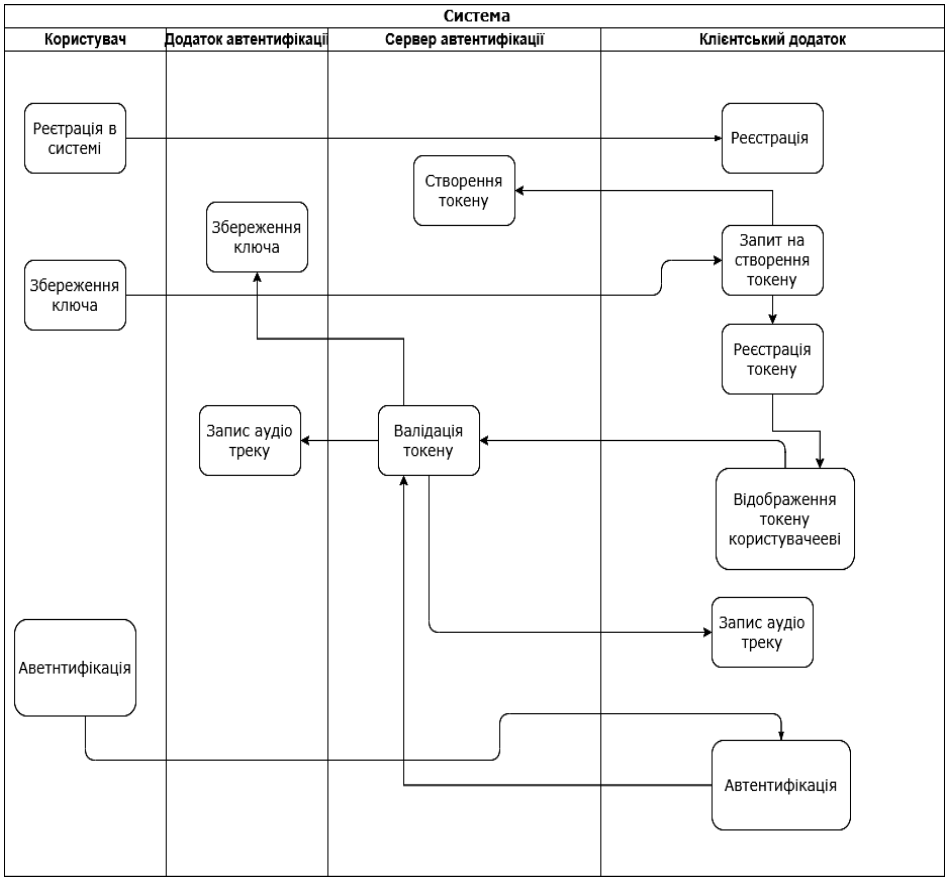


*Рис. 4. Загальна архітектура додатка*

Ключовою складовою загальної розробленої системи є саме сервер автентифікації, який виконує автентифікацію користувачів під час їх входу до системи, зберігає список виданих приватних

ключів, перевіряє права зовнішніх додатків на його використання, здійснює валідацію виданих ключів та за вибраним алгоритмом виконує порівняння аудіотреків, записаних із додатка автентифікації та із системи, до якої здійснюється автентифікація.

Для використання двофакторної автентифікації користувачеві необхідно відкрити в системі меню реєстрації двофакторної автентифікації, на екрані буде відображено секретний пароль у вигляді тексту та додатково у вигляді QR-коду. Для того щоб мати можливість зчитування секретного пароля, користувач повинен надати додатку права на використання вебкамери та мікрофона. Після зчитування секретного пароля за QR-кодом користувач повинен підтвердити отримання персонального ключа, натиснувши кнопку підтвердження на сторінці реєстрації токена. Маючи такий персональний ключ, користувач матиме змогу використовувати його для авторизації у багатьох системах і в онлайн-ресурсах, де реалізована підтримка двофакторної автентифікації.

На прикладі створеної тестової системи процес автентифікації починається одразу ж, коли користувач натисне кнопку входу. Введені ідентифікатор (логін) та пароль користувача надходять до системи, їх значення одразу перевіряється порівнянням із уже збереженими у базі даних. Виявивши збіг, система виконує перевірку того, чи видано користувачеві секретний ключ, і якщо такий ключ було зареєстровано, то система відправляє запит на перевірку цього ключа через вимогу до користувача надати ключ системі. Якщо надано неправильний ключ, система зробить декілька спроб його зчитати, зрештою сповістить користувача про можливу помилку, але вхід до системи залишиться закритим. Якщо неправильно введено ідентифікатор та логін або вперше введено до системи нові дані, робота з системою максимально ідентична до будь-яких інших реалізацій звичайного однофакторного входу до нової системи.

Робота сервера автентифікації полягає у тому, що, одержавши запит на ідентифікацію користувача, він надсилає два зустрічні повідомлення: одне до додатка автентифікації, інше до системи, до якої здійснюється спроба входу. Ці повідомлення є запитами на дозвіл почати запис аудіодоріжки. Тобто до клієнтського інтерфейсу із використанням мережевого сокета надходить запит, який автоматично активує мікрофон девайса чи комп'ютера, на яких використовується система у цей момент, і починає запис треку. Вебінтерфейс відображає статус мікрофона за допомогою індикатора під час його використання.

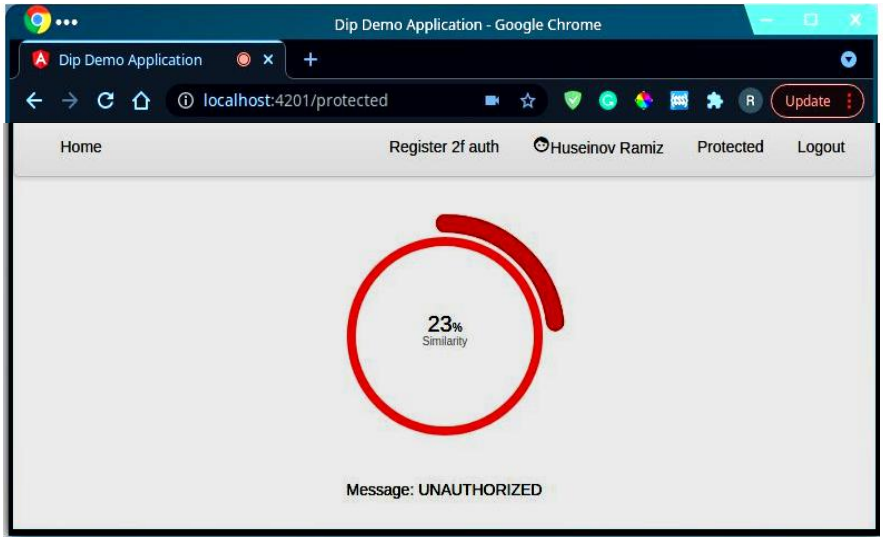


*Рис. 5. Результат невдалої автентифікації*

Після завершення запису отримані аудіотреки у форматі *.wav надсилаються на сервер автентифікації, де їх порівнюють для автентифікації та залежно від результату порівняння назад до системи повертається відповідь із дозволом автентифікації або відмовою. Задля запобігання витоку інформації в базі даних такі семпли не зберігаються.

Якщо логін і пароль користувача пройшли перевірку, але аналіз аудіосигналу не дав відповідної оцінки, користувач не має змоги повною мірою використовувати додаток. На рис. 5 зображено результат виконання саме такого сценарію.

Якщо автентифікація пройшла успішно на обох етапах перевірки, тобто на першому етапі введено логін і пароль існуючі та правильні, а на другому етапі збігаються отримані семпли, користувач отримує повний доступ до системи (рис. 6). Це реалізовано за допомогою спеціального API, доступного тільки для користувачів, які пройшли повний цикл автентифікації.

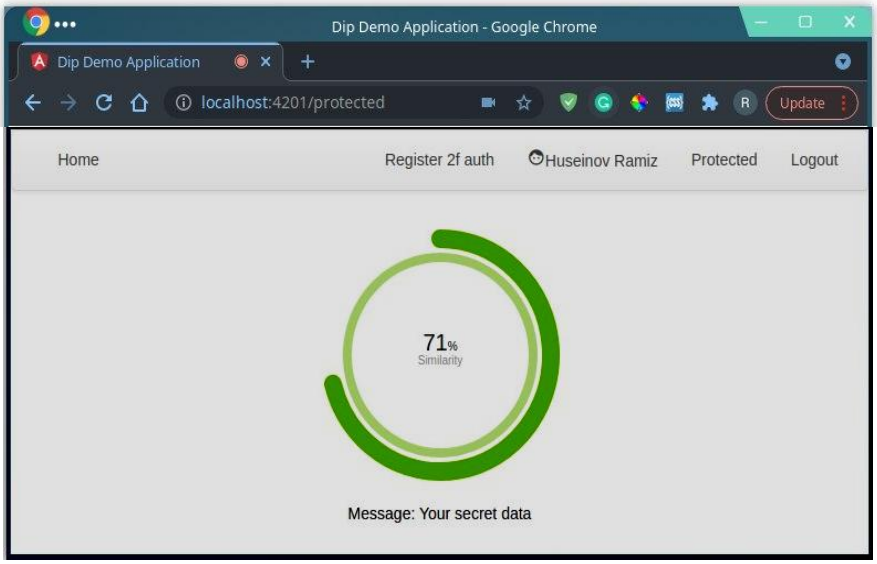


*Рис. 6. Результат успішної автентифікації*

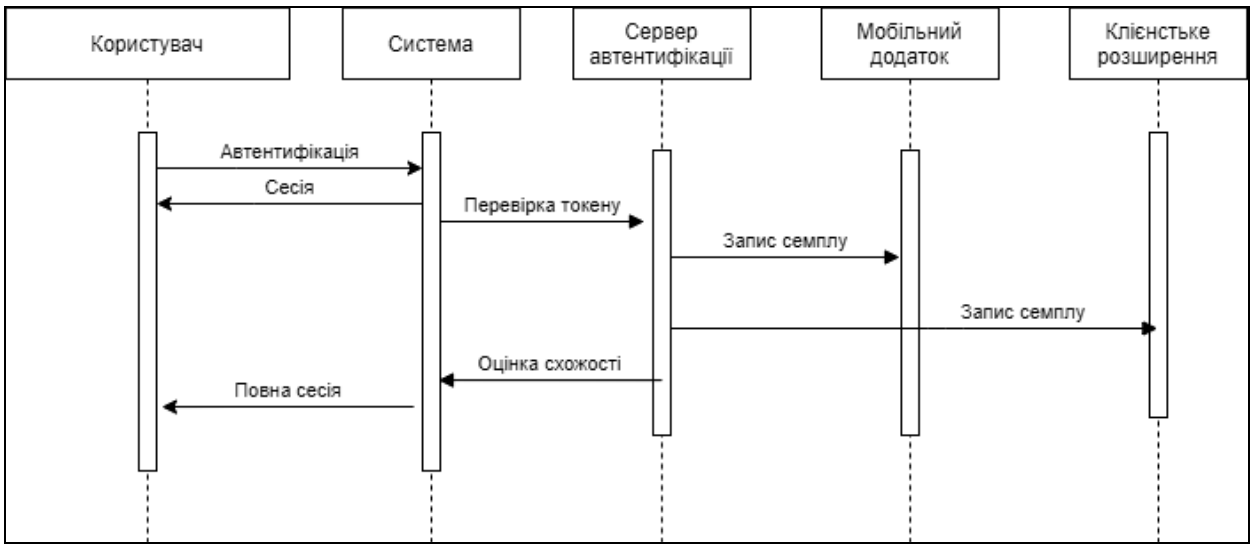


*Рис. 7. Діаграма послідовності розробленої системи*

Алгоритм роботи системи наведено на діаграмі послідовності (рис. 7). На рис. 7 послідовно простежується кожен наступний і всі одночасні кроки всередині систем і між їх складовими компонентами. Коли користувач бажає автентифікуватись у тестовій системі, сама система відслідковує його запит на перевірку наданих ідентифікаційних даних і надсилає запит до сервера автентифікації для того, щоб він ініціював запис аудіотреку. Сервер автентифікації надсилає два запити до відповідних систем: мобільного додатка та клієнтської системи. На мобільний додаток за допомогою вебсокета надходить запит ініціалізації запису сигналу, після запису треку його дані надсилають до відповідних серверів, використовуючи той самий канал вебсокетів. Після того як

сервер автентифікації отримав аудіосемпли, він виконує їх порівняння і видає відповідь, чи можна автентифікувати цього користувача.

**Висновки**

У статті досліджено проблему несанкціонованого доступу до даних користувачів у мережі інтернет, можливості підвищення надійності авторизації користувачів у системах. Запропоновано використання аудіосигналів у системах двофакторної автентифікації та описано розроблену систему двофакторної автентифікації. Запропонована система є другим фактором безпеки під час отримання доступу або входу до інформаційних ресурсів та використовує відповідність аудіотреку, записаного на токені-носії ключа до зафіксованого терміналом, з якого відбувається автентифікація.

Розроблена система надає додатковий фактор автентифікації, щоб унеможливити несанкціонований доступ до додатків. На відміну від аналогічних розробок, наведена у статті система не має потреби зберігати бібліотеку знімків голосів користувачів, оскільки автентифікація відбувається за допомогою порівняння двох аудіосигналів. Користувачеві не потрібно виконувати додаткові дії в додатках та копіювати тимчасовий пароль, тому запропонована система проста та зручна у використанні, як з боку адміністраторів і власників інтернет-ресурсів з можливістю реєстрації та входу, так і для користувачів, які мають бажання та необхідність реєструватись на вебресурсах, у вебдодатках і не хочуть витрачати час і ресурси на запам'ятовування та збереження паролів, але прагнуть до максимальної надійності та збереження власних даних у мережі.

**Список використаних джерел**

*[1] Проникнення інтернету в Україні. Available at: https://inau.ua/sites/default/files/file/1910/dani_ustanovchyh_doslidzhen_iii_kvartal_2019_roku.pdf (Accessed 12 December 2021).*

*[2] Integrity, internal control and security in information systems: Connecting governance and technology ed. Michael Gertz, Erik Guldentops, Leon Strous. ISBN 1-4020-7005.*

*[3] Idrus Syed Zulkarnain S., Cherrier E., Rosenberger C., Schwartzmann J.-J. (2013), A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences, 7 (5), pp. 95–107. ffhal-00912435*

*[4] Ometov, A. & Bezzateev, S. & Mäkitalo, N. & Andreev, S. & Mikkonen, T. & Koucheryavy, Y. (2018), Multi-Factor Authentication: A Survey. Cryptography. 2. 10.3390/cryptography2010001.*

*[5] RSA SecurID® 700 Authenticator. Available at: https://dustinimages.azureedge.net/media/d200001001274246/securid-authenticator-sid700-36-months-10-pack.pdf (Accessed 3 December 2020)*

*[6] MongoDB in Action Second Edition KYLE BANKER PETER BAKKUM SHAUN VERCH DOUGLAS GARRETT TIM HAWKINS ISBN: 9781617291609*

*[7] WAV File Format. Available at: https://docs.fileformat.com/audio/wav/ (Accessed 11 December 2021)*

## AUTHENTICATION SYSTEM BASED ON ACOUSTIC SIGNAL ANALYSIS

**S. Otrokh[1], O. Andriichuk[2], R. Huseinov[1], K. Olienieva[1]**

*[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prosp. Peremohy, Kyiv, 03056, Ukraine*

*[2] Institute for Information Recording of National Academy of Sciences of Ukraine, 2, Shpak Str., Kyiv, 03113, Ukraine.*

The paper has been devoted to the issues of authentication and authorization of users in systems running on the Internet are investigated, the problem of reliability of access and options for improving and enhancing the level of security and preservation of user data are considered. The article offers a solution to the problem of increasing reliability through the developed authentication system using the analysis of audio signals. The urgency of the work is that the problem of protection of user accounts becomes only more important with the spread of Internet technology in the lives of ordinary people.

**Key words:** *authentication; authorization; MFA*.