НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) інформаційних технологій

УДК 004.5:621.397.7

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету (Директор ННІ)	**Завідувач кафедри**
Інформаційних технологій	Комп'ютерних систем, мереж та кібербезпеки
(назва факультету (ННІ))	(назва факультету (ННІ))
_____ / Болбот І.М., д.т.н, проф. /	_____ / Касаткін Д.Ю., д.п.н., доцент /
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2024 р.	«___»_____2024 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему Дослідження ефективності методів проведення автентифікації користувачів в корпоративних інформаційно-телекомунікаційних системах

Спеціальність 123 «Комп'ютерна інженерія»
(код і назва)

Освітня програма Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми

д.п.н., професор	_____	Мамченко С.М.
(науковий ступінь та вчене звання)	(підпис)	(ПІБ)

Керівник магістерської кваліфікаційної роботи

д.т.н., професор	_____	Лахно В.А.
(науковий ступінь та вчене звання)	(підпис)	(ПІБ)

Виконав _____ Герасименко С.О.
(підпис) (ПІБ студента)

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних систем, мереж та кібербезпеки

д.п.н., доцент _____ Касаткін Д.Ю.
(науковий ступінь, вчене звання) (підпис) (ПІБ)
"____" _____ 20____ року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ
Герасименку Сергію Олександровичу
(прізвище, ім'я, по батькові)
Спеціальність 123 «Комп'ютерна інженерія»
(код і назва)
Освітня програма Комп'ютерні системи захисту інформації
(назва)
Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської роботи: Дослідження ефективності методів проведення автентифікації користувачів в корпоративних інформаційно-телекомунікаційних системах

затверджена наказом ректора НУБіП України від "01" листопада 2023 р. № 1999 "С"

Термін подання завершеної роботи на кафедру 27 листопада 2024 р.
(рік, місяць, число)

Вихідні дані до магістерської роботи: Аналіз сучасних методів проведення автентифікації користувачів, середовище розробки для мови програмування Python, біометричний пристрій для сканування відбитків пальців.

Перелік питань, що підлягають дослідженню:
1. Аналіз сучасних методів автентифікації користувачів та їх особливостей
2. Розробка та проектування гібридної системи автентифікації
3. Проведення тестування ефективності розробленої системи

Перелік графічного матеріалу (за потреби) _____

Дата видачі завдання "____" _____ 20____ р.

Керівник магістерської кваліфікаційної роботи _____ Лахно В.А.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Герасименко С.О.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи		Виконано
2	Аналіз предметної області		Виконано
3	Проектування системи		Виконано
4	Реалізація системи		Виконано
5	Тестування розробленої системи		Виконано
6	Оформлення пояснювальної записки		Виконано
7	Оформлення графічного матеріалу		Виконано

Студент _____ / Герасименко С.О. /
підпис ПІБ

Керівник проекту (роботи) _____ / Лахно В.А. /
підпис ПІБ

РЕФЕРАТ

Пояснювальна записка: 75 сторінок, 12 рисунків, 5 таблиць, 15 джерел.

АВТЕНТИФІКАЦІЯ, КОРИСТУВАЧ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВЕРИФІКАЦІЯ, ГІБРИДНА СИСТЕМА, КІБЕРБЕЗПЕКА, ІДЕНТИФІКАЦІЯ, ЗАХИСТ ДАНИХ, БІОМЕТРІЯ.

Об’єкт дослідження – процес автентифікації користувачів у корпоративних інформаційно-телекомунікаційних системах.

Мета роботи – Дослідження ефективності методів проведення автентифікації користувачів в корпоративних інформаційно-телекомунікаційних системах.

Проєкт складається з трьох розділів. Перший розділ присвячено огляду та аналізу сучасних методів автентифікації, які використовуються для захисту інформації. Розглянуто такі методи, як парольна автентифікація, автентифікація на основі токенів, сертифікатів та біометричних даних. Для кожного методу детально описано принципи роботи.

Другий розділ містить порівняльний аналіз ефективності різних методів автентифікації, що базується на критеріях безпеки, зручності використання та вартості впровадження. Також описано ризики, пов’язані з використанням окремих методів, та їхню стійкість до різних типів атак.

Третій розділ присвячено розробці програмного рішення для гібридної автентифікації, яке моделює процес автентифікації користувачів із використанням OTP та біометрії. Здійснено тестування системи, проведено збір і аналіз даних щодо ефективності розробленої системи, зокрема середнього часу перевірки та рівня помилкових спрацювань. Представлено висновки та рекомендації щодо застосування даного підходу в корпоративних мережах для забезпечення підвищеного рівня кібербезпеки.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

OTP (One-Time Password): Одноразовий пароль, який дійсний лише для одного сеансу або транзакції.

ІС (Інформаційна система): Сукупність апаратних та програмних засобів, призначених для обробки, зберігання, передачі і відображення інформації.

TLS (Transport Layer Security): Протокол захисту переданих даних у мережі.

API (Application Programming Interface): Інтерфейс програмування додатків, який дозволяє різним програмам взаємодіяти між собою.

DKIM (DomainKeys Identified Mail): Метод автентифікації електронних листів за допомогою цифрових підписів, що перевіряють походження повідомлення.

SFA (Single-Factor Authentication): Однофакторна автентифікація, яка використовує лише один метод підтвердження, наприклад, пароль.

2FA (Two-Factor Authentication): Двофакторна автентифікація, яка вимагає два методи підтвердження, зазвичай пароль і одноразовий код.

MFA (Multi-Factor Authentication): Багатофакторна автентифікація, яка використовує більше двох методів підтвердження особи.

FAR (False Acceptance Rate): Показник помилкового прийняття, який визначає, як часто система помилково приймає невірну автентифікацію.

FRR (False Rejection Rate): Показник помилкового відхилення, який визначає, як часто система неправильно відхиляє правильну автентифікацію.

JWT (JSON Web Token): Стандарт для створення даних із необробленою аутентифікацією, часто використовується для передачі між веб-серверами.

OAuth: Протокол авторизації, що дозволяє надавати доступ до ресурсів користувача без передачі паролів.

POST: HTTP метод запиту, який використовується для відправлення даних на сервер.

CBA (Certificate-Based Authentication): Автентифікація на основі сертифікатів, яка використовує цифрові сертифікати для підтвердження особи.

IoT (Internet of Things): Інтернет речей, концепція підключення до мережі різних пристроїв, що обмінюються даними.

Вступ

Сучасний світ цифрових технологій, в якому дедалі більше інформації передається, зберігається та обробляється в електронному форматі, ставить перед нами нові виклики щодо забезпечення кібербезпеки. Зростання кількості користувачів онлайн-сервісів, фінансових і корпоративних додатків та інтернет-комунікацій робить критично важливим питання захисту персональних та конфіденційних даних. Однією з ключових складових забезпечення безпеки доступу до таких даних є автентифікація — процес підтвердження особи користувача для надання йому дозволу на доступ до захищених ресурсів або інформації.

Автентифікація є першою лінією оборони в боротьбі з несанкціонованим доступом. Історично, одним із найпоширеніших способів автентифікації було використання паролів, проте цей метод має численні недоліки, такі як схильність до фішингових атак, крадіжки даних та вразливість через слабкі паролі, які користувачі часто використовують повторно. У зв'язку з цим, останніми роками розроблено більш сучасні методи, зокрема багатофакторну та біометричну автентифікацію, які надають вищий рівень безпеки, комбінуючи декілька різних факторів перевірки.

Одним із найбільш ефективних підходів для підвищення рівня безпеки є використання гібридних методів автентифікації, які об'єднують різні способи перевірки особи. Наприклад, поєднання одноразових паролів (OTP) та біометричної автентифікації дозволяє значно підвищити захист, оскільки кожен з методів покриває недоліки іншого. OTP створює унікальний код для кожної сесії, що робить його стійким до підбору чи використання в майбутньому, а біометрична перевірка відбитка пальця забезпечує

автентифікацію на основі фізичних характеристик користувача, які є унікальними та тяжкими для фальсифікації.

У цьому дослідженні проведено аналіз сучасних методів автентифікації, їх ефективності, переваг та недоліків. Особлива увага приділяється порівнянню традиційних та інноваційних методів, а також дослідженню гібридних підходів. Робота також включає практичну частину, в якій реалізовано систему гібридної автентифікації, що використовує комбінацію OTP і біометричного сканування, для забезпечення високого рівня безпеки в корпоративних системах. Моделювання роботи системи дозволило оцінити її стійкість до фішингових атак, ефективність у запобіганні несанкціонованому доступу, а також виявити можливості для покращення користувацького досвіду.

1. Огляд сучасних методів автентифікації

1.1. Загальні поняття автентифікації

Терміни «ідентифікація», «автентифікація» та «авторизація» становлять три основні поняття, що формують основу системи безпеки. Ідентифікація передбачає передачу ІС даних, що визначають ідентичність. Перед автентифікацією заявник зазвичай надає ІС відповідні облікові дані (наприклад, логін або електронну адресу), а система підтверджує ці дані через автентифікацію (наприклад, за допомогою пароля). Автентифікація – це процес підтвердження особи користувача. Для цього застосовуються різні механізми. В системі безпеки автентифікація виконує перевірку наданої користувачем інформації через базу даних. Авторизація – це процес надання користувачу певних прав доступу [1]. Схема доступу до ресурсів зображена на рис. 1.1.

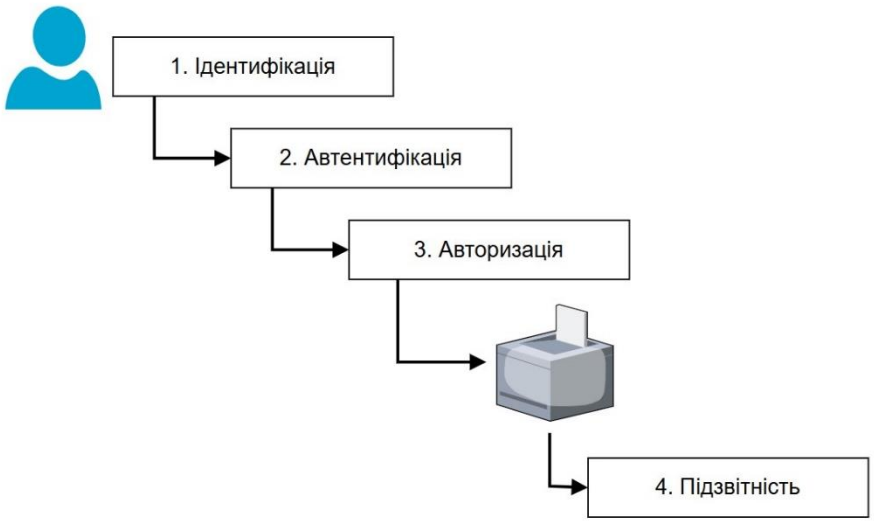

Рис. 1.1 - Схема доступу до ресурсів

Автентифікація є ключовим елементом управління ідентифікацією та доступом (IAM), який визначає, хто має право доступу до даних і які дії з ними

дозволені. Однак її значення розповсюджується й на інші сфери безпеки, зокрема:

- TLS: Більшість великих веб-ресурсів сьогодні використовують безпеку на транспортному рівні (TLS). Система TLS, окрім інших функцій, забезпечує автентифікацію веб-серверів, щоб користувацькі пристрої уникали завантаження фальшивих сайтів.
- API: Сучасні веб-додатки зазвичай працюють через API. Захищені API автентифікують обидві сторони інтеграції, що запобігає атакам на ці API.
- Електронна пошта: Автентифікація електронної пошти здійснюється за допомогою технології ідентифікованої пошти з доменним ключем (DKIM). DKIM перевіряє, що повідомлення надходить із серверів, авторизованих використовувати певний домен (наприклад, @cloudflare.com). Не верифіковані листи, ймовірно, потраплять у спам.

Оскільки комп'ютер не здатний «розпізнати» людину або інший комп'ютер так, як це робить людина, процес автентифікації використовує об’єктивні критерії, які комп'ютер може оцінити. Одним з таких критеріїв є перевірка певної характеристики, відомої лише даному користувачу або пристрою.

Цей вид автентифікації передбачає звірку певної вимірюваної особистої характеристики з відповідним цифровим записом. Характеристики, які перевіряються системою автентифікації, називаються «факторами». Сьогодні активно застосовуються три основні фактори автентифікації [2]:

1. Що відомо людині

Цей фактор базується на знаннях, які має лише користувач. Прикладом є пара «ім'я користувача-пароль». Також до цього належать контрольні запитання та PIN-коди.

2. Що є у людини

Цей фактор підтверджує наявність у користувача фізичного об'єкта, який засвідчує його особу. Як у повсякденному житті ключ дає доступ до квартири, так у цифрових системах перевіряють наявність токена.

Існують два види токенів: програмні та апаратні.

- Програмні токени: Це метод підтвердження володіння пристроєм (наприклад, смартфоном) через код, надісланий на цей пристрій, який потрібно ввести. Код може надсилатися через SMS або згенеровану додатком.
- Апаратні токени: Фізичні пристрої, які підключаються до комп'ютера або смартфона (через Bluetooth, USB тощо). Для доступу користувач підключає токен до пристрою.

Багато експертів вважають апаратні токени надійнішими, оскільки зловмисникам важче заволодіти ними, ніж перехопити програмний код.

3. Ким є людина

Цей фактор використовує унікальні фізичні характеристики користувача. Люди розпізнають один одного за зовнішнім виглядом або голосом; аналогічно, комп'ютери можуть використовувати сканування обличчя, відбиток пальця, сітківку ока, голос тощо.

Додаткові фактори автентифікації

Існують також додаткові фактори, які іноді застосовуються разом із основними трьома. До них належать такі показники, як місцезнаходження (де знаходиться користувач) і час (коли він звертається до системи).

1.2 Класифікація автентифікації

1.2.1 Фактори автентифікації

Автентифікація є основним компонентом забезпечення безпеки, незалежно від того, відбувається вона онлайн чи офлайн. Основна мета цього процесу — захист пристроїв, сервісів чи інформації від несанкціонованого доступу. У процесі автентифікації система перевіряє особу користувача, отримуючи дані, що підтверджують його унікальність. Після цього система порівнює надану інформацію з даними, які зберігаються в її базі. Якщо перевірка проходить успішно, користувач отримує доступ.

– Однофакторна автентифікація (SFA)

Найбільш відомим методом однофакторної автентифікації є використання логіну і пароля. Це простий, але досить ефективний спосіб ідентифікації користувачів, хоча його надійність багато в чому залежить від складності пароля.

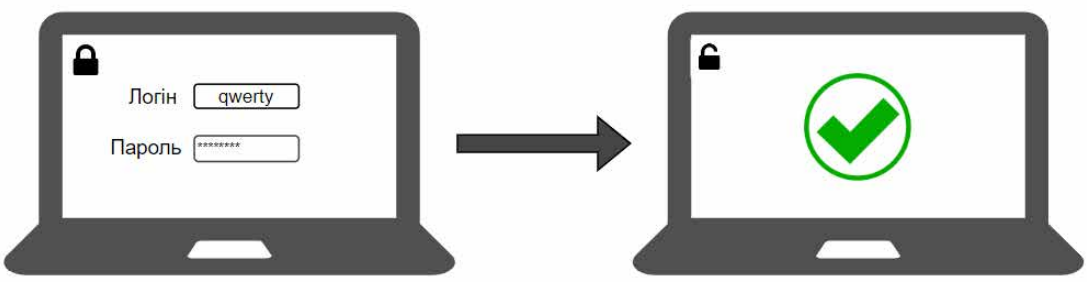

Рис. 1.2 - Однофакторна автентифікація

Переваги SFA

Основна перевага однофакторної автентифікації — її простота та зручність для користувача. Користувачі вводять свій логін і пароль, що зазвичай складається з поєднання букв, цифр і символів. Чим складніший пароль, тим важче зловмиснику його зламати. Такий підхід особливо підходить для незначних

додатків або сервісів, де додаткові рівні безпеки можуть здаватися надмірними.

Недоліки SFA

Значна проблема SFA полягає в її вразливості до компрометації, особливо коли користувачі використовують однакові паролі для кількох облікових записів. Це часто призводить до того, що паролі стають легкою мішенню для зловмисників, які можуть використовувати автоматизовані інструменти для підбору паролів. Окрім того, прості паролі, такі як імена, дати народження, стають легкою мішенню для фішингових атак. Таким чином, без додаткових заходів безпеки SFA є недостатньо ефективним для захисту критичних даних.

– Двофакторна автентифікація (2FA)

Двофакторна автентифікація є поліпшеним варіантом SFA, оскільки вона поєднує два різних фактори перевірки, наприклад, пароль і фізичний об'єкт, який належить користувачу, або біометричну характеристику. 2FA значно підвищує рівень безпеки завдяки комбінації факторів, які належать до трьох основних груп: знання (пароль), володіння (мобільний пристрій або токен) і біометрія (відбиток пальця чи сканування обличчя) [3].

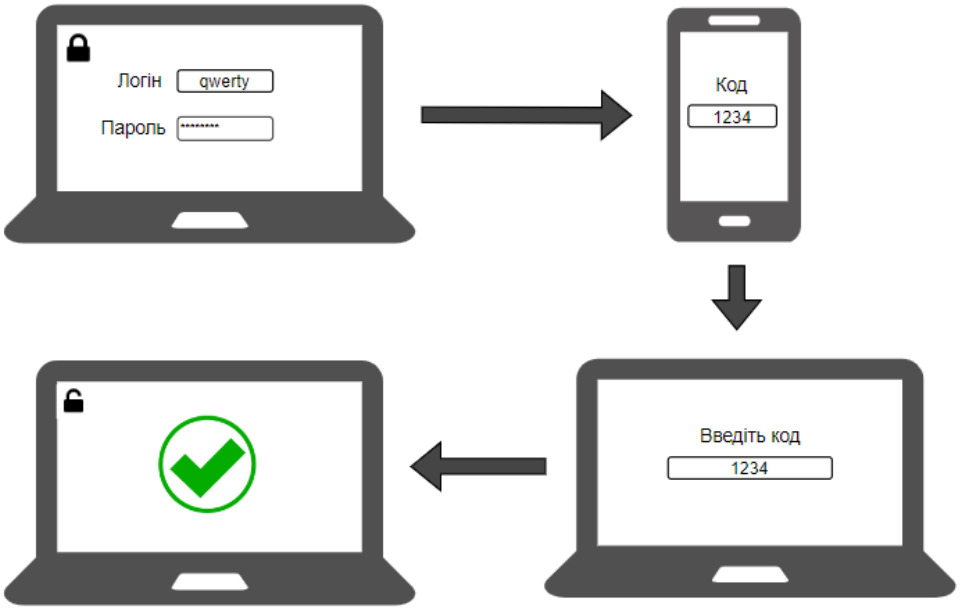

Рис. 1.3 – Двофакторна автентифікація

Переваги 2FA

Головна перевага 2FA — підвищена безпека, оскільки навіть якщо зловмисник отримає пароль, йому потрібен ще один елемент, якого він, ймовірно, не матиме. Доступність мобільних пристроїв, програмних токенів та RFID-карток спрощує процес автентифікації для користувача, дозволяючи зручно підтвердити свою особу. У випадку підозри на можливий несанкціонований доступ 2FA надає додатковий рівень безпеки.

Недоліки 2FA

Недоліком двофакторної автентифікації є її складність у реалізації, особливо для компаній, що потребують додаткового обладнання та підключення пристроїв. Наприклад, якщо у користувача немає доступу до мобільного пристрою чи токена, він може втратити можливість увійти в систему. Крім того, підключення та налаштування пристроїв для 2FA можуть вимагати додаткових зусиль, особливо в умовах обмеженого інтернет-зв'язку або наявності старих пристроїв.

– Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація (MFA) включає два чи більше факторів, що створюють додаткові рівні безпеки. Це особливо важливо у сферах, де високий рівень захисту є критично необхідним, наприклад, у фінансовій сфері або для захисту персональних даних. MFA зазвичай включає унікальні біометричні дані, такі як відбитки пальців чи сканування райдужної оболонки ока, що забезпечує точність і унеможливлює доступ для сторонніх осіб [4].

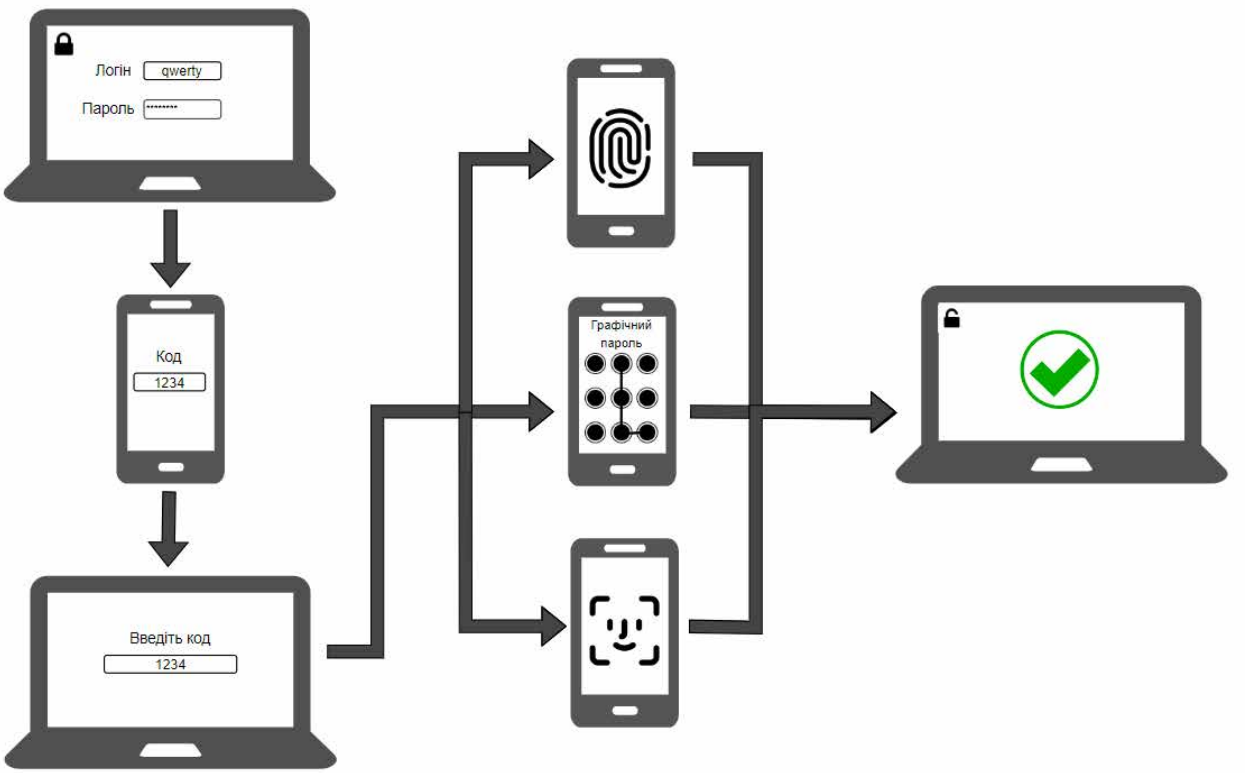

Рис. 1.4 - Багатофакторна автентифікація

Переваги MFA

Поєднання паролів, фізичних токенів та біометричних даних дозволяє досягти високого рівня захисту даних. Наприклад, при доступі до банкомату користувач використовує банківську картку (фактор власності) та PIN-код (фактор знання). Цей підхід дозволяє запобігти несанкціонованому доступу, навіть якщо зловмисник отримає один з факторів [5].

У сучасних додатках MFA зручний для користувачів завдяки інтеграції біометричних сканерів у смартфонах, таких як відбитки пальців або розпізнавання обличчя. Це знижує витрати на встановлення спеціального обладнання, полегшуючи доступ до систем з підвищеною безпекою.

Недоліки MFA

Використання біометрії має свої недоліки, зокрема можливі помилки ідентифікації через невідповідність даних, що були зібрані під час первинної реєстрації. Це може стати проблемою, особливо при використанні дешевих чи неточних пристроїв для зчитування біометричних даних. Помилкові прийняття (FAR) і відхилення (FRR) є поширеними проблемами, які можуть вплинути на точність роботи системи MFA. Наприклад, деякі користувачі можуть мати труднощі з доступом через технічні несправності чи неякісне обладнання.

Використання MFA у сучасних додатках:

1. Онлайн-освіта: У системах масових відкритих онлайн-курсів (MOOC) важливо підтверджувати особу студентів, щоб уникнути шахрайства. MFA може включати кілька рівнів автентифікації для підтвердження особи користувача під час здачі іспитів.
2. Фінансові сервіси: Банківські платформи потребують особливої безпеки під час виконання транзакцій. MFA допомагає уникнути шахрайства завдяки комбінації різних факторів для підтвердження особи під час кожного значного переказу.
3. Медичні системи: Доступ до електронних медичних записів потребує особливого захисту, оскільки ці дані є надзвичайно конфіденційними. MFA може надійно захищати медичну інформацію, використовуючи унікальні біометричні дані для кожного користувача.

Багатофакторна автентифікація значно ускладнює завдання зловмисникам, оскільки їм потрібно зламати декілька різних рівнів захисту, що робить цей метод надійним інструментом для захисту особистих і корпоративних даних.

1.2.2 Методи автентифікації

Відповідно до досліджень Веласкеса І., Каро А. та Родрігеса А. [11], існує близько п'ятнадцяти основних методів автентифікації, які можуть використовуватися як поодинці в однофакторній автентифікації, так і в комбінації для підвищення рівня захисту, як у двофакторній автентифікації (2FA).

Методи цієї групи діляться на три основні категорії відповідно до критеріїв, зазначених у таблиці 1.1:

Критерій	**Технологія**
Володіння	Смарт-карта мобільний телефон пароль токен безпеки
Знання	Когнітивний пароль ПІН-код особисті питання
Характеристики	Відбитки пальців сітківка риси обличчя геометрія рук

Таблиця 1.1 – Основні критерії автентифікації

Аналізуючи наведені методи, можна помітити, що категорія біометричних характеристик є найрізноманітнішою порівняно з іншими групами. Це не дивно, адже біометрія базується на унікальних фізичних

особливостях людини, таких як відбитки пальців чи структура сітківки, що дозволяє створити високоперсоналізований механізм захисту. Проте, біометрична автентифікація часто потребує дорогого обладнання та спеціалізованого програмного забезпечення, що обмежує її використання лише в окремих випадках, таких як урядові чи банківські установи. У загальному підході до багатофакторної автентифікації (MFA) оптимальним вважається використання різних методів із кожної групи критеріїв, поєднуючи їх у надійну систему.

Крім трьох основних груп факторів, в останні роки набуває популярності ще один критерій — місцезнаходження користувача. Враховуючи вашу локацію під час спроби автентифікації надається додатковий рівень захисту. Завдяки таким технологіям, як глобальна система позиціонування (GPS), IP-адреса та ідентифікатори мережевих веж, система може визначати, чи входить користувач з довіреного місця. Наприклад, якщо користувач успішно входить в систему з одного міста, а через кілька хвилин спроба входу відбувається з іншої країни, це може викликати підозру, і система автоматично обмежить доступ або вимагатиме додаткові підтвердження для перевірки особи. Це ефективно захищає від несанкціонованих входів і шахрайства.

Одним із найпоширеніших застосувань багатофакторної автентифікації (MFA) є доступ до конфіденційних даних, де потрібен максимально надійний захист. На рисунку 1.5 представлено сучасні джерела автентифікації, які все частіше використовуються для забезпечення безпеки. MFA стає обов’язковим для багатьох компаній, особливо для банківських платформ, медичних систем, державних установ і великих корпорацій, які оперують особистими даними клієнтів або важливою інформацією.

Цей підхід забезпечує всебічний захист завдяки комбінуванню кількох різних методів, що дозволяє створити не просто бар'єр, а багатошарову систему, здатну зупинити більшість сучасних атак на інформаційні системи.

1.3 Сучасні методи автентифікації користувачів

На сьогодні існує широкий спектр методів автентифікації, які забезпечують безпеку користувачів у цифрових системах. Кожен із них має свої особливості, переваги та недоліки, що робить їх застосування доречним у різних контекстах. Як показано на рисунку, найпопулярнішими методами є ті, які поєднують зручність і високий рівень безпеки. Ці методи включають традиційні підходи, такі як паролі, та сучасніші варіанти, такі як біометричні перевірки та двофакторна автентифікація (2FA) [6].

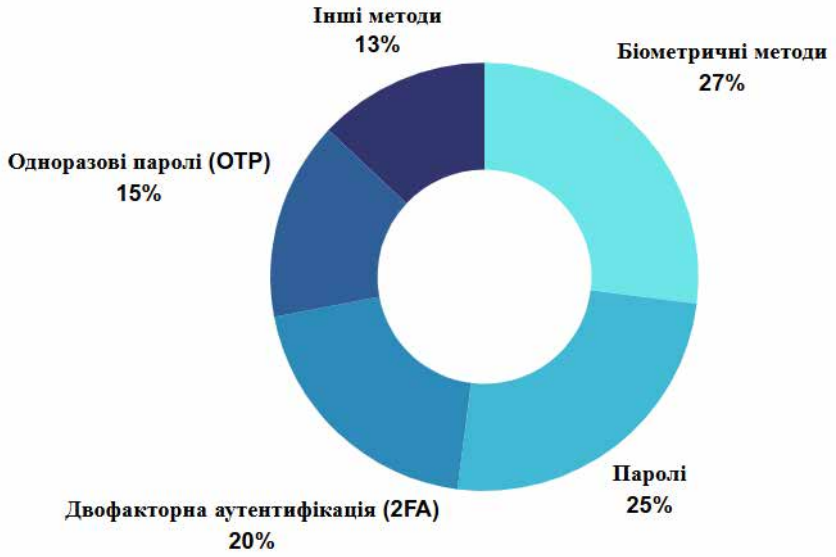

Рис. 1.5 - Найпопулярніші методи автентифікації безпеки

1.3.1 Парольна автентифікація

Парольна автентифікація є одним із найдавніших та найпоширеніших способів ідентифікації користувачів у цифрових системах. Принцип її роботи заснований на введенні користувачем унікального імені та пароля, які

порівнюються з даними, що зберігаються у системній базі. Якщо система знаходить обліковий запис, що відповідає введеним параметрам, користувач отримує доступ до потрібної інформації чи ресурсів. У більшості випадків ім’я користувача представлено адресою електронної пошти, що спрощує запам'ятовування, оскільки це часто є персональною та незмінною інформацією [7].

Переваги та простота реалізації

Парольна автентифікація має низку переваг, серед яких найбільш вагомою є простота реалізації. Для створення базової системи автентифікації достатньо забезпечити інтерфейс для вводу імені користувача та пароля і базу даних для зберігання облікових записів. Це робить метод доступним для широкого кола розробників та дозволяє швидко інтегрувати автентифікацію навіть у найпростіші веб-додатки.

Основні вразливості та виклики безпеки

Попри свою доступність і простоту, парольна автентифікація має низку суттєвих недоліків, пов’язаних з безпекою. Одна з ключових проблем — слабкі паролі, які користувачі часто використовують для різних облікових записів. Дослідження показують, що 65% користувачів схильні використовувати один і той самий пароль або його незначні варіації для кількох сервісів. Це відкриває доступ до численних облікових записів у разі компрометації одного з них. Крім того, значна частина користувачів обирає прості паролі, які легко зламати шляхом перебору, що ще більше посилює проблему.

Заходи для підвищення безпеки парольної автентифікації

Існують кілька перевірених способів покращення безпеки системи, яка базується на паролях:

1. Вимоги до складності паролів: Забезпечення високого рівня складності паролів є основою для надійної автентифікації. Використання довгих, унікальних комбінацій символів (включаючи великі та малі літери, цифри та спеціальні знаки) значно знижує ймовірність зламу.
2. Хешування паролів: Перед зберіганням у базі всі паролі мають бути хешовані за допомогою сучасних криптографічних алгоритмів (наприклад, bcrypt, MD5). Хешування унеможливлює зберігання паролів у відкритому вигляді, і навіть у разі витоку даних паролі будуть недоступні для прямого прочитання. Додаткове використання "сольових" значень до кожного пароля забезпечує ще більший рівень захисту.
3. Двофакторна автентифікація (2FA): Використання другого рівня перевірки автентичності значно підвищує безпеку. Один із поширених підходів — надсилання одноразового коду через SMS, електронну пошту або спеціальний мобільний додаток, такий як Google Authenticator. Це додає фізичний чи фактор знання, який зменшує ймовірність несанкціонованого доступу, навіть якщо пароль було зламано.
4. Моніторинг і блокування: Системи безпеки можуть автоматично блокувати обліковий запис після декількох невдалих спроб входу. Це захищає від атак типу brute-force, де зловмисник намагається відгадати пароль, перебираючи всі можливі комбінації. Додатково можна ввести обмеження на кількість спроб входу за певний проміжок часу або використовувати CAPTCHA для відсіювання автоматичних запитів.

Сфери застосування та обмеження

Метод автентифікації на основі пароля може бути прийнятним для систем, де безпека не є критичною, або у випадках, коли забезпечення простоти входу для користувача є більш пріоритетним. Наприклад, у випадку соціальних

мереж або деяких розважальних сервісів, де компрометація одного облікового запису не несе значної загрози, парольна автентифікація може бути єдиним необхідним рівнем захисту.

Проте для застосунків з високими вимогами до безпеки, таких як банківські чи медичні платформи, парольна автентифікація є недостатньою. У таких випадках варто розглянути додаткові методи, такі як багатофакторна автентифікація, біометричні параметри або системи на основі апаратних токенів, які надають більший рівень захисту. Використання гібридних моделей, що комбінують кілька методів автентифікації, дозволяє створити надійнішу та стійкішу до зламів систему.

Таким чином, парольна автентифікація, хоч і залишається популярною, вимагає підвищення стандартів безпеки у вигляді складних паролів, хешування, додаткових факторів перевірки та моніторингу підозрілої активності. Це дозволяє зберегти зручність користування, одночасно мінімізуючи ризики компрометації системи.

1.3.2 Автентифікація на основі токенів

Токен автентифікації (або auth token) — це згенерований комп'ютером код, який використовується для підтвердження особи користувача. Цей вид токенів надає доступ до вебсайтів, додатків, сервісів та програмних інтерфейсів (API), дозволяючи користувачам отримувати доступ до цих ресурсів без необхідності вводити свої облікові дані щоразу, коли вони відвідують ресурс [8].

Токени автентифікації зазвичай мають захищену, зашифровану структуру та створюються автоматично. Їх можна налаштувати так, щоб вони мали термін дії або могли бути відкликані, що підвищує рівень захисту від

можливих атак, таких як атаки методом підбору паролів або викрадення облікових даних. Можна уявити токени автентифікації як електронні ключі, що зберігають особисту інформацію, створюючи додатковий рівень захисту для доступу до даних або мережі через методи, такі як багатофакторна автентифікація (MFA).

Переваги токенів автентифікації:

1. Масштабованість: Токени автентифікації мають самодостатню структуру, що містить всю необхідну інформацію для ідентифікації. Це дозволяє серверу знижувати навантаження, оскільки йому не потрібно зберігати стан сеансу кожного користувача.
2. Гнучкість: Токени можуть генеруватися з будь-якого пристрою та платформи, що робить їх зручними для інтеграції в різних середовищах.
3. Безпека: Токени забезпечують додатковий рівень безпеки, оскільки можуть бути відкликані або встановлені з терміном дії, що захищає від атак типу brute-force або крадіжки паролів.

Види токенів

Автентифікаційні токени можуть бути як апаратними, так і програмними. Серед них можна виділити:

- JSON Web Tokens (JWT): самопідписані токени, що містять всю необхідну інформацію для ідентифікації.
- Токени оновлення (Refresh tokens): використовуються для подовження часу дії доступу без необхідності повторного входу.
- Федеративні токени: дозволяють доступ до кількох систем, використовуючи один набір облікових даних.
- Токени одноразового пароля (OTP): використовуються для додаткової безпеки через одноразові коди.

- API-токени: забезпечують безпечний доступ до API, дозволяючи уникнути передачі облікових даних.

Як працює автентифікація на основі токенів

Автентифікація на основі токенів складається з чотирьох основних етапів, які забезпечують безпечний і зручний доступ користувача до захищених ресурсів без необхідності повторного введення облікових даних:

1. Первинний запит (Initial Request)
   Спочатку користувач надсилає запит на доступ до захищеного ресурсу, підтверджуючи свою особу за допомогою звичайних облікових даних, таких як ім'я користувача та пароль. На цьому етапі токен ще не видається, і система ідентифікує користувача лише на основі базової інформації для первинної перевірки.
2. Верифікація (Verification)
   Система автентифікації перевіряє правильність наданих облікових даних. Якщо ім'я користувача та пароль відповідають записам у системі, відбувається перевірка прав доступу, які користувач має в межах захищеної системи або ресурсу. Цей етап також може включати додаткові рівні захисту, такі як багатофакторна автентифікація (MFA).
3. Видача токена (Tokens)
   Після успішної верифікації система видає токен користувачу. В залежності від типу токена, цей процес може включати різні підходи:
   - Апаратний токен: Вимагає фізичного надання токена користувачу. Це може бути USB-пристрій, смарт-картка або інший пристрій, який використовується для автентифікації.
   - Програмний токен: Генерується на сервері й передається в фоні, наприклад через API або захищене з'єднання, без необхідності втручання користувача. Програмні токени зберігаються у браузері

користувача або мобільному додатку для подальшого використання.

4. Зберігання та використання токена (Persistency) Токен, який отримав користувач, зберігається в зручному місці — в браузері (наприклад, у cookies або локальному сховищі), мобільному додатку чи навіть на фізичному носії (для апаратних токенів). Цей токен дозволяє користувачу автентифікуватися під час наступних запитів без повторного введення облікових даних. Токени мають певний термін дії, і коли він закінчується, користувачу може знадобитися повторне введення даних або запит на оновлення токена.

Для передачі інформації з метою автентифікаційної можуть використовуватися різні види токенів, наприклад, OAuth або JWT.

JWT-токени мають особливу структуру: вони складаються з заголовка, що вказує тип токена та алгоритм шифрування; корисного навантаження, що містить дані для ідентифікації; і підпису, який підтверджує автентичність інформації в токені.

Переваги автентифікації на основі токенів

Автентифікація з використанням токенів має значні переваги як для розробників, так і для кінцевих користувачів:

- Покращена безпека: Токени мають певний термін дії, що ускладнює несанкціонований доступ. Вони ефективніші за традиційні методи, які не вимагають повторного входу.
- Безстанова масштабованість: Оскільки сервер не зберігає інформацію про сеанси, система стає більш гнучкою до розширення.
- Зменшене навантаження на сервер: Токени зберігаються на стороні клієнта, що зменшує обсяг даних, які потрібно обробляти серверу.

- Крос-платформна сумісність: Токени можна використовувати на різних платформах, що спрощує інтеграцію між сервісами та додатками.
- Полегшена реалізація єдиного входу (SSO): Отримавши токен після автентифікації, користувач може отримувати доступ до інших служб у межах однієї екосистеми без повторного входу.

Типи токенів для автентифікації:

1. JWT (JSON Web Tokens): стандартизований спосіб передачі інформації між сторонами. Завдяки малому розміру, JWT легко передаються як параметри POST, HTTP-заголовки або URL-адреси. JWT складаються з трьох частин: заголовок, корисне навантаження та підпис, що захищає дані від модифікацій.
2. Токени оновлення: застосовуються для подовження часу дії сесії без повторного входу. Вони дозволяють зберігати сесії активними та покращують зручність користування, оскільки не потребують постійної повторної автентифікації.
3. Федеративні токени: надаються ідентифікаційними провайдерами (IdP), дозволяючи користувачам отримати доступ до кількох систем без необхідності окремо входити в кожну з них.
4. OTP-токени (одноразові паролі): одноразові паролі можуть генеруватися через мобільні додатки, наприклад, автентифікатори або за допомогою апаратних токенів.
5. API-токени: унікальні ідентифікатори, які заміняють небезпечну практику передачі облікових даних через HTTP.
6. Апаратні токени (USB-токени): фізичні пристрої, що використовуються для двофакторної або багатофакторної автентифікації. Вони можуть бути контактними або безконтактними, і дозволяють підвищити безпеку для важливих систем або даних.

Чи є автентифікація на основі токенів безпечною?

З розвитком кіберзлочинності необхідність вдосконалення заходів безпеки стає все актуальнішою. Сучасні кібератаки стають дедалі складнішими і спрямовані на отримання доступу до облікових даних користувачів через методи фішингу, атаки методом підбору паролів (brute force), або словникові атаки. Це означає, що покладатися тільки на паролі більше недостатньо для забезпечення безпеки.

Автентифікація на основі токенів, у поєднанні з іншими методами захисту, здатна створити більш надійний бар'єр від зловмисників. Оскільки токени прив'язані до конкретного пристрою, що їх згенерував (наприклад, смартфона або USB-ключа), це суттєво ускладнює спроби отримати несанкціонований доступ до облікових записів, навіть якщо пароль був скомпрометований. Унікальність та одноразовість використання токенів значно підвищують безпеку доступу до ресурсів.

Однак, попри численні переваги, автентифікація на основі токенів не є абсолютно безпечною. Токени, збережені на мобільних пристроях або інших носіях, мають свої вразливості. Наприклад, якщо токен передається у вигляді текстового повідомлення (SMS), він може бути перехоплений у процесі передачі. У разі втрати або крадіжки пристрою зловмисник може отримати доступ до токенів, що на ньому зберігаються.

Для максимальної безпеки варто уникати використання лише одного методу автентифікації. Автентифікація на основі токенів є ефективною, але вона повинна бути частиною більш комплексної стратегії безпеки, яка включає двофакторну або багатофакторну автентифікацію (2FA або MFA). Поєднання токенів з іншими засобами захисту допомагає створити більш надійний рівень безпеки, зменшуючи ризики, пов’язані з викраденням облікових даних або пристроїв.

1.3.3 Автентифікація на основі сертифікатів

У сучасному світі кібербезпеки однією з ключових проблем є захист організаційних мереж від несанкціонованого доступу з боку користувачів та пристроїв, особливо в умовах поширення практики "Bring Your Own Device" (BYOD), коли співробітники використовують свої власні пристрої для роботи. Це може створити потенційні ризики, пов'язані з неправильним налаштуванням пристроїв і доступом до мережі ненадійних або незахищених пристроїв. Одним із ефективних способів вирішення цієї проблеми є використання цифрових сертифікатів для підтвердження особистості користувачів та пристроїв. У цій статті ми детально розглянемо, що таке автентифікація на основі сертифікатів, процес їх життєвого циклу від запиту до видачі сертифіката, а також основні переваги та виклики такого підходу.

Автентифікація на основі сертифікатів (CBA) – це метод перевірки особи користувача або пристрою з використанням криптографічного цифрового сертифіката перед наданням доступу до мережі або ресурсу. Цей підхід відрізняється від традиційних методів, що базуються лише на паролі, оскільки цифровий сертифікат дозволяє підтвердити особистість не лише людей, але й будь-яких кінцевих пристроїв. Серед таких пристроїв можуть бути персональні комп'ютери, сервери, пристрої Інтернету речей (IoT), а також електронні паспорти.

Основна перевага CBA полягає в його високій надійності порівняно зі звичайним методом входу за логіном і паролем. Використання сертифікатів робить процес автентифікації більш захищеним від різного роду шахрайських схем, таких як фішинг. Окрім цього, цифровий сертифікат та закритий ключ зберігаються на пристрої користувача, що дозволяє автоматично входити у різні системи без необхідності кожного разу вводити облікові дані. Це

забезпечує зручність, мінімізуючи необхідність у додаткових діях користувача, оскільки процес перевірки здійснюється автоматично.

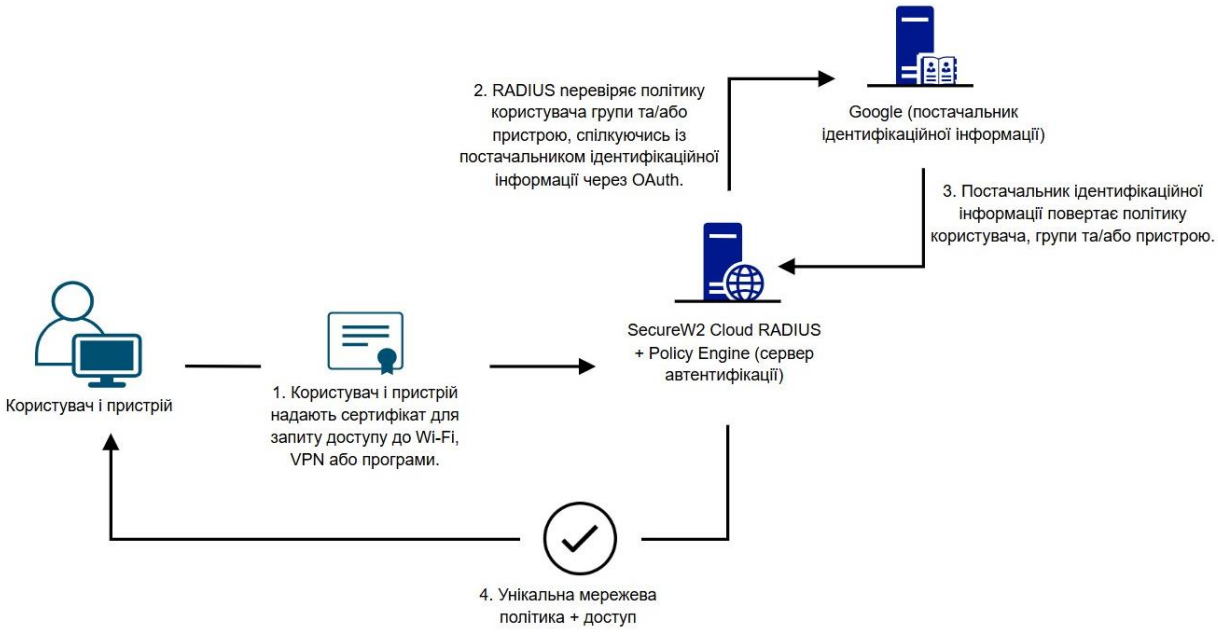

Рис. 1.6 - Автентифікація на основі сертифікатів

Основи криптографії з відкритим та закритим ключем

Цифрові сертифікати базуються на концепції пар ключів. Ключ – це певна інформація, яка використовується для шифрування даних, перетворюючи їх у вигляд, що здається випадковим. Як правило, ключ має вигляд довгого числового значення або рядка символів, що включають літери та цифри. Коли звичайні дані, які називаються "відкритим текстом", шифруються за допомогою алгоритму криптографії з використанням ключа, вони перетворюються у "зашифрований текст". Однак, використовуючи відповідний ключ, можна повернути зашифровану інформацію у вихідний вигляд.

У випадку криптографії з відкритим ключем використовуються дві частини ключа: відкритий та закритий ключ. Відкритий ключ доступний усім і може бути використаний для шифрування даних, але тільки власник закритого ключа може розшифрувати ці дані. Такий тип криптографії також називається

асиметричним, оскільки для обробки даних використовуються різні ключі. Це забезпечує додатковий рівень безпеки, оскільки навіть якщо відкритий ключ стає відомим, зашифровані дані залишаються недоступними без закритого ключа.

Рис. 1.7 – Схема криптографії з відкритим та закритим ключем

Роль цифрових сертифікатів у процесі автентифікації

Цифровий сертифікат служить своєрідним електронним паспортом, який підтверджує зв’язок між особою (або пристроєм) та її відкритим ключем. Сертифікати видаються спеціальними організаціями, які називаються центрами сертифікації (CA, Certificate Authority). Ці центри відповідають за верифікацію особи та створення довірчого зв’язку між користувачем та його відкритим ключем.

Процес автентифікації виглядає наступним чином: пристрій користувача створює запит на автентифікацію, який включає як відкритий, так і закритий ключ. Відкритий ключ стає доступним для всіх і дозволяє іншим системам ідентифікувати користувача шляхом перевірки сертифіката. Центр сертифікації підтверджує достовірність запиту, створюючи цифровий сертифікат, який є підтвердженням того, що даний відкритий ключ належить конкретному користувачу. Під час отримання запиту на автентифікацію інші системи можуть перевірити справжність користувача, зіставивши його цифровий сертифікат із базою даних CA.

Переваги та недоліки автентифікації на основі сертифікатів

Використання сертифікатів забезпечує низку переваг. По-перше, це значно підвищує рівень захисту, оскільки автентифікація не залежить від запам'ятовування паролів, які можуть бути викрадені або забуті. По-друге, СВА підходить для широкого спектру пристроїв, дозволяючи захистити не тільки робочі місця, але й різні IoT-пристрої, сервери та інші кінцеві точки.

Однак є також і певні недоліки. По-перше, процес налаштування та керування сертифікатами може бути складним та потребувати технічної компетенції, особливо якщо йдеться про велику мережу з багатьма користувачами. По-друге, необхідність оновлення сертифікатів через певний період часу потребує додаткових ресурсів на їх обробку та підтримку. І нарешті, якщо пристрій із закритим ключем буде втраченим або викраденим, це може становити загрозу безпеці.

Автентифікація на основі сертифікатів – це надійний метод захисту організаційних мереж, який базується на принципах криптографії з відкритим та закритим ключем. Вона забезпечує високий рівень захисту та сумісна з різними пристроями, надаючи можливість захистити як персональні комп'ютери, так і IoT-пристрої. Використання сертифікатів знижує ризик зловживань, пов'язаних з паролями, і мінімізує можливість несанкціонованого доступу. Незважаючи на деякі технічні труднощі в процесі налаштування та управління, СВА є ефективним рішенням для сучасного кіберпростору, де загрози безпеці зростають щодня.

1.3.4 Біометрична автентифікація

Біометрична автентифікація є сучасним та високотехнологічним способом перевірки особи користувача, що використовує унікальні фізичні або поведінкові характеристики людини для підтвердження її особистості. На відміну від традиційних методів, що базуються на паролях або токенах,

біометрія значно підвищує рівень безпеки, оскільки біометричні дані важко підробити або втратити. Основними прикладами біометричної автентифікації є відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока, а також голосовий ідентифікатор та аналіз геометрії долоні. Кожен метод має свої переваги, обмеження та специфічні умови використання [9].

Типи біометричних методів:

1. Відбитки пальців

   Відбитки пальців є одним із найбільш поширених та довготривало досліджуваних методів біометричної ідентифікації. Кожна людина має унікальний візерунок на пальцях, що формується природним чином під час розвитку. Сканери для зчитування відбитків пальців стали широко використовуваними, особливо у мобільних пристроях, банкоматах та інших системах контролю доступу.

   - Переваги: Легкість використання, швидкість зчитування, висока точність.
   - Недоліки: Можливість пошкодження або спотворення відбитків (наприклад, при фізичних травмах); сприйнятливість до спроб обману за допомогою підробок.
   - Сфери застосування: Мобільні пристрої, банківські системи, системи безпеки на підприємствах.
2. Розпізнавання обличчя

   Розпізнавання обличчя базується на аналізі унікальних рис обличчя, таких як форма очей, відстань між частинами обличчя, контури щелепи тощо. Сучасні технології використовують тривимірні моделі для підвищення точності та зменшення ризику спроб шахрайства, наприклад, за допомогою фотографій.

- Переваги: Зручність використання, відсутність необхідності дотику, швидкість розпізнавання.
- Недоліки: Складність забезпечення конфіденційності, вплив умов освітлення та розташування особи.
- Сфери застосування: Системи контролю доступу, аеропорти, мобільні пристрої, банківські послуги.

3. Сканування райдужної оболонки ока

   Сканування райдужної оболонки є одним з найбільш точних методів біометричної автентифікації. Райдуга ока кожної людини має унікальний малюнок, що залишається незмінним протягом усього життя. Сканери райдужної оболонки використовують спеціальні інфрачервоні датчики для детального аналізу цього візерунка.

   - Переваги: Висока точність, стійкість до зовнішніх змін та підробок.
   - Недоліки: Дорожнеча обладнання, необхідність спеціальних умов для сканування.
   - Сфери застосування: Банки, підприємства з високим рівнем безпеки, аеропорти, мобільні пристрої.

4. Голосовий ідентифікатор

   Голосова автентифікація базується на унікальних характеристиках голосу людини, включаючи висоту, тембр, акценти та інші особливості. Використовується як додатковий рівень захисту в багатофакторній автентифікації.

   - Переваги: Не потребує спеціального обладнання, можливість дистанційного застосування.
   - Недоліки: Чутливість до змін голосу (хвороба, вік), залежність від якості звукового обладнання.

- Сфери застосування: Телефонний банкінг, системи підтримки клієнтів, мобільні додатки з високими вимогами безпеки.

5. Геометрія долоні

   Геометрія долоні аналізує унікальні риси руки, такі як форма та розміри пальців, долоні, суглобів. Цей метод менш поширений, але ефективний у певних середовищах, де важлива висока точність і обмежений доступ.

   - Переваги: Висока стійкість до підробок, легкість у використанні.
   - Недоліки: Обмежена доступність пристроїв, може потребувати фізичного дотику.
   - Сфери застосування: Військові об'єкти, лабораторії, високозахищені приміщення.

Як працює біометрична автентифікація

Процес біометричної автентифікації складається з кількох етапів, що забезпечують високий рівень точності та захисту:

1. Збір біометричних даних
   На першому етапі дані, такі як відбитки пальців чи риси обличчя, зчитуються за допомогою спеціальних пристроїв. Ці дані формуються у цифровий формат, наприклад, за допомогою сенсорів або камер.
2. Обробка та аналіз
   Отримані дані проходять через спеціальні алгоритми, що створюють унікальний шаблон. Цей шаблон є лише цифровим відбитком біометричних даних і не містить інформації, яка б дозволила відтворити оригінальні характеристики людини.
3. Збереження шаблонів
   Шаблони біометричних даних зазвичай зберігаються у зашифрованій формі на серверах або на пристроях користувача. Збереження

відбувається таким чином, щоб шаблон не міг бути використаний для створення зворотного зображення даних.

4. Порівняння шаблонів
   Під час автентифікації отриманий шаблон порівнюється з еталонним, що зберігається у системі. У разі збігу користувач отримує доступ до системи або ресурсу.

Переваги та недоліки біометричної автентифікації

Біометричні методи мають значні переваги перед традиційними методами автентифікації, проте вони також мають деякі недоліки.

Переваги:

- Високий рівень безпеки: біометричні дані важко підробити або втратити.
- Зручність для користувачів: відсутність необхідності запам'ятовувати паролі.
- Покращена швидкість автентифікації: більшість біометричних методів працюють швидко, забезпечуючи миттєвий доступ.

Недоліки:

- Вразливість до фізичних змін: наприклад, травма пальця може ускладнити сканування.
- Вартість обладнання: багато методів потребують спеціальних сенсорів або камер.
- Проблеми з конфіденційністю: збір біометричних даних викликає побоювання щодо збереження та використання особистої інформації.

Чи є біометрична автентифікація безпечною?

Біометрія забезпечує високий рівень захисту, проте абсолютної безпеки немає. Сучасні методи захисту, такі як шифрування, запобігають спробам несанкціонованого доступу до біометричних даних, але існує ризик витоку інформації. Для посилення безпеки біометрія часто поєднується з іншими методами автентифікації, такими як токени або паролі, що дозволяє створити багатофакторну систему захисту, яка значно знижує ризики.

2. Порівняльний аналіз ефективності методів автентифікації

Вибір методу автентифікації залежить не лише від його здатності забезпечувати доступ, але й від потенційних проблем, з якими стикаються користувачі під час його використання. Як показано на рисунку, існує ряд поширених проблем, що впливають на ефективність різних методів автентифікації, включаючи складність запам'ятовування, потребу в додаткових пристроях та питання безпеки. Виявлення цих проблем дозволяє визначити слабкі сторони кожного методу, що особливо важливо для підбору оптимальних рішень у корпоративних середовищах [10].

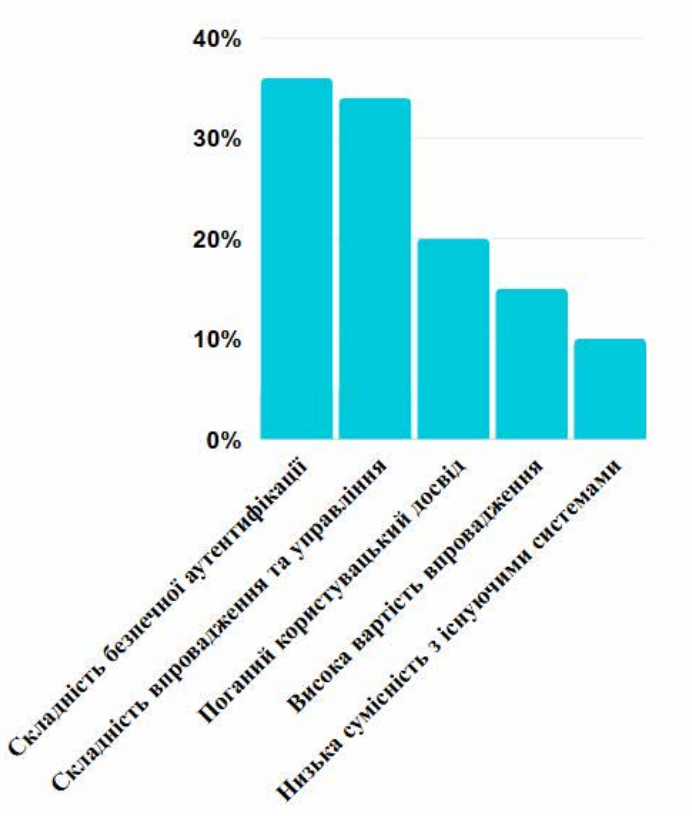

Рис. 2.1 - Основні проблеми під час використання методів автентифікації

2.1 Критерії ефективності методів автентифікації

Оцінка методів автентифікації має базуватись на кількох ключових критеріях, які допомагають визначити, наскільки ефективно та зручно кожен метод виконує свої функції. Різні критерії дозволяють врахувати потреби як користувачів, так і організацій, оптимізуючи вибір автентифікаційної технології залежно від специфічних вимог. Нижче розглянемо основні критерії оцінки методів автентифікації [12].

– Рівень безпеки

Безпека є першочерговим критерієм для автентифікації, оскільки цей процес визначає захист доступу до корпоративних даних і систем. Рівень безпеки автентифікації залежить від здатності методу протистояти різним типам кібератак, таким як атаки методом підбору (brute-force), фішинг, перехоплення облікових даних і атаки на канали зв'язку. Більш безпечні методи автентифікації часто використовують багатофакторну автентифікацію (2FA, MFA), яка поєднує кілька способів підтвердження особи користувача (наприклад, пароль і біометричні дані).

Методи з високим рівнем безпеки можуть включати токени з часовим обмеженням, біометричні дані або сертифікати, які важко підробити чи викрасти. Також важливим є рівень шифрування даних і спосіб їх зберігання: сильне шифрування й захищені канали передачі знижують ймовірність компрометації інформації що використовується для автентифікації.

– Зручність використання для кінцевого користувача

Зручність використання визначає, наскільки легко користувачі можуть застосовувати метод автентифікації у щоденній роботі, не стикаючись із надмірними труднощами. Методи, які вимагають від користувача багаторазових додаткових дій або потребують складного навчання, можуть знижувати ефективність роботи й створювати перешкоди. У цьому контексті

прості методи, як-от парольна автентифікація, є більш зручними для користувача, але вони можуть поступатися в плані безпеки.

Деякі сучасні методи, такі як біометрична автентифікація, мають перевагу через автоматизацію процесу, оскільки користувачам не потрібно запам’ятовувати складні паролі чи постійно вводити облікові дані. Інші ж методи, як от токени або сертифікати, можуть вимагати фізичного носія (смарт-картки, USB-токени), що зручно не для всіх сценаріїв використання. Найбільш зручні методи зазвичай є безперервними, тобто вимагають мінімальних дій з боку користувача під час роботи з ресурсами, які потребують автентифікації.

– Швидкість і продуктивність

Швидкість та продуктивність процесу автентифікації є важливими для забезпечення безперервної роботи користувачів із корпоративними системами. Тривалий процес автентифікації може затримувати доступ до потрібних ресурсів і знижувати ефективність роботи. Продуктивність також залежить від того, наскільки швидко система може обробити запити на автентифікацію у разі підвищеного навантаження (наприклад, при великій кількості одночасних входів у систему).

Методи, які покладаються на складні обчислювальні процеси або потребують взаємодії з зовнішніми сервісами для отримання підтверджень, можуть уповільнювати процес автентифікації. Зокрема, біометричні системи можуть вимагати часу на обробку даних від сенсорів. Проте завдяки сучасним обчислювальним потужностям більшість методів, включно з біометричними та токенами, здатні виконувати автентифікацію майже миттєво.

– Вартість впровадження та підтримки

Вартість є важливим критерієм для організацій, що вибирають метод автентифікації, оскільки він безпосередньо впливає на бюджет компанії.

Вартість автентифікації включає початкові витрати на впровадження (придбання обладнання, програмного забезпечення) та постійні витрати на підтримку (оновлення систем, заміна токенів, навчання співробітників). Деякі методи, як-от парольна автентифікація, є відносно дешевими, тоді як біометричні системи та токени часто вимагають великих інвестицій.

Організації повинні враховувати, що методи з високими початковими витратами можуть зменшувати витрати на підтримку, особливо якщо вони підвищують рівень безпеки і, як наслідок, знижують ризик витоків даних або втрат. Метод автентифікації на основі сертифікатів, наприклад, потребує ретельного налаштування й постійного контролю за оновленням сертифікатів, що може збільшувати витрати на підтримку. Однак він може бути економічно вигідним для великих організацій із численними системами й потребою в високій безпеці.

– Сумісність із різними системами

Сумісність є важливою для інтеграції методу автентифікації у вже існуючу корпоративну інфраструктуру. У разі використання застарілих систем або комплексної IT-інфраструктури, деякі методи можуть вимагати додаткових налаштувань або навіть неможливі до впровадження без значних змін. У цьому контексті найбільш універсальні методи, такі як парольна автентифікація або автентифікація на основі токенів, можуть інтегруватися в більшість систем, оскільки мають стандартні протоколи й підтримуються більшістю сучасних платформ.

Для багатофакторної автентифікації сумісність також означає можливість комбінувати різні методи (наприклад, паролі та одноразові коди). Важливо враховувати, чи підтримують конкретні системи автентифікацію на базі сертифікатів або біометричних даних. Якщо корпоративна інфраструктура є мультихмарною або включає численні хмарні й локальні ресурси, сумісність

стає критичною, і метод автентифікації повинен працювати без проблем у всіх середовищах.

2.2 Порівняльний аналіз традиційних методів автентифікації

У цьому розділі проведено детальний аналіз найбільш поширених традиційних методів автентифікації, що використовуються у корпоративних інформаційно-телекомунікаційних системах. Основними критеріями порівняння є безпека, зручність використання, витрати на впровадження та обслуговування, а також ступінь захищеності від різних видів атак. Дослідження спрямоване на оцінку ефективності та визначення найкращих підходів до автентифікації в різних умовах.

2.2.1 Парольна автентифікація

Парольна автентифікація є найпоширенішим методом, що заснований на факторі знання — користувач вводить унікальний пароль для доступу до системи [13].

Переваги**:**

- Простота використання**:** Паролі є легкими у використанні, не потребують спеціального обладнання, а також швидко засвоюються користувачами.
- Низька вартість впровадження**:** Упровадження та обслуговування паролів є відносно недорогими в порівнянні з іншими методами, що робить їх привабливими для малих та середніх організацій.
- Широке поширення**:** Практично всі системи підтримують парольну автентифікацію, що робить її універсальною і зручною для користувачів.

Недоліки**:**

- Низький рівень безпеки**:** Паролі часто легко зламати, особливо коли користувачі вибирають прості або загальні комбінації. Крім того, відсутність вимоги зміни паролів ускладнює підтримку безпеки на високому рівні.
- Уразливість до атак**:** Паролі піддаються фішинговим атакам, атакам методом грубої сили (brute-force) та словниковим атакам (dictionary attacks).
- Проблеми з керуванням паролями**:** Користувачі часто забувають паролі або використовують однакові паролі для різних облікових записів, що підвищує ризик компрометації.

Приклади використання**:** Парольна автентифікація використовується у більшості систем, від соціальних мереж до корпоративних ресурсів, завдяки простоті інтеграції.

Оцінка**:** В умовах, коли необхідний базовий рівень захисту та немає критичних ризиків, цей метод є прийнятним, але для підвищення безпеки його доцільно поєднувати з додатковими методами, як-от двофакторною автентифікацією.

2.2.2 Автентифікація на основі токенів

Токени представляють собою фізичні чи програмні засоби, що генерують тимчасові коди для підтвердження особи користувача.

Переваги**:**

- Підвищена безпека**:** Одноразові паролі (OTP) та тимчасові коди ускладнюють несанкціонований доступ, навіть якщо пароль користувача компрометовано.

- Захист від повторного використання**:** Тимчасові коди, які генеруються токенами, мають обмежений час життя, що знижує ризик компрометації.
- Універсальність**:** Деякі токени можуть бути інтегровані з мобільними додатками, що полегшує доступ без потреби у додатковому фізичному пристрої.

Недоліки**:**

- Витрати на впровадження**:** Вартість апаратних токенів є значною, що може зробити їх менш привабливими для малих компаній.
- Потреба в управлінні**:** Системи токенів потребують належного управління для заміни втрачених чи зламаних пристроїв, а також для контролю терміну дії токенів.
- Вразливість до фішингу**:** Зловмисники можуть отримати одноразовий пароль через фішингові атаки або техніки соціальної інженерії.

Приклади використання**:** Токени зазвичай застосовуються для доступу до корпоративних мереж або банківських систем, де рівень безпеки є критичним.

Оцінка**:** Токени забезпечують високий рівень безпеки та є ефективними для захисту від компрометації паролів. Рекомендується їх впровадження для організацій із середнім або високим рівнем вимог до безпеки.

2.2.3 Автентифікація на основі сертифікатів

Сертифікати представляють собою криптографічні ключі, які видаються користувачам для доступу до системи.

Переваги**:**

- Високий рівень безпеки**:** Криптографічні сертифікати забезпечують надійний захист і використовуються в середовищах з високими вимогами до безпеки.
- Захист від фальсифікації**:** Сертифікати є значно важчими для компрометації, ніж паролі чи токени, що знижує ризик зламів.
- Автоматизоване управління**:** У випадку інтеграції з інфраструктурою публічних ключів (PKI) сертифікати можуть автоматично перевипускатись, замінюватися та оновлюватися.

Недоліки**:**

- Висока вартість впровадження та обслуговування**:** Створення та управління PKI інфраструктурою потребує значних фінансових ресурсів, що може бути непосильним для малих компаній.
- Складність управління ключами**:** Управління сертифікатами потребує суворого контролю за термінами їх дії, оновленням та зберіганням.
- Залежність від сертифікаційного центру (CA)**:** Компрометація CA призводить до компрометації всіх пов'язаних сертифікатів, що може поставити під загрозу безпеку всієї системи.

Приклади використання**:** Сертифікати широко використовуються в корпоративних мережах, у фінансових установах, а також у великих організаціях для захисту конфіденційної інформації.

Оцінка**:** Автентифікація на основі сертифікатів є ефективним вибором для організацій, де потрібен високий рівень захисту, зокрема в умовах критичних для безпеки середовищ.

2.3 Порівняльний аналіз сучасних методів автентифікації

У зв'язку зі зростанням кількості кібератак і підвищенням вимог до безпеки доступу, традиційні методи автентифікації поступово поступаються місцем сучасним технологіям, які надають додаткові рівні захисту і зручності. До цих методів належать біометричні дані, одноразові паролі та поведінкові характеристики користувачів, що дозволяють ідентифікувати їх на основі унікальних фізіологічних і поведінкових характеристик.

2.3.1 Біометричні методи автентифікації

Біометричні методи автентифікації використовують унікальні фізичні або поведінкові характеристики людини, включаючи відбитки пальців, обличчя, райдужну оболонку ока та голос. Кожен з цих методів має свої специфічні переваги та недоліки за зазначеними критеріями.

– Автентифікація за відбитками пальців

Відбитки пальців — це один із найпоширеніших біометричних методів, який використовує унікальний малюнок ліній на пальцях для ідентифікації особи.

- Безпека: Відбитки пальців забезпечують середній рівень захисту, оскільки цей біометричний метод є поширеним і має потенційну вразливість до підробок, особливо за допомогою латексних відбитків.
- Зручність: Відбитки пальців легко використовувати; достатньо прикласти палець до сканера, що робить метод популярним серед мобільних пристроїв.
- Витрати: Вартість впровадження є відносно невисокою через доступність сканерів відбитків пальців.

- Захищеність від атак: Вразливий до фізичних атак, таких як знімання відбитків зі скляних поверхонь. Сканери можуть бути обмануті підробленими відбитками.

Переваги:

- Легкість використання і швидкість сканування.
- Висока точність для одноособової автентифікації.

Недоліки:

- Можливість підробки або викрадення відбитків.
- Втрата доступу у випадку фізичної травми або пошкодження пальців.

– Автентифікація за обличчям

Цей метод розпізнавання обличчя використовує особливості рис обличчя для автентифікації особи. Сучасні системи можуть розпізнавати особу навіть при зміні кута огляду або освітлення.

- Безпека: Високий рівень безпеки завдяки складним алгоритмам обробки зображень, але у випадку простих сканерів можливі обмани за допомогою фотографій.
- Зручність: Висока, оскільки для доступу достатньо подивитися в камеру.
- Витрати: Вартість системи залежить від рівня технологій. Складніші системи вимагають високоякісних камер і програмного забезпечення.
- Захищеність від атак: Складні системи мають хорошу стійкість до атак за допомогою фото, проте деякі дешевші варіанти можна обманути.

Переваги:

- Зручність і швидкість у використанні.

- Можливість розпізнавання на відстані, що забезпечує безконтактний доступ.

Недоліки:

- Вразливість до обману за допомогою фото у випадку недосконалих систем.
- Зниження точності при поганому освітленні або значних змінах у зовнішності (наприклад, борода).

– Автентифікація за райдужною оболонкою ока

Райдужна оболонка ока є унікальною для кожної людини і не змінюється з часом, що робить її надійним методом біометричної автентифікації.

- Безпека: Високий рівень захищеності завдяки унікальності райдужної оболонки.
- Зручність: Менш зручний метод, оскільки вимагає точного позиціонування очей перед сканером.
- Витрати: Значні, оскільки сканери райдужної оболонки є дорогими та складними в обслуговуванні.
- Захищеність від атак: Практично неможливо підробити через складність структури райдужної оболонки, однак можливі деякі оптичні обмани.

Переваги:

- Висока точність та безпека, практично неможливість підробки.
- Довговічність даних, адже райдужна оболонка не змінюється з часом.

Недоліки:

- Висока вартість обладнання.
- Обмежена зручність, оскільки вимагає точної позиції.

Загальний порівняльний аналіз

Метод	Безпека	Зручність	Витрати	Захищеність від атак
Відбитки пальців	Середній	Висока	Низькі	Вразливий до підробок
Обличчя	Висока	Висока	Середні	Вразливий до атак через фото
Райдужна оболонка ока	Дуже висока	Низька	Високі	Стійкий до більшості атак

Таблиця 2.1 – Порівняльний аналіз біометричних рис для автентифікації

Сучасні методи автентифікації забезпечують різний рівень захисту та мають свої переваги й недоліки. Методи на основі біометрії є особливо привабливими завдяки унікальності характеристик кожної людини, але мають ризики, пов'язані з безпекою та конфіденційністю даних.

Для корпоративних мереж або критично важливих об’єктів рекомендується комбінування методів (MFA) для підвищення рівня безпеки. У разі великої кількості користувачів рекомендуються більш доступні й легкі у використанні методи, такі як розпізнавання обличчя чи відбитки пальців, що забезпечує ефективність і швидкість роботи, але із застосуванням додаткових захистів від потенційних атак.

2.3.2 Автентифікація на основі одноразових паролів (OTP)

Одноразові паролі (OTP) — це унікальні коди, які генеруються для кожного сеансу автентифікації або транзакції. Вони забезпечують високий рівень захисту, оскільки навіть у разі перехоплення такого пароля

зловмисником його неможливо використати повторно. OTP є важливим компонентом двофакторної автентифікації, забезпечуючи додатковий рівень безпеки поряд із основним паролем.

OTP-коди можуть генеруватися через різні методи:

- Алгоритми TOTP (Time-Based One-Time Password) — коди, що діють протягом обмеженого часу (наприклад, 30 секунд).
- HOTP (HMAC-Based One-Time Password) — коди, що генеруються на основі подій, таких як вхід користувача, і залишаються дійсними до використання.
- SMS OTP — код, що надсилається на зареєстрований номер телефону користувача.
- E-mail OTP — код, що надсилається на електронну пошту.

Переваги:

1. Висока безпека: OTP значно підвищує рівень безпеки, оскільки код діє обмежений час або один раз, знижуючи ризик використання скомпрометованих паролів.
2. Зручність у використанні: Коди OTP легко отримати через мобільний додаток, SMS або e-mail, що спрощує процес автентифікації.
3. Захист від фішингових атак: Навіть якщо зловмисник перехопить OTP, він не зможе скористатися ним після закінчення терміну дії.

Недоліки:

1. Вразливість до атак на SMS та e-mail: У випадку SMS OTP існує ризик перехоплення коду через злом SIM-карт або перехоплення повідомлень, що надсилаються на електронну пошту.
2. Залежність від додаткового пристрою: OTP потребує доступу до мобільного пристрою або e-mail. У випадку втрати або пошкодження пристрою користувач не зможе увійти в систему.

3. Витрати на підтримку та впровадження: Використання OTP через SMS або e-mail потребує постійних витрат на обслуговування інфраструктури для надсилання повідомлень.

Порівняння за критеріями

Критерій	**Оцінка**
Безпека	Висока, але залежить від надійності доставки коду (SMS, e-mail можуть бути вразливими).
Зручність використання	Висока для користувачів, особливо з мобільними додатками.
Витрати	Залежить від вибраного методу доставки (SMS дорожчий, додатки дешевші).
Захищеність від атак	Захищеність від фішингових атак, але вразливий до перехоплення SMS або e-mail OTP.

Таблиця 2.2 – Оцінка автентифікації на основі OTP

OTP-коди стали одним із найпопулярніших методів для безпечної автентифікації користувачів, особливо в фінансових установах та інших організаціях, де є підвищений ризик компрометування. Їх перевага в простоті та відносно високому рівні безпеки, особливо при застосуванні в поєднанні з іншими методами автентифікації.

2.3.3 Автентифікація на основі поведінкових біометричних даних

Поведінкова біометрія використовує індивідуальні риси поведінки користувача для ідентифікації, включаючи такі характеристики, як динаміка набору тексту, патерни натискання на екран, ритм ходи, манера використання

миші та інші параметри. Цей метод є більш динамічним, оскільки базується на унікальних поведінкових особливостях, які є важкими для копіювання.

Переваги

1. Непомітність для користувача: Поведінкову біометрію можна збирати у фоновому режимі, що знижує необхідність взаємодії з користувачем.
2. Підвищена безпека: Поведінкові дані важко підробити, оскільки зловмисник навряд чи зможе імітувати унікальні динамічні особливості конкретного користувача.
3. Можливість безперервної автентифікації: Поведінкова біометрія дозволяє здійснювати безперервну автентифікацію користувача протягом всієї сесії.

Недоліки

1. Неоднорідність поведінкових шаблонів: Унікальні поведінкові особливості можуть змінюватися через стрес, втому чи інші зовнішні фактори, що впливає на точність ідентифікації.
2. Необхідність у великих обсягах даних: Для налаштування алгоритмів потрібні великі обсяги даних, зібрані протягом тривалого часу.
3. Витрати на впровадження: Високі витрати на розробку і впровадження систем, що обробляють поведінкові дані, а також на навчання алгоритмів.

Порівняння за критеріями

Критерій	**Оцінка**
Безпека	Висока, оскільки поведінкові патерни важко підробити, але вони можуть варіюватися.

Зручність використання	Дуже висока завдяки фоновому збору даних без додаткових дій з боку користувача.
Витрати	Високі, оскільки потрібні складні алгоритми і велика кількість даних.
Захищеність від атак	Дуже висока стійкість до атак, спрямованих на імітацію поведінки.

Таблиця 2.3 – Оцінка автентифікації на основі поведінкових біометричних даних

Поведінкова біометрія забезпечує високий рівень безпеки і може використовуватися для безперервної автентифікації користувачів у середовищах з висковим ризиком.

2.4 Висновки порівняльного аналізу ефективності методів автентифікації

2.4.1 Порівняння методів за ключовими критеріями

Для ефективного вибору методів автентифікації у корпоративних системах необхідно провести порівняльний аналіз за ключовими критеріями. Нижче представлено таблицю, яка порівнює основні методи автентифікації за такими параметрами: рівень безпеки, зручність використання, витрати на впровадження та обслуговування, а також захищеність від різних видів атак[14].

Метод автентифікації	**Рівень безпеки**	**Зручність використання**	**Витрати на впровадження та обслуговування**	**Захищеність від атак**

Парольна автентифікація	Низький-середній. Вразлива до фішингу, грубої сили, словникових атак.	Висока. Легко впроваджується та використовується, не потребує додаткового обладнання.	Низькі. Вимагає лише налаштування системи для зберігання та перевірки паролів.	Слабка захищеність від фішингу та атак методом перебору.
Автентифікація на основі токенів	Середній-високий. Залежить від типу токенів (апаратні токени безпечніші за програмні).	Середня. Вимагає наявності токена або мобільного додатку, може бути незручним у випадку втрати токена.	Середні. Вартість апаратних токенів вища, програмні токени дешевші, але потребують підтримки додатків.	Середня захищеність. Вразливий до перехоплення токенів та атак "Man-in-the-Middle".
Автентифікація на основі сертифікатів	Високий. Використовує криптографічні методи, що ускладнює підробку та викрадення сертифікатів.	Середня. Потребує налаштування інфраструктури PKI, але забезпечує автоматизовану автентифікацію після	Високі. Необхідність у створенні та управлінні сертифікатами, придбання сертифікаційних центрів.	Висока захищеність. Стійкий до фішингу та атак на паролі, але залежить від безпеки сертифікаційного центру.

		налаштування.		
Біометрична автентифікація	Дуже високий. Використовує унікальні фізичні або поведінкові характеристики, що важко підробити.	Висока. Простота використання без необхідності запам'ятовувати паролі або носити додаткові пристрої.	Високі. Вимагає спеціалізованого обладнання (сканери відбитків пальців, камери для розпізнавання обличчя тощо).	Висока захищеність. Проте вразливий до певних видів атак, таких як підробка біометричних даних, але сучасні технології мінімізують ці ризики.
Одноразові паролі (OTP)	Високий. Коди діють лише один раз або обмежений час, що ускладнює їх повторне використання.	Середня. Потребує додаткових дій для отримання та введення OTP (через SMS, email або додаток).	Середні. Вимагає налаштування систем для генерації та доставки OTP, особливо якщо використовуються SMS або email.	Висока захищеність від фішингу та атак на паролі, але вразливий до перехоплення OTP через небезпечні канали передачі.
Автентифікація на основі	Високий. Використовує унікальні	Дуже висока. Працює в фоновому	Високі. Потребує складних	Дуже висока захищеність. Важко

поведінкових біометричних даних	поведінкові характеристики, такі як швидкість набору тексту, рухи миші тощо.	режимі без необхідності додаткових дій з боку користувача.	алгоритмів та великих обсягів даних для налаштування та обробки.	підробити поведінкові патерни, але може бути вразливий до змін у поведінці користувача.

1. Парольна автентифікація залишається основним методом завдяки своїй простоті та низьким витратам на впровадження. Однак її низький рівень безпеки робить її вразливою до різних типів атак, тому рекомендується використовувати паролі в поєднанні з іншими методами автентифікації, наприклад, двофакторною автентифікацією.
2. Автентифікація на основі токенів забезпечує середній до високого рівень безпеки, особливо якщо використовуються апаратні токени. Цей метод є гнучким і може інтегруватися з різними системами, але вимагає додаткових витрат на обладнання та підтримку.
3. Автентифікація на основі сертифікатів є дуже безпечною завдяки використанню криптографічних ключів, але потребує складної інфраструктури для управління сертифікатами. Цей метод ідеально підходить для великих корпорацій з високими вимогами до безпеки.
4. Біометрична автентифікація пропонує дуже високий рівень безпеки та зручність для користувачів, оскільки не потребує запам'ятовування паролів. Проте високі витрати на обладнання та ризики, пов'язані з конфіденційністю біометричних даних, роблять цей метод менш доступним для деяких організацій.
5. Одноразові паролі (OTP) є ефективним додатковим рівнем захисту, що ускладнює доступ зловмисникам навіть у випадку компрометації пароля. Проте залежність від додаткових пристроїв та потенційна вразливість до

перехоплення OTP через небезпечні канали передачі можуть бути суттєвими недоліками.

6. Автентифікація на основі поведінкових біометричних даних забезпечує дуже високий рівень захисту, оскільки поведінкові патерни важко підробити. Вона також дуже зручна для користувачів, працюючи в фоновому режимі. Однак високі витрати на впровадження та потреба у великій кількості даних для налаштування системи можуть бути бар'єром для її широкого використання.

2.5 Рекомендації для різних корпоративних середовищ

Вибір методів автентифікації має бути адаптований під специфічні потреби та особливості кожного корпоративного середовища. Нижче наведені рекомендації для застосування різних методів автентифікації, які враховують рівень безпеки, зручність, витрати та відповідність вимогам окремих типів корпоративних середовищ [15].

– Малі та середні підприємства

Для малого та середнього бізнесу часто обмежений бюджет на інформаційну безпеку, що впливає на вибір методів автентифікації. Однак навіть невеликі організації потребують надійного захисту, особливо якщо мають справу з конфіденційною інформацією, персональними даними або фінансовими операціями.

- Рекомендований метод: Двофакторна автентифікація (2FA) з використанням одноразових паролів (OTP) або токенів на основі додатків (наприклад, Google Authenticator, Authy).

- Додаткові заходи: Використання сильних паролів та регулярне оновлення паролів; налаштування багатофакторної автентифікації для критично важливих ресурсів.
- Переваги: Невисокі витрати на впровадження, проста інтеграція та помірний рівень захисту.
- Недоліки: Додаткова перевірка OTP може створювати незручності для користувачів.

– Великі підприємства та організації з підвищеними вимогами до безпеки

Великі компанії, особливо ті, що працюють у сфері фінансових послуг, медицини, телекомунікацій чи технологій, мають високі вимоги до безпеки. Для таких організацій критично важливим є захист конфіденційної інформації та зниження ризиків кібератак.

- Рекомендований метод: Багатофакторна автентифікація (MFA) із залученням сертифікатів, апаратних токенів або біометричних даних.
- Додаткові заходи: Розгортання інфраструктури відкритих ключів (PKI) для управління цифровими сертифікатами, запровадження політик обмеженого доступу та регулярний моніторинг дій користувачів.
- Переваги: Максимальний рівень захисту та мінімізація ризиків компрометації облікових записів.
- Недоліки: Високі витрати на впровадження та підтримку, потреба в навчанні користувачів.

– Організації, що працюють віддалено або мають розподілені команди

Організації з віддаленими командами, які працюють на різних пристроях та в різних мережах, мають додаткові вимоги до мобільності та безпеки доступу.

- Рекомендований метод: Автентифікація на основі одноразових паролів (OTP) разом із сертифікатною автентифікацією.

- Додаткові заходи: Використання VPN для захищеного підключення до корпоративних ресурсів, захист пристроїв користувачів антивірусним ПЗ, забезпечення багатофакторної автентифікації.
- Переваги: Оптимальна безпека для віддалених підключень, зниження ризику несанкціонованого доступу.
- Недоліки: Потребує підвищеного контролю за пристроями користувачів та навчання користувачів для належного використання захищених каналів доступу.

– Організації зі швидким обігом персоналу (наприклад, сфера обслуговування)

У таких організаціях персонал часто змінюється, що може створювати ризики несанкціонованого доступу до даних. У цій сфері важливо мати методи автентифікації, які легко оновлювати для нових працівників і блокувати для тих, хто залишає компанію.

- Рекомендований метод: Автентифікація на основі біометричних даних або одноразових паролів.
- Додаткові заходи: Автоматизовані системи для управління обліковими записами, інтеграція з системою управління персоналом для швидкого блокування доступу.
- Переваги: Забезпечення оперативного доступу для нових співробітників та швидке блокування доступу при зміні складу персоналу.
- Недоліки: Системи поведінкової біометрії можуть мати високу вартість для впровадження, а одноразові паролі можуть вимагати додаткових дій з боку користувачів.

– Державні установи та освітні заклади

Державні установи та навчальні заклади мають особливі вимоги щодо захисту конфіденційної інформації (особисті дані, студентські записи, фінансові

документи), але можуть мати обмежений бюджет на впровадження складних систем автентифікації.

- Рекомендований метод: Двофакторна автентифікація на основі паролів та токенів (наприклад мобільні токени).
- Додаткові заходи: Впровадження політик управління доступом, навчання співробітників і студентів безпечному користуванню системами.
- Переваги: Забезпечення достатнього рівня захисту при відносно невисоких витратах на впровадження та підтримку.
- Недоліки: Уразливість до атак, пов’язаних із соціальною інженерією та фішингом, вимагає постійного навчання користувачів.

Наведені рекомендації відображають специфічні потреби кожного типу корпоративного середовища та дозволяють максимально ефективно використовувати наявні ресурси для забезпечення безпеки. Використання оптимальних методів автентифікації в поєднанні з додатковими заходами безпеки сприяє зниженню ризиків несанкціонованого доступу та підвищенню загальної інформаційної безпеки організації.

3. Розробка та моделювання гібридної системи автентифікації

У сучасних умовах захист даних став однією з ключових проблем для корпоративних інформаційно-телекомунікаційних систем. Збільшення кібератак та фішингових кампаній вимагає використання надійних методів автентифікації. Традиційні паролі більше не можуть забезпечити належний рівень безпеки через низку вразливостей: повторне використання паролів, соціальну інженерію, фішингові атаки та нехтування користувачами правилами їх створення. У такому середовищі стає очевидним, що необхідні багаторівневі системи автентифікації.

Біометричні методи (наприклад, розпізнавання обличчя або відбитків пальців) є прогресивним підходом до автентифікації, оскільки використовують унікальні фізіологічні характеристики. Проте біометрія теж має свої обмеження: можливі похибки під час розпізнавання, технічні збої або ризики збереження біометричних даних. Для підвищення надійності безпеки пропонується гібридна система автентифікації, яка комбінує біометрію та двофакторну автентифікацію (2FA). Такий підхід підвищує ефективність автентифікації, адже навіть якщо один з факторів буде скомпрометований, система залишиться захищеною.

3.1 Концепція та архітектура гібридної системи автентифікації

Гібридна система побудована на основі двох основних компонентів:

Генерація та перевірка одноразового пароля (OTP). OTP генерується за допомогою алгоритму TOTP (Time-based One-Time Password), який створює

короткий код, що дійсний протягом визначеного проміжку часу. Це дозволяє знизити ймовірність повторного використання пароля або його перехоплення.

Біометричне сканування відбитка пальця. Система підключена до біометричного датчика ELAN WBF Fingerprint Sensor, що дозволяє ідентифікувати користувача на основі його фізичних характеристик. Завдяки використанню Windows Biometric Framework (WBF) сканування інтегрується з операційною системою, що забезпечує ефективну та безпечну обробку біометричних даних.

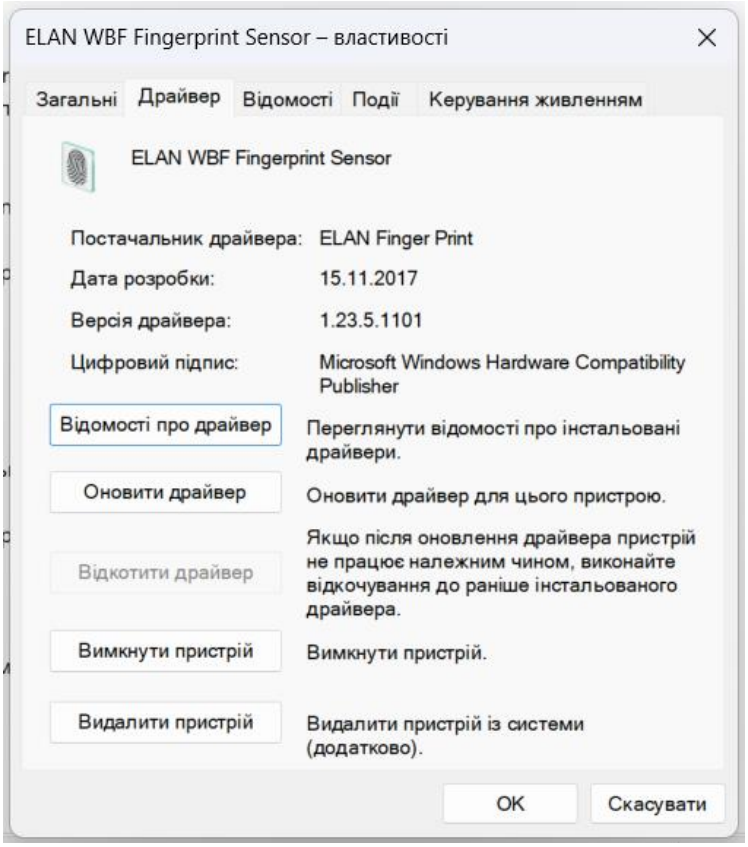

Рис. 3.1 – драйвер ELAN WBF Fingerprint Sensor

Алгоритм гібридної автентифікації включає такі етапи**:**

1. Генерація OTP. Для кожної сесії автентифікації генерується новий код OTP.
2. Перевірка OTP. Користувач вводить отриманий OTP. Якщо код введено правильно, система переходить до наступного етапу.

3. Біометрична автентифікація. Після введення правильного OTP користувач прикладає палець до сканера для підтвердження особи.
4. Логування результатів. Після проходження обох етапів результати автентифікації записуються для подальшого аналізу.

3.2 Опис бібліотек та функцій

Бібліотеки**:**

- Бібліотека pyotp - використовується для створення одноразових паролів на основі алгоритму TOTP (Time-based One-Time Password), що дозволяє генерувати тимчасові паролі з обмеженим терміном дії. Ця бібліотека широко застосовується для двофакторної автентифікації (2FA) завдяки своїй надійності та простоті інтеграції.
- Бібліотека win32com.client - використовується для роботи з Windows Biometric Framework (WBF), який забезпечує інтеграцію біометричних сканерів з операційною системою Windows. Це дозволяє ініціювати та керувати процесом біометричного сканування, а також отримувати результати автентифікації.
- Бібліотека csv - використовується для збереження результатів автентифікації у вигляді таблиці. Це дозволяє створювати звіти про процес автентифікації, аналізувати час та ефективність кожної сесії.

Функціональні елементи системи забезпечують виконання повного циклу гібридної автентифікації:

- generate_otp(secret) – функція генерує OTP на основі секретного ключа, необхідного для автентифікації користувача.

- verify_otp(secret, otp) – функція перевіряє введений користувачем OTP на відповідність згенерованому коду. У випадку невірного коду система припиняє автентифікацію.
- fingerprint_scan() – ініціює біометричне сканування, чекає на прикладення пальця користувачем та зчитує відбиток для перевірки. Повертає результат перевірки та час, витрачений на сканування.
- log_authentication_result(user_id, otp_time, biometric_time, total_time) – функція зберігає результати кожної сесії автентифікації у CSV-файл, що дозволяє проводити подальший аналіз.

  Система зберігає такі параметри для аналізу:

  - Час введення OTP – вимірюється як різниця між часом генерації та введення коду.
  - Час біометричного сканування – враховує затримку сканування, пов'язану з реакцією на введення пальця.
  - Загальний час автентифікації – сумарний час на OTP і біометрію.

- authenticate_user(user_id) – основна функція, яка запускає повний процес автентифікації користувача, включаючи генерацію OTP, його введення, перевірку та біометричне сканування.

3.3 Реалізація гібридної системи: Лістинг

Для ефективного моделювання та тестування системи розроблено програму на Python. Вона дозволяє симулювати процес автентифікації, збирати статистику та аналізувати ефективність запропонованого підходу. Програма реалізує всі ключові елементи: реєстрацію подій, вимірювання часу проходження перевірок та аналіз результатів.

```
import win32com.client
import pyotp
import time
import csv

# Ініціалізація секретного ключа для OTP
user_secret = pyotp.random_base32()

# Функція для генерації OTP
def generate_otp(secret):
    totp = pyotp.TOTP(secret)
    return totp.now()

# Функція для перевірки OTP
def verify_otp(secret, otp):
    totp = pyotp.TOTP(secret)
    return totp.verify(otp, valid_window=1)

# Функція для ініціалізації WBF і перевірки відбитка пальця
def fingerprint_scan():
    try:
        # Ініціалізація WBF
        wbf_manager                                                    =
win32com.client.Dispatch("WBF2Lib.Wbf2BiometricControl")
        wbf_manager.Start()  # Запуск сканера

        # Очікування
        while wbf_manager.IsFingerPresent == 0:
            time.sleep(0.5)

        # Перевірка відбитку
        biometric_success = wbf_manager.CaptureSample()
        scan_time = 2
        wbf_manager.Stop()  # Зупинка сканера
```

```
            return biometric_success == 0, scan_time
        except Exception as e:
            print(f"Помилка під час сканування: {e}")
            return False, 0


# Функція для логування результатів
def log_authentication_result(user_id, otp_time, biometric_time, total_time):
    with open('authentication_log.csv', mode='a', newline='') as file:
            writer = csv.writer(file)
            writer.writerow([user_id,    otp_time,    biometric_time, total_time])


# Основна функція для процесу авторизації
def authenticate_user(user_id):
    print(f"\nПроцес автентифікації для користувача {user_id}")


    # Генерація OTP для кожної спроби
    generated_otp = generate_otp(user_secret)
    print(f"(Для тестування: OTP = {generated_otp})")  # Показ OTP для тестування


    # Час введення OTP
    start_time_otp = time.time()
    otp_input = input("Введіть OTP: ")
    otp_time = time.time() - start_time_otp


    # Перевірка OTP
    otp_success = verify_otp(user_secret, otp_input)
    if not otp_success:
        print("Невірний OTP!")
        log_authentication_result(user_id, otp_time, 0, otp_time)
        return False
```

```
    print("OTP перевірено успішно!")

    # Біометричне сканування
    biometric_success, biometric_time = fingerprint_scan()
    if not biometric_success:
        print("Біометрична перевірка не пройдена!")
        log_authentication_result(user_id, otp_time,
biometric_time, otp_time + biometric_time)
        return False
    print("Біометрична перевірка пройдена успішно!")

    # Успішна автентифікація
    total_time = otp_time + biometric_time
    print("Автентифікація пройдена успішно!")
    log_authentication_result(user_id, otp_time, biometric_time,
total_time)
    return True

# Цикл для виконання автентифікації
user_id = "user_123"
for _ in range(10):
    authenticate_user(user_id)
```

3.4 Моделювання та аналіз ефективності системи

Нижче на рисунках 3.2-3.4 наведено приклад моделювання гібридної системи:

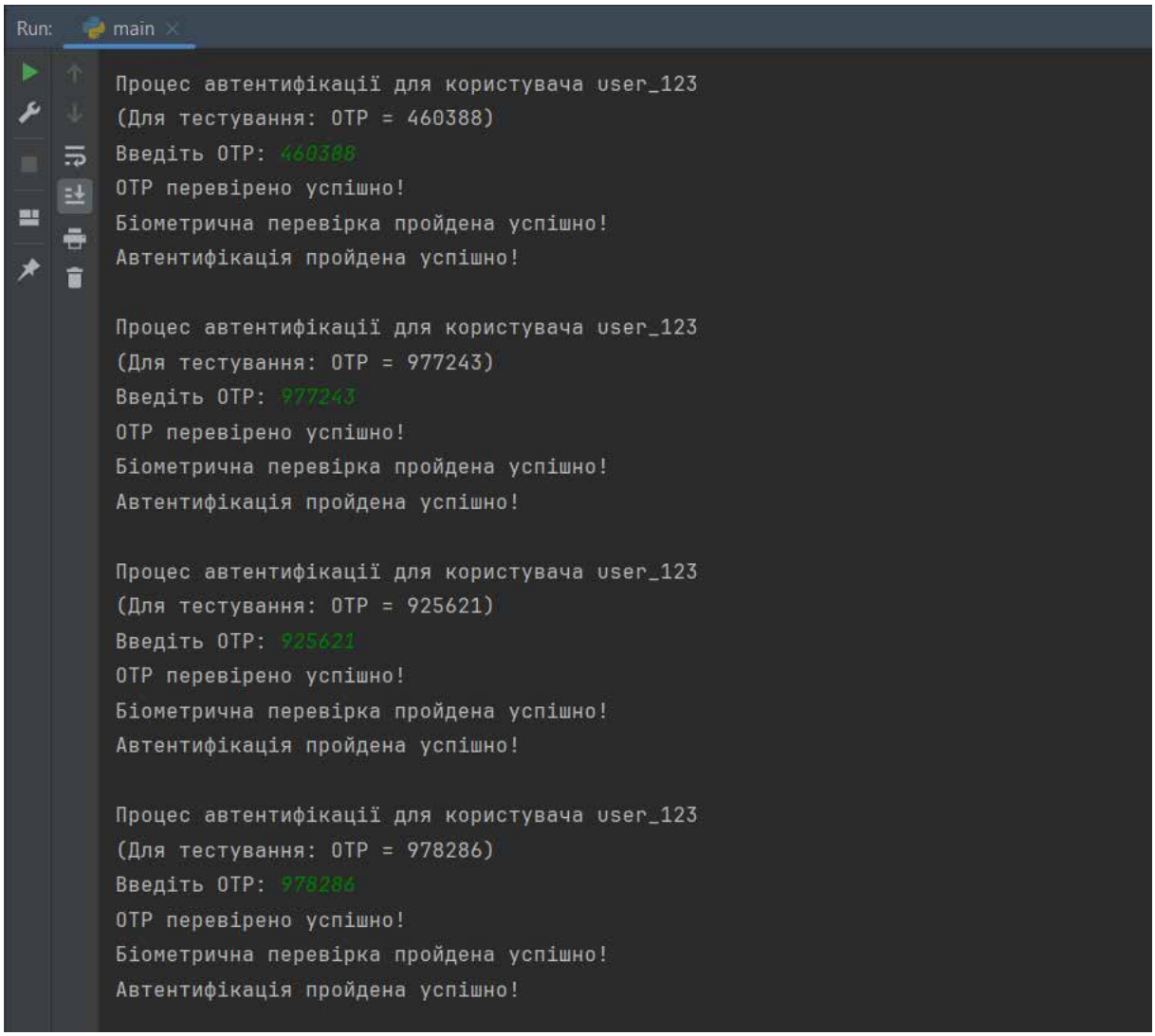

Рис. 3.2 - Перевірка роботи програми

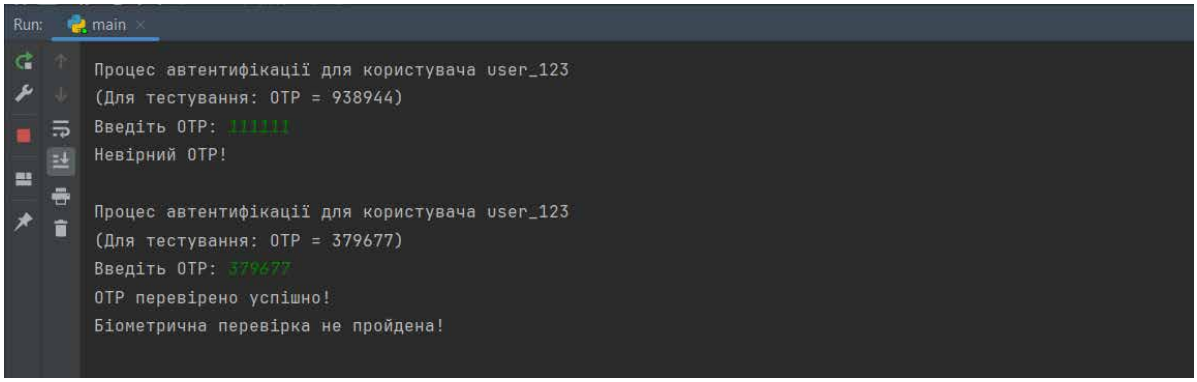

Рис. 3.3 - Перевірку хибних спрацювань

authentication_log.csv

	C1	C2	C3	C4
1	user_123	4.816234827041626	2.102395163775056	6.918629990816682
2	user_123	4.4876415729522705	2.5798565418410733	7.067498114793343
3	user_123	4.992366313934326	1.3527454284151381	6.345111742349465
4	user_123	5.478209495544434	1.0241179827034166	6.50232747824785
5	user_123	8.527953147888184	1.9147215433332287	10.442674691221413
6	user_123	5.238358974456787	2.5112908692147147	7.749649843671502
7	user_123	7.421347618103027	1.9604342099336112	9.381781828036639
8	user_123	5.789489030838013	2.509925878650083	8.299414909488096
9	user_123	5.683372497558594	2.7400057831274696	8.423378280686062
10	user_123	5.993312120437622	2.9580924099982395	8.951404530435862
11	user_123	7.908192873001099	1.4712554474399797	9.379448320441078
12	user_123	4.460258483886719	2.2633586762985116	6.72361716018523
13	user_123	6.70684552192688	1.518836661070045	8.225682182996925
14	user_123	4.303285837173462	1.6819394779487067	5.985225315122168
15	user_123	3.691945791244507	1.892137023222942	5.584082814467449
16	user_123	3.8912158012390137	2.6564339710508937	6.547649772289907
17	user_123	4.042342662811279	1.9343118176540297	5.976654480465309
18	user_123	4.666167259216309	1.9928222771233246	6.658989536339633
19	user_123	4.699586868286133	1.5959683388832033	6.295555207169336
20	user_123	4.835578441619873	2.023006248330379	6.858584689950252
21	user_123	4.613821506500244	1.672793973247597	6.286615479747841
22	user_123	4.045721054077148	1.7745798044703227	5.820300858547471
23	user_123	5.434239864349365	2.7280540723086704	8.162293936658035
24	user_123	5.813643217086792	1.386419280255205	7.200062497341997
25	user_123	4.226229906082153	2.2965864102765816	6.522816316358735

Рис. 3.4 - Логування результатів автентифікації

3.5 Результати аналізу

Розроблена та реалізована гібридна система автентифікації була піддана тестуванню з метою оцінки ефективності та надійності. Під час тестування проводився аналіз часу, витраченого на кожен етап автентифікації, та кількості відмов, зокрема помилок при біометричній перевірці.

В результаті тестування було зібрано дані про 100 спроб входу. Система включала два етапи перевірки — введення одноразового пароля (OTP) та біометричне сканування відбитка пальця. За результатами тестування отримано такі середні показники часу:

- Середній час на введення та перевірку OTP становить 4.95 секунд. Цей показник включає час, необхідний користувачеві для введення пароля, та час на обробку й верифікацію системою.
- Середній час на біометричну автентифікацію дорівнює 2.05 секунд. Цей час охоплює процес сканування відбитка пальця, перевірку його відповідності та обробку результатів.

Таким чином, загальний середній час на одну успішну сесію автентифікації становить близько 7 секунд, що є прийнятним показником для комплексної системи автентифікації, що забезпечує високу надійність.

Також за результатами тестування було встановлено, що приблизно 2% всіх спроб автентифікації завершувалися відмовами через похибки біометричної перевірки. Відмови могли бути спричинені наступними факторами:

- Погана якість сканування відбитка — недостатній контакт пальця з сенсором або сторонні забруднення на поверхні сканера.
- Збої в роботі біометричного сенсора — можливі технічні труднощі або недостатньо точне зчитування відбитка.

Показник відмов на рівні 2% є прийнятним у рамках стандартів біометричних систем, хоча він і вказує на можливість поліпшення технічних параметрів або умов використання сенсора.

3.6 Висновки щодо гібридної системи автентифікації

Розроблена гібридна система автентифікації, що поєднує одноразові паролі (OTP) і біометричну перевірку відбитка пальця, продемонструвала високу надійність і ефективність. Проведений аналіз часу виконання підтверджує швидкість і зручність кожного з етапів для користувачів: середній час на перевірку OTP становить 4.95 секунд, а на біометричне сканування — 2.05

секунд. Загальний середній час виконання автентифікації у 7 секунд є прийнятним, а частота відмов у 2% вказує на точність та стабільність системи, що дозволяє значно знизити ризики несанкціонованого доступу.

Система підтвердила свою ефективність як надійний спосіб автентифікації, який включає додаткові рівні безпеки за рахунок поєднання OTP та біометричної перевірки. Незважаючи на окремі похибки в біометричному зчитуванні, система загалом відповідає вимогам корпоративного середовища з підвищеними стандартами безпеки.

Дана система автентифікації може бути ефективно використана в середовищах, де потрібен високий рівень безпеки для доступу до інформаційно-телекомунікаційних систем, зокрема в таких сферах, як:

1. Фінансові та банківські установи: Гібридна система може забезпечити додатковий рівень захисту для онлайн-банкінгу та внутрішніх систем доступу до фінансових даних.
2. Медичні та державні установи: Використання біометрії разом з OTP забезпечує контроль доступу до конфіденційних та персональних даних пацієнтів, зменшуючи ризики несанкціонованого доступу.
3. Корпоративні системи управління: Система може бути впроваджена в великих організаціях, які обробляють критично важливу інформацію. Гібридний підхід значно підвищує захист від зловмисників та зменшує ризики фішингових атак.
4. Інформаційно-технологічні компанії та дата-центри: У цих компаніях захист інфраструктури і даних є пріоритетом. Поєднання OTP та біометричної автентифікації надійно захистить сервери, бази даних та інші IT-ресурси від несанкціонованого доступу.

Загалом, розроблена гібридна система автентифікації є надійним і ефективним рішенням, яке підходить для використання у високонадійних середовищах з

підвищеними вимогами до безпеки. Вона може бути інтегрована як частина багаторівневої стратегії захисту, де надійність доступу є критично важливим фактором.

Висновок

Проведене дослідження підтверджує важливість використання сучасних методів автентифікації для підвищення рівня безпеки доступу до корпоративних інформаційно-телекомунікаційних систем. В процесі порівняльного аналізу було вивчено різні підходи до автентифікації, зокрема такі методи, як парольна, токена, сертифікатна та біометрична автентифікація. Кожен з методів має свої переваги та недоліки, що залежить від контексту використання та потреб корпоративного середовища. Окрему увагу приділено гібридним системам, які об'єднують декілька методів для досягнення оптимального рівня захисту.

Розроблена та протестована гібридна система автентифікації на базі одноразових паролів (OTP) і біометричної перевірки відбитка пальця продемонструвала високу ефективність. Проведені тести показали, що середній час перевірки OTP становить 4,95 секунди, а біометричне сканування відбувається за 2,05 секунди. Загальний час автентифікації у 7 секунд є оптимальним для забезпечення зручності використання та підтримки високого рівня безпеки. Незначний рівень відмов у 2%, пов'язаний із біометричними похибками, не впливає на загальну ефективність системи.

Гібридна система автентифікації довела свою стійкість та комплексність, і підходить для середовищ із високими вимогами до безпеки, таких як фінансові установи, державні організації та корпоративні мережі, де безпека конфіденційних даних є критично важливою. Вона також може знайти застосування в банківських системах, медичних інформаційних системах та інших середовищах, що потребують захисту персональних даних.

Таким чином, результати дослідження свідчать про високу ефективність гібридних методів автентифікації для захисту корпоративних систем, що надає

можливість для подальшого впровадження цих технологій в організаціях із підвищеними вимогами до безпеки доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ахрамович. В.М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К.:-2016 .-№4.- с. 47-51

2. Jhansi Rani CH, Shammi Munnisa SK. A survey on web authentication methods for web applications. Int J Comput Sci Inf Technol. 2016;7(4):1678–1680.

3. Shteingart H, Gordon AN, Gazit J. Two-factor authentication. In: Microsoft technology licensing. Redmond, WA (US): LLC; 2016.

4. Tsai C-H, Su P-C. The application of multi-server authentication scheme in internet banking transaction environments. Germany: Springer-Verlag GmbH; 2020.

5. Dasgupta D, Roy A, Nag A. Advances n user authentication. 1st ed. USA: Springer International Publishing; 2017.

6. Preferred ways to sign-in to online accounts, apps, and smart devices in selected countries in 2023. URL: https://www.statista.com/statistics/1448883/preferred-security-authentication-methods-in-selected-countries/ (дата звернення: 01.11.2024)

7. Kun AL, Royer T, Leone A. Using tap sequences to authenticate drivers. In: Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications – AutomotiveUI ’13. 2013.

8. Busold C, Taha A, Wachsmann C, Dmitrienko A, Seudié H, Sobhani M, Sadeghi AR. Smart keys for cyber-cars: Secure smartphone-based NFC-enabled car immobilizer. In: Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 18–20 February 2013. New York: ACM; 2013.

9. Lawrence O'Gorman, December 2003, Comparing Passwords, Tokens, and Biometrics for

User Authentication. Proceedings of the IEEE, Vol. 91, No. 12, pp.2019-2040

10. Main issues faced when using authentication methods worldwide in 2023 URL: https://www.statista.com/statistics/1343836/pain-points-of-authentication-methods-worldwide/ (дата звернення: 01.11.2024)

11. Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: A systematic literature review. In: Information and software technology. Chile: Chillán; 2018.

12. C. Braz and J.-M. Robert. Security and usability: the case of the user authentication methods. In International Conference of the Association Francophone d'Interaction Homme-Machine, 2006.

13. S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: measuring the effect of password composition policies. In ACM CHI Conference on Human Factors in Computing Systems, 2011.

14. S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. Does my password go up to eleven?: the impact of password meters on password selection. In ACM CHI Conference on Human Factors in Computing Systems, 2013.

15. C. S. Weir, G. Douglas, M. Carruthers, and M. Jack. User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security, 28(1), 2009.