Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Макаров Максим Володимирович

на здобуття ступеня вищої освіти Бакалавра

Система двофакторної автентифікації інформаційної системи (або сайту)

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 2101021.21.01.13 ПЗ

Виконав студент 4 курсу група КБ-20-1 Максим МАКАРОВ
Керівник канд. техн. наук, доцент Вікторія ОРЛЕНКО
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

19 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Макарову Максиму Володимировичу

1 Тема роботи Система двофакторної автентифікації інформаційної системи (або сайту)

Керівник роботи к.т.н. доцент Вікторія ОРЛЕНКО

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи Проаналізувати особливості реалізації атак на відновлення паролю у мережі. Обрати тип нейронної мережі для ідентифікації зловмисного трафіку. Розробити алгоритм виявлення атаки. Підготувати набори даних для навчання нейронної мережі. Здійснити навчання нейронної мережі. Реалізувати систему виявлення атак. Розробити тестове середовище. Оцінити ефективність розробленої системи.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Огляд предметної області. Засоби реалізації атак. Засоби захисту від атак на паролі. Розробка алгоритмів реалізації та підготовки даних. Вибір нейронної мережі. Алгоритм виявлення атаки у мережі. Система виявлення атаки на відновлення паролю у мережі. Опис реалізації. Розгортання тестового середовища. Оцінка ефективності.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Архітектура системи двофакторної автентифікації інформаційної системи. Алгоритм двофакторної автентифікації. Оцінка ефективності системи виявлення атаки на відновлення паролю у мережі.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Максим МАКАРОВ

Керівник кваліфікаційної роботи Вікторія ОРЛЕНКО

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система двофакторної автентифікації інформаційної системи (або сайту)»

Автор роботи: студент групи КБ–20–1 Макаров М. В.

Керівник роботи: к.т.н. доц. Орленко В.С.

Пояснювальна записка: 63с., 24 рисунки, 8 таблиць, 45 джерел, 3 креслення.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: інформаційна система, автентифікація, двофакторна автентифікація, підбір паролю.

У кваліфікаційній роботі розроблено систему двофакторної автентифікації інформаційної системи, що може бути використана і для сайту. Було проведено аналіз систем автентифікації, проаналізовано їх переваги і недоліки, визначено прийнятні для першого та другого етапів автентифікації підходи.

Запропоновано структуру системи двофакторної автентифікації. Розроблено алгоритм двофакторної автентифікації. Розроблено програмну систему, що реалізує процес двофакторної автентифікації та проведено її тестування.

19.06.2024

ABSTRACT

Course project: «System of two-factor authentication of the information system (or site)»

Author of the work: Makarov Maksym.

Supervisor: Viktoria Orlenko

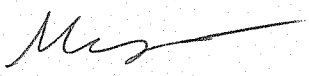
Amount: 63 p., 24 figures, 8 tables, 45 sources, 3 drawings.

INFORMATION SYSTEM, AUTHENTICATION, TWO-FACTOR AUTHENTICATION, PASSWORD SELECTION.

In the qualification work, a system of two-factor authentication of the information system was developed, which can be used for the site as well. An analysis of authentication systems was carried out, their advantages and disadvantages were analyzed, acceptable approaches for the first and second stages of authentication were determined.

The structure of the two-factor authentication system is proposed. A two-factor authentication algorithm has been developed. A software system implementing the two-factor authentication process was developed and tested.

19.06.2024



ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

2FA – Two-Factor Authentication (Двофакторна автентифікація).

OTP – One-Time Password (Одноразовий пароль).

UML – Unified Modeling Language (Уніфікована мова моделювання).

TOTP – Time-Based One-Time Password (Одноразовий пароль, заснований на часі).

HOTP – HMAC-Based One-Time Password (Одноразовий пароль, заснований на алгоритмі HMAC).

SMS – Short Message Service (Служба коротких повідомлень).

PIN – Personal Identification Number (Персональний ідентифікаційний номер).

API – Application Programming Interface (Інтерфейс програмування застосунків).

TLS – Transport Layer Security (Безпека транспортного рівня).

SSL – Secure Sockets Layer (Рівень захищених сокетів).

FIDO – Fast Identity Online (Швидка онлайн-ідентифікація).

GDPR – General Data Protection Regulation (Загальний регламент захисту даних).

PCI DSS – Payment Card Industry Data Security Standard (Стандарт безпеки даних індустрії платіжних карток).

SIM – Subscriber Identity Module (Модуль ідентифікації абонента).

USB – Universal Serial Bus (Універсальна послідовна шина).

NFC – Near Field Communication (Ближній зв'язок).

ВСТУП

Сучасні наукові бібліотеки є не лише центрами зберігання інформації, але й комплексними системами, які забезпечують доступ до знань у цифровому форматі. У зв’язку зі стрімким розвитком інформаційних технологій і збільшенням кількості користувачів бібліотечних послуг зростає потреба у створенні ефективної комп'ютерної мережі. Вона має задовольняти високі вимоги до швидкодії, доступності та безпеки, а також підтримувати широкий спектр сервісів, таких як онлайн-доступ до каталогів, електронні ресурси, резервування літератури тощо.

Актуальність цієї роботи зумовлена тим, що багато існуючих бібліотек використовують застарілі мережеві інфраструктури, які не відповідають сучасним стандартам продуктивності та безпеки. Це обмежує їхні можливості інтеграції з новими технологіями, такими як хмарні сервіси для зберігання даних, автоматизовані системи моніторингу та управління трафіком, а також механізми захисту інформації від кіберзагроз. Належним чином розроблена комп'ютерна мережа дозволяє не лише забезпечити стабільну роботу бібліотеки, але й сприяти розвитку цифрової освіти та наукових досліджень.

Передумови для проведення цієї роботи включають аналіз поточного стану бібліотечних мереж, дослідження сучасних мережевих технологій і вивчення практичних вимог, які висувають користувачі та адміністрація бібліотеки. Основними завданнями є забезпечення сегментації трафіку, доступу до цифрових ресурсів, створення системи резервного копіювання та впровадження засобів для моніторингу. Особливу увагу слід приділити впровадженню протоколів безпеки, які дозволяють захистити мережу від атак та несанкціонованого доступу.

Мета роботи полягає у розробці проєкту комп'ютерної мережі для наукової бібліотеки, яка відповідатиме сучасним стандартам і потребам користувачів. Завдання включають вибір оптимальної топології мережі, впровадження VLAN для розмежування доступу, налаштування маршрутизаторів, комутаторів і точок доступу, а також проведення тестування для забезпечення відповідності технічним вимогам.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

1.1 Концепція двофакторної аутентифікації

Аутентифікація — це процес перевірки достовірності особи або пристрою, які претендують на доступ до певної системи або ресурсу. Метою аутентифікації є підтвердження, що суб'єкт, який намагається увійти в систему, є тим, за кого він себе видає. Це важливий етап забезпечення інформаційної безпеки та контролю доступу.

Аутентифікація включає етапи, де користувач представляє свої облікові дані, такі як ім'я користувача або ID та перевірку поданих облікових даних.

Основні методи автентифікації включають паролі, біометричні дані та одноразові коди.

Одноразовий пароль — це код, який генерується для однократного використання і зазвичай відправляється на мобільний телефон користувача або генерується за допомогою спеціального додатку. OTP є одним із найпоширеніших способів реалізації другого фактора в 2FA.

Біометрична автентифікація використовує унікальні фізичні характеристики користувача, такі як відбитки пальців, сканування обличчя або райдужної оболонки ока, для перевірки його особи. Це один з найбільш надійних методів другого фактора автентифікації завдяки складності підробки біометричних даних.

Токен автентифікації — це фізичний або віртуальний пристрій, який генерує одноразові паролі або інші види аутентифікаційних даних. Токени можуть бути апаратними (наприклад, USB-ключі) або програмними (наприклад, мобільні додатки).

Аутентифікаційний додаток — це програмне забезпечення, яке генерує одноразові паролі для двофакторної автентифікації. Відомі додатки включають Google Authenticator, Authy, та Microsoft Authenticator. Вони зазвичай працюють на основі алгоритмів TOTP (Time-based One-Time Password) або HOTP (HMAC-based One-Time Password).

SMS-автентифікація — це метод двофакторної автентифікації, де одноразовий пароль надсилається на мобільний телефон користувача через SMS. Хоча цей метод є зручним, він менш захищений від атак перехоплення повідомлень або SIM-свопінгу.

Двофакторна автентифікація (2FA) — це метод підвищення безпеки, що вимагає від користувача надання двох різних типів аутентифікаційних даних перед отриманням доступу до системи або ресурсу. Ці фактори можуть включати щось, що користувач знає (пароль), щось, що користувач має (мобільний телефон для отримання одноразового коду), або щось, що користувач є (відбиток пальця або інше біометричне дане).

Попри додатковий рівень захисту, двофакторна автентифікація не є бездоганною. Основні уразливості включають фішинг, коли зловмисники отримують обидва фактори, перехоплення SMS-повідомлень, а також атаки на самі системи генерації одноразових паролів.

Соціальна інженерія — це методи маніпуляції людьми з метою отримання конфіденційної інформації, такої як паролі або інші аутентифікаційні дані. Навіть при використанні 2FA, користувачі можуть бути вразливі до атак соціальної інженерії, коли зловмисники обманом отримують доступ до другого фактора.

Безпека кінцевих точок охоплює методи захисту кінцевих пристроїв, таких як комп'ютери та мобільні телефони, які використовуються для доступу до мережевих ресурсів. Важливість безпеки кінцевих точок зростає при використанні 2FA, оскільки компрометація кінцевого пристрою може означати компрометацію обох факторів автентифікації.

Основні принципи 2FA.

Принцип «Щось, що ви знаєте». Цей принцип базується на використанні інформації, яку знає лише користувач. До найпоширеніших прикладів належать паролі, PIN-коди та відповіді на секретні запитання. Пароль — це рядок символів, який використовується для підтвердження ідентичності користувача. До вимог безпеки паролів належать мінімальна довжина, складність (використання великих та малих літер, цифр, спеціальних символів) і періодична їх зміна. Паролі відзначаються простотою використання та легкістю впровадження, але вони

можуть бути легко вгадані або викрадені, а також вимагають від користувача запам'ятовування. PIN-код — це короткий цифровий код, зазвичай складається з 4-6 цифр. Його перевагами є швидкість введення та зручність для мобільних пристроїв, проте він менш стійкий до підбору, особливо якщо код короткий. Секретні питання та відповіді дозволяють користувачеві відновити доступ у разі забуття пароля, однак часто відповіді на такі питання легко вгадуються або знаходяться в публічних джерелах. Основними перевагами принципу "Щось, що ви знаєте" є простота реалізації, відомість користувачам та низькі витрати, оскільки він не потребує додаткових пристроїв чи спеціального обладнання. Водночас цей принцип вразливий до різних видів атак, таких як фішинг, брутфорс-атаки та кейлогери, що фіксують натискання клавіш.

Принцип аутентифікації "Щось, що ви маєте" базується на використанні фізичних предметів або електронних пристроїв, які належать користувачу і служать для підтвердження його ідентичності. Серед найпоширеніших прикладів можна виділити смарт-карти, апаратні токени, мобільні телефони з додатками для генерації одноразових паролів (OTP) та USB-ключі. Смарт-карти містять вбудований мікропроцесор, який зберігає криптографічні ключі та виконує автентифікацію. Апаратні токени генерують одноразові паролі на основі алгоритмів, синхронізованих з сервером автентифікації. Мобільні телефони з додатками OTP, такими як Google Authenticator або Microsoft Authenticator, створюють одноразові коди, які користувач вводить для доступу до системи. USB-ключі, зокрема YubiKey, підключаються до комп'ютера і використовують криптографічні методи для підтвердження особи користувача. Принцип "Щось, що ви маєте" має ряд переваг, серед яких підвищений рівень безпеки порівняно з паролями, оскільки фізичний предмет значно важче вкрасти або підробити. Використання таких предметів знижує ризики фішингових атак і захищає від брутфорс-атак. Однак цей метод має і недоліки, зокрема можливість втрати або пошкодження фізичного пристрою, що може призвести до тимчасової неможливості доступу до системи. Також існують додаткові витрати на придбання та обслуговування таких пристроїв. Незважаючи на ці недоліки, принцип "Щось, що ви маєте" залишається одним з ефективних методів підвищення безпеки

аутентифікації, особливо коли використовується у поєднанні з іншими методами, такими як "Щось, що ви знаєте" або "Щось, що ви є" для багатофакторної аутентифікації.

Принцип аутентифікації "Щось, що ви є" базується на біометричних даних користувача, які є унікальними фізичними або поведінковими характеристиками. Цей метод широко використовується через високу надійність і складність підробки біометричних даних. Основними прикладами є відбитки пальців, розпізнавання обличчя, райдужної оболонки ока, голосу, а також аналізу поведінки, наприклад, динаміка набору тексту або ритм ходи. Відбитки пальців є одним з найпоширеніших методів завдяки їх унікальності і простоті використання. Розпізнавання обличчя стало особливо популярним завдяки поширенню смартфонів з відповідними технологіями, що забезпечують швидке і зручне підтвердження особи. Райдужна оболонка ока має високий рівень точності, але потребує спеціалізованого обладнання для сканування. Голосова аутентифікація дозволяє користувачам підтверджувати свою особу шляхом вимови певних фраз або слів, але може бути вразливою до змін голосу через хвороби або оточуючий шум. Аналіз поведінкових характеристик, таких як динаміка набору тексту або ритм ходи, стає дедалі популярнішим завдяки розвитку машинного навчання і здатності систем виявляти унікальні патерни поведінки кожного користувача. Основними перевагами біометричної аутентифікації є висока безпека і зручність для користувачів, оскільки вони не потребують запам'ятовування паролів чи носіння додаткових пристроїв. Однак, існують певні ризики і недоліки, зокрема можливість обману системи за допомогою високоякісних підробок або використанням силового методу. Крім того, біометричні дані не можна змінити у разі їх компрометації, що підвищує важливість забезпечення їхнього захисту. Біометричні системи також можуть бути дорогими у впровадженні і потребують значних ресурсів для обробки та зберігання даних. Успішність аутентифікації залежить від якості зібраних даних і точності алгоритмів розпізнавання, що вимагає постійного вдосконалення технологій і методів захисту.

Двофакторна автентифікація є додатковим рівнем безпеки, що використовується для забезпечення того, що користувачі є тими, за кого вони себе

видають. Спочатку користувач вводить своє ім'я користувача та пароль, що представляє перший фактор — "щось, що ви знаєте". Після цього система вимагає введення другого фактора, що може бути "щось, що ви маєте" або "щось, що ви є". Найпоширеніший метод другого фактора — це одноразовий пароль (OTP), який може бути надісланий користувачеві через SMS, електронну пошту або генеруватися додатком для аутентифікації, таким як Google Authenticator або Authy. OTP зазвичай має короткий термін придатності, наприклад, шестизначним числом, яке дійсне лише протягом декількох хвилин, що мінімізує ризик його використання зловмисниками. Інший метод — використання апаратних токенів, наприклад, USB-ключів або смарт-карт, які генерують або зберігають одноразові паролі. Користувач підключає цей токен до свого пристрою для підтвердження своєї особи. Також можливе використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя або сканування райдужної оболонки ока. Коли користувач вводить правильний OTP або використовує біометричні дані, система перевіряє обидва фактори і надає доступ до облікового запису. Таким чином, навіть якщо зловмисник отримає перший фактор (пароль), без другого він не зможе отримати доступ до облікового запису. Двофакторна автентифікація значно підвищує рівень безпеки, оскільки комбінує два незалежні методи підтвердження особи, що робить атаки набагато складнішими для здійснення.

Одноразові паролі (One-Time Passwords, OTP) є засобом автентифікації, який забезпечує додатковий рівень безпеки порівняно зі статичними паролями. OTP використовуються лише один раз для входу в систему або підтвердження транзакції, після чого стають недійсними. Це значно знижує ризик несанкціонованого доступу, оскільки навіть якщо зловмисник перехопить пароль, він не зможе використати його повторно. OTP можуть генеруватися різними способами. Одним з найпоширеніших методів є використання апаратних токенів або програмних додатків, які генерують паролі на основі синхронізації з сервером або поточного часу. Користувач вводить цей пароль разом зі своїм звичайним паролем для отримання доступу до системи. Такий підхід часто застосовується в банківських системах та інших сферах, де необхідний високий рівень безпеки.

OTP можуть надсилатися користувачам через SMS, електронну пошту або інші засоби зв'язку. Наприклад, після введення звичайного пароля користувач отримує SMS з одноразовим паролем, який він має ввести для завершення процесу автентифікації. Цей метод зручний, оскільки не потребує додаткового обладнання, але залежить від надійності мобільного зв'язку. Одним з ключових принципів роботи OTP є алгоритми генерації, такі як HMAC-based One-Time Password (HOTP) і Time-based One-Time Password (TOTP). HOTP генерує паролі на основі лічильника, який збільшується при кожному використанні пароля, тоді як TOTP використовує поточний час для генерації паролів, що робить їх дійсними лише протягом короткого періоду.

OTP мають численні переваги, зокрема підвищену безпеку та зменшення ризику фішингу, оскільки перехоплений пароль не можна використовувати повторно. Вони також захищають від атак повторного використання (replay attacks), оскільки кожен пароль має короткий термін дії або використовується лише один раз. Проте, цей метод має й певні недоліки, такі як можливість втрати доступу до генератора паролів або проблеми з доставкою паролів через SMS або електронну пошту. Також є ризик синхронізаційних проблем між сервером і генератором OTP, що може призвести до відмови в доступі.

Різні системи використовують OTP для додаткової безпеки при виконанні важливих операцій. Наприклад, деякі банківські системи вимагають підтвердження транзакцій за допомогою OTP, надісланих на мобільний телефон клієнта. Це забезпечує додатковий рівень захисту навіть у випадку компрометації основного пароля. Інші системи можуть використовувати OTP для двофакторної аутентифікації (2FA), де користувач вводить статичний пароль та OTP, що генерується на момент входу.

OTP також можуть бути інтегровані з біометричними методами аутентифікації для створення ще більш надійної системи безпеки. Комбінація біометричних даних, таких як відбитки пальців або розпізнавання обличчя, з одноразовими паролями значно ускладнює завдання зловмисникам, що намагаються отримати несанкціонований доступ.

Загалом, одноразові паролі залишаються ефективним засобом автентифікації, що широко використовується для захисту чутливої інформації та забезпечення безпеки в різних системах. Вони забезпечують додатковий рівень захисту порівняно зі статичними паролями, але вимагають належного управління та підтримки для забезпечення їх ефективності та надійності.

Автентифікаційні додатки (Authentication Apps) є інструментами, що використовуються для двофакторної аутентифікації (2FA) з метою підвищення безпеки користувачів під час доступу до онлайн-акаунтів та інших ресурсів. Ці додатки генерують одноразові паролі (One-Time Passwords, OTP). Автентифікаційні додатки зазвичай встановлюються на смартфони або інші мобільні пристрої і працюють за принципом генерації кодів, що змінюються через короткі проміжки часу, зазвичай кожні 30 або 60 секунд. Для налаштування додатка користувач зазвичай сканує QR-код або вводить секретний ключ, наданий сервісом, який підтримує 2FA. Цей ключ синхронізує додаток з акаунтом користувача, дозволяючи генерувати відповідні коди. Однією з основних переваг автентифікаційних додатків є підвищена безпека, оскільки навіть якщо звичайний пароль користувача буде скомпрометований, зловмисник не зможе отримати доступ без одноразового пароля з додатка. Крім того, на відміну від SMS-кодів, які можуть бути перехоплені або зламані, автентифікаційні додатки не залежать від мобільної мережі і менш уразливі до атак. Відомими прикладами автентифікаційних додатків є Google Authenticator, Microsoft Authenticator та Authy. Вони забезпечують широкий спектр функцій, включаючи можливість резервного копіювання і відновлення даних, а також підтримку кількох акаунтів. Однак, використання автентифікаційних додатків вимагає додаткових зусиль від користувачів, зокрема необхідності мати доступ до мобільного пристрою для отримання коду. Крім того, втрата або крадіжка пристрою може створити певні труднощі в доступі до акаунтів, тому важливо налаштувати резервні методи відновлення. Автентифікаційні додатки стають все більш популярними завдяки їхній ефективності в захисті персональних даних та значному зниженню ризиків несанкціонованого доступу.

Аутентифікація за допомогою SMS та електронної пошти є поширеними методами багатофакторної аутентифікації, що додають додатковий рівень безпеки до основного методу, такого як пароль. При аутентифікації за допомогою SMS користувачу надсилається одноразовий код на його мобільний телефон, який він повинен ввести в систему для підтвердження своєї особи. Цей метод є досить зручним, оскільки більшість людей постійно мають при собі мобільні телефони. Однак він має деякі недоліки, зокрема можливість перехоплення SMS або атак через сім-картки. Крім того, якщо користувач знаходиться поза зоною покриття мобільної мережі, він не зможе отримати код.

Аутентифікація за допомогою електронної пошти полягає у надсиланні користувачу листа з одноразовим кодом або спеціальним посиланням, яке він повинен використати для підтвердження своєї особи. Цей метод також є зручним, оскільки більшість людей мають доступ до своїх електронних пошт. Перевагою є те, що електронна пошта менш залежить від наявності мобільного зв'язку. Проте, цей метод також має вразливості: зловмисники можуть отримати доступ до електронної пошти користувача через фішинг або інші методи атак. Обидва методи значно підвищують рівень безпеки у порівнянні з використанням лише пароля, однак жоден з них не є абсолютно захищеним від можливих загроз. Ефективність цих методів багато в чому залежить від того, наскільки добре захищені мобільні пристрої та облікові записи електронної пошти користувачів, а також від обізнаності самих користувачів щодо кібербезпеки.

Автентифікація за допомогою апаратних токенів, також відома як апаратні токени або апаратні ключі, є методикою підвищення безпеки при доступі до інформаційних систем. Вона передбачає використання фізичного пристрою для генерування одноразових паролів або криптографічних ключів, які необхідні для автентифікації користувача. Такі токени можуть бути різних форм, включаючи смарт-карти, USB-ключі, або навіть невеликі брелоки.

Основний принцип роботи апаратних токенів полягає в генерації унікального коду, який вводиться користувачем під час процесу входу в систему разом зі звичайним паролем. Це додає додатковий рівень безпеки, оскільки зловмиснику для успішної атаки недостатньо лише зламати пароль – йому також потрібен

фізичний доступ до апаратного токена. Коди, що генеруються токенами, зазвичай мають обмежений термін дії (наприклад, 30 секунд), після чого вони стають недійсними, що значно ускладнює можливість їх використання зловмисником.

Токени можуть працювати за різними механізмами генерації кодів. Найбільш поширеним є часово-обмежений одноразовий пароль (Time-Based One-Time Password, TOTP), де код генерується на основі поточного часу і секретного ключа, збереженого в токені. Іншим підходом є HMAC-based One-Time Password (HOTP), де код генерується на основі лічильника і секретного ключа. Обидва методи гарантують, що кожен згенерований код є унікальним і непередбачуваним.

Важливою особливістю апаратних токенів є їхня захищеність від фізичного втручання. Вони зазвичай мають захист від спроб злому і витоку інформації, зберігаючи криптографічні ключі в захищеному середовищі. Деякі токени також підтримують додаткові функції, такі як шифрування даних або електронний підпис.

Використання апаратних токенів особливо популярне в середовищах з високими вимогами до безпеки, наприклад, у банківській сфері, корпоративних мережах та урядових установах. Вони забезпечують двофакторну автентифікацію (2FA), де поєднуються "щось, що ви знаєте" (пароль) і "щось, що ви маєте" (токен). Це значно знижує ризик несанкціонованого доступу навіть у випадку компрометації пароля.

Апаратні токени також мають свої недоліки. Вони можуть бути втрачені або викрадені, що потребує наявності резервних методів доступу та швидкого реагування на подібні інциденти. Також їх використання може бути менш зручним для деяких користувачів порівняно з іншими методами автентифікації, такими як мобільні додатки або SMS-коди.

Загалом, автентифікація за допомогою апаратних токенів є ефективним і надійним способом забезпечення безпеки інформаційних систем, особливо в контексті захисту від фішингу та інших видів атак, спрямованих на компрометацію автентифікаційних даних.

Біометрична автентифікація є технологією, що використовує унікальні фізичні або поведінкові характеристики людини для підтвердження її особи. Вона забезпечує високий рівень безпеки та зручності в порівнянні з традиційними

методами автентифікації, такими як паролі чи PIN-коди. Серед фізичних характеристик, що використовуються для біометричної автентифікації, найбільш поширеними є відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока та голосова автентифікація. Поведінкові біометричні дані можуть включати аналіз підпису, манеру друкування на клавіатурі, а також особливості руху тіла.

Процес біометричної автентифікації складається з декількох етапів. Спочатку відбувається збір біометричних даних користувача під час реєстрації. Ці дані зберігаються у вигляді шаблону в базі даних. Під час спроби автентифікації, користувач надає свої біометричні дані, які порівнюються з раніше збереженим шаблоном. Якщо вони співпадають, користувач отримує доступ до системи. Надійність біометричної автентифікації залежить від точності зібраних даних та алгоритмів їх обробки. Для зменшення ймовірності помилок використовуються різноманітні методи шифрування та багатофакторна автентифікація.

Переваги біометричної автентифікації включають високий рівень безпеки, оскільки біометричні дані важко підробити чи вкрасти, зручність використання для користувачів, які не потребують запам'ятовування паролів, а також швидкість автентифікації. Проте є і недоліки, серед яких висока вартість впровадження та обслуговування біометричних систем, можливість порушення конфіденційності, оскільки біометричні дані є унікальними та незмінними, а також ризик зловживання чи несанкціонованого доступу до біометричних баз даних. Таким чином, біометрична автентифікація є перспективною технологією, що поєднує в собі зручність і високий рівень безпеки, однак потребує ретельного впровадження та захисту даних для мінімізації потенційних ризиків.

Двофакторна автентифікація (2FA) є додатковим рівнем безпеки, який використовується для забезпечення захисту онлайн-акаунтів та даних користувачів. Основний принцип роботи 2FA полягає у вимозі двох окремих факторів для підтвердження особи користувача: щось, що користувач знає (наприклад, пароль), та щось, що користувач має (наприклад, мобільний телефон). Ця комбінація значно ускладнює для неавторизованих осіб отримання доступу до акаунтів навіть у випадку, якщо пароль було зламано або викрадено.

Механізми роботи системи 2FA можуть варіюватися, але загалом вони включають кілька основних етапів. Спочатку користувач вводить свій пароль для входу в акаунт. Після успішної верифікації пароля система генерує запит на введення другого фактора автентифікації. Цей другий фактор може бути реалізований різними способами, такими як SMS-повідомлення, генератори одноразових паролів (OTP), мобільні додатки-автентифікатори або апаратні токени.

SMS-повідомлення є одним із найпоширеніших методів реалізації 2FA. Після введення пароля користувач отримує SMS з одноразовим кодом, який потрібно ввести на сайті для завершення автентифікації. Хоча цей метод є зручним, він має певні недоліки, зокрема можливість перехоплення повідомлень або атаки типу SIM-swap, коли зловмисники отримують контроль над SIM-картою користувача.

Генератори одноразових паролів (OTP), такі як Google Authenticator або Authy, забезпечують більш високий рівень безпеки. Ці додатки генерують коди, які змінюються кожні 30 або 60 секунд і не залежать від мережевих з'єднань, що знижує ризик перехоплення. Апаратні токени, як-от ключі безпеки YubiKey, також є надійним варіантом, оскільки вони генерують одноразові коди без необхідності підключення до Інтернету і можуть вимагати фізичного контакту для підтвердження автентифікації.

Мобільні додатки-автентифікатори можуть використовувати інші методи підтвердження, наприклад push-повідомлення. У цьому випадку після введення пароля користувач отримує повідомлення на свій смартфон із запитом підтвердити спробу входу. Це забезпечує додатковий рівень захисту, оскільки для підтвердження автентифікації потрібен фізичний доступ до мобільного пристрою користувача.

Незалежно від конкретного методу реалізації, основна мета 2FA полягає в зменшенні ризику несанкціонованого доступу до акаунтів та даних користувачів. Поєднання двох факторів автентифікації значно ускладнює завдання для зловмисників, оскільки для успішного входу їм потрібно мати доступ до обох факторів одночасно. Таким чином, двофакторна автентифікація стає важливим інструментом для забезпечення кібербезпеки в сучасному цифровому світі.

Порівняння методів аутентифікації з визначенням переваг двофакторної системи можна представити у вигляді таблиці 1.1:

Таблиця 1.1 – Порівняння методів автентифікації

Метод аутентифікації	Опис	Переваги	Недоліки
Парольна аутентифікація	Використання секретного слова або фрази	Простота використання, низька вартість впровадження	Вразливість до атак методом підбору, фішинг-атак, крадіжок паролів
Біометрична аутентифікація	Використання фізіологічних характеристик (відбитки пальців, сканування обличчя, райдужка ока)	Висока точність, неможливість забути або втратити біометричні дані	Висока вартість впровадження, можливість помилок, питання конфіденційності
Смарт-карти та токени	Використання фізичних пристроїв для генерації або зберігання аутентифікаційних даних	Висока безпека, складність підробки	Висока вартість виробництва та обслуговування, можливість втрати або крадіжки
Двофакторна аутентифікація (2FA)	Поєднання двох різних методів аутентифікації (наприклад, пароль і одноразовий код з SMS)	Висока безпека, захист від багатьох видів атак, складність компрометації обох факторів одночасно	Додаткова складність для користувачів, необхідність додаткового обладнання або програмного забезпечення

Двофакторна аутентифікація (2FA) має значні переваги порівняно з іншими методами аутентифікації. Поєднання двох різних факторів аутентифікації значно підвищує рівень безпеки, оскільки навіть якщо один з факторів буде скомпрометовано, зловмиснику буде необхідно подолати ще один бар'єр. Це забезпечує захист від більшості атак, включаючи фішинг, атаки методом підбору паролів та крадіжки паролів. Недоліком є додаткова складність для користувачів, оскільки вони повинні мати доступ до другого фактора (наприклад, мобільного телефону для отримання одноразового коду). Однак, ці незручності є незначними порівняно з підвищенням рівня безпеки, що надається двофакторною аутентифікацією.

1.2 Методи першого фактора аутентифікації

Перший фактор двофакторної аутентифікації зазвичай базується на знанні користувача. Це може бути пароль, ПІН-код, графічний пароль або відповідь на питання безпеки.

Паролі є найпоширенішим методом аутентифікації, який використовується як перший фактор у двофакторній аутентифікації. Використання паролів має як свої переваги, так і недоліки. Однією з головних переваг паролів є їх простота та зручність. Паролі легко запам'ятати, і користувачі звикли до їх використання у повсякденному житті. Крім того, впровадження системи паролів є відносно недорогим для організацій, що робить цей метод доступним для широкого кола застосувань. Паролі можуть бути легко змінені у випадку підозри на їх компрометацію, що додає гнучкості у забезпеченні безпеки.

Однак, паролі мають і суттєві недоліки. Одним із найбільших викликів є те, що багато користувачів створюють слабкі паролі, які легко вгадати або підібрати. Використання простих паролів, таких як "123456" або "password", робить системи вразливими до атак методом підбору паролів. Крім того, багато користувачів схильні використовувати один і той самий пароль для різних облікових записів, що означає, що компрометація одного облікового запису може призвести до

компрометації інших. Паролі також можуть бути вкрадені через фішинг-атаки, де зловмисники обманним шляхом отримують доступ до облікових даних користувачів. Соціальна інженерія та атаки методом грубої сили також становлять серйозну загрозу для безпеки паролів.

Крім того, існує проблема управління паролями. Користувачам важко запам'ятати численні складні паролі для різних облікових записів, що призводить до використання небезпечних практик, таких як записування паролів або зберігання їх у незахищених місцях. Використання менеджерів паролів може допомогти у вирішенні цієї проблеми, але не всі користувачі готові або здатні правильно їх використовувати.

У двофакторній аутентифікації паролі виконують функцію першого фактора, що базується на знанні користувача, і це суттєво підвищує загальний рівень безпеки. Поєднання пароля з другим фактором, таким як одноразовий код, відправлений на мобільний телефон, або біометричний метод, значно зменшує ризик компрометації облікового запису. Однак, для максимальної ефективності цього підходу необхідно дотримуватися рекомендацій щодо створення складних паролів, їх регулярної зміни та використання унікальних паролів для кожного облікового запису. Таким чином, хоча паролі мають свої недоліки, вони залишаються важливим і ефективним елементом системи двофакторної аутентифікації за умови правильного використання та поєднання з додатковими методами захисту.

Використання Пін-кодів (Personal Identification Numbers) як першого фактора двофакторної аутентифікації має свої переваги та недоліки.

До основних переваг використання Пін-кодів належить їх простота та зручність. Користувачам легко запам'ятати короткий числовий код, який зазвичай складається з 4-6 цифр. Це дозволяє швидко і легко вводити Пін-код для доступу до системи, що робить цей метод зручним для широкого кола користувачів. Крім того, Пін-коди часто використовуються в поєднанні з фізичними пристроями, такими як банкомати, мобільні телефони або смарт-карти, що додає додатковий рівень захисту. Наприклад, навіть якщо хтось отримає доступ до пристрою, йому все одно потрібно знати Пін-код для завершення аутентифікації.

Проте Пін-коди мають і суттєві недоліки. Один із головних недоліків полягає в їх вразливості до атак методом підбору, особливо якщо користувачі обирають прості або поширені комбінації, такі як "1234" або "0000". Це значно знижує ефективність Пін-кодів як засобу захисту. Крім того, Пін-коди можуть бути вразливими до атак методом спостереження, коли зловмисники можуть підглянути, як користувач вводить свій Пін-код. Цей тип атак особливо поширений у громадських місцях, де є ризик фізичного спостереження.

Ще один недолік полягає у можливості забути або втратити Пін-код. Хоча Пін-коди зазвичай короткі та прості, користувачі можуть їх забути, особливо якщо вони використовують різні коди для різних систем. Це може призвести до блокування доступу і потреби у відновленні або зміні Пін-коду, що вимагає додаткових зусиль і може бути незручним для користувачів.

Незважаючи на ці недоліки, Пін-коди все ще залишаються популярним методом аутентифікації завдяки своїй простоті та зручності. У контексті двофакторної аутентифікації їх використання може бути виправданим, оскільки додавання другого фактора значно підвищує загальний рівень безпеки системи. Другий фактор може бути чимось, що користувач має (наприклад, мобільний телефон для отримання одноразового коду) або чимось, що користувач є (біометричні дані), що робить компрометацію системи значно складнішою. Таким чином, Пін-коди можуть бути ефективним першим фактором аутентифікації в рамках багатофакторної системи, забезпечуючи баланс між зручністю та безпекою.

Графічні паролі, як метод аутентифікації, мають свої переваги і недоліки, особливо коли використовуються в якості першого фактора двофакторної аутентифікації. Однією з головних переваг графічних паролів є те, що вони можуть бути більш зручними для користувачів, які мають труднощі з запам'ятовуванням складних текстових паролів. Графічні паролі використовують візуальні шаблони або малюнки, які часто легше запам'ятати і відтворити, ніж традиційні текстові паролі. Це може підвищити зручність використання і зменшити кількість випадків, коли користувачі забувають свої паролі.

Крім того, графічні паролі можуть бути більш стійкими до деяких типів атак, таких як атаки методом підбору паролів або фішинг-атаки. Зловмисникам

складніше автоматизувати підбір графічних паролів, оскільки вони включають в себе візуальні елементи, які важко перехопити або передбачити. Це робить графічні паролі надійнішими в порівнянні з текстовими паролями, особливо якщо вони використовуються в поєднанні з іншими методами аутентифікації.

Однак графічні паролі мають і суттєві недоліки. Один з основних недоліків полягає в тому, що вони можуть бути менш безпечними, якщо їх спостерігати або записувати. Наприклад, якщо хтось спостерігає за користувачем під час введення графічного пароля, він може легко його запам'ятати і відтворити. Крім того, деякі користувачі можуть вибирати прості і легко передбачувані графічні паролі, що знижує їхню ефективність як методу аутентифікації.

Іншим недоліком є те, що графічні паролі можуть бути складнішими для впровадження та підтримки в порівнянні з текстовими паролями. Системи, що використовують графічні паролі, потребують спеціального програмного забезпечення або інтерфейсів, які можуть бути менш універсальними і сумісними з різними пристроями та платформами. Це може збільшити витрати на розробку і підтримку таких систем.

У підсумку, графічні паролі можуть бути корисним методом аутентифікації, що підвищує зручність використання для деяких користувачів і забезпечує певний рівень захисту від традиційних атак на текстові паролі. Однак, їхні недоліки, такі як вразливість до спостереження та складність впровадження, вимагають ретельного розгляду при виборі цього методу як першого фактора двофакторної аутентифікації.

Використання питань та відповідей на питання безпеки як першого фактора двофакторної аутентифікації має свої переваги та недоліки. Серед переваг можна виділити простоту використання та доступність. Питання безпеки є легкими для запам'ятовування користувачами, оскільки відповіді на них зазвичай стосуються особистої інформації, яка мало змінюється з часом. Наприклад, користувач може легко згадати ім'я свого першого домашнього улюбленця або місто, де він народився. Це робить цей метод зручним, особливо для тих, хто може мати проблеми із запам'ятовуванням складних паролів.

Однак, використання питань та відповідей на питання безпеки має суттєві недоліки з точки зору безпеки. По-перше, багато таких питань можуть мати відповіді, які легко дізнатися або знайти в інтернеті, особливо в еру соціальних мереж. Зловмисники можуть скористатися публічно доступною інформацією для підбору відповідей, що значно знижує ефективність цього методу. По-друге, навіть якщо питання обрані з більшою обережністю, деякі відповіді можуть бути здогадані або виведені за допомогою соціальної інженерії. Наприклад, зловмисник може видати себе за знайомого або співробітника служби підтримки, щоб витягнути необхідну інформацію у користувача.

Крім того, користувачі часто обирають прості або очевидні відповіді, що робить їх легкими мішенями для атак методом підбору. Відповіді на питання безпеки, на відміну від паролів, зазвичай не мають вимог до складності, що додатково підвищує ризик їхнього компрометації. І хоча питання безпеки можуть бути корисними як додатковий рівень захисту, покладатися на них як на основний або єдиний метод аутентифікації не рекомендується через вищезгадані вразливості.

Таким чином, хоча використання питань та відповідей на питання безпеки є зручним і простим для користувачів, воно має серйозні недоліки з точки зору безпеки. Це робить цей метод менш надійним у порівнянні з іншими методами аутентифікації, особливо у випадках, коли потрібен високий рівень захисту.

Перший фактор аутентифікації забезпечує базовий рівень захисту, але він може бути вразливим до різних атак, таких як фішинг, підбір паролів або соціальна інженерія. Саме тому для підвищення безпеки використовують другий фактор, що додає додатковий рівень перевірки і робить компрометацію системи значно складнішою.

1.3 Методи другого фактора аутентифікації

В якості другого фактору автентифікації зазвичай застосовують:

- одноразові паролі (OTP);
- апаратні токени;

– біометрична автентифікація;

– Push-сповіщення;

– асиметрична криптографія;

– PIN-коди та паролі.

Одноразові паролі (OTP) як другий фактор автентифікації є досить популярним методом, що ґрунтується на використанні тимчасових паролів, які генеруються для кожної нової сесії або дії. Ці паролі можуть надсилатися на мобільний телефон через SMS, електронну пошту або генеруватися спеціальними додатками на смартфоні, такими як Google Authenticator чи Microsoft Authenticator.

Особливість OTP полягає в тому, що вони мають короткий термін дії, зазвичай кілька хвилин, після чого стають недійсними. Це робить їх стійкими до атак типу "перехоплення", оскільки отримати одноразовий пароль не гарантує довготривалого доступу до системи. Також такі паролі генеруються випадковим чином, що знижує ризик зламу або вгадування.

Основною перевагою використання OTP є його гнучкість та доступність. Користувачам не потрібно мати спеціальне обладнання для його використання, достатньо лише смартфона. Крім того, цей метод відносно простий у налаштуванні та використанні, що сприяє його поширенню. Одноразові паролі також не зберігаються на сервері в явному вигляді, що знижує ризик компрометації.

Однак є й недоліки. Використання SMS для надсилання OTP вразливе до атак на мобільні мережі, таких як SIM-swapping, де зловмисник може отримати контроль над телефонним номером користувача. Додатково, для генерації OTP через додатки потрібен доступ до мобільного пристрою, що може бути проблематичним у випадку його втрати або пошкодження. Ще однією слабкістю є те, що OTP не захищені від фішингових атак, оскільки користувач може неусвідомлено ввести одноразовий пароль на фальшивому сайті.

Таким чином, одноразові паролі є зручним і досить безпечним методом, але потребують додаткових заходів захисту, особливо при використанні через ненадійні канали зв'язку, такі як SMS.

Апаратні токени як другий фактор автентифікації відрізняються високим рівнем безпеки та використовують фізичні пристрої для генерування одноразових паролів або криптографічних ключів. Користувачеві необхідно підключити такий пристрій до комп'ютера або смартфона (через USB, NFC або Bluetooth) для завершення процесу автентифікації. Найпоширенішими прикладами апаратних токенів є токени FIDO U2F (Universal 2nd Factor) та FIDO2, як YubiKey.

Особливість апаратних токенів полягає в тому, що вони зберігають криптографічні ключі всередині себе, і ці ключі ніколи не покидають пристрій, що унеможливлює їхню крадіжку через мережу. Також токени можуть бути захищені PIN-кодами, що додає додатковий рівень безпеки. Більшість токенів працює на основі асиметричної криптографії, де приватний ключ зберігається на токені, а публічний ключ використовується сервером для верифікації автентичності.

Перевага використання апаратних токенів полягає у їхній стійкості до різних типів атак, включно з фішингом, оскільки токен напряму взаємодіє з автентифікаційним сервером і не дозволяє зловмисникам перенаправити запит. Крім того, їх неможливо скопіювати або зламати дистанційно, що робить їх значно безпечнішими порівняно з одноразовими паролями, надсиланими через SMS або мобільні додатки.

Проте є й недоліки. По-перше, користувачі повинні постійно мати токен із собою, і в разі його втрати або пошкодження доступ до облікових записів може бути заблокований до моменту відновлення доступу. Також апаратні токени можуть бути відносно дорогими, що може обмежити їхнє впровадження у великих організаціях. Для деяких користувачів цей метод може бути менш зручним через потребу в додатковому обладнанні.

Таким чином, апаратні токени пропонують високий рівень захисту, особливо у чутливих середовищах, але вимагають фізичного зберігання і відповідного управління ними з боку користувача.

Біометрична автентифікація як другий фактор автентифікації використовує унікальні фізіологічні або поведінкові характеристики користувача для підтвердження його особи. Це можуть бути відбитки пальців, сканування обличчя, райдужної оболонки ока або навіть розпізнавання голосу. Завдяки тому, що

біометричні дані є унікальними для кожної людини і практично не піддаються підробці, цей метод стає популярним для підвищення безпеки в різних системах.

Однією з основних особливостей біометричної автентифікації є те, що вона не вимагає запам'ятовування паролів або носіння фізичних токенів. Користувач використовує власні фізіологічні дані, які завжди з ним. Це робить процес автентифікації більш зручним та швидким. Крім того, біометричні дані є складними для копіювання або підробки, що значно ускладнює зловмисникам доступ до системи.

Перевага біометричної автентифікації полягає в її високому рівні безпеки, оскільки фізіологічні дані є унікальними і їх важко підробити. Системи на основі біометрії можуть забезпечити швидкий і безперебійний процес автентифікації, що покращує користувацький досвід. Також біометрія дозволяє підвищити захист у випадках, коли користувачі часто забувають свої паролі або втратили доступ до інших факторів автентифікації.

Однак біометрична автентифікація має і певні недоліки. Одним із основних викликів є конфіденційність і безпека зберігання біометричних даних. У разі витоку таких даних їх неможливо змінити, як це можна зробити з паролями чи токенами. Крім того, біометричні системи не завжди працюють бездоганно — наприклад, відбиток пальця може бути не розпізнаний через механічні пошкодження шкіри, або ж система може помилково не розпізнати обличчя через зміну зовнішності. Ще одним обмеженням є вартість впровадження таких систем, особливо у масштабних корпоративних мережах.

Отже, біометрична автентифікація пропонує високу безпеку та зручність для користувачів, але вимагає надійного зберігання біометричних даних і може бути не ідеальною в умовах, коли технологічні помилки або збої можуть обмежити доступ до систем.

Push-сповіщення як метод другого фактора автентифікації передбачає надсилання повідомлень на мобільний пристрій користувача з метою підтвердження спроби входу в систему або виконання певної дії. Цей метод працює наступним чином: під час автентифікації система надсилає push-сповіщення на смартфон, і користувач повинен схвалити або відхилити запит на доступ. Для

підтвердження часто використовується мобільний додаток, наприклад, Duo Security, Microsoft Authenticator чи Google Authenticator.

Особливістю цього методу є його інтерактивність і зручність для користувача. На відміну від одноразових паролів або апаратних токенів, користувачеві не потрібно вводити жодних додаткових даних — він лише підтверджує або відхиляє сповіщення одним натисканням. Це суттєво спрощує процес автентифікації та економить час, що робить цей метод популярним у корпоративних середовищах і серед звичайних користувачів.

Основна перевага push-сповіщень полягає в тому, що вони захищені від багатьох типів атак, зокрема фішингу. Зловмисники не можуть легко перенаправити або підробити запит на автентифікацію, оскільки користувач безпосередньо отримує повідомлення на свій пристрій. Крім того, цей метод забезпечує високу зручність і швидкість, що є важливим фактором для покращення користувацького досвіду. Push-сповіщення також можуть бути інтегровані з додатковими рівнями безпеки, такими як біометрія або PIN-коди.

Однак є й недоліки. Основна вразливість полягає в залежності від доступу до мобільної мережі або інтернету. У разі втрати зв'язку або несправності мобільного пристрою користувач може не отримати сповіщення і, відповідно, не зможе завершити автентифікацію. Ще однією потенційною проблемою є можливість втоми користувачів від постійних сповіщень (push notification fatigue), що може призвести до неуважного підтвердження запитів і підвищення ризику компрометації облікових записів.

Загалом, push-сповіщення є зручним і ефективним методом автентифікації, особливо у поєднанні з іншими факторами, але потребують надійного доступу до мобільних пристроїв і мереж.

Асиметрична криптографія як метод другого фактора автентифікації базується на використанні двох ключів — публічного та приватного. Приватний ключ зберігається лише у користувача, і він ніколи не передається по мережі, тоді як публічний ключ відомий серверу або стороннім сторонам і використовується для перевірки автентичності операцій. Коли користувач ініціює автентифікацію,

система генерує запит, який підписується приватним ключем користувача, а сервер використовує публічний ключ для перевірки цього підпису.

Особливість цього методу полягає у високій надійності захисту даних, оскільки ключі не передаються в явному вигляді через мережу, і злам або перехоплення не дають зловмиснику можливості отримати доступ до приватного ключа. Асиметрична криптографія захищена від багатьох типів атак, таких як перехоплення трафіку або віддалений злам. Системи на основі асиметричної криптографії часто використовують апаратні токени або смарт-картки, які зберігають приватні ключі і виконують підписування запитів без їх витоку.

Основна перевага використання асиметричної криптографії як другого фактора автентифікації полягає в її надзвичайно високій безпеці. Навіть якщо зловмисники зможуть перехопити трафік або отримати доступ до облікового запису, вони не зможуть виконати автентифікацію без приватного ключа. Крім того, цей метод дозволяє повністю виключити можливість фальсифікації автентифікаційних даних, оскільки підписані запити можуть бути верифіковані лише за допомогою відповідного публічного ключа.

Втім, цей метод також має свої недоліки. Основна складність полягає в управлінні приватними ключами — їх необхідно надійно зберігати, зазвичай у захищених апаратних пристроях, таких як смарт-картки чи апаратні токени. У разі втрати або пошкодження токена доступ до облікового запису може бути втрачений, що створює додаткові виклики для користувача. Крім того, впровадження системи на основі асиметричної криптографії може бути досить дорогим і складним у масштабах великої організації.

Таким чином, асиметрична криптографія забезпечує найвищий рівень безпеки серед методів автентифікації, але вимагає складного управління ключами і може бути менш зручною для повсякденного використання через необхідність апаратної підтримки.

PIN-коди та паролі як другий фактор автентифікації є одними з найстаріших і найпоширеніших методів забезпечення безпеки. Вони зазвичай використовуються у поєднанні з іншими факторами, такими як апаратні токени або біометричні дані, для створення багаторівневої системи автентифікації.

Основною особливістю PIN-кодів та паролів є те, що вони покладаються на знання користувача, тобто на інформацію, яку він запам'ятовує та вводить вручну під час автентифікації. Паролі зазвичай складаються з комбінації літер, цифр та спеціальних символів, тоді як PIN-коди — це числові послідовності. Важливою вимогою є складність та унікальність паролів, оскільки прості або повторювані паролі можуть бути вразливими до атак, таких як брутфорс чи словникові атаки.

Перевага використання PIN-кодів і паролів як другого фактора автентифікації полягає у їх простоті і загальнодоступності. Цей метод не потребує спеціального обладнання, і його легко інтегрувати в більшість систем. Крім того, на відміну від апаратних токенів або біометрії, він не залежить від фізичних пристроїв, що можуть бути загублені або пошкоджені. Також паролі та PIN-коди легко змінювати у випадку компрометації, що додає гнучкості.

Проте недоліки цього методу очевидні. Паролі та PIN-коди вразливі до зламу через слабкі паролі, фішингові атаки або перехоплення даних. Багато користувачів використовують прості або однакові паролі для кількох систем, що значно підвищує ризик компрометації. Окрім цього, атаки типу кейлогінгу можуть фіксувати введені паролі або PIN-коди, що також створює загрозу. Якщо PIN-коди чи паролі використовуються без належного захисту, вони стають слабким місцем у системі автентифікації.

Таким чином, PIN-коди та паролі залишаються доступним і простим методом автентифікації, проте їх ефективність значною мірою залежить від складності та надійності цих даних. Для підвищення безпеки їх варто використовувати в поєднанні з іншими факторами, такими як токени або біометрія, для забезпечення більш надійного захисту.

Ефективність використання методів другого фактора автентифікації залежить від конкретного контексту застосування, вимог безпеки та зручності для користувача. Одноразові паролі (OTP), апаратні токени, біометрична автентифікація, push-сповіщення, асиметрична криптографія, а також PIN-коди та паролі мають свої сильні сторони, проте жоден із цих методів не є універсально безпечним. OTP забезпечують гнучкість і простоту використання, але вразливі до атак на канали зв'язку, такі як SIM-swapping. Апаратні токени гарантують високу

безпеку через ізольоване зберігання криптографічних ключів, але потребують фізичного носія, що може бути втрачений або пошкоджений. Біометрична автентифікація пропонує унікальність і зручність, проте залишається питання щодо конфіденційності та незмінності біометричних даних у разі витоку. Push-сповіщення спрощують процес автентифікації, але залежать від стабільного доступу до мобільного зв'язку та можуть стати джерелом ризику через неуважність користувачів. Асиметрична криптографія забезпечує максимальний рівень захисту, але її реалізація є складною і вимагає управління ключами. PIN-коди та паролі є найпростішим методом, але їхня безпека значною мірою залежить від складності паролів і звичок користувача.

Загалом, для досягнення найкращої ефективності доцільно комбінувати кілька методів автентифікації, щоб забезпечити належний баланс між зручністю та безпекою. Основні недоліки кожного з методів включають вразливість до атак через фішинг, слабкість каналів передачі даних, проблеми з управлінням фізичними пристроями та труднощі у захисті біометричних даних. Комбінація декількох факторів мінімізує ризики компрометації, створюючи багатошарову захист, який ускладнює зловмисникам доступ до системи.

1.4 Мультифакторні аутентифікаційні системи

Огляд відомих мультифакторних систем автентифікації демонструє широкий спектр рішень, що поєднують різні методи першого та другого факторів для забезпечення надійного захисту користувачів. Багато компаній пропонують системи, які використовують комбінації паролів, біометрії, апаратних токенів та одноразових паролів (OTP) з метою досягнення оптимальної безпеки та зручності.

Однією з провідних систем є Duo Security від Cisco, яка комбінує паролі як перший фактор автентифікації з кількома варіантами другого фактора, включаючи push-сповіщення, одноразові паролі через додаток Duo Mobile, біометрію (розпізнавання відбитків пальців або обличчя) та апаратні токени. Duo Security

забезпечує гнучкість у виборі другого фактора, дозволяючи користувачам обрати найбільш зручний і доступний метод.

Система Google Authenticator також широко використовується для генерації одноразових паролів, які слугують другим фактором у поєднанні з паролем як першим фактором. Це рішення доступне для різних платформ і часто використовується в поєднанні з іншими методами, такими як push-сповіщення або біометрія, залежно від інтеграції з іншими сервісами.

Microsoft Authenticator пропонує подібний функціонал і забезпечує підтримку кількох факторів автентифікації, включаючи паролі, push-сповіщення та одноразові паролі (OTP). Крім того, система інтегрована з Windows Hello, що дозволяє використовувати біометричні дані, такі як розпізнавання обличчя або відбитків пальців, як частину багатофакторної автентифікації.

YubiKey є апаратним токеном, що працює на основі асиметричної криптографії і використовується в багатьох системах для надійної автентифікації. Він може бути інтегрований з паролями або іншими факторами (наприклад, одноразовими паролями чи біометрією) для створення мультифакторного захисту. YubiKey підтримує стандарти FIDO U2F та FIDO2, що робить його сумісним з різними платформами, включаючи Google, Microsoft і багато інших сервісів.

Okta є ще однією відомою системою ідентифікації та автентифікації, що пропонує мультифакторний підхід, комбінуючи паролі, одноразові паролі (OTP), push-сповіщення, біометрію та апаратні токени. Okta забезпечує можливість налаштування політик безпеки, що дозволяє організаціям обирати різні фактори в залежності від ризику, ролі користувачів або чутливості системи.

RSA SecurID використовує одноразові паролі, які можуть генеруватися через апаратні токени або мобільні додатки. У поєднанні з паролями як першим фактором, RSA SecurID забезпечує стійкий до атак метод автентифікації. Ця система також підтримує асиметричну криптографію для додаткового захисту.

Кожна з цих систем має свої сильні сторони, пропонуючи різноманітні комбінації факторів автентифікації для досягнення оптимального рівня захисту. Вони забезпечують як зручність для користувачів, так і високий рівень безпеки, оскільки поєднання різних факторів суттєво знижує ризик компрометації системи.

В таблиці 1.2 представлено ключові особливості кожної системи з точки зору безпеки, зручності та можливих обмежень.

Таблиця 1.2 – Системи мультифакторної автентифікації

Система	Переваги	Недоліки
Duo Security	- Підтримка кількох методів автентифікації (паролі, OTP, push-сповіщення, біометрія) - Гнучкість у виборі другого фактору - Зручність та швидкість використання	- Залежність від мобільних пристроїв - Можливість фальшивих підтверджень через push-сповіщення
Google Authenticator	- Широке використання - Простота в налаштуванні - Підтримка одноразових паролів (OTP)	- Відсутність функцій резервного копіювання - Не підтримує push-сповіщення або біометрію
Microsoft Authenticator	- Інтеграція з Windows Hello для використання біометрії - Підтримка OTP і push-сповіщень - Легка інтеграція з Microsoft сервісами	- Обмежена підтримка для платформ поза екосистемою Microsoft - Залежність від інтернет-з'єднання
YubiKey	- Висока безпека завдяки апаратному зберіганню ключів - Підтримка стандартів FIDO U2F та FIDO2 - Не потребує підключення до мережі	- Необхідність фізичного носія (токена) - Можливість втрати або пошкодження апаратного токена

Таблиця 1.2 (Кінець) – Системи мультифакторної автентифікації

Система	Переваги	Недоліки
Okta	- Різноманітні фактори автентифікації (паролі, OTP, push-сповіщення, біометрія, токени) - Гнучка налаштовуваність політик безпеки - Підтримка багатьох платформ і служб	- Складність у налаштуванні для малих підприємств - Висока вартість для великих організацій
RSA SecurID	- Надійність одноразових паролів (OTP) - Підтримка апаратних токенів і мобільних додатків - Інтеграція з іншими системами безпеки	- Високі витрати на апаратні токени - Складність налаштування для користувачів без технічної підготовки

1.5 Постановка задачі.

Аналіз відомих систем вказує доцільність розробки системи, що забезпечує двофакторну автентифікацію з можливістю вибору другого методу автентифікації.

З огляду на це необхідно вирішити такі задачі:

- реалізувати класичну автентифікацію на основі введення пароля, з зберіганням паролів у захищеному вигляді з використанням хеш-функцій для захисту від компрометації бази даних;
- після введення правильного пароля користувачеві має бути наданий вибір отримання одноразового коду (через SMS-повідомлення на заздалегідь зареєстрований номер телефону або через електронну пошту на зареєстровану адресу);
- одноразовий код має бути випадково згенерованим та мати обмежений строк дії;

- код повинен бути використаний лише один раз;
- одноразовий пароль (OTP) має бути складним та випадковим;
- має бути реалізована система, яка не дозволяє використовувати один і той самий код повторно, навіть у разі закінчення терміну його дії;
- підключення надійного провайдера SMS-послуг;
- SMS має містити одноразовий код і текст повідомлення, який інформує користувача про спробу автентифікації;
- обробляти випадки, коли SMS-повідомлення не можуть бути доставлені;
- інтеграція з поштовими сервісами для відправки одноразового коду на електронну пошту;
- лист має містити одноразовий код і текст повідомлення, який інформує користувача про спробу автентифікації;
- система повинна обробляти випадки, коли повідомлення не можуть бути доставлені;
- не зберігати OTP у відкритому вигляді, використовувати методи шифрування або хешування для зберігання одноразових кодів до моменту їх використання або закінчення строку дії;
- захистити канали передачі даних (SSL/TLS) для запобігання перехоплення кодів;
- реалізувати захист від атак типу "людина посередині" (MitM), фішингу та перехоплення SMS або e-mail;
- після введення пароля користувачу повинна бути запропонована можливість обрати, куди надсилати одноразовий код — на електронну пошту чи на телефон;
- інтуїтивно зрозумілий інтерфейс для введення коду з можливістю повторного запиту нового коду у разі його неотримання.
- забезпечити адміністраторам систему моніторингу спроб входу користувачів та можливість переглядати логи автентифікації;
- реалізувати механізми блокування облікових записів після кількох невдалих спроб автентифікації або неправильного введення OTP.

- можливість налаштування сповіщень про підозрілі спроби входу;
- підтримка масштабування системи для великої кількості користувачів.
- система має бути доступною у веб, а також підтримувати інтеграцію з мобільними додатками.

2 СИСТЕМА ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

2.1 Стандарти та протоколи двофакторної аутентифікації

OpenID Connect (OIDC) — це протокол автентифікації, який побудований поверх протоколу авторизації OAuth 2.0 і дозволяє автентифікувати користувачів за допомогою маркерів (токенів). Його головна мета — надавати спрощений та уніфікований спосіб автентифікації для користувачів через єдину точку входу. OIDC надає механізм для передачі інформації про автентифікованого користувача (наприклад, ідентифікатор користувача, адреса електронної пошти) від ідентифікаційного провайдера до клієнтської програми.

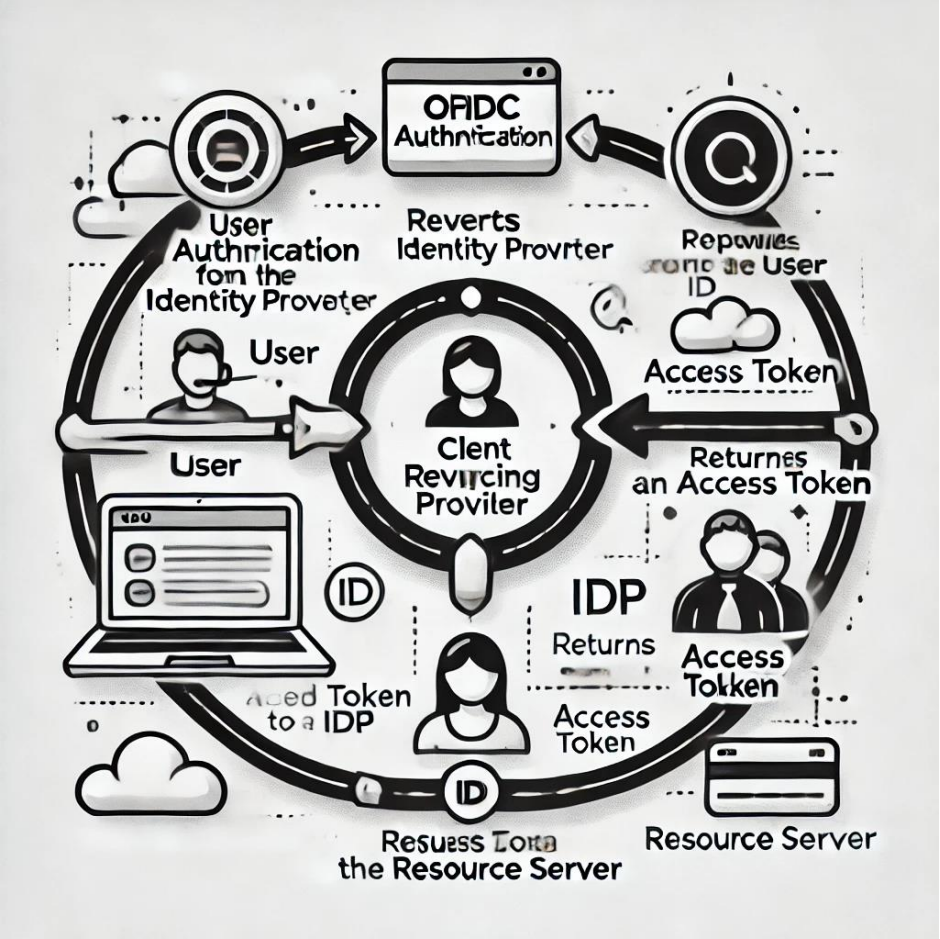


Рисунок 2.1 Процес автентифікації за допомогою OpenID Connect

Основні компоненти OpenID Connect.

Постачальник ідентифікації (Identity Provider, IdP) – це система, яка виконує функції автентифікації користувачів. Вона відповідає за зберігання облікових записів користувачів і обробку їхнього входу. Відомі постачальники – Google, Microsoft, Facebook.

Клієнт (Реліант-партнер, Relying Party, RP) – це додаток або веб-сервіс, який потребує автентифікації користувача через OIDC і довіряє постачальнику ідентифікації для виконання цієї функції. Клієнт отримує маркери (токени), які підтверджують автентифікацію користувача та дозволяють виконувати операції від імені цього користувача.

Маркер ID Token – головний маркер в OpenID Connect, який підтверджує, що користувач автентифікований і містить інформацію про користувача, таку як унікальний ідентифікатор користувача (sub), його ім'я, електронна пошта тощо. ID Token підписується цифровим підписом постачальника ідентифікації, що гарантує його цілісність.

Маркер Access Token – маркер, який дозволяє клієнту отримати доступ до захищених ресурсів користувача.

Маркер Refresh Token – маркер, який використовується для оновлення Access Token без необхідності повторної автентифікації користувача.

Точка доступу Authorization Endpoint — точка, через яку користувач передає свої облікові дані для автентифікації.

Точка доступу Token Endpoint — точка, через яку клієнт отримує маркери (ID Token, Access Token, Refresh Token) після автентифікації.

Точка доступу UserInfo Endpoint — точка, через яку клієнт може отримати детальну інформацію про користувача, автентифікованого через OIDC, за допомогою Access Token.

Процес автентифікації за OpenID Connect:

1. Запит авторизації. Клієнт перенаправляє користувача до постачальника ідентифікації, де користувач вводить свої облікові дані для автентифікації. Запит передається на Authorization Endpoint.

2. Авторизація користувача. Постачальник ідентифікації перевіряє введені облікові дані. Якщо вони правильні, користувач отримує доступ і дає дозвіл клієнту на використання своїх даних.

3. Отримання токенів. Після успішної автентифікації клієнт отримує ID Token і Access Token через Token Endpoint. Ці токени використовуються для доступу до ресурсів користувача.

4. Доступ до ресурсів. Клієнт може використовувати Access Token для запитів до UserInfo Endpoint або інших захищених ресурсів.

5. Оновлення токенів. Коли Access Token стає недійсним (через закінчення терміну дії), клієнт може використати Refresh Token для отримання нового Access Token без потреби у повторній автентифікації користувача.

Переваги OpenID Connect:

Сумісність з OAuth 2.0. OIDC побудований на основі OAuth 2.0, що робить його гнучким і придатним для використання з існуючими системами авторизації.

Зручність для користувачів. Користувачі можуть використовувати один обліковий запис для автентифікації в багатьох додатках і сервісах без необхідності створювати нові облікові записи для кожної системи.

Безпека. Використання цифрових підписів і шифрування для захисту маркерів гарантує безпечну автентифікацію та передачу даних.

Універсальність. OpenID Connect підтримується багатьма великими провайдерами автентифікації, такими як Google, Microsoft, Facebook, що робить його зручним для інтеграції в будь-які веб-додатки чи мобільні системи.

Недоліки OpenID Connect:

Складність налаштування. Хоча OIDC забезпечує високу безпеку, його реалізація може бути складною, особливо для розробників, які вперше стикаються з цим протоколом.

Залежність від постачальника ідентифікації. Якщо клієнт використовує стороннього постачальника ідентифікації, він стає залежним від його політик і доступності. У разі збою у провайдера автентифікація не буде доступною.

OAuth 2.0 — це стандартний протокол авторизації, який дозволяє додаткам отримувати обмежений доступ до ресурсів користувача без передачі його пароля. Він забезпечує безпечний механізм делегування доступу через спеціальні маркери доступу (access tokens) див. рис. 2.2.

Основні компоненти:

1. Ресурсний сервер — система, яка зберігає захищені ресурси (наприклад, API).

2. Клієнт — додаток, що запитує доступ до ресурсів.

3. Сервер авторизації — видає маркери доступу після успішної аутентифікації.

4. Ресурсний власник — користувач, який надає дозвіл на доступ.

Основні етапи процесу:

1. Запит дозволу. Клієнт перенаправляє користувача на сервер авторизації для надання згоди.

2. Отримання коду авторизації. Сервер повертає тимчасовий код після підтвердження.

3. Обмін коду на маркер доступу. Клієнт відправляє код на сервер авторизації та отримує маркер доступу.

4. Використання маркера. Клієнт звертається до ресурсного сервера з маркером для отримання даних.

Типи потоків:

- Authorization Code Flow — для додатків із серверною частиною.

- Implicit Flow — для SPA або додатків без серверної частини.

- Resource Owner Password Credentials Flow — для внутрішніх додатків.

- Client Credentials Flow — для доступу без участі користувача (машина-машина).

OAuth 2.0 широко використовується в сучасних веб-додатках для інтеграції із сервісами як-от Google, Facebook, GitHub.

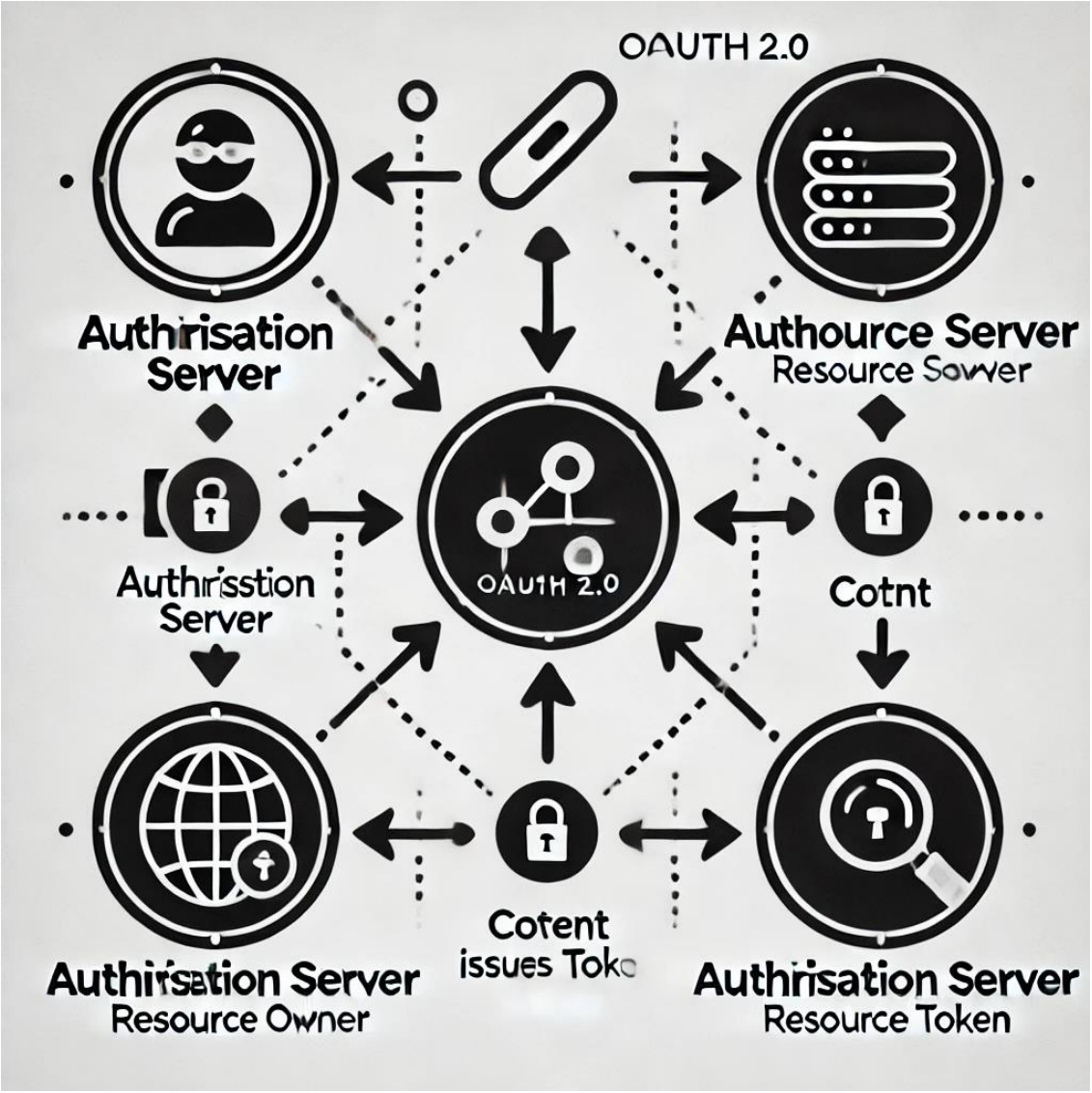


Рисунок 2.2 Процес автентифікації за допомогою OAuth 2.0

Переваги OAuth 2.0:

1. Безпека без передачі пароля. Користувачі надають доступ додаткам без розголошення своїх облікових даних.

2. Гранульоване управління доступом. Можна надати доступ лише до певних ресурсів або функцій.

3. Підтримка різних типів клієнтів. Працює як з веб-додатками, так і з мобільними або десктопними додатками.

4. Широке поширення. Підтримується багатьма великими платформами, що спрощує інтеграцію сторонніх сервісів.

5. Простота відкликання доступу. Користувач може легко скасувати доступ без зміни пароля.

6. Гнучкість у сценаріях авторизації. Підтримує різні потоки для різних типів додатків (наприклад, для серверних, клієнтських або автономних додатків).

Недоліки OAuth 2.0:

1. Відсутність вбудованої аутентифікації. Хоча OAuth 2.0 часто використовують для аутентифікації, цей протокол не був спочатку розроблений для цього (наприклад, необхідність OpenID Connect для повної аутентифікації).

2. Складність реалізації. Для коректного впровадження потрібне глибоке розуміння специфікації та безпекових ризиків.

3. Вразливість до атак. При неправильному налаштуванні можливі атаки, як-от перехоплення маркерів (token hijacking) або фішинг.

4. Ненадійність імпліцитного потоку. Через передачу маркера в URL виникають ризики перехоплення (не рекомендується для нових проєктів).

5. Відсутність стандартизованого шифрування маркерів. Специфікація не регламентує шифрування маркерів, що може спричинити витік інформації при зберіганні вразливих токенів.

OAuth 2.0 — це потужний, але чутливий до правильної реалізації протокол, який підвищує безпеку взаємодії між додатками та користувачами, якщо впроваджений належним чином.

Що таке SAML?

SAML (Security Assertion Markup Language) — це відкритий стандарт для обміну аутентифікаційною та авторизаційною інформацією між різними сторонами. Він забезпечує єдиний вхід (SSO), що дозволяє користувачам входити в різні системи, використовуючи одні й ті ж облікові дані. SAML використовується для взаємодії між постачальником ідентифікації (Identity Provider, IdP) та постачальником послуг (Service Provider, SP).

Основна концепція SAML полягає в тому, що користувач аутентифікується в IdP, який потім передає аутентифікаційний токен (SAML Assertion) SP, дозволяючи доступ до ресурсів без повторного введення паролю.

Компоненти SAML

1. Identity Provider (IdP) — відповідальний за аутентифікацію користувачів і видачу SAML-токенів.

2. Service Provider (SP) — отримує та перевіряє SAML-токени, надаючи доступ до своїх ресурсів.

3. SAML Assertion — XML-документ, який містить інформацію про користувача, підтверджену IdP.

Принцип роботи SAML

1. Користувач намагається отримати доступ до захищеного ресурсу на стороні SP.

2. SP перенаправляє користувача до IdP для аутентифікації.

3. IdP аутентифікує користувача та генерує SAML Assertion.

4. Користувач повертається на SP з SAML Assertion, яку SP перевіряє.

5. Після успішної перевірки SP надає доступ до запитаного ресурсу.

Переваги SAML

1. Зручність для користувача — підтримка SSO знижує кількість разів, коли користувач вводить облікові дані.

2. Безпека — SAML використовує цифрові підписи та шифрування для захисту даних.

3. Масштабованість — підходить для інтеграції з великою кількістю систем, оскільки є універсальним стандартом.

4. Мінімізація облікових даних — зменшується кількість збережених паролів, що знижує ризик компрометації даних.

5. Сумісність — працює з різними платформами та системами завдяки широкому підтриманню стандарту.

Недоліки SAML

1. Складність налаштування — потребує глибоких знань протоколу для коректної інтеграції IdP і SP.

2. Залежність від IdP — якщо IdP виходить з ладу, користувачі не зможуть отримати доступ до сервісів.

3. Проблеми з мобільними додатками — SAML складно інтегрувати у мобільні платформи через їх обмежену підтримку веб-браузерів.

4. Великий обсяг XML — SAML використовує об'ємні XML-документи, що може впливати на продуктивність у складних системах.

5. Відсутність гнучкості — менш підходить для сучасних API або мікросервісних архітектур у порівнянні з OAuth або OpenID Connect.

SAML продовжує бути важливим стандартом для корпоративних середовищ завдяки своїй надійності та широкому розповсюдженню.

2.2 Безпека та виклики впровадження системи двофакторної автентифікації

Фішинг є однією з найпоширеніших загроз, яка може обійти двофакторну автентифікацію. Це тип соціальної інженерії, спрямований на обман користувача з метою викрадення його облікових даних. Навіть якщо використовується двофакторна автентифікація, зловмисники можуть отримати і пароль, і одноразовий код, щоб отримати доступ до облікового запису.

Процес фішингу при 2FA починається зі створення підробленого вебсайту, який візуально і функціонально нагадує легітимний ресурс. Користувача можуть залучити на цей сайт за допомогою фішингових електронних листів, повідомлень у соціальних мережах або навіть через SMS. На цьому етапі користувач вводить свої облікові дані, включаючи логін, пароль та код 2FA, вважаючи, що знаходиться на офіційному сайті.

Як тільки користувач надсилає свої дані, зловмисник отримує їх у реальному часі. Оскільки одноразові коди 2FA мають обмежений термін дії, зловмисники швидко використовують ці дані для входу на справжній сайт. У такий спосіб двофакторна автентифікація втрачає свою ефективність, оскільки зловмисник отримує доступ до обох факторів автентифікації одночасно.

Одним із сучасних підходів є використання фішингових сайтів у поєднанні з Man-in-the-Middle-атаками. Зловмисник, виступаючи як посередник, передає дані між користувачем і легітимним сайтом, створюючи ілюзію безпечного з'єднання.

Це дозволяє обійти навіть додаткові заходи безпеки, такі як перевірка пристрою чи місцезнаходження.

Основним способом захисту від фішингу є використання апаратних ключів U2F або FIDO2. Ці технології працюють на основі криптографічних протоколів і не дозволяють передачу одноразового коду, що значно знижує ймовірність успішної атаки. Іншим ефективним заходом є навчання користувачів розпізнавати ознаки фішингових атак та впровадження багаторівневого контролю доступу.

Перехоплення кодів є серйозною загрозою для безпеки двофакторної автентифікації, коли одноразові паролі (OTP) чи коди аутентифікації опиняються в руках зловмисників через втручання в процес передачі. Це може відбуватися як через технологічні вразливості, так і через цілеспрямовані атаки на користувача або інфраструктуру.

Одним із найпоширеніших методів перехоплення є атака на мобільні мережі. Наприклад, через вразливості в протоколі SS7, який використовується для обміну інформацією між операторами зв'язку. Зловмисники можуть відстежувати або перенаправляти SMS-повідомлення, отримуючи доступ до OTP, надісланих користувачеві для аутентифікації.

Суттєвою загрозою є SIM-свопінг. У цьому випадку хакери видають себе за користувача, звертаючись до служби підтримки оператора мобільного зв'язку з метою перевипуску SIM-карти. Після успішного перевипуску зловмисники отримують доступ до всіх повідомлень та викликів жертви, включно з SMS-кодами для двофакторної автентифікації.

Інший спосіб перехоплення передбачає використання шкідливого програмного забезпечення. Шкідливі програми можуть бути встановлені на смартфон або комп’ютер без відома користувача. Таке ПЗ часто працює у фоновому режимі, відстежуючи вхідні повідомлення або перехоплюючи дані безпосередньо з додатків для генерації кодів, наприклад, Google Authenticator або Authy.

Значною загрозою можуть стати атаки "людина посередині" (Man-in-the-Middle). Під час цієї атаки зловмисник перехоплює дані, що передаються між користувачем і сервером, зокрема коди двофакторної автентифікації. Це може

відбуватися через незахищені мережі Wi-Fi або з використанням підроблених вебсайтів, які зовні ідентичні до справжніх.

Навіть легітимні програми для обміну повідомленнями можуть бути скомпрометовані, якщо зловмисник отримує доступ до облікового запису або резервних копій даних. У такому випадку будь-які OTP, що надходять через ці платформи, стають доступними для хакера.

Щоб зменшити ризик перехоплення кодів, користувачам рекомендується уникати SMS як основного методу отримання OTP, віддаючи перевагу більш безпечним методам, як-от апаратні ключі або додатки для генерації кодів. Також важливо використовувати зашифровані канали зв'язку і двофакторну автентифікацію на всіх критичних сервісах для мінімізації можливих наслідків компрометації.

SIM-свопінг — це атака, спрямована на перенесення номера телефону жертви на SIM-карту, контрольовану зловмисником. Це дозволяє йому отримувати всі дзвінки та SMS-повідомлення, включно з одноразовими кодами (OTP), які часто використовуються для двофакторної автентифікації.

Процес атаки починається з того, що зловмисник збирає особисту інформацію жертви. Це може бути ім'я, дата народження, адреса або останні транзакції, які часто використовуються для верифікації в службі підтримки мобільного оператора. Потім зловмисник звертається до оператора зв'язку та видає себе за жертву, заявляючи про втрату чи пошкодження SIM-карти, що нібито потребує її заміни. Успішна верифікація дозволяє оператору перенести номер телефону на нову SIM-карту.

Після перенесення номера зловмисник отримує доступ до всіх SMS, включно з OTP для входу в облікові записи. Таким чином, навіть якщо користувач має сильний пароль, атака стає успішною завдяки викраденню другого фактора автентифікації. Це особливо небезпечно для фінансових сервісів, електронної пошти або соціальних мереж, які можуть використовувати SMS як єдиний або резервний метод 2FA.

Небезпека цієї атаки полягає в її складності для виявлення на початковому етапі. Жертва може лише помітити втрату сигналу на своєму пристрої, що може

бути сприйнято як технічна несправність. Тим часом зловмисник уже має доступ до чутливих ресурсів.

Щоб знизити ризик SIM-свопінгу, слід використовувати додатки для генерації OTP або апаратні токени, які не залежать від мобільної мережі. Корисним також є встановлення додаткових PIN-кодів на SIM-карту через оператора, що ускладнює процес її заміни без дозволу власника.

Зловживання резервними методами двофакторної автентифікації виникає тоді, коли зловмисники експлуатують альтернативні способи підтвердження особи для обходу основних механізмів безпеки. Резервні методи використовуються у випадках, коли користувач не може отримати код через основний канал, наприклад, втрачено доступ до смартфона чи токена. Зловмисники можуть маніпулювати цими резервними методами для отримання доступу до облікових записів.

Ця загроза пов'язана з недостатнім захистом таких методів або їх надмірною доступністю. Наприклад, якщо резервний код надсилається на електронну пошту, а поштовий сервіс має слабкий рівень захисту, зловмисник може спочатку отримати доступ до поштової скриньки і скористатися цим для входу в інші сервіси. Аналогічно, виклики на телефон чи надсилання коду через SMS можуть бути вразливими до атак, таких як перехоплення повідомлень або SIM-свопінг.

Інша проблема – це соціальна інженерія. Зловмисники можуть обманом переконати користувача або службу підтримки видати резервний код чи тимчасово відключити 2FA. Якщо компанія не забезпечує належних процедур перевірки, цей шлях може стати слабким місцем.

Деякі користувачі зберігають резервні коди у небезпечних місцях, наприклад, у текстових файлах без захисту паролем або навіть у фізичних записах, які легко вкрасти. Це також робить їх доступними для зловмисників. Використання простих методів відновлення облікових записів без додаткових перевірок і багатоступеневої ідентифікації створює додаткові ризики.

Для мінімізації цієї загрози важливо обмежити використання слабких резервних методів, забезпечити їхній захист шифруванням і багатофакторною перевіркою, а також навчати користувачів щодо безпечного зберігання резервних кодів.

Використання застарілих методів двофакторної автентифікації (2FA) є серйозною загрозою для безпеки. Такі методи стають менш ефективними через сучасні атаки, технічні обмеження та загальну слабкість. Основні ризики включають:

1. SMS та голосові дзвінки. Ці методи є популярними, але вразливими через перехоплення повідомлень, атаки на SIM-карти (SIM-swapping) або перенаправлення дзвінків. Зловмисники можуть отримати доступ до коду підтвердження навіть без прямого доступу до пристрою користувача.

2. Статичні коди чи паролі. Деякі системи використовують заздалегідь згенеровані статичні коди. Якщо вони зберігаються в незахищеному вигляді або потрапляють у руки зловмисників, це відкриває прямий доступ до облікового запису.

3. E-mail як 2FA. Автентифікація через електронну пошту залежить від безпеки самого поштового сервісу. Якщо обліковий запис електронної пошти компрометований, зловмисник може отримати контроль над іншими сервісами, пов’язаними з цим e-mail.

4. Одноразові паролі через мобільні додатки. Деякі мобільні додатки створюють одноразові паролі, але вони стають небезпечними, якщо сам пристрій заражений шкідливим програмним забезпеченням або викрадено.

5. Застарілі токени або апаратні пристрої. Фізичні токени або апаратні ключі, які використовують застарілі криптографічні алгоритми, можуть бути скомпрометовані через технічні вразливості чи фізичне викрадення.

Ризики використання застарілих методів можуть бути зменшені, якщо перейти до сучасних і більш безпечних варіантів 2FA, таких як апаратні ключі з підтримкою протоколу FIDO2, біометричні методи або push-сповіщення у зашифрованих додатках.

Man-in-the-Middle (MITM) атака є типом кібератаки, коли зловмисник перехоплює або змінює комунікацію між двома сторонами без їхнього відома. У контексті двофакторної автентифікації (2FA) така атака створює значну загрозу, особливо якщо автентифікація здійснюється через менш захищені канали або без належного шифрування.

Опис механізму MITM-атаки при двофакторній автентифікації:

- Зловмисник створює фальшивий сервер або інтерфейс, який імітує легітимний сайт або систему.

- Користувач вводить свої облікові дані, включаючи пароль. Ці дані перехоплюються зловмисником.

- Коли система запитує другий фактор автентифікації, наприклад код з SMS або застосунку, користувач вводить його.

- Зловмисник перехоплює цей код і негайно використовує його для входу в реальну систему, поки код ще дійсний.

Ризики та слабкі місця, які сприяють успішності атаки:

- Відсутність шифрування на стороні клієнта або сервера.

- Використання SMS як другого фактору, адже його можна перехопити через методи атак на мобільні мережі.

- Недостатній захист від фішингових атак, які можуть ввести користувача в оману.

- Відсутність механізмів виявлення аномальної активності, наприклад логіну з різних IP-адрес за короткий час.

Способи захисту від MITM-атаки в 2FA:

- Використання багатофакторної автентифікації з фізичними токенами або біометрією.

- Шифрування всього трафіку за допомогою протоколів HTTPS та TLS.

- Впровадження автентифікації на основі часу (наприклад, тимчасових кодів TOTP).

- Використання антифішингових функцій, таких як FIDO2 або U2F токени.

- Постійне навчання користувачів для розпізнавання фальшивих сайтів та інтерфейсів.

Таким чином, MITM-атака залишається серйозною загрозою, особливо якщо 2FA впроваджено без врахування сучасних рекомендацій безпеки.

Фізичний доступ до пристрою є суттєвою загрозою в контексті двофакторної автентифікації. Це пов’язано з тим, що зловмисник, отримавши фізичний контроль

над пристроєм, може скористатися різними методами для обходу захисту. Основні аспекти загрози включають такі моменти:

- Крадіжка або втрата пристрою. Якщо зловмисник отримає доступ до смартфона чи іншого гаджета, він може перехопити тимчасові коди або доступ до додатків, які використовуються для генерації одноразових паролів.

- Використання скомпрометованого обладнання. При фізичному доступі до комп'ютера чи смартфона можна інсталювати шпигунське ПЗ для перехоплення даних або паролів.

- Експлуатація незахищеного доступу. Зловмисник може скористатися пристроєм, якщо він не заблокований або якщо використовуються слабкі механізми блокування, наприклад, прості PIN-коди чи паролі.

- Викрадення SIM-карти. Доступ до мобільного телефону дає змогу зловмиснику замінити SIM-карту і отримати контроль над SMS-кодами, які часто використовуються як другий фактор.

- Використання апаратних інтерфейсів. Зловмисники можуть підключитися до порту USB для клонування даних або обходу механізмів блокування.

Фізичний доступ до пристрою значно підвищує ризики, тому важливо захищати пристрої багаторівневими методами, наприклад, шифруванням, блокуванням екрану за допомогою надійних паролів та використанням функцій віддаленого блокування чи очищення даних.

Шкідливі браузерні розширення є значною загрозою для безпеки, особливо в контексті двофакторної автентифікації. Ці загрози мають кілька аспектів:

1. Збір даних користувача

Шкідливі розширення можуть перехоплювати дані, введені в браузері, включаючи логіни, паролі та одноразові коди двофакторної автентифікації. Це можливо завдяки широким дозволам, які часто запитують розширення.

2. Фішинг-атаки

Деякі розширення здатні перенаправляти користувача на підроблені веб-сайти, схожі на справжні, щоб викрасти облікові дані або двофакторні коди.

3. Маніпуляція браузерним вмістом

Шкідливі розширення можуть змінювати вигляд і функціонал сторінок, вставляючи шкідливий код, або блокувати справжні елементи двофакторної автентифікації.

4. Захоплення токенів доступу

Деякі розширення можуть перехоплювати сеансові токени, які зберігаються в браузері, дозволяючи атакувальникам обходити двофакторну автентифікацію.

5. Обхід двофакторного захисту

Деякі розширення можуть працювати у зв'язці зі шкідливими програмами, автоматизуючи процес отримання одноразових кодів та передачі їх зловмисникам.

6. Шкідливі оновлення

Навіть на перший погляд безпечні розширення можуть бути скомпрометовані після оновлення, якщо їхній контроль перейде до зловмисників.

Щоб захиститися від подібних загроз, варто дотримуватися рекомендацій.

- Використовувати лише перевірені розширення від відомих розробників.
- Регулярно перевіряти дозволи, надані розширенням.
- Оновлювати розширення через офіційні джерела.
- Застосовувати апаратні ключі для двофакторної автентифікації, оскільки їх важче скомпрометувати.

Соціальна інженерія є значною загрозою навіть при використанні двофакторної автентифікації. Вона передбачає маніпуляцію людьми для отримання доступу до конфіденційної інформації чи облікових записів. Основні методи впливу в цьому контексті включають:

1. Фішинг. Зловмисники створюють підроблені вебсайти або розсилають електронні листи. Вони імітують справжні сервіси і запитують у жертви коди автентифікації, надіслані на телефон або електронну пошту.

2. Вішинг і смішинг. Через телефонні дзвінки (вішинг) або текстові повідомлення (смішинг) шахраї видають себе за співробітників компанії, службу підтримки або навіть банківські установи. Вони переконують жертву надати одноразові коди доступу.

3. Псевдотерміновість. Атаки базуються на створенні ситуацій, які вимагають термінової дії. Наприклад, шахрай стверджує, що обліковий запис буде заблоковано, якщо не підтвердити доступ, надавши код.

4. Імперсонація організацій. Зловмисники можуть імітувати справжні запити від популярних платформ, таких як Google, Facebook або фінансових установ. Це включає повідомлення про незвичну активність або спроби входу.

5. Злом через довіру. Жертву змушують повірити, що атака є технічною перевіркою або частиною легітимного процесу. Таким чином отримуються потрібні дані.

6. Підміна SIM-картки. Використання соціальної інженерії для отримання контролю над SIM-карткою жертви. Це дозволяє зловмисникам перехоплювати SMS із кодами автентифікації.

Ці методи дозволяють обійти механізми двофакторної автентифікації, навіть якщо технічні засоби захисту працюють належним чином. Ефективна протидія включає навчання користувачів основам безпеки, використання альтернативних методів автентифікації (апаратні токени чи біометрія) та обмеження залежності від SMS або електронної пошти.

Відсутність резервного доступу є однією з ключових загроз при двофакторній автентифікації, яка може мати серйозні наслідки для користувачів. Проблема виникає, коли користувач втрачає доступ до одного з факторів автентифікації і не має способу відновити доступ до свого облікового запису. Ця ситуація може виникнути через кілька причин.

Втрата фізичного пристрою. Користувач може втратити телефон, який використовується для отримання кодів автентифікації через SMS, застосунок, або апаратний токен.

Поломка або несправність пристрою. Телефон або інший пристрій можуть зламатися, бути пошкодженими або недоступними через технічні проблеми.

Недоступність резервного коду. Користувач може не зберегти або втратити резервні коди, які зазвичай надаються при налаштуванні двофакторної автентифікації.

Зміна контактної інформації. Наприклад, якщо змінено номер телефону, але нові дані не оновлені в системі автентифікації.

Відсутність резервного доступу створює ризик того, що навіть законний власник облікового запису не зможе повернути контроль над своїми даними. Це може призводити до втрати важливої інформації, фінансових збитків або навіть втрати довіри до сервісу.

Щоб уникнути цієї загрози, необхідно забезпечити кілька рівнів резервного доступу. Це може включати надання резервних кодів, використання додаткових контактних даних, наприклад, електронної пошти, або підтримку можливості верифікації через службу підтримки після проходження суворої перевірки.

Вразливості в апаратних токенах є серйозною загрозою при використанні двофакторної автентифікації. Вони можуть виникати через недоліки в дизайні, реалізації або експлуатації токенів. Можна виділити такі аспекти проблеми.

Фізична компрометація. Апаратний токен можна втратити, викрасти або пошкодити. Зловмисники, отримавши фізичний доступ до токена, можуть спробувати витягти з нього секретну інформацію.

Недоліки прошивки чи апаратного забезпечення. Уразливості в мікропрограмному забезпеченні токенів можуть дозволити зловмисникам використовувати експлойти для отримання доступу до ключів або інших конфіденційних даних.

Атаки на передачу даних. Якщо токен передає дані без належного шифрування, зловмисник може перехопити ці дані через атаки "людина посередині" або інші методи.

Клонування токена. Деякі токени можуть бути клоновані, якщо вони мають слабкі механізми захисту від несанкціонованого копіювання.

Фальшиві токени. Існує ризик підробки токенів або використання шкідливих пристроїв, які імітують функціональність автентифікаційних апаратів.

Соціальна інженерія. Зловмисники можуть обманом змусити користувача передати їм токен або одноразовий код, згенерований пристроєм.

Обмеження сумісності. Деякі токени мають слабкі місця через залежність від застарілих або вразливих стандартів зв'язку, таких як USB або NFC.

Проблеми з керуванням ключами. Недоліки у процедурі створення, зберігання чи оновлення ключів шифрування можуть полегшити доступ до них для зловмисників.

Відсутність оновлень. Якщо виробник не забезпечує регулярні оновлення прошивки, токен залишається вразливим до нових атак.

Для мінімізації ризиків важливо використовувати сучасні токени, регулярно оновлювати їх прошивку, налаштовувати надійні механізми передачі даних і навчати користувачів безпечному поводженню з апаратними пристроями.

Для забезпечення максимального рівня безпеки та захисту приватності при впровадженні системи двофакторної автентифікації необхідно враховувати низку ключових рекомендацій. По-перше, слід використовувати сучасні методи автентифікації, такі як апаратні токени або програми-генератори одноразових кодів, оскільки вони значно зменшують ризик компрометації порівняно зі смс-кодами. По-друге, потрібно забезпечити регулярне оновлення програмного забезпечення і прошивки пристроїв, що використовуються в системі, для усунення можливих вразливостей. По-третє, слід використовувати шифрування для передачі даних між користувачем і системою, щоб запобігти перехопленню або модифікації інформації.

По-четверте, важливо навчати користувачів основам безпеки, зокрема розпізнаванню спроб фішингу, з якими зловмисники можуть виманювати коди або доступ до токенів. По-п’яте, варто запровадити політики управління апаратними пристроями, включаючи можливість їх віддаленого блокування або видалення даних у разі втрати чи крадіжки. По-шосте, необхідно забезпечити контроль доступу до критично важливих систем і застосувати методи багаторівневого захисту для особливо чутливих даних. По-сьоме, слід періодично проводити аудит безпеки системи для виявлення потенційних слабких місць та забезпечення відповідності актуальним стандартам кібербезпеки.

Крім того, доцільно використовувати унікальні токени чи коди для кожного пристрою або сесії, щоб зменшити ризик повторного використання скомпрометованих даних. Також важливо забезпечити наявність резервних способів автентифікації для відновлення доступу, не створюючи при цьому

додаткових ризиків. У підсумку, інтеграція двофакторної автентифікації має супроводжуватися постійним моніторингом і вдосконаленням системи для реагування на нові загрози та забезпечення високого рівня приватності.

2.3 Стандарти та регулювання

Системи двофакторної автентифікації регулюються низкою міжнародних стандартів і нормативних вимог, які забезпечують високий рівень захисту інформації, особливо в умовах зростаючих кіберзагроз. Одним із ключових стандартів є ISO 27001, що встановлює вимоги до систем управління інформаційною безпекою і спрямований на забезпечення конфіденційності, цілісності та доступності інформації. Цей стандарт передбачає впровадження належних технічних і організаційних заходів контролю доступу, зокрема багатофакторної автентифікації, яка захищає інформаційні системи від несанкціонованого доступу. Він підкреслює важливість інтеграції таких механізмів у загальну стратегію управління ризиками.

У рамках рекомендацій NIST, зокрема документа NIST SP 800-63, надаються докладні інструкції щодо реалізації цифрової автентифікації. Цей стандарт класифікує автентифікаційні механізми за рівнями впевненості, де багатофакторна автентифікація є необхідною для забезпечення високого рівня довіри. Він також рекомендує використовувати комбінацію різних факторів, таких як знання (паролі), володіння (апаратні токени) і біометричні дані, для мінімізації ризиків компрометації облікових записів.

Регламент GDPR, який регулює обробку персональних даних у країнах Європейського Союзу, вимагає від організацій впровадження відповідних технічних і організаційних заходів безпеки. Двофакторна автентифікація розглядається як ефективний спосіб захисту персональних даних від несанкціонованого доступу, оскільки забезпечує додатковий рівень захисту навіть у разі компрометації пароля. GDPR акцентує на необхідності зменшення ризиків

витоку конфіденційної інформації, зокрема шляхом використання надійних механізмів автентифікації.

У США такі регулятивні вимоги, як HIPAA, спрямовані на захист медичних даних і передбачають обов'язкове впровадження процедур автентифікації користувачів, які працюють з чутливими системами охорони здоров'я. Вимоги HIPAA включають заходи щодо захисту інформації, такі як двофакторна автентифікація, яка значно ускладнює несанкціонований доступ до електронних медичних записів. У фінансовій сфері директива PSD2, що діє в ЄС, вимагає від фінансових установ застосування сильної клієнтської автентифікації для проведення онлайн-транзакцій і управління доступом до банківських систем. Це означає, що клієнти повинні підтверджувати свою особу за допомогою щонайменше двох незалежних факторів.

Додатково стандарти PCI DSS, що регулюють безпеку обробки платіжних даних, також зобов'язують організації застосовувати двофакторну автентифікацію для адміністраторів та користувачів, які мають доступ до систем, де обробляються платіжні дані. Це необхідно для зменшення ризику компрометації облікових записів та запобігання шахрайству. Cybersecurity Framework, розроблений NIST, акцентує увагу на інтеграції багатофакторної автентифікації в системи управління доступом як одного з найбільш ефективних методів забезпечення безпеки. Цей підхід особливо важливий для організацій, які обробляють критично важливу інформацію, оскільки він забезпечує додатковий рівень захисту навіть у випадку компрометації інших заходів безпеки.

Окрім цього, локальні стандарти багатьох країн також включають вимоги щодо використання двофакторної автентифікації для захисту державних систем, електронного уряду та критичних інфраструктур. Зокрема, в багатьох випадках передбачено впровадження апаратних токенів або біометричних систем автентифікації, які забезпечують більш високий рівень безпеки. Усі ці стандарти та регулятивні вимоги спрямовані на впровадження комплексного підходу до захисту інформаційних систем, використовуючи двофакторну автентифікацію як одну з ключових технологій для запобігання сучасним загрозам.

2.4 Висновки

У розділі представлено аналіз сучасних підходів до реалізації двофакторної автентифікації (2FA) як одного з ключових інструментів забезпечення кібербезпеки. Основну увагу приділено протоколам OpenID Connect, OAuth 2.0 та SAML, що є базовими для інтеграції систем багатофакторної автентифікації у веб-додатки, мобільні системи та корпоративні мережі. Зроблено акцент на архітектурних особливостях і основних етапах функціонування кожного протоколу, включно з механізмами передачі маркерів доступу та забезпеченням захисту даних користувачів.

Окремо розглянуто проблеми, що супроводжують впровадження двофакторної автентифікації в сучасних умовах. Серед ключових викликів виділено фішинг, перехоплення кодів автентифікації, атаки "людина посередині" та ризики, пов’язані з фізичним доступом до пристроїв. Детально проаналізовано сценарії, у яких навіть сучасні технології автентифікації можуть бути вразливими до дій зловмисників через неправильне налаштування систем або використання застарілих методів. Зроблено висновок, що вирішення цих проблем вимагає комплексного підходу, який включає як технологічні, так і організаційні заходи.

У дослідженні підкреслено переваги сучасних методів двофакторної автентифікації, таких як апаратні токени з підтримкою протоколу FIDO2, які забезпечують високий рівень захисту завдяки використанню криптографії. Наведено рекомендації щодо інтеграції багатофакторної автентифікації, орієнтовані на зменшення ризиків компрометації. Наголошено на важливості дотримання міжнародних стандартів, таких як ISO 27001 та NIST SP 800-63, які регламентують підходи до автентифікації користувачів.

3 РЕАЛІЗАЦІЯ СИСТЕМИ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

3.1 Архітектура та компоненти системи

Система двофакторної авторизації сайту складається з кількох основних компонентів, кожен із яких виконує специфічні завдання. Основною метою цієї системи є забезпечення високого рівня безпеки користувацьких даних та запобігання несанкціонованому доступу рис. 3.1.

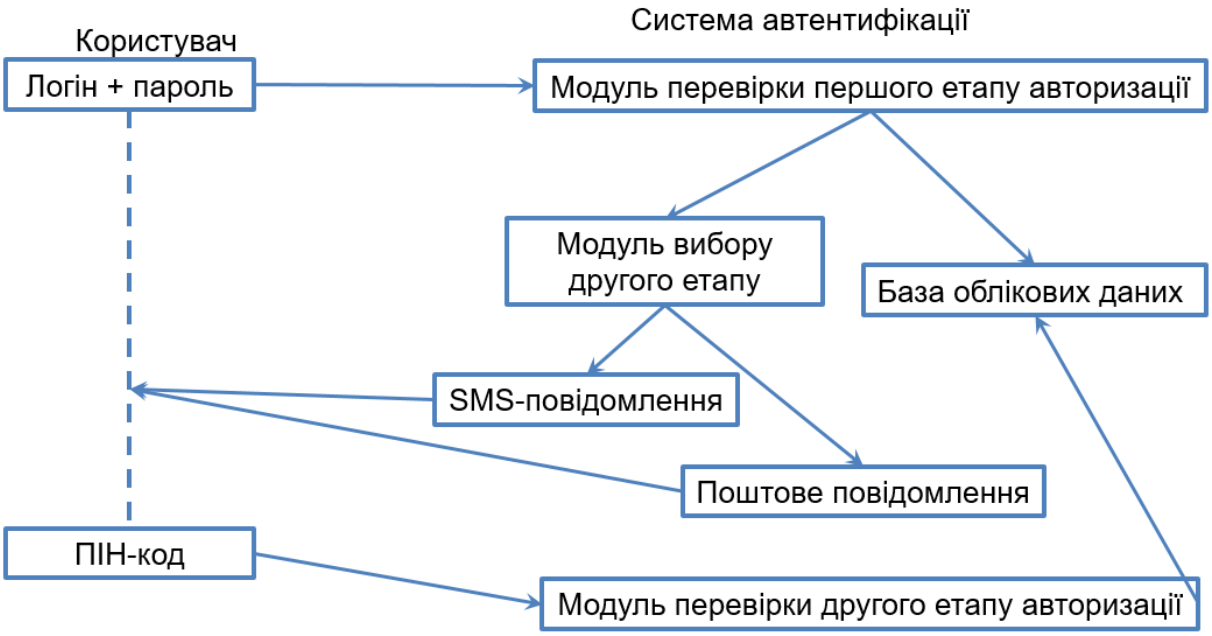


Рисунок 3.1 Система двофакторної авторизації сайту

Компоненти системи:

1. Модуль обробки облікових записів. Відповідає за зберігання даних користувачів, включаючи їхні ідентифікатори, паролі, електронну пошту або номери телефонів. Виконує функції аутентифікації першого рівня, зокрема перевірку правильності введених логіну та пароля.

Модуль забезпечує:

– Отримання введених користувачем даних для первинної аутентифікації.
– Перевірка логіну та пароля за базою даних.
– Ініціалізація другого етапу авторизації.

Функції, реалізовані в модулі:

– Зберігання даних користувачів, включаючи логін, хеш пароля, електронну пошту або номер телефону.
– Перевірка правильності введених логіну та пароля під час аутентифікації.
– Управління ролями користувачів для визначення їхніх прав доступу.
– Підтримка операцій зі скидання пароля (ініціація зміни пароля та перевірка токену для його відновлення).
– Забезпечення збереження та оновлення даних облікових записів.

2. Модуль генерації кодів автентифікації. Відповідальний за створення одноразових кодів доступу (OTP). Використовує криптографічні алгоритми для генерації кодів, які мають обмежений термін дії.

Модуль забезпечує:

– Генерація криптографічно захищеного OTP-коду.
– Збереження коду разом із міткою часу в базі даних.

Функції, реалізовані в модулі:

– Генерація криптографічно захищених OTP-кодів з використанням алгоритмів HMAC або TOTP.
– Збереження OTP-коду в базі даних разом із міткою часу створення.
– Забезпечення унікальності коду для кожного сеансу.
– Визначення терміну дії кожного згенерованого коду.

3. Модуль сповіщень. Забезпечує доставку OTP-кодів користувачу за допомогою SMS, електронної пошти або через мобільні додатки. Контролює коректність доставки повідомлення, а також час його отримання.

Модуль забезпечує:

– Формування повідомлення з кодом доступу.
– Надсилання повідомлення користувачу через вибраний канал.

Функції, реалізовані в модулі:

– Формування повідомлення з OTP-кодом або іншими інструкціями.

– Надсилання повідомлень через електронну пошту, SMS, месенджери або пуш-сповіщення.
– Перевірка статусу доставки повідомлень.
– Логування процесу надсилання для забезпечення аудиту.

4. Модуль перевірки. Верифікує введений користувачем код автентифікації. Виконує перевірку терміну дії коду, а також його відповідності збереженому значенню.

Модуль забезпечує:

– Отримання введеного коду від користувача.
– Перевірка відповідності отриманого коду збереженому.
– Аналіз терміну дії коду.

Функції, реалізовані в модулі:

– Отримання коду автентифікації від користувача через інтерфейс системи.
– Перевірка відповідності введеного коду збереженому значенню.
– Валідація терміну дії OTP-коду.
– Інформування центрального модуля управління про результат перевірки.

5. Модуль інтерфейсу. Забезпечує взаємодію користувача із системою через веб-інтерфейс або мобільний додаток. Відображає повідомлення про помилки, етапи автентифікації та підтвердження успішного входу.

Модуль забезпечує:

– Відображення форм для введення даних користувача.
– Інформування про статус автентифікації.

Функції, реалізовані в модулі:

– Відображення форми для введення логіну та пароля на першому етапі авторизації.
– Показ інтерфейсу для введення OTP-коду на другому етапі.
– Інформування користувача про успішну автентифікацію або помилки в процесі.
– Налаштування елементів інтерфейсу відповідно до вимог брендування.

6. Центральний модуль управління. Координує взаємодію між іншими компонентами системи. Зберігає журнали дій для забезпечення аудиту та моніторингу безпеки.

Модуль забезпечує:

– Логування дій користувача та системних подій.
– Передача даних між модулями.
– Надання системного доступу після успішної перевірки.

Функції, реалізовані в модулі:

– Контроль послідовності виконання операцій між модулями (обробка запиту, перевірка, верифікація).
– Логування всіх дій користувача та системних подій.
– Верифікація стану кожного модуля перед початком сесії.
– Надання доступу до ресурсу після успішного завершення всіх етапів авторизації.
– Аналіз журналів дій для виявлення аномальної активності.

Запропонована структура забезпечує надійність процесу двофакторної авторизації та дозволяє адаптувати систему до різних сценаріїв використання, чітке розділення функцій між модулями, що дозволяє легко масштабувати систему, підвищувати її безпеку та адаптивність до нових вимог.

3.2 UML-діаграма класів

Подамо UML-діаграму, на якій зображено структуру системи автентифікації, що складається з п'яти класів і взаємозв'язків між ними.

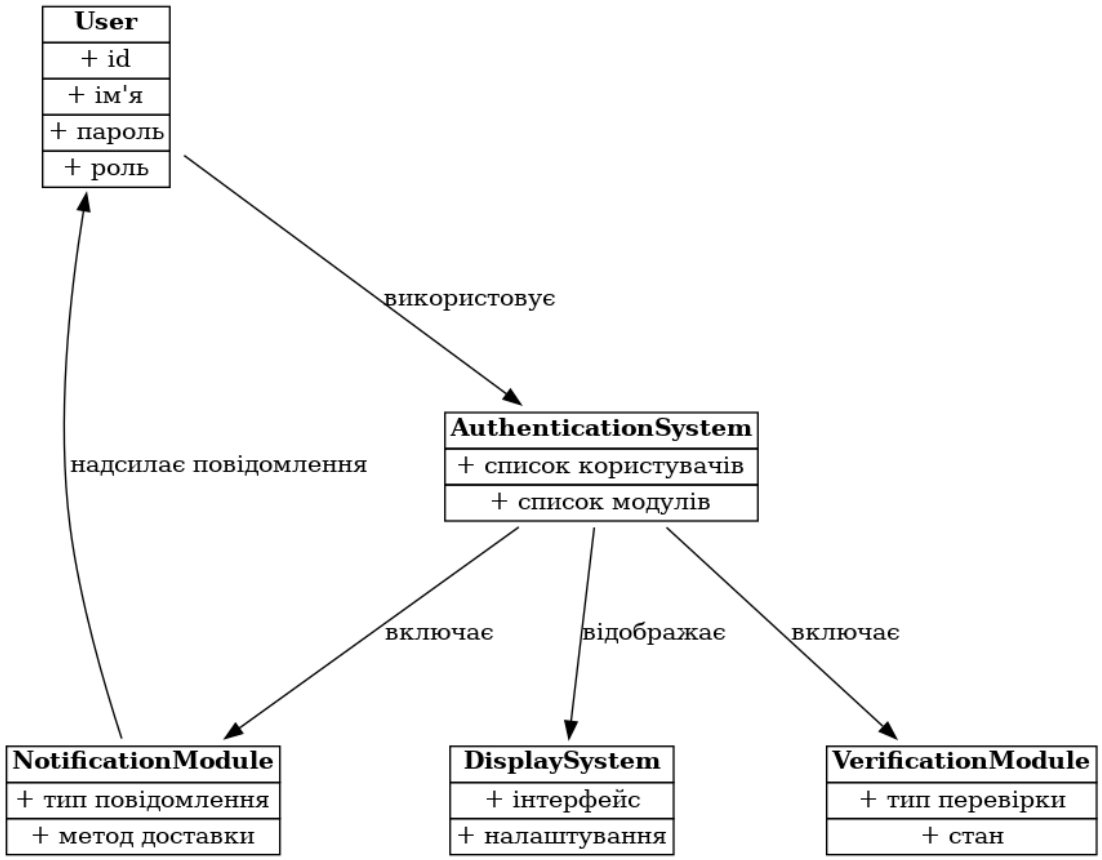


Рисунок 3.2 UML-діаграма системи двофакторної авторизації сайту

Опис ключових компонентів:

1. User (Користувач):

Атрибути:

– `+ id` — унікальний ідентифікатор користувача.

– `+ ім'я` — ім'я користувача.

– `+ пароль` — пароль для автентифікації.

– `+ роль` — роль, яка визначає рівень доступу.

Клас взаємодіє із системою автентифікації, використовуючи її для авторизації.

2. AuthenticationSystem (Система автентифікації):

Атрибути:

– `+ список користувачів` — перелік зареєстрованих користувачів.

– `+ список модулів` — перелік інтегрованих модулів.

Основний клас, який забезпечує автентифікацію користувачів і управління модулями системи. Використовується класом `User` для авторизації. Включає три додаткові модулі: NotificationModule, DisplaySystem, VerificationModule.

3. NotificationModule (Модуль сповіщень):

Атрибути:

– `+ тип повідомлення` — тип повідомлень, які надсилаються користувачеві (наприклад, SMS, email).

– `+ метод доставки` — механізм надсилання повідомлень.

Забезпечує функцію надсилання повідомлень від системи автентифікації до користувача.

4. DisplaySystem (Система відображення):

Атрибути:

– `+ інтерфейс` — опис інтерфейсу для взаємодії з користувачем.

– `+ налаштування` — параметри налаштування відображення.

Відповідає за візуалізацію даних, пов'язаних із автентифікацією.

5. VerificationModule (Модуль перевірки):

Атрибути:

– `+ тип перевірки` — механізм верифікації (наприклад, пароль, двофакторна автентифікація).

– `+ стан` — поточний стан перевірки (успішно чи ні).

Відповідає за виконання основних процедур автентифікації.

Зв'язки між класами:

– `User` використовує `AuthenticationSystem`.

– `AuthenticationSystem` включає `NotificationModule`, `DisplaySystem` і `VerificationModule`.

– `AuthenticationSystem` надсилає повідомлення через `NotificationModule`.

– `AuthenticationSystem` відображає інформацію через `DisplaySystem`.

Дана діаграма демонструє взаємодію класів, що забезпечують комплексну систему автентифікації з підтримкою сповіщень, верифікації та відображення даних.

3.3 Розробка системи

Розробка системи двофакторної авторизації потребує поетапного підходу, який забезпечить надійність, безпеку та відповідність функціональним вимогам. Процес розробки включає декілька ключових етапів, які необхідно виконати в суворій послідовності.

Перший етап полягає в аналізі вимог. На цьому етапі визначаються основні функціональні та нефункціональні вимоги до системи. До функціональних належать автентифікація користувача, генерація одноразових кодів, надсилання повідомлень та їхня верифікація. Нефункціональні вимоги включають захист від несанкціонованого доступу, високу доступність, масштабованість та відповідність нормативним стандартам безпеки, таким як GDPR або PCI DSS. Також визначається набір підтримуваних каналів зв’язку, наприклад електронна пошта, SMS або мобільні застосунки.

Другий етап — проектування архітектури системи. На цьому етапі створюється UML-діаграма класів, яка відображає структуру системи. Визначаються ключові компоненти, такі як модуль обробки облікових записів, модуль генерації кодів, модуль сповіщень, модуль верифікації та модуль інтерфейсу. У кожного модуля визначаються відповідні методи та взаємодії між компонентами. Обираються технології для розробки серверної частини (Java), бази даних для зберігання інформації про користувачів (MySQL) та протоколи для захисту передачі даних (TLS/SSL).

Третій етап полягає у розробці компонентів системи. Реалізація починається з модуля обробки облікових записів, який відповідає за управління користувачами та їхніми даними. Потім розробляється модуль генерації одноразових кодів, що забезпечує криптографічно захищену генерацію OTP. Після цього створюється

модуль сповіщень, який інтегрується з API для надсилання SMS або електронних листів. Модуль верифікації забезпечує перевірку коректності введених кодів та контроль їхнього терміну дії. Модуль інтерфейсу організовує взаємодію з користувачем, відображаючи необхідну інформацію та реагуючи на введені дані.

Четвертий етап включає інтеграцію компонентів. На цьому етапі компоненти об'єднуються у єдину систему. Впроваджується центральний модуль управління, який координує роботу між іншими модулями. Перевіряється, чи коректно відбувається взаємодія між модулями, включаючи передачу даних між модулем обробки облікових записів і модулем генерації кодів, а також доставку повідомлень через модуль сповіщень.

П'ятий етап передбачає тестування. Для перевірки функціональності розробляються юніт-тести, які охоплюють кожен модуль. Тестування включає сценарії коректної авторизації, некоректного вводу даних, обробки помилок, перевірки безпеки та масштабованості. Також проводиться інтеграційне тестування для перевірки взаємодії між компонентами. Особлива увага приділяється безпеці, зокрема тестуванню на проникнення для виявлення потенційних вразливостей.

Шостий етап — деплоймент та впровадження. Система розгортається у тестовому середовищі для остаточної перевірки. Після цього проводиться міграція у продуктивне середовище. Забезпечується налаштування моніторингу для відстеження роботи системи, включаючи обробку помилок, продуктивність та час відповіді.

Останній етап — підтримка та оновлення. Після впровадження здійснюється постійний моніторинг роботи системи для забезпечення її стабільності. У разі необхідності додаються нові функції, оптимізуються існуючі модулі або виправляються знайдені недоліки. Також проводиться регулярне оновлення компонентів для захисту від нових загроз.

Послідовне виконання зазначених етапів забезпечує створення ефективної, безпечної та масштабованої системи двофакторної авторизації, що відповідає сучасним вимогам.

3.4 Впровадження системи двофакторної авторизації

Етапи впровадження системи двофакторної авторизації мають чітку структуру, яка забезпечує її плавну інтеграцію в існуючу інфраструктуру з мінімальними ризиками для безпеки та доступності. Успішне впровадження вимагає послідовного виконання наступних кроків.

Першим етапом є підготовка інфраструктури. Визначаються технічні вимоги до серверів, баз даних, мережевого обладнання та програмного забезпечення. На цьому етапі встановлюються та налаштовуються сервери для розгортання системи. Забезпечується ізоляція середовища для двофакторної авторизації з метою мінімізації впливу на інші компоненти інформаційної системи. Також проводиться аналіз сумісності нової системи з існуючими рішеннями, зокрема перевірка інтеграції з базами даних користувачів та корпоративними службами каталогів, такими як Active Directory.

Другий етап включає початкову конфігурацію системи. Установлюється програмне забезпечення, що реалізує двофакторну авторизацію. Проводиться налаштування бази даних для збереження інформації про користувачів, їхні автентифікаційні дані та історію верифікації. Конфігуруються канали доставки повідомлень, такі як SMS-шлюзи, поштові сервери або API мобільних застосунків. Налаштовуються алгоритми генерації одноразових кодів з урахуванням безпеки та сумісності зі стандартами, такими як TOTP (Time-Based One-Time Password) або HOTP (HMAC-Based One-Time Password).

Третій етап передбачає інтеграцію системи з існуючими сервісами. Впроваджується підтримка двофакторної авторизації у веб-застосунках, мобільних клієнтах та інших інструментах, які використовуються користувачами. Для цього додаються відповідні програмні інтерфейси (API), через які нова система здійснює перевірку користувачів. Проводиться оновлення інтерфейсу користувача для забезпечення можливості вводу одноразового коду після введення основного пароля. Також інтегрується модуль керування користувачами, що дозволяє адміністраторам додавати, видаляти чи блокувати акаунти.

Четвертий етап включає тестування інтеграції. Система впроваджується у тестовому середовищі, яке повністю імітує робочі умови. Виконуються сценарії автентифікації, що охоплюють як стандартні, так і виняткові ситуації. Зокрема, перевіряється обробка некоректних кодів, перевищення ліміту спроб входу та робота з різними каналами доставки повідомлень. Особливу увагу приділяють перевірці часу відповіді системи, стабільності її роботи під навантаженням та відповідності стандартам безпеки.

П'ятий етап — поетапне впровадження у продуктивне середовище. Система активується для невеликої групи користувачів, наприклад, адміністративного персоналу чи підрозділу технічної підтримки. Це дозволяє виявити можливі проблеми та адаптувати систему до реальних умов. На основі відгуків вносяться зміни у налаштування або функціонал. Після успішного завершення цього етапу відбувається поступове розширення доступу до системи для інших користувачів.

Шостий етап передбачає навчання користувачів. Розробляються інструкції для співробітників, які пояснюють принципи роботи двофакторної авторизації, порядок входу в систему та способи відновлення доступу у разі втрати можливості пройти перевірку. Також проводяться навчальні сесії для адміністративного персоналу, які охоплюють керування користувачами, моніторинг роботи системи та реагування на інциденти.

Сьомий етап включає налаштування моніторингу та управління. Впроваджується система збору журналів, яка дозволяє відстежувати спроби входу, використання кодів та роботу каналів доставки повідомлень. Встановлюються пороги для автоматичного сповіщення адміністрації у разі виявлення підозрілої активності, такої як надмірна кількість невдалих спроб входу чи одночасний доступ з різних географічних регіонів. Забезпечується резервне копіювання критичних даних, включаючи журнали та базу користувачів.

Останній етап — повномасштабне впровадження та підтримка. Система активується для всіх користувачів. Проводиться постійний моніторинг її роботи для забезпечення стабільності та продуктивності. У разі необхідності вносяться корективи у конфігурацію чи додаються нові функції. Також впроваджується

регулярне оновлення компонентів системи для захисту від потенційних вразливостей та відповідності сучасним стандартам безпеки.

Ця послідовність етапів дозволяє не лише ефективно впровадити систему двофакторної авторизації, але й забезпечити її довгострокову надійність та відповідність вимогам користувачів і організації.

3.5 Висновки

У розділі представлено розробку системи двофакторної авторизації сайту, що включає аналіз її архітектури, опис основних компонентів, а також етапи реалізації та впровадження. Зокрема, було запропоновано структуру системи, яка складається з модулів обробки облікових записів, генерації кодів автентифікації, сповіщень, перевірки, інтерфейсу та центрального модуля управління. Для кожного компонента детально описано його функціональність і роль у загальній архітектурі.

У процесі розробки розглянуто поетапний підхід, який включає аналіз вимог, проектування UML-діаграм, реалізацію програмних модулів, інтеграцію компонентів та тестування. Це забезпечило створення системи з високим рівнем безпеки, адаптивності та масштабованості. Крім того, запропоновано етапи впровадження, які охоплюють підготовку інфраструктури, початкову конфігурацію, інтеграцію з існуючими сервісами, тестування, поетапний запуск у продуктивне середовище, навчання користувачів і налаштування моніторингу.

Розроблена система дозволяє ефективно захищати доступ до ресурсів, використовуючи двофакторну автентифікацію як базовий механізм. Вона забезпечує надійну перевірку користувачів через комбінацію первинного пароля та одноразового коду, що надсилається безпечними каналами. Впровадження запропонованої системи підвищує загальний рівень інформаційної безпеки, знижує ризик несанкціонованого доступу та створює гнучкі можливості для подальшої інтеграції з іншими сервісами.

ВИСНОВКИ

Автором в процесі виконання кваліфікаційної роботи було розроблено систему двофакторної авторизації.

У роботі проаналізовано концепцію, методи та протоколи двофакторної автентифікації, а також виявлено основні проблеми, пов’язані з її впровадженням. Особливу увагу приділено огляду існуючих рішень, включаючи методи першого і другого факторів автентифікації, а також мультифакторні системи. Описано стандарти, які забезпечують інтеграцію двофакторної автентифікації з сучасними системами. На основі проведеного аналізу розроблено архітектуру системи, яка включає ключові компоненти: модуль обробки облікових записів, генерації одноразових кодів, сповіщень, верифікації та інтерфейсу.

Робота містить UML-діаграму, яка детально ілюструє взаємодію між компонентами системи. Реалізовано опис основних етапів розробки, включаючи вибір криптографічних алгоритмів, налаштування каналів зв’язку та інтеграцію з базою даних. Важливим аспектом є впровадження багаторівневого тестування для забезпечення безпеки та стабільності. Крім цього, запропоновано покроковий план впровадження системи в реальне середовище, що включає інтеграцію, налаштування моніторингу та навчання користувачів.

Результатом роботи стала система, що забезпечує підвищений рівень безпеки доступу до інформаційних ресурсів. Її впровадження дозволяє мінімізувати ризики несанкціонованого доступу, зокрема шляхом запобігання фішинговим атакам, компрометації паролів та соціальній інженерії. Водночас система є масштабованою та адаптованою для інтеграції з іншими сервісами, що підвищує її ефективність у корпоративних середовищах. Запропоноване рішення поєднує безпеку, зручність використання та відповідність сучасним стандартам, що є важливим для задоволення вимог організацій у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Website Rating[Електронний ресурс]. Режим доступу: https://www.websiterating.com/research/internet-statistics-facts/

2. Chen, F., Zhao, B., Gao, Y. et al. BTDA: Two-factor dynamic identity authentication scheme for data trading based on alliance chain. J Supercomput 79, 19118–19137 (2023). https://doi.org/10.1007/s11227-023-05393-y

3. W3Techs[Електронний ресурс]. Режим доступу: https://w3techs.com/technologies/overview/content_management

4. Kolomiitsev, S., Sievierinov O., Fedorchenko, V., & Sukhoteplyi, V. (2023). Analysis of two-factor authentication plugins for WordPress. Radiotekhnika, 3(214), 26–31. https://doi.org/10.30837/rt.2023.3.214.03

5. Al-saggaf, A.A., Sheltami, T., Alkhzaimi, H. et al. Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing. Arab J Sci Eng 48, 2347–2357 (2023). https://doi.org/10.1007/s13369-022-07235-0

6. Website Rating [Електронний ресурс]. Режим доступу:https://www.websiterating.com/research/cybersecurity-statistics-facts/

7. Lavanya, S., Saravanakumar, N.M. Secured two factor authentication, graph based replication and encryption strategy in cloud computing. Multimed Tools Appl 82, 16105–16125 (2023). https://doi.org/10.1007/s11042-022-13838-4

8. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі //Системи обробки інформації. 2015. No9. С.101–104.

9. Sengupta, A., Singh, A., Kumar, P. et al. A secure and improved two factor authentication scheme using elliptic curve and bilinear pairing for cyber physical systems. Multimed Tools Appl 81, 22425–22448 (2022). https://doi.org/10.1007/s11042-022-12227-1

10. DeveloperWordPress[Електронний ресурс] Режим доступу: https://developer.wordpress.org/plugins/intro/what-is-a-plugin/

11. Asadianfam, S., Talebi, M.J. & Nikougoftar, E. ECG-based authentication systems: a comprehensive and systematic review. Multimed Tools Appl 83, 27647–27701 (2024). https://doi.org/10.1007/s11042-023-16506-3

12. Репозиторій плагінів WordPress [Електронний ресурс].Режим доступу: https://wordpress.org/plugins/

13. Bao, D., You, L. Two-factor identity authentication scheme based on blockchain and fuzzy extractor. Soft Comput 27, 1091–1103 (2023). https://doi.org/10.1007/s00500-021-05936-6

14. Wordpress Codex [Електроний ресурс].Режим доступа: https://codex.wordpress.org/Main_Page

15. Sudha, M.N., Rajendiran, M., Specht, M. et al. A low-area design of two-factor authentication using DIES and SBI for IoT security. J Supercomput 78, 4503–4525 (2022). https://doi.org/10.1007/s11227-021-04022-w

16. AyoadeO., AfolabiA. S., AwelewaA. T.A Review of Two Factor Authentication//International Journal of Computer Science and Information Security.2018.Vol.16, no. 6.P. 35–42,

17. Radha, S., Jeyalaksshmi, S. Deterministic Hash and Linear Congruential BlowFish Extreme Learning for User Authentication in Cloud Computing. SN COMPUT. SCI. 4, 796 (2023). https://doi.org/10.1007/s42979-023-02155-8

18. Аналіз плагінів двофакторної автентифікації для системи WordPress / С. О. Коломійцев, О. В. Сєвєрінов, В. М. Федорченко, В. М. Сухотеплий // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2023. – Вип. 214. – С. 26–31. – DOI: 10.30837/rt.2023.3.214.03.

19. Khan, H.U., Sohail, M., Nazir, S. et al. Role of authentication factors in Fin-tech mobile transaction security. J Big Data 10, 138 (2023). https://doi.org/10.1186/s40537-023-00807-3

20. T. Musa et al. Analysis of Complex Networks for Security Issues using Attack Graph. International Conference on Computer Communication and Informatics (ICCCI). 2019. PP. 1-6. DOI: 10.1109/ICCCI.2019.8822179.

21. Tyagi, G., Kumar, R. An efficient user authentication and key agreement scheme for wireless sensor networks using physically unclonable function. Int. J. Inf. Secur. 23, 935–962 (2024). https://doi.org/10.1007/s10207-023-00770-3

22. B. Vaishnavi, D. Savant, D. Rupali, A. Kasar. A Review on Network Security and Cryptography. Research Journal of Engineering and Technology. 2021. Vol. 12, No. 4. DOI: 10.52711/2321-581X.2021.00019

23. Gomes, D.R., Lins, F.A.A., Nóbrega, O.O. et al. Security Evaluation of Authentication Requirements in IoT Gateways. J Netw Syst Manage 31, 67 (2023). https://doi.org/10.1007/s10922-023-09754-z

24. O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, E. O. Asani. Modified Advanced Encryption Standard Algorithm for Information Security. Symmetry. 2019. Vol. 11. DOI: https://doi.org/10.3390/sym11121484

25. Puthiyidam, J.J., Joseph, S. & Bhushan, B. Enhanced authentication security for IoT client nodes through T-ECDSA integrated into MQTT broker. J Supercomput 80, 8898–8932 (2024). https://doi.org/10.1007/s11227-023-05789-w

26. Amarudin, R. Ferdiana, Widyawan. A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods. 4th International Conference on Informatics and Computational Sciences (ICICoS). 2020. PP. 1-6. DOI: 10.1109/ICICoS51170.2020.9299068

27. Nikooghadam, M., Amintoosi, H. & Shahriari, H.R. REACH: Robust Efficient Authentication for Crowdsensing-based Healthcare. J Supercomput 80, 8434–8468 (2024). https://doi.org/10.1007/s11227-023-05749-4

28. I. A. Khan, D. Pi, N. Khan. A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks. Appl Intell. 2021. Vol. 51. PP. 7306–7321. DOI: https://doi.org/10.1007/s10489-021-02222-8

29. Uppuluri, S., Lakshmeeswari, G. Secure multiparty access and authentication based on advanced fuzzy extractor in smart home. Soft Comput 28, 4899–4914 (2024). https://doi.org/10.1007/s00500-023-09182-w

30. Arwa Aldweesh, Abdelouahid Derhab, Ahmed Z. Emam. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and

open issues. Knowledge-Based Systems. 2020. Vol. 189. DOI: https://doi.org/10.1016/j.knosys.2019.105124

31. Kaliya, N., Pawar, D. Unboxing fog security: a review of fog security and authentication mechanisms. Computing 105, 2793–2819 (2023). https://doi.org/10.1007/s00607-023-01208-3

32. M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, M. Ma. Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics. IEEE Access. 2019. Vol. 7. PP. 158481-158491. DOI: 10.1109/ACCESS.2019.2945682

33. Ma, Y., Shi, W., Li, X. et al. Provable secure authentication key agreement for wireless body area networks. Front. Comput. Sci. 18, 185811 (2024). https://doi.org/10.1007/s11704-023-2548-4

34. K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, M. Xu. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access. 2020. Vol. 8. PP. 222310-222354. DOI: 10.1109/ACCESS.2020.3041951

35. Kumari, D., Singh, K. Lightweight secure authentication and key agreement technique for smart grid. Peer-to-Peer Netw. Appl. 17, 451–478 (2024). https://doi.org/10.1007/s12083-023-01585-8

36. W. Wang, J. Song, G. Xu, Y. Li, H. Wang, C. Su. ContractWard: Automated Vulnerability Detection Models for Ethereum Smart Contracts. IEEE Transactions on Network Science and Engineering. 2021. Vol. 8, No. 2. PP. 1133-1144. DOI: 10.1109/TNSE.2020.2968505

37. Fanfakh, A., Noura, H. & Couturier, R. Simultaneous encryption and authentication of messages over GPUs. Multimed Tools Appl 83, 4757–4789 (2024). https://doi.org/10.1007/s11042-023-15451-5

38. W. Dimitrov, B. Jekov, E. Kovatcheva, L. Petkova. AN ANALYSIS OF THE NEW CHALLENGES FACING CYBER SECURITY EXPERTISE. 12th International Conference on Education and New Learning. 2020. PP. 2978-2986. DOI: 10.21125/edulearn.2020.0890

39. Tu, Z., Zhou, H., Li, K. et al. Blockchain-based differentiated authentication mechanism for 6G heterogeneous networks. Peer-to-Peer Netw. Appl. 16, 727–748 (2023). https://doi.org/10.1007/s12083-022-01437-x

40. Ikuobase Emovon, Okpako Stephen Oghenenyerovwho. Application of MCDM method in material selection for optimal design: A review. Results in Materials. 2020. Vol. 7. DOI: https://doi.org/10.1016/j.rinma.2020.100115

41. Hussan, M., Parah, S.A. & Qureshi, G.J. Reversible data hiding framework with content authentication capability for e-health. Multimed Tools Appl 83, 35335–35353 (2024). https://doi.org/10.1007/s11042-023-17019-9

42. Gang Kou, Pei Yang, Yi Peng, Feng Xiao, Yang Chen, Fawaz E. Alsaadi. Evaluation of feature selection methods for text classification with small datasets using multiple criteria decision-making methods. Applied Soft Computing. 2020. Vol. 86. DOI: https://doi.org/10.1016/j.asoc.2019.105836

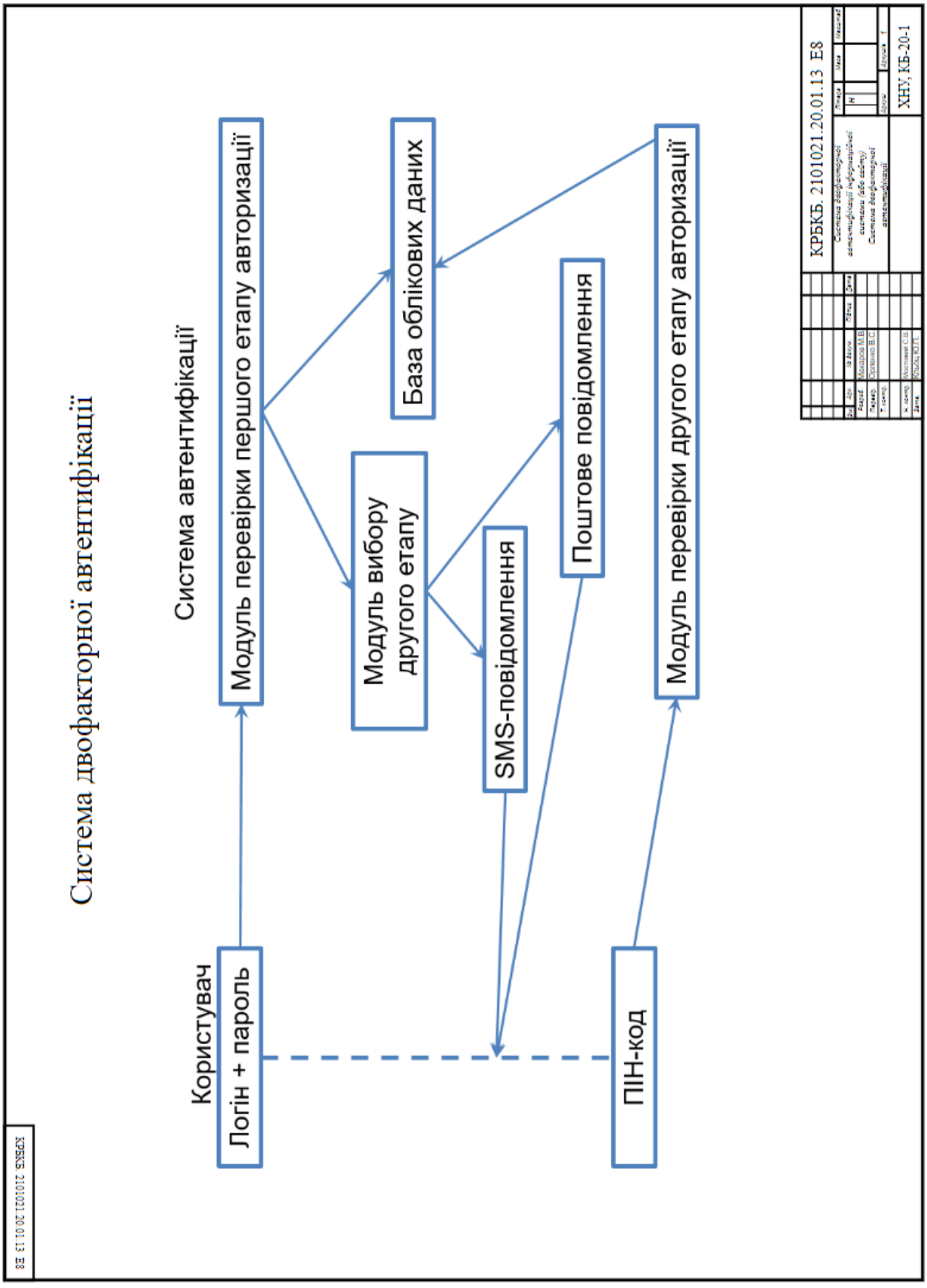
43. Elsheikh, A.G., El-Banby, G.M., Elazm, A.A. et al. Application of MACE filter with DRPE for cancelable biometric authentication. J Opt 53, 101–116 (2024). https://doi.org/10.1007/s12596-023-01172-3

44. Atif Ahmad, Jeb Webb, Kevin C. Desouza, James Boorman. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. Computers & Security. 2019. Vol. 86. PP. 402-418. DOI: https://doi.org/10.1016/j.cose.2019.07.001

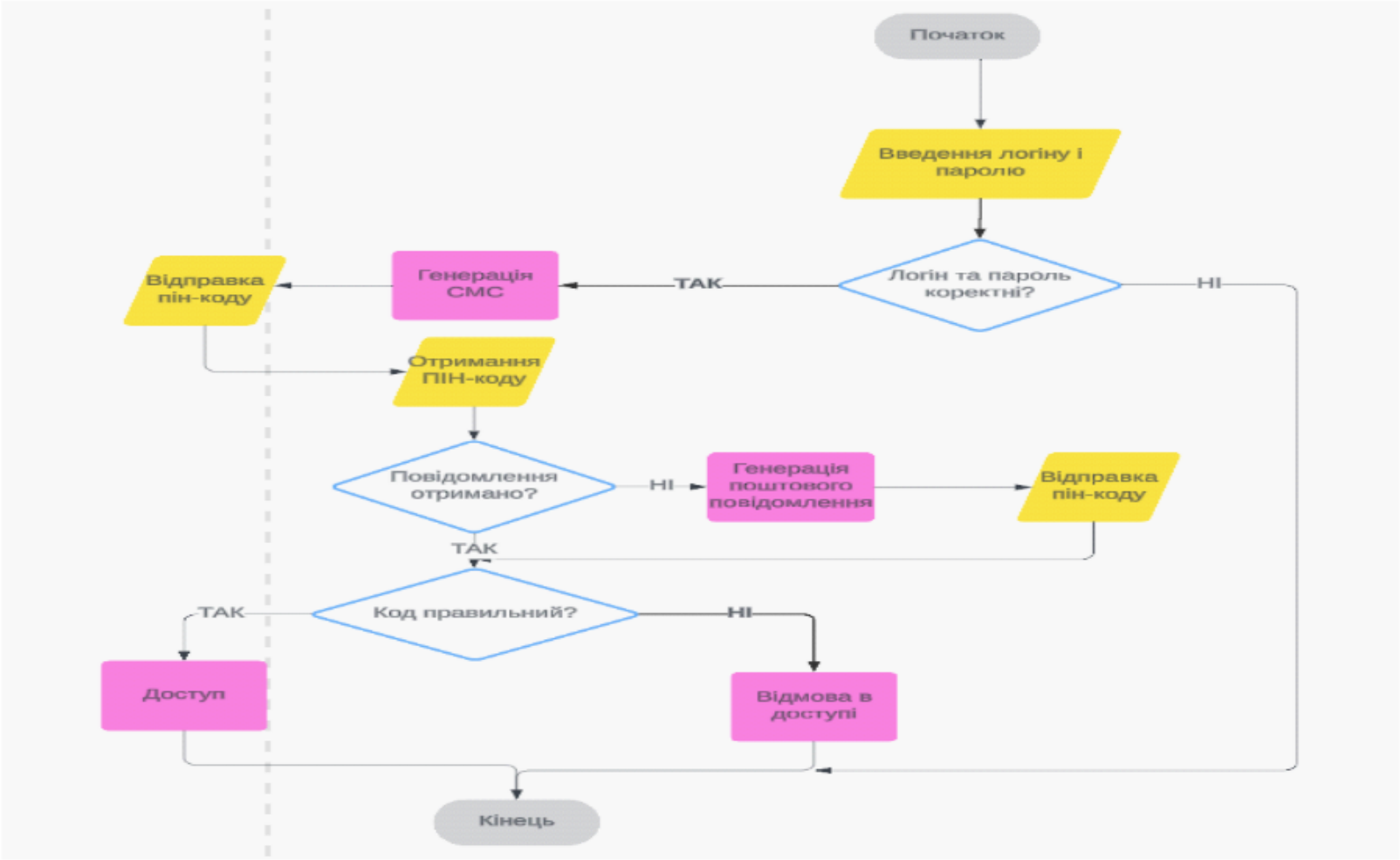
45. Praveen Kumar, E., Priyanka, S. A password less authentication protocol for multi-server environment using physical unclonable function. J Supercomput 79, 21474–21506 (2023). https://doi.org/10.1007/s11227-023-05437-3

ДОДАТОК А

Графічні матеріали

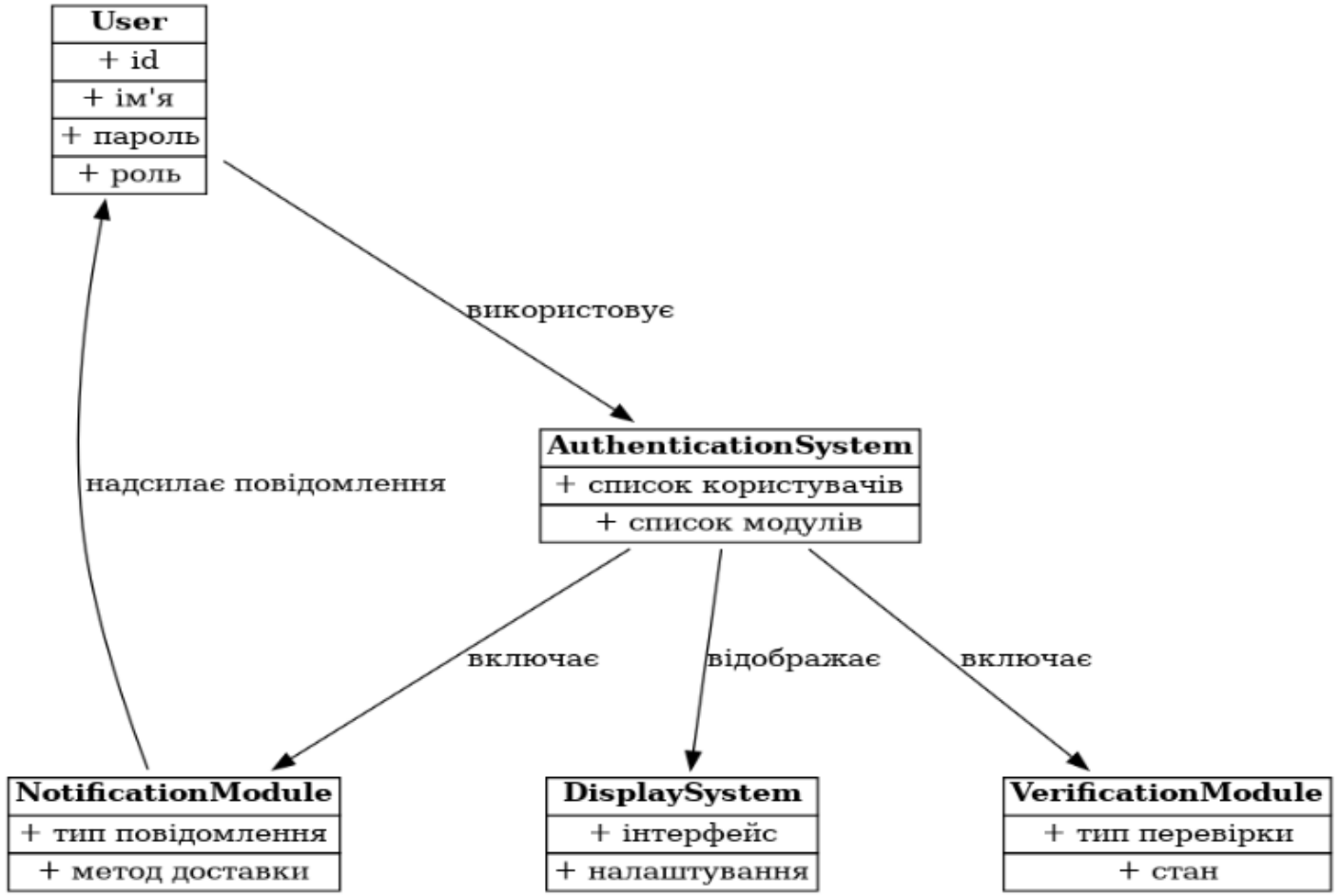


Алгоритм роботи системи



						КРБКБ. 2101021.20.01.13 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система двофакторної автентифікації інформаційної системи (або сайту) Алгоритм роботи системи	Літера	Маса	Масштаб
Розроб.		Макаров М.В.				Н		
Перевір.		Орленко В.С.						
Т. контр.						Аркуш	Аркушів 1	
Н. контр.		Мостовий С.В.				ХНУ, КБ-20-1		
Затв.		Кльоц Ю.Л.						

Діаграма класів



Зм.	Арк.	№ докум.	Підпис	Дата	КРБКБ. 2101021.20.01.13 Е8	
Розроб.		Макаров М.В.			Система відображення автентифікації інформаційної системи (або сайту)	Літера: Н; Маса; Масштаб
Перевір.		Орленко В.С.			Діаграма класів	Аркуш 1; Аркушів
Т. контр.						
Н. контр.		Мостовий С.В.				ХНУ, КБ-20-1
Затв.		Кльоц Ю.П.				

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1		Завдання на кваліфікаційну	1	
				роботу		
А4		2		Анотація	1	
А4		3	КРБКБ. 2101021.21.01.13 ПЗ	Система двофакторної	63	
				автентифікації інформаційної		
				системи (або сайту)		
				Пояснювальна записка		
А2		4	КРБКБ. 2101021.21.01.13 Е8	Система двофакторної	1	
				автентифікації		
А2		5	КРБКБ. 2101021.21.01.13 Е8	Алгоритм роботи	1	
				роботи системи		
А2		6	КРБКБ. 2101021.21.01.13 Е8	Діаграма класів	1	

Зм.	Арк.	№ Докум.	Підп.	Дата	КРБКБ. 2101021.21.01.13 ВП		
Розробив		Макаров М.В.			Система двофакторної автентифікації інформаційної системи (або сайту) Відомість проєкту	Літера	Аркуш 1 / Аркушів 1
Перев.		Орленко В.С.				н	
Н. контр.		Мостовий С.В.				ХНУ, КБ-20-1	
Затв.		Кльоц Ю.П.					

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Макаров Максим Володимирович
Тема: «Система двофакторної автентифікації інформаційної системи (або сайту)» Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «*Кібербезпека*»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 68;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою системи двофакторної автентифікації сайту. Було проведено аналіз відомих підходів до реалізації автентифікації, визначено їх переваги та недоліки. Обґрунтовано вибір першого етапу автентифікації та запропоновано для другого етапу використовувати SMS або поштове повідомлення. Робота має на меті забезпечити доступ до захищуваних ресурсів навіть за умови перебоїв в роботі інформаційних систем та забезпечити при цьому належний рівень безпеки.
2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено дослідження концепції двофакторної автентифікації, аналіз методів першого та другого факторів, підходи до реалізації мультифакторної автентифікації. У другому розділі розглянуто стандарти та протоколи двофакторної автентифікації, технології та методи, що використовуються при двофакторній автентифікації. Проаналізовано питання безпеки та викликів при впровадженні таких систем. В третьому розділі представлено архітектуру розробленої системи, опис розробки та впровадження прийнятих рішень. Проведено оцінку ефективності впровадження такої системи.
4. Позитивні сторони кваліфікаційної роботи полягають у тому що, застосування розробленої системи двофакторної автентифікації з можливістю вибору однієї з альтернатив 2-го фактору дозволяє забезпечити більшу доступність сервісу при перебоях в роботі сервісів для авторизації, що в загальному збільшить доступність інформаційної системи. В свою чергу можливість вибору методу другого фактору авторизації не ускладнює роботу користувачів з системою. Також використання альтернативних варіантів для другого фактору не зменшує загальну безпеку інформаційної системи, оскільки обидва фактори мають високий рівень надійності, а автентифікаційні дані зберігаються в межах однієї системи.

5. Негативні сторони проекту: _в роботі не достатньо уваги приділено безпеці автентифікаційних даних, що зберігаються в інформаційній системі. Також в роботі недостатньо висвітлено особливості використання методів автентифікації.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Матеріал кваліфікаційної роботи здебільшого чіткий та структурований, однак є деяка непослідовність роботи, що не дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці не достатньо наглядних пояснень, та деякі розділи варто розширити. Графічний матеріал не в повному обсязі дозволяє побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «задовільно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 5 » червня 2023 . _____ (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система двофакторної автентифікації інформаційної системи (або сайту)

Автор: Макаров Максим Володимирович

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Науковий керівник: Орленко В.С.

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1.03% і адресується до 142 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи В.С. Орленко

Завідувач кафедри КБ Ю.П. Кльоц

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

ID: 132631 Назва: Система двофакторної автентифікації інформаційної системи (або сайту) Додано в БД: 2024-06-26 Автора: Макаров М.В. Керівники: Орленко В.С. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	59224	539	591 (1%)	5 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015975242

Дата перевірки:
06.12.2023 10:20:47 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2023 10:45:16 EET

ID користувача:
100008300

Назва документа: Макаров_**плагіат**

Кількість сторінок: 78 **Кількість слів:** 14900 **Кількість символів:** 118285 **Розмір файлу:** 2.86 MB **ID файлу:** 1015654798

1.03%
Схожість

Найбільша схожість: 0.46% з Інтернет-джерелом (https://el-conf.com.ua/wp-content/uploads/2020/04/8%D1%87%D0%B...

0.82% Джерела з Інтернету	137	Сторінка 80
0.54% Джерела з Бібліотеки	47	Сторінка 80

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	1