DOI 10.31891/2307-5732-2024-341-5-16
УДК 004.4

ЯКОВИН СЕРГІЙ
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0002-3335-2892
e-mail: syakovyn@gmail.com
МЕЛЬНИЧУК СТЕПАН
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0002-6973-4235
e-mail: stenni@ukr.net
МАНУЛЯК ІРИНА
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0002-0072-1532
e-mail: manyulyak-iryna@ukr.net
СЛАБІНОГА МАРІАН
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0002-7296-0356
e-mail: mslabinoha@gmail.com

БЕЗПАРОЛЬНА ТА ОДНОФАКТОРНА АВТОРИЗАЦІЯ КОРИСТУВАЧІВ З ОБМЕЖЕНИМИ НАВИЧКАМИ ДЛЯ ОСВІТНІХ ДИСТАНЦІЙНИХ ТЕХНОЛОГІЙ НА ОСНОВІ КОМУНІКАЦІНИХ КАНАЛІВ GSM

Питання обмеження доступу та авторизації користувачів є актуальними практично для будь-яких інформаційних систем. Сучасна ситуація в шкільній освіті породжує низку викликів, пов'язаних із необхідністю залучення до онлайн-навчання учнів початкової школи. Зазначений тип користувачів характеризується низькою самоорганізацією, неуважністю, відсутністю сформованих навичок читання та письма тощо. Впровадження дистанційної освіти в нашій країні активізувалося у зв'язку з війною та карантинними обмеженнями.

Необхідність забезпечення належного рівня надійності зберігання даних, їх цілісності, швидкого доступу, а також реалізації зручних користувальницьких інтерфейсів потребує постійного вдосконалення існуючих та розробки нових організаційно-алгоритмічних рішень апаратно-програмної авторизації в комп'ютерних системах.

Одним із можливих рішень, запропонованих авторами, є використання одноразових паролів з обмеженим терміном дії. Зазначений підхід не новий. Однак практична реалізація алгоритму авторизації, заснованого на багатофакторній авторизації, включає голосового GSM канал для отримання одноразового пароля користувачами згаданого типу. Ключовим аспектом запропонованого підходу є те, що спектр таких голосових повідомлень спотворюється фрагментами випадкових сигналів з контрольованою інформаційною ентропією, що ускладнює їх автоматичне розпізнавання системами перехоплення цифрових паролів.

В ході дослідження розглянуто кілька способів створення та передачі одноразового пароля для авторизації в інформаційній системі. Запропоновано рішення, що ґрунтується на використанні голосового каналу стільникової мережі. Така реалізація вимагає використання додаткового обладнання, зокрема GSM-модему, що підходить для систем, які працюють в межах однієї країни.

Представлено рішення на основі використання GPRS-каналу та відповідних програмних засобів стільникового телефону. Така реалізація вимагає попередньої реєстрації пристрою в інформаційній системі як ініціатора створення одноразового пароля.

Ключові слова: авторизація, безпарольний доступ, голосовий ключ, одноразовий пароль, множинний доступ, алгоритми авторизації.

YAKOVYN SERHIY, MELNYCHUK STEPAN, MANULIAK IRYNA, SLABINOHA MARIAN
Ivano-Frankivsk national technical university of oil and gas

PASSWORDLESS AND ONE-FACTOR AUTHORIZATION OF USERS WITH LIMITED SKILLS FOR EDUCATIONAL DISTANCE TECHNOLOGIES BASED ON GSM COMMUNICATION CHANNELS

Issues of access restriction and user authorization are relevant for almost any information systems. The current situation in school's education produces a row of challenges related to the necessity of involving into online education primary school students. The mentioned type of users is characterized by inattention, low self-organization, the absence of developed reading and writing skills, etc. The implementation of the distant education in our country was intensified due to the war and quarantine restrictions.

The need to ensure the appropriate level of reliability of data storage, their integrity, quick access, as well as the implementation of convenient user interfaces requires constant improvement of existing and development of new organizational and algorithmic solutions for hardware and software authorization in computer systems.

One of the possible solutions proposed by the authors is using one-time passwords with a limited validity period. The mentioned approach is not new. However, the practical implementation of the authorization algorithm, based on multifactor authorization, involves separated voice exchange channels to obtain a one-time password by the end user. The key aspect of the proposed approach is that the spectrum of such voice messages is distorted by fragments of random signals with controlled information entropy, and this makes it difficult for them to be automatically recognized by digital password interception systems.

During research, several methods were considered regarding the creation and transfer of a one-time password to the user for authorization in the information system. A solution based on using the voice channel of a cellular network is presented. Such an implementation requires usage of additional hardware, in particular a GSM modem, which is appropriate for systems operated within the borders of one country.

The solution based on using the GPRS channel and the corresponding software tools of the landline phone is presented. This implementation requires prior registration of the device in the information system as the initiator of creating a one-time password.

Keywords: authorization, voice key, one-time password, passwordless, multiple access, authorization algorithms.

Постановка проблеми

Актуальність проблеми пошуку ефективних рішень для подолання проблем, що виникають при авторизації визначається інтенсивним розвитком систем множинного доступу. Зокрема, у сфері надання освітніх послуг доступні варіанти авторизації є надто складними для деяких користувачів. Тобто постає проблема організації ефективної та максимально простої технології авторизації на основі наявних апаратно-програмних рішень.

Залежно від функціонального призначення, структури, складності інформаційної системи, а також обсягу та важливості даних на практиці використовуються різні алгоритми авторизації користувачів. Однофакторна аутентифікація вважається найпоширенішою, завдяки своїй зручності та простоті. Практична реалізація алгоритмів, в більшості випадків, базується на використанні паролів різної складності та довжини. Пароль має бути секретним і достатньо складним, щоб стороння особа не змогла його вгадати, а спроби дізнатися його іншими способами, особливо підібрати грубою силою, призводять до значних обчислювальних або матеріальних витрат [1, 2].

Однак зазначений вид авторизації не забезпечує достатньої надійності. У такій ситуації для підвищення безпеки інформаційні системи використовують відразу кілька факторів – багатофакторну авторизацію. Такими факторами можуть бути інформація, відома тільки конкретному користувачеві, наприклад, PIN-код, код підтвердження, код відновлення тощо, якась особиста річ (мобільний телефон, спеціальний цифровий пристрій, електронна карта, флешка тощо). Також часто використовуються унікальні властивості користувача, наприклад, спектр голосу, відбитки пальців, зображення сітківки ока тощо [1, 2].

Крім того, популярні алгоритми, засновані на використанні одноразових паролів з обмеженим терміном дії. Найчастіше для отримання одноразових паролів використовуються спеціальні апаратні пристрої (токени), або такий пароль генерується системою і відправляється у вигляді короткого повідомлення кінцевому користувачеві. Однак цей підхід часто вимагає використання окремого безпечного інформаційного каналу.

Також варто зазначити, що вартість і експлуатаційні витрати також є важливими факторами ефективності систем авторизації. Мається на увазі, що багатофакторна автентифікація не завжди себе виправдовує. Це пов’язано з необхідністю використання спеціалізованого обладнання та програмного забезпечення для опрацювання сигналів і даних [3], що призводить до додаткових, часто невиправданих, витрат.

Огляд останніх джерел

Інтенсивний розвиток мережевих сервісів, особливо у сфері освітніх послуг, викликаний війною в нашій країні та введенням карантинних обмежень через COVID-19. Така ситуація призводить до посиленого переходу від локальних до розподілених інформаційних систем у сфері надання освітніх послуг. У такій ситуації захист і управління доступом до персональних даних окремих користувачів або організацій залишається актуальним завданням. Фактично, одна з проблем полягає у тому, що необхідно забезпечити доступ учнів початкової школи до інформаційних освітніх ресурсів. Це призводить до низки психологічних, організаційних і технічних проблем.

Зазначена категорія здобувачів освіти характеризується початковим рівнем читання, письма та вмінням користуватися дистанційними інформаційними системами шкільного спрямування. Важливо відзначити різницю між використанням інформаційних технологій для навчання та розваг. Крім того, здатність до самоорганізації та дисципліни зазначеної категорії учнів потребує додаткового контролю та поведінки з боку батьків. В результаті маємо запит на розробку простих і зручних інтерфейсних рішень для учнів початкових класів [1, 2].

У такій ситуації захист та управління доступом до персональних даних окремих здобувачів освіти (користувачів) є складним завданням. Ефективність вирішення такого завдання практично визначає подальший розвиток і перспективи використання комп’ютерних систем з розподіленими інформаційно-обчислювальними ресурсами в освітній сфері. Практична реалізація технологій авторизації користувачів традиційно базується на використанні типових систем авторизації, забезпечених відповідними апаратно-програмними ресурсами [3, 5].

Таким чином, об’єктом дослідження є процеси формування голосових повідомлень в освітніх інформаційних системах авторизації користувачів.

Предметом дослідження є методи та засоби формування та передачі одноразових паролів у вигляді повідомлень у каналах голосового зв’язку.

Метою роботи є адаптація типових, поширених технологій авторизації для потреб здобувачів освіти, які характеризується початковим рівнем читання, письма та вмінням користуватися дистанційними інформаційними системами шкільного спрямування, зокрема шляхом спотворення спектру голосових повідомлень, що не сприймаються на слух але суттєво ускладнить застосування систем автоматичного перехоплення паролів з аудіоканалу.

Виклад основного матеріалу

Одним із шляхів розширення набору технологій безпарольного доступу на основі однофакторної авторизації є вдосконалення процедури передачі одноразових паролів по голосовому каналу стільникової мережі. Загальна структура комп’ютерної системи авторизації на основі використання аудіоканалу стільникової мережі подана на рисунку 1.

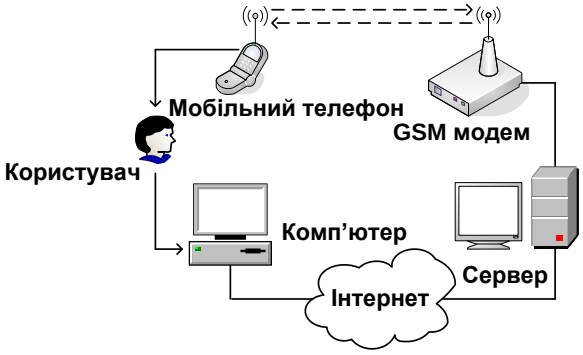

Рис. 1. Схема апаратної структури системи авторизації на основі голосового каналу зв'язку

Як можна побачити, функціонування системи базується на використанні додаткового апаратного забезпечення, а саме GSM модему з активною SIM-картою стільникового зв'язку. Для забезпечення необхідної пропускної здатності системи авторизації необхідно передбачити використання кількох GSM-модемів. Це означає створення пулу доступу GSM-модемів через GSM-шлюз і налаштування переадресації вхідних викликів. Ідея не нова, але запропоноване вдосконалення є простим і зручним рішенням, що дозволить покращити без пекові питання типових рішень. Однак розвиток технологій цифрового опрацювання сигналів привів до появи ефективних систем розпізнавання голосових повідомлень, заснованих на кореляційному, спектральному та інших методах аналізу. В результаті перехоплення голосових повідомлень-паролів в системах з множинним доступом спрощується і його можна автоматизувати.

Для підвищення безпеки зазначеної технології авторизації автори пропонують використовувати спотворення фрагментів голосового повідомлення-пароля випадковими сигналами з контрольованою інформаційною ентропією станів таких сигналів [4].

В ході проведення досліджень розглянуто вплив спотворення фрагмента голосового повідомлення (для набору цифр від 0 до 9), що відповідає голосним звукам української мови. Параметри АЦП, які використовувалися для створення голосових фрагментів, виводили 16 біт, частота дискретизації 11025 Гц. Спектри "а" та "е" для одного диктора, отримані в результаті натурних експериментів подано на рис. 2.

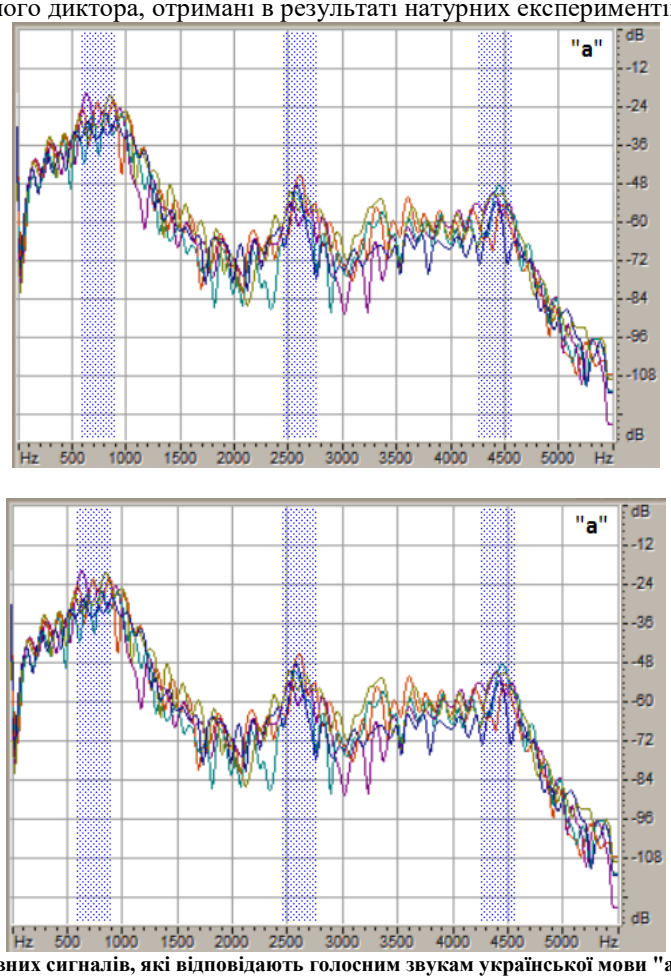

Рис. 2. Спектри мовних сигналів, які відповідають голосним звукам української мови "а" та "е" відповідно

Варто зазначити, що забезпечити стабільну повторюваність часових і амплітудних характеристик голосових повідомлень диктора порівняно складно. Як наслідок, маємо обмеження на частини спектру, придатні для ідентифікації голосних.

Але навіть за таких умов легко виділити відповідні частини спектру для ідентифікації голосних звуків. За результатами експериментальних досліджень, наведених на рис.2, частотні вектори ідентифікації голосних "а" та "е" становлять [750, 2650, 4400] ± 80Гц та [650, 1750, 2500] ± 80Гц.

Фактично, слід мати на увазі, що енергія відповідних ділянок спектру істотно залежить від особливостей вимови диктора. На основі експериментів встановлено, що введення (не змішування) випадкових фрагментів сигналу (до 18 відліків) з контрольованою інформаційною ентропією дозволяє отримати схожі частотні вектори для різних голосних, зберігаючи їх помітними для слухача (користувача, який отримує одноразовий пароль). Спектри спотвореної голосної "а" та неспотвореної голосної "е" одного і того ж диктора подані на рис. 3.

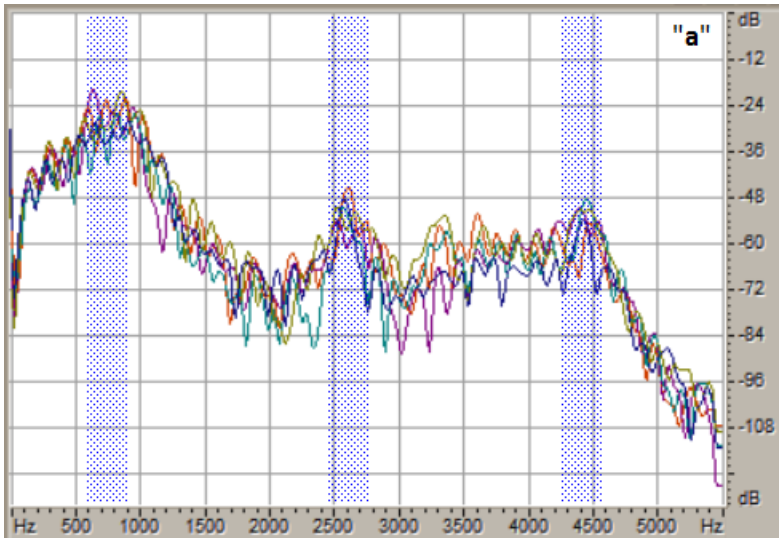

Рис. 3. Спектри мовних сигналів, що відповідають звукам "а" зі спотвореннями і "е" без спотворень

Як можна побачити, отримані спектральні характеристики спотвореної голосної "а" схожі на спектральні характеристики неспотвореної голосної "е". Для порівняння слід подивіться на рис. 2. Таким чином, як наслідок, неможливо однозначно розрізнити аналізовані голосні звуки за спектром. Варто зазначити, що розмір і амплітуда випадкових частин сигналу з контрольованою інформаційною ентропією вибирається випадковим чином із набору попередньо генерованих реалізацій.

У результаті невелике ускладнення алгоритму генерації голосового повідомлення істотно ускладнює автоматичне розпізнавання такого повідомлення-паролю на основі аналізу спектру сигналу. Крім того, в ході авторизації також перевіряється унікальний номер телефону користувача, яки відносно складно підмінити.

Іншим варіантом авторизації може бути безпарольний доступ реалізується за унікальним номером стільникового телефону користувача. Таким чином, суттєво підвищується складність несанкціонованого втручання, оскільки за відсутності SIM-карти абонента заміна номера стільникового телефону можлива лише через доступ до апаратного забезпечення оператора стільникової мережі.

Структура бази даних для користувачів такої системи повинна містити поля для зберігання телефонних номерів абонентів стільникової мережі. Традиційно заповнення номерів телефонів користувачів покладено на операторів системи, які гарантують актуальність користувача. Таким чином, для отримання доступу до інформаційної системи необхідно зареєструвати стільниковий пристрій (наприклад, простий мобільний телефон, що дозволяє голосовий зв'язок), який належить користувачу інформаційної системи.

Частина серверного програмного забезпечення, яке керує модемом GSM, повинна мати доступ до баз даних, у яких зберігаються дані щодо раніше зареєстрованих користувачів. Фактично, в ході сеансу стільникового з’єднання програмне забезпечення перевіряє відповідність номера телефону, наданого модемом GSM, у базі даних. Якщо такий номер виявлено в базі даних, програмне забезпечення генерує одноразовий пароль (голосове повідомлення зі спотвореними фрагментами голосних випадковими сигналами з контрольованою інформаційною ентропією) і відправляє його в звуковому вигляді на GSM-модем. Далі GSM-модем відтворює отримане звукове повідомлення-пароль в поточному сеансі стільникового зв'язку.

Паралельно підсистема авторизації інформаційної системи активує генерований пароль. Однак слід зазначити, що пароль активується лише на обмежений інтервал часу, достатній для його використання, після його закінчення він автоматично знищується системою. Загальна послідовність взаємодії компонентів запропонованої системи авторизації представлена на рисунку 4.

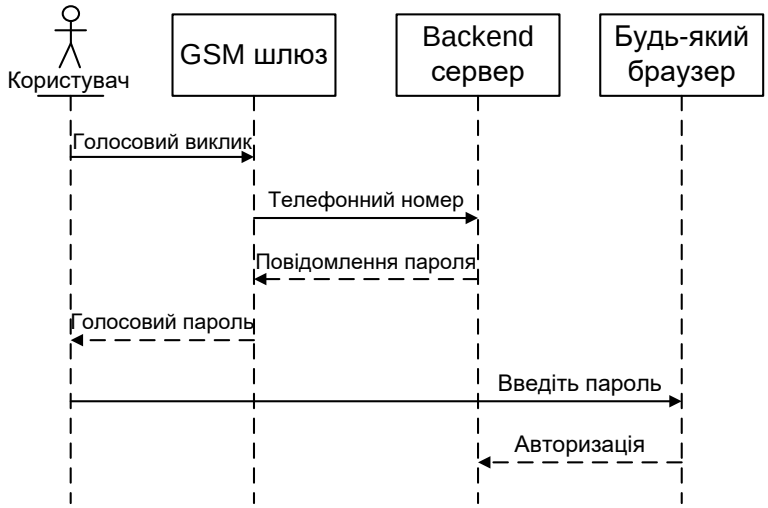

Рис. 4. UML - діаграма послідовності взаємодії компонентів системи авторизації

З огляду на застосування в освітній сфері, зокрема для учнів початкових класів, запропоновані рішення можуть забезпечити достатню ефективність, простоту та зручність використання. Насправді розгортання системи не потребує значних фінансових витрат як від навчального закладу, так і від батьків. Для доступу до освітнього ресурсу чи інформаційної системи не потрібно запам'ятовувати пароль, а обмежений часовий інтервал використання одноразового пароля додатково ускладнює його використання сторонніми особами.

Особливості імплементації технології авторизації на основі безпарольного методу

Іншою важливою проблемою є підготовка та мотивація здобувачів освітніх послуг (учнів початкової школи), які погано знають абетку та цифри, не володіють навичками читання, письма тощо. У такій ситуації доцільно розглянути можливість адаптації технології безпарольного доступу за допомогою мобільних пристроїв батьків.

У цьому випадку варто розглянути авторизацію, що базується на використанні протоколу WebAuthn [5, 6], який підтримується сучасними Internet-браузерами. Нижче подано приклад можливої реалізації коду, яка дозволяє авторизацію користувача, написану на JavaScript.

```
  const publicKeyCredentialCreationOptions = { challenge:
Uint8Array.from(
   randomStringFromServer, c => c.charCodeAt(0)),
rp: {  name: "Duo Security", id: "duosecurity.com",},
user: { id: Uint8Array.from("UZSL85T9AFC",
                            c => c.charCodeAt(0)),
 name: "lee@webauthn.guide", displayName: "Lee",},
pubKeyCredParams: [{alg: -7, type: "public-key"}],
authenticatorSelection:
{  authenticatorAttachment: "cross-platform", },
timeout: 60000, attestation: "direct" };
 const credential = await navigator.credentials.
 create({publicKey:publicKeyCredentialCreationOptions});
```

Як і в попередньому випадку, перш за все, необхідно передбачити первинну реєстрацію мобільного пристрою (як правило, смартфон), яким володіє користувач інформаційної системи. Як можна побачити, спочатку користувач спілкується з бекенд-сервером через мобільний браузер. Після цього користувач реєструється в системі за допомогою типового інтерфейсу користувача: пароля, TOTP-пристрою тощо.

Потім користувачеві потрібно ініціювати створення відкритого та закритого асиметричних ключів (реалізованих через виклики WebAuthn API). Закритий ключ зберігається на мобільному пристрої користувача. Відкритий ключ надсилається на бекенд-сервер, який завершує процедуру реєстрації мобільного пристрою користувача [7, 8].

Варто зазначити, що з цього моменту реєстрація користувача на цьому мобільному пристрої можлива за допомогою пари ключів. Мобільний браузер надсилає ім'я користувача (ім'я учня початкової школи). Внутрішній сервер відповідає довільним текстом і очікує, що браузер підпише його закритим ключем. Після того як браузер надсилає підписаний текст назад, сервер перевіряє підпис за допомогою відкритого ключа. У випадку, якщо підпис дійсний, користувач успішно авторизований у системі.

Для авторизації з іншого пристрою (наприклад, з планшета або ПК) користувач (учень початкової школи) відкриває сайт або захищений ресурс у браузері на цьому пристрої. Використовуючи наданий web-

інтерфейс, користувач запитує авторизацію для входу. Зауважте, що мобільний пристрій має бути попередньо авторизовано у згаданій системі. Діаграма послідовності UML, яка показує авторизацію користувача в інформаційній системі з іншого пристрою (браузера), показана на рис. 5.

Як можна побачити, спочатку користувач відкриває сторінку входу в інформаційну систему на будь-якому пристрої. Потім користувач ініціює авторизацію, яка надсилається до серверної частини. У свою чергу сервер надсилає запит на підтвердження авторизації на раніше зареєстрований мобільний пристрій. Пристрій, на який надсилається запит, визначається іменем користувача.

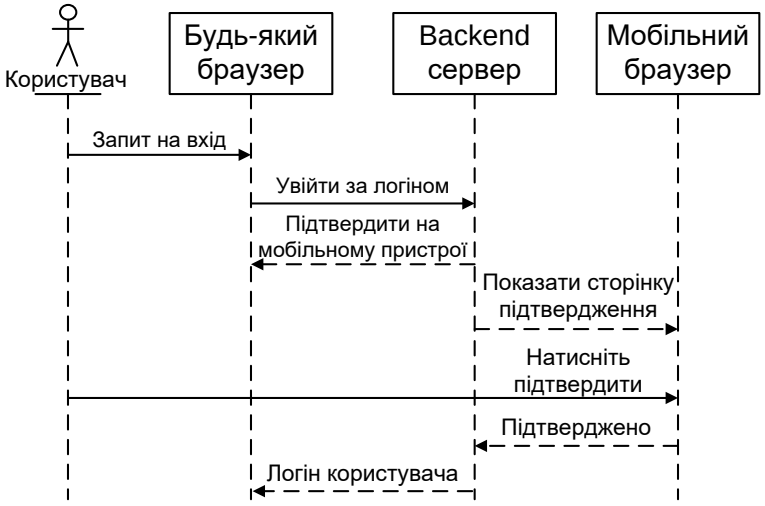

Рис. 5. UML-діаграма послідовності авторизації користувача з будь-якого пристрою за допомогою попередньо зареєстрованого стільникового терміналу з протоколом WebAuthn

Таким чином, використання імені користувача без наявності попередньо зареєстрованого мобільного пристрою унеможливлює авторизацію. Іншими словами, авторизований користувач повинен підтвердити запит на авторизацію в іншому браузері на своєму зареєстрованому мобільному пристрої. Потім, отримавши підтвердження, серверний сервер авторизує вхід з іншого браузера, завершуючи процедуру автентифікації користувача. Також необхідно враховувати ситуацію, коли мобільний пристрій користувача ще не авторизовано, тобто немає каналу зв'язку для підтвердження особи користувача. Діаграма послідовності UML, яка показує взаємодію користувача з інформаційною системою з іншого пристрою за відсутності каналу підтвердження, подано на рис. 6.

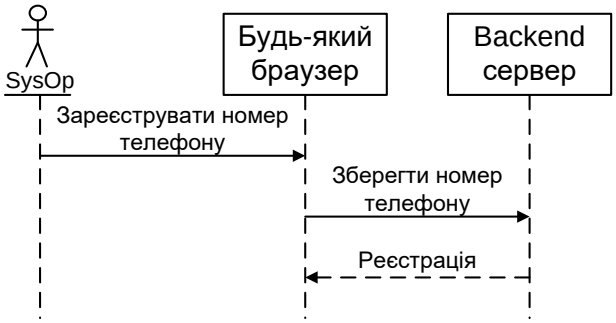

Рис. 6. UML - діаграма послідовності авторизації користувача з будь-якого пристрою, коли попередньо зареєстрований мобільний пристрій за протоколом WebAuthn не знаходиться в мережі

Як можна побачити, на цьому етапі користувач (учень початкової школи) відкриває web-сторінку інформаційної системи на будь-якому пристрої. Використовуючи типовий web-інтерфейс користувача, користувач ініціює запит на авторизацію, який надсилається на внутрішній сервер. У свою чергу внутрішній сервер створює та надсилає відповідь із запитом на авторизацію попередньо зареєстрованого мобільного пристрою. У разі успішної авторизації мобільного пристрою користувача подальша взаємодія між пристроєм користувача та інформаційною системою відбувається так само, як показано на рис. 4.

Однак необхідно відзначити зазначені недоліки авторизації, особливо необхідність окремий мобільний пристрій (пристрій, що належить батькам), підключений до Інтернету. Крім того, цей мобільний пристрій має підтримувати найновіші web-переглядачі, щоб мати можливість використовувати WebAuthn API. Без цього реалізація описаної авторизації без пароля неможлива.

Висновки

Враховуючи рівень інформаційних завдань, запропонована адаптація мережевих сервісів для взаємодії з учнями початкових класів не потребує складних систем контролю доступу. Важливо забезпечити простоту і зручність використання, що опосередковано впливає на інтерфейс взаємодії з користувачами, які не мають належного рівня підготовки.

Використання випадкових сигналів з контрольованою інформаційною ентропією їх станів для спотворення спектра голосових повідомлень (паролів, що передаються по каналу голосового зв'язку) дозволяє розширити функціональність існуючих технологій авторизації без залучення додаткових апаратних рішень. А також ускладнює завдання обробки голосових сигналів для систем автоматичного захоплення паролів.

У результаті отримали подальший розвиток технології та методи авторизації на основі одноразових паролів з обмеженим терміном дії. Описані технології авторизації дозволяють досягти прийнятного рівня зручності та функціональності у використанні освітніх інформаційних систем.

Слід зазначити, що технології ідентифікації за апаратними характеристиками пристроїв зв'язку потребують розширення функціональних можливостей, а також різних каналів обміну даними.

References

1. Christofer Ericson, Two-factor Authentication in Smartphones: Implementations and Attacks. Sweden: Department of Electrical and Information Technology Lund University, 2015. 69 p.

2. Paul A. Grassi, James L. Fenton, Authentication and Lifecycle Management. U.S. National Institute of Standards and Technology, 2017. 78.

3. Galiv V.M. Users authentication methods for access to information web-resources. Proceedings of the II international scientific and practical conference Applied Scientific And Technical Research, Apr. 2018, 23 p.

4. Melnychuk, S., Manuliak, I., Analysis of the passive fragments influence in broadband signals with manipulated information entropy on the data transmission reliability. 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, pp. 567–570.

5. Passwordless protection Reduce your risk exposure with passwordless authentication. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup

6. Brown A. Passwordless Authentication: A Complete Guide. https://www.transmitsecurity.com/blog/passwordless-authentication-guide.

7. IANA: Web authentication (WebAuthn) registries (Aug 2020), https://www.iana.org/assignments/webauthn/webauthn.xhtml.

8. W3C: Web authentication: An API for accessing public key credentials - level 3.W3C first public working draft (Apr 2021). https://www.w3.org/TR/2021/WDwebauthn-3-20210427/.