МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) Автоматизації і комп'ютерних систем
Кафедра Інформаційних технологій, штучного інтелекту і кібербезпеки

«До захисту в ЕК»	**«До захисту допущено»**
Директор інституту(декан факультету)	Завідувач кафедри
_____ Андрій Форсюк	_____ Сергій Грибков
(підпис) (ім'я та прізвище)	(підпис) (ім'я та прізвище)
«12» лютого 2024р.	«12» лютого 2024р.

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

зі спеціальності 122 «Комп'ютерні науки»
(код та назва спеціальності)
освітньо-професійної програми Інформаційні управляючі системи та технології
на тему: Дослідження захисту ресурсів та персональних даних в інтернеті за допомогою мультифакторної автентифікації

Виконав: здобувач 2 курсу, групи ІС-2-3М

Зяхор Дмитро Олександрович _____
(прізвище, ім'я, по батькові повністю) (підпис)

Керівник Струзік Владислав Анатолійович _____
(прізвище , ім'я та по батькові повністю) (підпис)

Консультанти Сергій ГРИБКОВ _____
(ім'я та прізвище) (підпис)
Владислав СТРУЗІК _____
(ім'я та прізвище) (підпис)
_____ _____
(ім'я та прізвище) (підпис)

Рецензент Віктор СІДЛЕЦЬКИЙ _____
(ім'я та прізвище) (підпис)

Я як здобувач(ка) Національного університету харчових технологій розумію і підтримую політику університету з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволеної допомоги під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач _____
(підпис)

Київ - 2024р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) Автоматизації і комп'ютерних систем

Кафедра інформаційних технологій, штучного інтелекту і кібербезпеки

Освітній ступінь Магістр

Спеціальність 122 «Комп'ютерні науки»
(код і назва)

Освітньо-професійна програма Інформаційні управляючі системи і технології
(назва)

ЗАТВЕРДЖУЮ
Завідувач
кафедри Інформаційних технологій, штучного інтелекту і кібербезпеки

Грибков С.В.
"19" грудня 2023року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Зяхора Дмитра Олександровича
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження захисту ресурсів та персональних даних в інтернеті за допомогою мультифакторної автентифікації,
керівник роботи Струзік Владислав Анатолійович,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «19» грудня 2023 р. № 1006-кс
2. Строк подання здобувачем роботи: 22.01.2024
3. Вихідні дані до роботи:
1. Відкриті інформаційні джерела по темі автентифікації. 2. Відкриті інформаційні джерела по темі інтернет-загроз. 3. Відкриті інформаційні джерела по темі кібербезпеки. 4.Наукові дослідження по темі кібербезпеки.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
1. Ідентифікація, автентифікація та авторизація. Їх поняття, види та роль в безпеці веб-ресурсів. 2. Поширені інтернет загрози для веб-ресурсів та їхніх користувачів. Способи боротьби з ними. 3. Існуючі методи мультифакторної автентифікації. Переваги та недоліки кожного з них.
4. Розробка системи системи рекомендацій щодо вибору методу мультифакторної автентифікації та впровадження їх в програмне рішення.
5. Тестування розробленої системи.
5. Перелік графічного матеріалу:
1. Діаграма використання методів MFA.
2. Фрагменти роботи розробленого додатку.
6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Струзік В. А., доцент, кандидат технічних наук		
2	Грибков С. В., професор, доктор технічних наук		
3	Грибков С. В., професор, доктор технічних наук		
4	Струзік В. А., доцент, кандидат технічних наук		

7. Дата видачі завдання: «19» грудня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Видача завдання	19.12.2023	Виконав
	Пошук теоретичних матеріалів	20.12.2023	Виконав
	Написання розділу 1	24.12.2023	Виконав
	Аналіз та дослідження визначень автентифікації та авторизації	29.12.2023	Виконав
	Аналіз методів мультифакторної автентифікації	04.01.2023	Виконав
	Написання розділу 2	07.01.2023	Виконав
	Аналіз поширених загроз для користувачів веб-сервісів в Інтернеті	09.01.2023	Виконав
	Аналіз існуючих методів мультифакторної автентифікації	11.01.2023	Виконав
	Аналіз вимог автентифікації	13.01.2023	Виконав
	Написання розділу 3	16.01.2023	Виконав
	Розробка логіки взаємодії програми з користувачем	17.01.2023	Виконав
	Розробка інтерфейсу та проведення тестування	18.01.2024	Виконав
	Написання розділу 4	20.01.2024	Виконав
	Створення автореферату та презентації	21.01.2024	Виконав

Здобувач _____ (підпис) Зяхор Д. О. (прізвище та ініціали)

Керівник роботи _____ (підпис) Струзік В. А. (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота присвячена дослідженню сучасних підходів до захисту ресурсів та персональних даних в інтернеті шляхом впровадження мультифакторної автентифікації. У роботі аналізуються основні виклики та загрози для інтернет-безпеки, а також розглядаються принципи функціонування та ефективність мультифакторної автентифікації в контексті захисту ресурсів та особистих даних. Розкривається практичне використання мультифакторної автентифікації в різних галузях та аналізуються сучасні тенденції розвитку цієї технології. Дослідження враховує існуючі нормативно-правові аспекти, а також пропонує практичні рекомендації щодо вдосконалення захисту в інтернет-середовищі. Кількість таблиць – 7, ілюстрацій – 3. Використано 18 джерел.

Ключові слова: ЗАХИСТ, ПЕРСОНАЛЬНІ ДАНІ, ІНТЕРНЕТ-БЕЗПЕКА, МУЛЬТИФАКТОРНА АВТЕНТИФІКАЦІЯ, ТЕХНОЛОГІЧНІ ЗАГРОЗИ.

SUMMARY

This thesis explores contemporary approaches to securing resources and personal data on the internet through the implementation of multi-factor authentication. The work analyzes primary challenges and threats to internet security, while also examining the operational principles and effectiveness of multi-factor authentication in the context of resource and personal data protection. Practical applications of multi-factor authentication across various domains are elucidated, and modern trends in the technology's development are investigated. The research takes into account existing regulatory and legal aspects, proposing practical recommendations for enhancing protection in the online environment. The thesis includes 7 tables, 3 illustrations, and references 18 sources.

Keywords: PROTECTION, PERSONAL DATA, INTERNET SECURITY, MULTI-FACTOR AUTHENTICATION, TECHNOLOGICAL THREATS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Скорочення	Розшифрування
OAuth	Open Authorization
OpenID	OpenID Connect
SAML	Security Assertion Markup Language
USB	Universal Serial Bus
SMS	Short Message Service
ACL	Access Control List
OTP	One-Time Password
IAM	Identity and Access Management
MFA	Multi-Factor Authentication
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
GPS	Global Positioning System

ВСТУП

Актуальність дослідження полягає в тому, що інтернет загрози та порушення безпеки стають все більш поширеними і складними. Хакерські атаки, фішинг, крадіжка персональних даних та інші злочинні дії в мережі становлять серйозну загрозу для безпеки користувачів інтернету.

Мультифакторна автентифікація є ефективним інструментом для боротьби з цими загрозами. Вона забезпечує додатковий шар захисту, вимагаючи від користувача надання додаткових факторів для підтвердження своєї особи, тому дослідження в галузі мультифакторної автентифікації має великий потенціал для вдосконалення безпеки в інтернеті. Воно спрямоване на розробку нових методів та технологій, які дозволять забезпечити надійний та зручний спосіб ідентифікації користувачів. Дослідження може охоплювати такі елементи, як аналіз поточних методів MFA, виявлення потенційних вразливостей, розробку нових алгоритмів та протоколів, оцінку використання біометричних даних в плані MFA, вивчення впливу MFA на зручність та прийняття користувачами. Дослідження у цій області може привести до покращення безпеки інтернету, зменшення ризиків злочинних дій та захисту приватності користувачів. Впровадження нових методів MFA може мати велике значення для різних сфер, включаючи фінансові установи, медичні організації, урядові структури, онлайн-сервіси та інші сегменти, де безпека та захист даних є критично необхідними елементами.

Зв’язок роботи з науковими програмами, планами, темами кафедри, університету. Наукова робота виконувалась згідно з науково-дослідною роботою на кафедрі інформаційних технологій, штучного інтелекту і кібербезпеки «Дослідження та використання сучасних інформаційних технологій для виконання функцій та завдань виробничого і організаційного управління підприємств харчової галузі» (0120U105386 2020–2025 рр.) Національного університету харчових технологій.

Мета дослідження. Метою кваліфікаційної роботи є дослідження та рекомендації створення підсистеми автентифікації в залежності від можливих загроз несанкціонованого проникнення у веб-орієнтовану інформаційну систему.

Об'єктом дослідження є контроль доступу до веб-орієнтованої інформаційної системи.

Предметом дослідження є методи автентифікації.

Для виконання поставлених завдань будуть використані такі методи дослідження:

- емпіричний метод для дослідження загроз при автентифікації в інформаційних системах;
- метод порівняння при досліджені популярних методів мультифакторної автентифікації;
- метод аналізу та синтезу для визначення рекомендацій для підбору методів автентифікації з метою захисту від поширених загроз.

Науковою новизною є формування рекомендацій для підбору методів автентифікації з метою захисту від поширених загроз.

Практичне значення полягає у створенні та використанні рекомендаційної системи для побудови підсистеми автентифікації, що сприятиме підвищенню рівня безпеки та конфіденційності особистих даних користувачів.

Основним особистим внеском є сформовані рекомендації для підбору методів автентифікації та створена рекомендаційна система для побудови підсистеми автентифікації для власних проєктів.

Робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 70 сторінок.

РОЗДІЛ 1. АВТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ: ОСНОВИ ЗАХИСТУ РЕСУРСІВ ТА ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ

1.1. Автентифікація та авторизація в Інтернеті

Автентифікація та авторизація є необхідними компонентами інформаційної безпеки, особливо в плані сучасного інтернету, де злочинці постійно шукають способи доступу до чужих ресурсів та персональних даних. Розуміння цих процесів та розробка ефективних методів їх реалізації є основою для забезпечення безпеки користувачів та захисту їх приватності.

Автентифікація – це процес перевірки ідентичності користувача, щоб забезпечити доступ до певних ресурсів чи послуг. Цей етап у веб та інформаційній безпеці передбачає встановлення довіреного зв'язку між користувачем та системою.

У процесі автентифікації зазвичай використовуються різноманітні методи та засоби для перевірки ідентичності користувача. Найпоширенішими з них є використання пароля, секретних запитань, біометричних даних (таких як відбитки пальців, розпізнавання обличчя або сканування райдужної оболонки ока) або використання спеціальних пристроїв, наприклад, електронних карток або USB-ключів. Пароль є одним з найпоширеніших методів автентифікації. Користувач обирає унікальний пароль, який відомий лише йому, і при майбутніх спробах входу в систему він повинен вказати цей пароль для підтвердження своєї ідентичності. Необхідно використовувати складні паролі, які складаються з комбінації букв, цифр та символів, для забезпечення високого рівня безпеки. Секретні питання є ще одним методом автентифікації, який використовується для перевірки особи користувача. Користувач вибирає питання, на яке лише він знає відповідь, і при вході в систему йому необхідно надати правильну відповідь на це запитання. Цей метод може бути менш безпечним, оскільки деякі відповіді можуть бути відомі іншим

людям або знайти їх у відкритих джерелах, тому необхідно обирати запитання, на які відповіді важко вгадати.

Крім традиційних методів автентифікації, використання біометричних даних стає все більш поширеним. Біометричні дані можуть бути використані для ідентифікації особи, так як вони унікальні для кожної людини. Наприклад, система може вимагати сканування відбитків пальців або розпізнавання обличчя для підтвердження особи користувача [1].

Авторизація – це надзвичайно важливий процес, який забезпечує контроль над доступом користувачів до певних ресурсів або послуг. Вона гарантує, що лише уповноважені особи мають можливість отримати доступ до конфіденційної інформації, функціональності або привілеїв. Під час процесу авторизації надаються права на доступ чи функціоналу після успішної ідентифікації та автентифікації. Авторизація включає в себе визначення ролі або рівня доступу, який користувач має після успішної автентифікації. Це означає, що система може надати різні привілеї та обмеження в залежності від ролі користувача, наприклад, адміністратора, модератора або звичайного користувача. Такий підхід дозволяє ефективно управляти рівнями доступу та контролювати, які ресурси або послуги можуть бути використані користувачем [2].

Забезпечення надійної автентифікації та авторизації стає все більш складним завданням, оскільки зловмисники постійно вдосконалюють свої методи несанкціонованого проникнення в інформаційні системи. Тому дослідження в галузі розвитку нових методів та технологій автентифікації та авторизації є надзвичайно необхідним. Наприклад, розробка нових методів біометричної автентифікації, використання машинного навчання для виявлення підозрілих дій або розробка стандартів та протоколів безпеки є активними напрямками досліджень.

Автентифікація та авторизація також широко використовуються в різних інформаційних системах та мережах, де доступ до ресурсів обмежується залежно від ролі або привілеїв користувача. Наприклад, веб-

сайти можуть вимагати автентифікацію перед наданням доступу до особистих облікових записів, електронної пошти або інших приватних даних користувача. Також, в корпоративних оточеннях, автентифікація та авторизація використовуються для контролю доступу співробітників до внутрішніх ресурсів, таких як файлові сервери, бази даних тощо. На сьогоднішній день існує багато методів автентифікації, які варіюються за рівнем безпеки та зручності використання. Крім традиційного введення ідентифікатора користувача та пароля, можуть використовуватися такі методи, як одноразові паролі, двофакторна автентифікація (наприклад, через SMS-повідомлення або мобільний додаток), використання апаратних токенів або смарт-карток, а також біометричні методи, такі як відбитки пальців, розпізнавання обличчя або сканування райдужки ока.

Що стосується авторизації, то вона може бути реалізована за допомогою різних підходів, включаючи рольову модель, де користувачам надаються ролі з певним набором привілеїв, або на основі політик доступу, де визначаються конкретні правила доступу до ресурсів. У більш складних системах авторизація може включати багаторівневий контроль доступу залежно від контексту або характеристик користувача.

Використання автентифікації та авторизації має декілька головних переваг. По-перше, це допомагає запобігти несанкціонованому доступу до ресурсів та даних, що може призвести до крадіжки, втрати чи пошкодження інформації. По-друге, це дозволяє керувати правами доступу різних користувачів та обмежувати їхні можливості використання системи або додатків, що допомагає забезпечити конфіденційність та цілісність даних. По-третє, ці процеси допомагають відстежувати та реєструвати дії користувачів системі, що необхідно для аудиту та виявлення порушень безпеки.

Для досягнення ефективної автентифікації та авторизації, часто використовуються різні методи і технології. Наприклад, для автентифікації можуть використовуватись двофакторна автентифікація (поєднання пароля

та коду, отриманого на мобільний пристрій), автентифікація на основі сертифікатів, автентифікація на основі біометричних даних тощо. Для авторизації можуть використовуватись ролі та правила, системи керування доступом, списки контролю доступу (ACL) та інші механізми.

Крім того, існують деякі передові концепції та практики в галузі автентифікації та авторизації, які допомагають поліпшити безпеку систем. Наприклад, одним з таких підходів є управління ідентичністю та доступом (IAM), що дозволяє централізовано керувати ідентичностями та доступом користувачів до різних систем та ресурсів [3]. Іншим підходом є використання технологій одноразових паролів (OTP) для підвищення безпеки автентифікації.

Існує ряд різних технологій автентифікації, які можуть використовуватися для перевірки особи користувача.

Паролі – це найпоширеніша технологія автентифікації. Вони прості у використанні, але менш безпечні, оскільки паролі доволі легко підібрати можуть бути легко зламані, якщо вони не є достатньо складними. Тому рекомендується використовувати довгі та унікальні паролі, а також регулярно їх змінювати.

Одноразові коди – це метод автентифікації, при якому користувач отримує одноразовий код на свій телефон або інший пристрій. Цей код використовується для підтвердження особи користувача.

Біометричні ідентифікатори – це метод автентифікації, при якому користувачі використовують свої біометричні дані для підтвердження своєї особи. До біометричних даних належать відбитки пальців, обличчя, сітківка ока та голос.

Фактор присутності – це метод автентифікації, при якому користувач повинен бути фізично присутнім у певному місці, щоб отримати доступ до ресурсу або послуги. Наприклад, для доступу до комп'ютера в офісі користувач повинен ввести свій пароль і відбиток пальця.

Мультифакторна автентифікація є більш безпечним варіантом, оскільки вона вимагає від користувача надання двох або більше факторів безпеки. Наприклад, це може бути поєднання пароля з одноразовим кодом, отриманим на мобільний пристрій, або використання біометричних даних разом з паролем. Це робить процес автентифікації більш складним для зламування, оскільки зловмиснику потрібно мати доступ до кількох факторів одночасно. Варто зазначити, що мультифакторна автентифікація вимагає додаткового обладнання або програмного забезпечення для забезпечення реалізації. Це може включати мобільні пристрої, токени безпеки або біометричні сканери. Хоча це може створювати додаткові витрати та складнощі у використанні, переваги вищого рівня безпеки часто виправдовують ці зусилля.

Основною проблемою автентифікації в Інтернеті є те, що вона часто не адаптується до нових загроз. Зловмисники постійно розробляють нові методи злому автентифікаційних систем. Це означає, що розробники автентифікаційних систем повинні постійно вдосконалювати свої системи, щоб вони могли протистояти новим загрозам [4].

Фішинг є одним зі способів соціального інжинірингу, при якому зловмисники намагаються отримати конфіденційну інформацію, таку як облікові дані або фінансові реквізити, шляхом імітації довірених веб-сайтів або електронних листів. Наприклад, зловмисник може надіслати електронний лист, який виглядає як лист від банку, і просити користувача ввести свої облікові дані на підробленому веб-сайті. Після введення цих даних зловмисники отримують доступ до них і можуть використати для своїх злочинних цілей.

Розвідка паролів це процес збору паролів користувачів з різних джерел. Наприклад, зловмисник може використовувати інформацію з скомпрометованих баз даних веб-сайтів, де паролі були збережені у відкритому вигляді або використовувалися не криптостійкі алгоритми хешування. Вони також можуть використовувати програми, які шукають

відкриті мережі Wi-Fi та збирають паролі, які передаються від користувачів під час автентифікації.

Атака з проникненням полягає у пошуку та використанні вразливостей у програмному забезпеченні для отримання несанкціонованого доступу до даних. Зловмисники можуть використовувати різні методи, включаючи використання вразливостей в операційних системах або програмах, встановлених на пристроях користувачів. Це може дозволити їм отримати доступ до облікових записів або шифрованих даних.

Атака brute-force – це атака, при якій зловмисники випробовують всі можливі комбінації паролів, поки не знайдуть правильну. За допомогою спеціальних програм або скриптів зловмисники можуть автоматизувати цей процес і швидко перебрати велику кількість можливих паролів. Ця атака може бути ефективною проти слабких або недостатньо складних паролів.

Атака за словником – це атака, при якій зловмисники використовують список поширених паролів або словників для спроб вгадати пароль користувача. Замість перебору всіх можливих комбінацій, зловмисники перевіряють лише певні паролі зі списку. Це може бути ефективно, якщо користувач використовує слабкий або поширений пароль, такий як "123456" або "password". Зловмисники можуть використовувати автоматизовані скрипти, щоб швидко перебрати велику кількість паролів зі списку.

При обранні паролю доцільно використовувати комплексний підхід, що передбачає поєднання різноманітних символів – цифр, літер верхнього та нижнього регістрів, спеціальних символів. Така структура паролю ускладнює його повне відновлення шляхом систематичного перебору можливих комбінацій (атаки методом грубої сили). Рекомендованої довжини пароля не менше 8 символів. Також доцільно уникати очевидних

та легко вгадуваних комбінацій, наприклад набір послідовних чи однакових символів (таблиця 1.1), особистих даних користувача тощо.

Таблиця 1.1. Список найпопулярніших паролів за 2021, 2022 та 2023 роки

Рік	**Список популярних паролів**					
2021	123456	password	qwerty	admin	Дата народження	123123
2022	111111	123456	12345678	abc123	87654321	000000
2023	122333	123456	welcome	football	9876543210	qwerty123

Як видно, популярні паролі з року в рік не сильно змінюються. Вони складаються з простих послідовностей цифр або слів, які легко запам'ятати. Однак такі паролі дуже легко зламати, тому важливо використовувати складні паролі, що складаються з різноманітних символів.

Періодична зміна паролів допомагає ускладнити процес несанкціонованого доступу третіх осіб, які могли отримати доступ до попередніх комбінацій. Рекомендується встановлювати цикл оновлення паролів, наприклад, кожні три місяці. Така періодичність дає змогу мінімізувати ризик застосування попередніх комбінацій зловмисниками та ускладнити їх завдання. Водночас це дозволяє суттєво знизити ймовірність компрометації облікового запису користувача у разі викрадення попереднього пароля.

Мультифакторна автентифікація (MFA) надає додатковий рівень безпеки до процесу автентифікації. Крім пароля, MFA вимагає додаткового підтвердження, такого як одноразовий код, відбиток пальця або підтвердження через мобільний додаток. Це робить важчим для зловмисників отримати доступ до облікового запису, навіть якщо вони знають пароль користувача [5].

Антивірусні програми та брандмауери є важливими інструментами для захисту від зловмисних програм і вразливостей в комп'ютерній

системі. Вони можуть виявляти шкідливе програмне забезпечення, блокувати шкідливі сайти та перешкоджати несанкціонованому доступу до даних користувача. Потрібно регулярно оновлювати програми захисту, щоб мати актуальні їх версії і розпізнавати нові загрози.

Виробники прикладних програм часто випускають оновлення, метою яких є усунення технічних вразливостей та впровадження інших заходів із підвищення рівня кібербезпеки. Регулярне оновлення програмних пакетів, включаючи операційні системи, веб-браузери, плагіни та інші додатки, є необхідним для забезпечення належного рівня захищеності. Зокрема, це дозволяє уникнути використання зловмисниками виявлених вразливостей з метою несанкціонованого доступу до даних користувача.

Процес автентифікації користувачів в Інтернеті постійно удосконалюється шляхом впровадження розробниками нових підходів та технологій, спрямованих на посилення кібербезпеки. Одним з перспективних напрямів є аналіз поведінкових патернів користувача, що ґрунтується на унікальних особливостях його взаємодії з пристроєм. Розглядаються також інноваційні підходи, такі як автентифікація на базі блокчейн-технологій та розподілених реєстрів, які дозволяють створювати надійні та незмінювані записи про процес автентифікації.

Разом із впровадженням інноваційних технологічних рішень, спрямованих на поліпшення процесу автентифікації, відбувається удосконалення самих методів автентифікації користувачів. Прикладом є застосування одноразових паролів (OTP), які генеруються шляхом алгоритмічної обробки часових або випадкових факторів та можуть бути використані лише один раз. Це забезпечує додатковий рівень захищеності, оскільки OTP стають недійсними після першого використання.

Принцип дії OTP полягає в наступному. Під час реєстрації користувач отримує токен, який генерує одноразові паролі на підставі вбудованого алгоритму і періодично оновлюваних секретних ключів. Під час автентифікації на сервер надсилається поєднання логіну та поточного

OTP з токена. Це унеможливлює використання викрадених раніше паролів або подолання атак шляхом здійснення чисельних спроб.

Застосування одноразових паролів є ефективним рішенням для підвищення рівня кібербезпеки, оскільки воно дозволяє усунути низку існуючих ризиків:

- виключає можливість використання раніше компрометованих чи викрадених паролів, оскільки кожен OTP є унікальним та недійсним після першого використання;
- унеможливлює застосування атак методом «грубої сили» із спробою систематичного відгадування паролю, оскільки потрібно вгадати саме актуальний одноразовий пароль;
- підвищує необхідний рівень складності атак для зловмисника, оскільки для успішної ідентифікації необхідно мати доступ до самого OTP-токену користувача;
- гарантує додатковий рівень безпеки при використанні мобільних та інших віддалених пристроїв обмеженого доступу.

1.2. Мультифакторна автентифікація

Вибір конкретних стандартів та протоколів для реалізації MFA залежить від багатьох чинників, зокрема від особливостей інфраструктури та середовища застосування. До найбільш поширених належать:

- OpenID Connect (OIDC), побудований на основі OAuth 2.0 із використанням токенів для ідентифікації;
- Security Assertion Markup Language (SAML) – XML-протокол для обміну повідомленнями про автентифікацію та авторизацію;
- Стандарти FIDO Alliance (FIDO U2F, FIDO2), що дозволяють використовувати фізичні ключі та біометрію;
- Протоколи одноразових паролів, зокрема Time-based One Time Password (TOTP);

- WebAuthn – веб-стандарт для автентифікації через браузер із залученням фізичних пристроїв.

Застосування цих стандартів сприяє ефективній реалізації MFA та підвищенню рівня кіберзахищеності інформаційних систем та ресурсів.

MFA є ефективним засобом підвищення безпеки автентифікації. Вона робить неможливим для зловмисників отримати доступ до облікового запису користувача, навіть якщо вони знають його пароль.

Основна перевага MFA – це її підвищений рівень безпеки. Проста автентифікація, наприклад, логін і пароль, є недостатньо безпечною, оскільки її можна зламати за допомогою фішингу, розвідки паролів або атаки brute-force.

MFA вимагає від користувача надати два або більше факторів безпеки для підтвердження своєї особи. Це робить її більш безпечною, оскільки її складніше зламати. Наприклад, якщо зловмисник отримає доступ до пароля користувача, він все одно не зможе отримати доступ до його облікового запису, якщо він не знає іншого фактора безпеки, наприклад, одноразового коду, який надсилається на пристрій користувача [6].

Отримання одноразових кодів є зручним та доступним методом для користувачів. Цей процес може здійснюватися шляхом отримання кодів через текстові повідомлення, мобільні додатки або за допомогою спеціальних апаратних пристроїв безпеки, таких як токени або USB-ключі (Додаток А**)**. Вибір методу залежить від індивідуальних потреб та зручності кожного користувача. Важливою характеристикою одноразових кодів є їхній вбудований елемент безпеки – вони призначені для одноразового використання і не можуть бути повторно використані. Це забезпечує високий рівень безпеки, оскільки, навіть якщо код потрапить у чиїсь руки, його обмежена використовуваність робить його некорисним. В порівнянні з повторно використовуваними паролями, які можуть бути

скомпрометовані і використані без дозволу, одноразові коди забезпечують додатковий рівень безпеки та захисту.

Користувачі мають можливість вибирати, коли і де вони бажають використовувати MFA, для найбільш критичних акаунтів, таких як банківські або електронні платіжні системи. Або для менш важливих акаунтів, користувачі можуть обрати менш обтяжливі методи автентифікації або використовувати MFA лише при підозрілих або незвичайних діях. Такий гнучкий підхід дозволяє користувачам налаштовувати рівень безпеки відповідно до своїх потреб і комфорту. Наприклад, якщо зловмиснику вдалося отримати доступ до пароля, він все одно не зможе успішно пройти автентифікацію без наявності фізичного пристрою або біометричних даних користувача. Такий підхід захищає від фішингу та парольних атак, коли зловмисники намагаються отримати паролі шляхом соціальної інженерії або перехоплення. МФА також спрощує процес автентифікації для користувачів, оскільки вони можуть використовувати зручні фізичні пристрої або біометричні дані, замість складних паролів або ручного введення додаткової інформації.

MFA є гнучкою та масштабованою системою, яка може бути адаптована до різних сценаріїв та потреб організацій. Це дозволяє вибирати найефективніші методи та фактори автентифікація для досягнення потрібного рівня безпеки. Втім, впровадження MFA може бути складним і вимагати додаткових технологічних рішень, налаштування систем та навчання користувачів. Деякі методи MFA можуть бути менш зручними для користувачів, особливо якщо вони потребують постійного доступу до фізичних пристроїв або виконання біометричних процедур [7]. Незважаючи на це, MFA залишається одним з найефективніших способів захисту облікових записів та забезпечення безпеки ідентифікації. Постійні дослідження та розвиток MFA можуть привести до вдосконалення методів і факторів ідентифікації, що забезпечать ще більшу безпеку та зручність використання у майбутньому.

MFA поділяється на кілька типів в залежності від кількості факторів, що вимагаються:

- двофакторна автентифікація (2FA);
- трифакторна автентифікація (3FA);

1) *Двофакторна автентифікація* (2FA) передбачає використання двох факторів для автентифікації користувача. Зазвичай фактори поділяють на три категорії: інформація, відома користувачеві (наприклад, пароль); річ, що перебуває у володінні користувача (наприклад, пристрій); біометричні характеристики самого користувача.

Прикладами 2FA є введення паролю з подальшим отриманням одноразового коду на мобільний пристрій або використання біометрії в поєднанні з паролем. 2FA підвищує рівень захисту порівняно з однофакторною автентифікацією.

2) *Трифакторна автентифікація (3FA)* вимагає трьох незалежних факторів – усіх перерахованих під час опису 2FA. Наприклад, це може бути комбінація паролю, пристрою (наприклад, безконтактної картки) та біометрії (розпізнавання обличчя). 3FA забезпечує ще вищий рівень захисту, проте може бути складнішою у реалізації та використанні через необхідність керувати трьома різними типами ідентифікаційних факторів.

Вибір між дво- та трифакторною автентифікацією залежатиме від конкретних обставин кожної організації чи сервісу.

Двофакторна автентифікація, з одного боку, забезпечує значне підвищення рівня захисту в порівнянні з однофакторною. Вона є надійним рішенням для багатьох випадків використання, пропонуючи гарне співвідношення безпеки та зручності.

Проте трифакторна автентифікація дає ще більш високий ступінь захищеності, що може бути критичним для систем, де зберігаються особливо важливі чи секретні дані. Зокрема, для державних установ, банків, критичної інфраструктури.

Таблиця 1.2. Порівняння 2FA і 3FA

Характеристика	**2FA**	**3FA**
Кількість факторів безпеки	2	3
Види факторів безпеки	Знання + Власність	Знання + Власність + Фізична присутність
Безпека	Висока	Найвища
Зручність використання	Висока	Висока
Доступність	Можливі проблеми	Можливі проблеми
Проблеми з використанням	Користувачі можуть забути свій пароль або секретне запитання та відповідь	Користувачі можуть забути свій пароль, секретне запитання та відповідь, або не мати можливості надати свої фізіологічні дані
Приклади реалізації	Одноразові коди, мобільні додатки безпеки, апаратні пристрої безпеки	Одноразові коди, мобільні додатки безпеки, апаратні пристрої безпеки, фізіологічні дані

Водночас трифакторна автентифікація є складнішою в імплементації та експлуатації, вимагаючи більших витрат та зусиль.

Впровадження багатофакторної автентифікації може принести користь різним організаціям, зокрема корпораціям, державним установам та приватним користувачам. Наприклад:

- Корпорації використовують об'ємні ресурси та дані, які важливість для зловмисників. Багатофакторна автентифікація здатна захистити ці активи від несанкціонованого доступу шляхом перевірки особи за допомогою декількох незалежних факторів. Наприклад, корпоративні поштові ящики можуть бути використані для викрадення конфіденційної інформації або поширення шкідливого ПЗ. 2FA дозволяє захистити доступ до пошти шляхом вимоги другого фактора у вигляді одноразового коду на мобільному пристрої. Аналогічним чином можуть бути захищені системи ERP та CRM, що містять цінні дані.
- Державні органи оперують персональними та конфіденційними даними громадян. 3FA здатна забезпечити їх високий

рівень конфіденційності, наприклад комбінацією паролю, одноразового коду та біометричних даних, таких як відбиток пальця або сканування обличчя.

1.3. Методи мультифакторної автентифікації

SMS-підтвердження (англ. SMS-based authentication) є одним з найпростіших та найпопулярніших методів реалізації MFA. Суть методу полягає у надсиланні користувачеві одноразового коду у формі SMS-повідомлення на зареєстрований мобільний телефон. Користувач повинен ввести отриманий код під час процедури автентифікації для підтвердження своєї особи.

Так, при спробі входу до особового облікового запису користувач спочатку вводить свій пароль. У цей момент система надсилає одноразовий код за допомогою SMS на мобільний телефон користувача. Для завершення процесу автентифікації необхідно правильно ввести отриманий код протягом певного часового інтервалу (зазвичай 1-5 хвилин). Це дозволяє підтвердити особу власника облікового запису, навіть якщо його початковий пароль був викрадений.

Тому, SMS-підтвердження є простим та ефективним методом перевірки особи користувача. Його переваги полягають у наступному:

Переваги SMS-підтвердження:

- Простота реалізації та зрозумілість принципу дії – отримання одноразового SMS-коду на мобільний телефон та його введення для підтвердження особи є зручним та простим способом ідентифікації для більшості користувачів навіть без спеціальних знань в галузі кібербезпеки та ІТ-технологій.
- Сумісність з більшістю мобільних телефонів – практично всі сучасні смартфони та ключові телефони здатні отримувати та відображати SMS, що робить цей метод доступним для переважної більшості власників мобільних пристроїв.

- Універсальність застосування у різноманітних сферах, включаючи не тільки фінансові, соціальні і електронну комерцію, а й державні послуги, освіту та розваги.

Недоліки SMS-підтвердження:

- Для отримання SMS-повідомлення користувач повинен мати активний мобільний телефон і підключення до мобільної мережі. У випадку поганого зв'язку або відсутності сигналу користувач може зіткнутися з проблемою отримання коду підтвердження.
- SMS-підтвердження має певну вразливість до атак, таких як SIM-своппінг або викрадення номера телефону. Це може дозволити зловмисникам отримати доступ до SMS-повідомлень, які містять коди підтвердження, і використовувати їх для несанкціонованого доступу до облікових записів користувача.
- Затримки в доставці SMS-повідомлення може бути непередбачуваним і залежить від багатьох факторів, таких як навантаження мережі зв'язку або проблеми з доставкою на боку оператора мобільного зв'язку. Це може спричинити затримки у процесі отримання коду підтвердження та використання його користувачем.
- В деяких випадках, залежно від тарифного плану або оператора мобільного зв'язку, користувач може бути стягнута додаткова оплата за отримання SMS-повідомлення. Особливо при використанні послуги підтвердження великої кількості разів, це може призвести до додаткових витрат для користувача.

SMS-підтвердження може застосовуватися поштовими сервісами для автентифікації користувача під час створення нового облікового запису чи зміни параметрів безпеки. У цьому випадку користувач отримує SMS з одноразовим кодом підтвердження, який необхідно ввести на веб-сайті чи в додатку для завершення процедури реєстрації чи редагування налаштувань.

Фінансові установи також широко використовують цей метод для забезпечення захищеності банківських операцій та доступу до інтернет-банкінгу. Користувачі отримують одноразові підтверджувальні коди SMS для проведення транзакцій, таких як переказ коштів або зміна контактної інформації.

Багато компаній реалізовують SMS-підтвердження для контролю доступу до приміщень або IT-систем. При цьому працівники отримують коди SMS-підтвердження для отримання фізичного чи віртуального доступу на вході.

Також SMS-підтвердження активно застосовується розробниками мобільних додатків для автентифікації та реєстрації.

Додаток для автентифікації – це мобільний додаток, який генерує одноразові коди для автентифікації. Користувач повинен ввести код, згенерований додатком, для підтвердження своєї особи. Додатки для автентифікації стали популярними альтернативами SMS-підтвердженню і забезпечують більшу безпеку та зручність для користувачів.

Популярні додатки для автентифікації:

- Google Authenticator;
- Authy;
- Microsoft Authenticator;
- Duo Mobile;
- LastPass Authenticator.

Ці додатки є надійними та зручними для забезпечення другого етапу перевірки ідентичності користувача.

Таблиця 1.3. Порівняльна таблиця додатків для двофакторної автентифікації

Додаток	**Google Authenticator**	**Authy**	**Microsoft Authenticator**	**Duo Mobile**	**LastPass Authenticator**
Безкоштовний	Так	Так (з обмеженнями)	Так	Так (для особистого використання)	Так (для використання з обліковим записом LastPass)
Простий у використанні	Так	Може бути складним для деяких	Так	Може бути складним для деяких	Так
Підтримка платформ	Широка	Широка	Широка	Широка	Широка
Резервне копіювання в хмару	Ні	Так	Так	Так	Так
Відновлення без пристрою	Ні	Так	Так	Так	Так
Відкритий код	Так	Ні	Так	Ні	Ні
Відновлення за допомогою OTP	Так	Так	Ні	Так	Так
Незалежне використання	Так	Так	Так	Так	Ні, потребує LastPass

Процес багатофакторної автентифікації з використанням мобільного додатка:

1) Під час спроби входу до особового облікового запису користувачі спочатку вводять традиційний логін та пароль, що є першим

етапом перевірки ідентичності шляхом перевірки правильності введених даних.

2) Наступним етапом є запуск мобільного додатка 2FA на смартфоні. При цьому за допомогою Time-based One-time Password або HMAC-based One-time Password алгоритмів генерується одноразовий пароль, який базується на секретному ключі між додатком та сервером.

3) Одержаний токен користувач вводить на веб-сайті чи у програмі, з якої здійснює вхід. Це підтверджує фізичний доступ до мобільного та ідентичність власника облікового запису.

4) Після перевірки чинності та справжності отриманого коду сервер надає доступ до запитуваних ресурсів користувачу, завершивши таким чином процес двофакторної автентифікації. Така схема є надійним та безпечним способом захисту особистої інформації.

Переваги використання додатків для автентифікації:

- вони забезпечують вищий рівень захищеності порівняно з традиційними SMS-повідомленнями, оскільки одноразові коди генеруються безпосередньо на пристрої користувача, що ускладнює їх перехоплення або підміну;
- додатки 2FA допомагають уникнути фішингових атак, оскільки зловмисникам важко ввести жертву в оману щодо необхідності надати одноразовий пароль, який генерується локально;
- вони можуть виступати резервним варіантом захисту на випадок втрати чи компрометації основного пароля;
- працюють навіть без доступу до мережі чи в роумінгу, оскільки забезпечують генерацію OTP безпосередньо на пристрої;
- відсутність додаткової плати за доставку повідомлення;
- захищеність від SIM-своппінг атаки.

Недоліки додатків для автентифікації:

- для використання додатка для автентифікації користувач повинен мати пристрій, на якому він встановлений. а якщо користувач

втратить свій телефон або він буде пошкоджений, це обмежить доступ користувача до свого облікового запису, доки він не встановить додаток на новому пристрої або не відновить доступ до попереднього;

- деякі додатки для автентифікації можуть бути обмежені у своїй використаності, оскільки не всі сервіси підтримують їх, що вимагає використання кілька різних додатків для автентифікації для доступу до різних сервісів, що може бути не зручним для користувача;
- якщо користувач втратить свій пристрій або забуде його, користувач може звернутися за підтримкою до провайдера автентифікації для відновлення доступу до свого облікового запису;
- деякі додатки для автентифікації можуть мати затримки в генерації кодів автентифікації або в процесі підтвердження. Це може бути незручним для користувачів, особливо якщо вони потребують швидкого доступу до свого облікового запису;
- використання додатків для автентифікації передбачає встановлення та оновлення програмного забезпечення на пристроях користувача. Це може бути додатковою перешкодою для користувачів, які не бажають або не можуть встановити додатки на свої пристрої.

Додатки для автентифікації широко використовуються різними організаціями, включаючи корпорації, урядові організації та індивідуальних користувачів. Наприклад, додатки для автентифікації можуть використовуватися для автентифікації користувачів в системах електронної пошти, банківських системах і системах управління доступом.

Фізичні пристрої безпеки – це пристрої, які використовуються для автентифікації користувачів. Ці пристрої можуть бути у формі смарт-карт, ключів безпеки або інших пристроїв. Вони пропонують додатковий рівень безпеки та забезпечують унікальні фізичні аспекти для ідентифікації користувача [7].

При спробі входу в обліковий запис користувачеві пропонується ввести свій пароль, що є першим етапом автентифікації. Додатково до

паролю користувачеві пропонується використати фізичний пристрій безпеки для підтвердження своєї особи. Цей фізичний пристрій може бути у формі смарт-карти, ключа безпеки або іншого подібного пристрою.

Після введення пароля користувачеві пропонується вставити фізичний пристрій безпеки в порт на пристрої або наблизити його до сканера, якщо такий встановлений. Після цього фізичний пристрій безпеки генерує унікальний код або ключ, який використовується для підтвердження особи користувача. Цей код або ключ може бути заснований на криптографічних алгоритмах та унікальних ідентифікаторах, що забезпечує високий рівень безпеки.

Фізичні пристрої безпеки забезпечують додатковий рівень безпеки, оскільки потребують фізичної присутності самого користувача та його фізичного пристрою. Це ускладнює заволодіння обліковим записом зловмиснику, який володіє паролем, але не має фізичного пристрою безпеки.

Переваги фізичних пристроїв безпеки такі:

- фізичні пристрої безпеки надають додатковий рівень безпеки для автентифікації користувачів. Вони забезпечують унікальні фізичні аспекти, такі як фізичні ключі або біометричні дані, для підтвердження особи користувача. Це ускладнює заволодіння обліковим записом зловмисникам, навіть якщо вони знають пароль;
- фізичні пристрої безпеки надійно захищають від атак фішингу. Зловмисники, намагаючись отримати доступ до облікових записів користувачів, не зможуть успішно здійснити атаку, оскільки не мають доступу до фізичного пристрою безпеки, необхідного для підтвердження особи користувача;
- використання фізичних пристроїв безпеки дозволяє встановити двофакторну автентифікацію, що підвищує рівень безпеки облікових записів. Користувачі повинні ввести свій пароль та мати фізичний

пристрій безпеки для успішного входу, що зробить обліковий запис набагато складнішим для несанкціонованого доступу;

- кожен фізичний пристрій безпеки має унікальний ідентифікатор, що дозволяє точно автентифікувати користувача. Це допомагає уникнути проблем, пов'язаних з дублюванням або підробкою ідентифікаційних даних.

Фізична присутність – це метод автентифікації, який вимагає від користувача бути фізично присутнім у певному місці. Це може бути зроблено за допомогою картки-ключу, відбитка пальця або іншого біометричного фактора. Цей метод зазвичай включає в себе використання фізичних пристроїв безпеки або біометричних факторів для забезпечення доступу до об'єкта або системи.

Принцип роботи проходить після введення правильного пароля, користувачеві пропонується використати картку-ключ або здійснити сканування відбитка пальця для додаткового підтвердження його особи. Якщо користувач має картку-ключ, він вставляє її у відповідний порт на пристрої автентифікації. При цьому, пристрій зчитує інформацію з картки-ключа і порівнює її з попередньо збереженими даними. Якщо дані співпадають, користувач отримує доступ. Якщо ж користувач використовує сканер відбитка пальця, йому пропонується наблизити свій палець до пристрою сканування. Сканер розпізнає унікальні характеристики відбитка пальця і порівнює їх з попередньо збереженими даними. Якщо відбиток пальця збігається зі збереженими даними, користувач отримує доступ до свого облікового запису. Використання картки-ключа або біометричних факторів для підтвердження особи користувача забезпечує більш високий рівень безпеки, оскільки такі фактори є унікальними для кожної особи і важко підробити або підмінити. Це дозволяє запобігти несанкціонованому доступу до об'єкта або системи і захистити конфіденційну інформацію користувача.

Таблиця 1.3. Переваги та недоліки фізичної присутності

Перевага	Недолік	Обґрунтування
Високий рівень безпеки	Фізична присутність обмежена в часі та місці	Фізична присутність вимагає присутності самої особи, що забезпечує високий рівень безпеки. Картка-ключ або біометричні фактори, такі як відбиток пальця, є унікальними для кожної людини, що ускладнює можливість підробки або підміни. Однак фізична присутність вимагає, щоб користувач був фізично присутнім у певному місці для отримання доступу. Це може бути незручним, особливо коли користувачі знаходяться віддалено або коли необхідно швидко отримати доступ.
Відсутність несанкціонованого доступу	Витрати на використання фізичних пристроїв	Оскільки фізична присутність вимагає фізичної присутності користувача, це унеможливлює несанкціонований доступ до об'єкта або системи. Це особливо важливо в ситуаціях, коли доступ до конфіденційної інформації або обмеженого приміщення є критичним. Однак використання фізичних пристроїв, таких як картка-ключ, може вимагати додаткових витрат на їх придбання та обслуговування. Це може бути накладними витратами для організацій або користувачів, особливо якщо потрібно використовувати багато таких пристроїв.
Велика стійкість до втрати або крадіжки	Можливість втрати або пошкодження фізичних пристроїв	Фізичні пристрої або біометричні дані важко втратити або викрасти порівняно з паролями або іншими електронними методами автентифікації. Картка-ключ може бути збережена в безпечному місці, а відбиток пальця є унікальним для кожної особи і не може бути

Перевага	Недолік	Обґрунтування
		втрачений. Однак існує ризик втрати або пошкодження картки-ключа або інших фізичних пристроїв, що може призвести до втрати доступу або потреби в їх заміні. Втрачені або пошкоджені пристрої також можуть потребувати додаткового часу і зусиль для відновлення доступу.
Зручність використання	Потенційні проблеми з приватністю	Фізична присутність може бути відносно зручним методом автентифікації. Користувачам не потрібно запам'ятовувати складні паролі або використовувати додаткові пристрої для отримання доступу. Вони просто повинні мати при собі картку-ключ або використовувати свій власний біометричний фактор. Однак використання біометричних факторів, таких як відбиток пальця, може породити проблеми з приватністю. Зберігання і обробка біометричних даних повинні бути здійснені з високим рівнем захисту, щоб уникнути можливого витоку особистої інформації.

Використання фізичної присутності користувача є поширеним методом двофакторної перевірки особи та широко впроваджується в різноманітних сферах, зокрема фінтех-компаніями. Так, наприклад Monobank дозволяє отримати доступ до особистого кабінету без згенерованого SMS-паролю, проходячи ідентифікацію шляхом сканування обличчя за допомогою камери мобільного пристрою.

Біометрія – це метод автентифікації, який використовує фізіологічні або поведінкові характеристики людини для ідентифікації та верифікації її особистості [8]. Фізіологічні характеристики включають такі фактори, як відбиток пальця, структура обличчя, структура райдужної оболонки ока, розподіл судин на руці, голосові особливості тощо. Поведінкові

характеристики можуть включати такі речі, як почерк, спосіб ходьби, манера набору тексту і навіть реакції на певні стимули.

Першим кроком процесу автентифікації є введення пароля. Користувачеві пропонується ввести свій пароль для доступу до облікового запису або системи. Пароль вважається першим рівнем ідентифікації особи і є стандартним методом доступу до багатьох облікових записів. Після успішного введення пароля настає час для збору біометричних даних. Користувачеві пропонується надати свої унікальні біометричні характеристики. В залежності від типу біометричних даних для їх збору використовуються спеціальні сенсори, камери та/або мікрофони. Після збору біометричних даних вони порівнюються зі збереженими в системі шаблонами. Ці шаблони були створені на попередніх етапах реєстрації користувача. Під час порівняння система аналізує унікальні характеристики, визначені біометричними даними, і порівнює їх зі збереженими шаблонами. Якщо порівняння показує високу відповідність, то особа підтверджується, і доступ до облікового запису надається. Звичайно є переваги так і недоліки

Біометричні дані є умовно унікальними для кожної особи, що робить їх надійними засобом автентифікації [8]. Використання фізіологічних або поведінкових характеристик ускладнює можливість підробки або шахрайства, оскільки вони важко піддаються підробленню. Біометричні системи автентифікації забезпечують зручність для користувачів. Вони не вимагають запам'ятовування паролів чи носіння додаткових пристроїв, таких як токени або картки доступу. Користувачі можуть легко використовувати свої фізіологічні або поведінкові характеристики для ідентифікації.

Біометричні системи можуть працювати дуже швидко, забезпечуючи миттєвий доступ до системи або облікового запису. Оскільки процес автентифікації відбувається в режимі реального часу, користувачі не витрачають зайвого часу на чекання або введення паролів. Біометрія

дозволяє уникнути проблеми слабких паролів, які можуть бути викрадені або легко вгадані. Замість цього, користувачі можуть використовувати свої фізіологічні або поведінкові характеристики, які є важкими до підробки.

Недоліки також є одним з основних недоліків біометрії є проблеми, пов'язані з приватністю та захистом даних. Біометричні дані є дуже особистою інформацією, оскільки вони пов'язані з унікальними фізіологічними або поведінковими характеристиками особи. Це означає, що втрата або пошкодження цих даних може мати серйозні наслідки для приватності користувача. Якщо біометричні дані потрапляють в недоброчесні руки, вони можуть бути використані для несанкціонованого доступу до систем або для злочинних цілей, таких як шахрайство або шантаж [8].

Хоча біометричні системи автентифікації є дуже надійними, вони також можуть мати недоліки. Наприклад, іноді можуть виникати проблеми з точністю та надійністю сканування біометричних даних. Наприклад, сканер відбитків пальців може не завжди правильно розпізнавати відбитки в разі, якщо шкіра пальців занадто суха або волога. Також виникають питання щодо точності сканування обличчя у разі, якщо особа змінила зачіску, макіяж або має деякі фізичні зміни. Ще одним недоліком біометрії є незручність, пов'язана з помилками в процесі автентифікації. Наприклад, якщо сканер відбитків пальців не розпізнає відбиток, користувачеві доведеться повторювати процедуру або шукати альтернативний спосіб входу до системи. Це може викликати додаткові труднощі та затримки, особливо в ситуаціях, коли швидкий доступ до системи є критично необхідним. Впровадження біометричних систем вимагає значних витрат. Це пов'язано з придбанням спеціалізованого обладнання, розгортанням інфраструктури, навчанням персоналу та підтримкою системи.

Географічний контроль – це метод, що використовується для визначення та контролю місцезнаходження об'єктів або пристроїв за допомогою географічної інформації. Цей метод базується на використанні

глобальних позиційних систем (GPS), супутникової навігації, мереж зв'язку та інших технологій, що дозволяють визначити точне місцезнаходження об'єктів у реальному часі. Один з основних елементів географічного контролю – це використання GPS. GPS використовує сигнали з супутників для визначення географічних координат точки на поверхні Землі. GPS забезпечує глобальне покриття, що дозволяє використовувати географічний контроль практично в будь-якій точці світу. Географічний контроль використовується в різних сферах діяльності. У сфері транспорту він дозволяє відстежувати місцезнаходження транспортних засобів, контролювати їх рух та маршрутизацію. Наприклад, вантажні компанії можуть використовувати географічний контроль, щоб відстежувати маршрути та час доставки товарів, а також контролювати безпеку вантажів.

У сфері логістики географічний контроль допомагає визначити найближчі склади або розподільні центри до пунктів призначення, що дозволяє ефективно планувати маршрути та зменшити витрати на доставку. Також географічний контроль може бути використаний для відстеження місцезнаходження товарів під час їх переміщення по ланцюжку постачання.

У сфері безпеки і правопорядку географічний контроль дозволяє відстежувати місцезнаходження поліцейських автомобілів, патрульних бригад та інших службових осіб для оперативного реагування на надзвичайні ситуації та злочини. Також він може бути використаний для встановлення вірогідного місцезнаходження осіб під час розслідування злочинів.

У сфері екології географічний контроль може бути використаний для відстеження розподілу та руху диких тварин, моніторингу зміни рослинного покриву, контролю незаконної рубки лісів та інших екологічних проблем. Використання географічного контролю дозволяє

збирати дані про природні ресурси та впливати на прийняття рішень з екологічного управління.

Крім вищезгаданих прикладів, географічний контроль може мати застосування в багатьох інших галузях, таких як геологічне дослідження, сільське господарство, міське планування, туризм та багато інших. Він дозволяє збирати, аналізувати та використовувати географічну інформацію для прийняття рішень, планування та оптимізації процесів.

Мікротранзакції – це метод здійснення фінансових операцій, який передбачає проведення невеликих платежів або переказів грошей в електронному форматі [9]. Цей метод базується на ідеї здійснення високостатусних, невеликих операцій, які можуть бути виконані швидко і з мінімальними комісійними витратами. Мікротранзакції зазвичай використовуються в електронній комерції, мобільних платежах, онлайн-іграх та інших сферах діяльності, які потребують швидкого та зручного здійснення фінансових операцій.

Традиційні фінансові системи, такі як банки, зазвичай стягують високі комісійні витрати за обробку малих сум грошей, що робить непрактичним проведення таких операцій. Мікротранзакції пропонують альтернативу, де вартість операцій значно знижена, а процес здійснення максимально спрощений.

Один з варіантів реалізації мікротранзакцій – використання криптовалют. Криптовалюти, такі як Bitcoin або Ethereum, дозволяють здійснювати швидкі та недорогі платежі будь-де у світі без посередництва банків чи інших фінансових установ. Криптовалютні транзакції можуть бути здійснені в режимі реального часу із низькими комісійними витратами, що робить їх ідеальними для мікротранзакцій.

Ще один популярний метод мікротранзакцій – це використання платіжних систем, таких як PayPal, Apple Pay або Google Pay. Ці системи дозволяють користувачам здійснювати швидкі та зручні платежі за допомогою мобільних пристроїв або веб-платформ. Вони забезпечують

безпеку та шифрування даних, а також широкий спектр функцій для зручного здійснення мікротранзакцій [9]. Мікротранзакції також мають велике значення в сфері онлайн-ігор та цифрового контенту. У багатьох випадках вони дозволяють гравцям здійснювати невеликі платежі за доступ до платформ або додаткового ігрового контенту. Це дозволяє гравцям отримувати більше задоволення від гри та розширювати її функціонал. Окрім того, мікротранзакції широко використовуються в сфері соціальних мереж та онлайн-платформ. Наприклад, користувачі можуть здійснювати невеликі платежі за підтримку улюблених творців контенту, отримання преміум-функцій або доступу до ексклюзивного контенту. Це дозволяє забезпечити фінансову підтримку для творців та платформ, а також збільшити залучення та взаємодію спільноти користувачів.

Необхідним аспектом мікротранзакцій є їх безпека. Завдяки розумним системам шифрування та технологіям автентифікації, мікротранзакції забезпечують високий рівень захисту фінансових даних та особистої інформації користувачів. Це дозволяє знизити ризики шахрайства та незаконного доступу до грошових коштів.

1.4 Постановка задачі

У цьому розділі ми детально розглянули основи автентифікації та авторизації і проаналізували їх важливу роль у забезпеченні безпеки ресурсів та особистих даних в Інтернеті. Вивчаючи основи цих процесів, ми встановили ключові компоненти, що лежать в основі систем безпеки в сучасному цифровому середовищі. Ми розкрили сутність автентифікації та авторизації як двох фундаментальних складових, на яких ґрунтується безпека в Інтернеті. Автентифікація, або перевірка ідентичності користувача, виконує важливу функцію перед наданням доступу до ресурсів. У той же час, авторизація визначає, які конкретні дії та ресурси доступні автентифікованому користувачеві.

Зосередивши увагу на мультифакторній автентифікації, ми підкреслили її важливість у підвищенні рівня безпеки. Мультифакторна автентифікація, поєднуючи різні методи перевірки, робить процес входу більш надійним та вишуканим. Це є важливим кроком у запобіганні несанкціонованому доступу та забезпеченні конфіденційності даних.

У розділі також було розглянуто різноманітні методи мультифакторної автентифікації. Вивчення різних підходів, таких як використання паролів, біометричних даних та одноразових кодів, дозволило нам розуміти різноманітність інструментів, які можуть бути використані для підвищення безпеки інтернет-платформ.

Підсумовуючи даний розділ, поставимо мету дослідження кваліфікаційної роботи, а саме дослідження та рекомендації створення підсистеми автентифікації в залежності від можливих загроз несанкціонованого проникнення у веб-орієнтовану інформаційну систему. А також визначимо об’єкт та предмет дослідження – це контроль доступу до веб-орієнтованої інформаційної системи та методи автентифікації відповідно.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТА АНАЛІЗ ІСНУЮЧИХ ЗАГРОЗ ДЛЯ КОРИСТУВАЧІВ ТА ІНТЕРНЕТ-РЕСУРСІВ В ІНТЕРНЕТІ

У даному розділі буде визначено та проаналізовано поширені загрози для користувачів веб-ресурсів та самих веб-ресурсів. Буде визначено їхні ознаки, способи виявлення, а також розглянуто варіанти захисту та протидії для подібного роду загроз.

Цей розділ має на меті дослідити поширені інтернет-загрози та, проаналізувавши їх, виявити способи захисту та боротьби з ними, щоб запобігти несанкціонованому втручанню зловмисників до веб-ресурсів.

2.1. Аналіз брутфорс-атак

Брутфорс-атака (від англ. brute force – груба сила) – це метод злому облікових записів користувачів шляхом підбору пароля методом їх перебору [10]. Тобто суть цього методу полягає у переборі всіх можливих значень паролю, що рано чи пізно призведе до його вгадування.

Цей спосіб можна розглядати як математичне завдання, вирішення якого можна знайти, використавши досить велику кількість спроб. Саме тому для брутфорс-атак застосовують спеціальне програмне забезпечення, яке значно спрощує пошук правильної комбінації. Однак, це не завжди є раціонально з точки зору часових затрат. Хоч і програма перебирає паролі значно швидше за людину, це все рівно може зайняти надто багато часу.

Метод брутфорс-атак можна класифікувати за видом таким чином:

1. Персональний злом – метод спрямований на отримання доступу до облікового запису конкретного користувача або адміністратора [10]. Зазвичай персональні взломи відбуваються не відразу, а після виманювання у користувача логіну, персональних даних та будь-якої іншої персональної інформації. На основі отриманих даних проводиться атака. Це відбувається в такій послідовності: 1) до спеціальної програми вводиться адреса інтернет-ресурсу, до якого потрібен доступ; 2) також в

програмі вводиться логін користувача; 3) на основі персональних даних та інших ключових слів створюється словник, який підключається до програми злому.

Тобто, якщо пароль користувача буде оснований на персональних даних, які зловмисник зміг отримати, то підбір паролю може зайняти досить малий проміжок часу.

2. Брут-чек – це метод спрямований на підбір великої кількості паролів на відміну від персонального злому [10]. Тобто мета даного методу заволодіти якомога більшою кількістю акаунтів користувачів на різних інтернет ресурсах. Атака даним методом проводиться приблизно так: 1) до програми злому підключається база логінів та паролів будь-яких поштових сервісів; 2) проксі лист для маскування вузла перед сервісами пошти для запобігання виявлення атаки; 3) в налаштуваннях брутфорс-програми зловмисник вказує список сайтів та ключових слів, за якими буде здійснюватись пошук в електронній скриньці жертви повідомлень з цими сайтами або словами (при реєстрації на ресурсі заповнюється поле електронної пошти, куди буде вислано дані для входу на ресурс, програма буде шукати дані листи та копіювати логін та пароль до окремого файлу); 4) ініціюється запуск програми злому.

Тобто даний метод націлений на отримання доступу до великої кількості облікових записів за раз.

3. Застосування брутфорс-методу у зв’язці з іншими утилітами для злому. Використовується для отримання доступу до віддаленого персонального комп’ютера. Алгоритм дії за даним методом такий: 1) відбувається пошук мережі де буде здійснюватися атака; 2) добуваються електронні адреси користувачів або беруться з бази; 3) в налаштуваннях програми злому вводяться електронні скриньки користувачів та IP-адреси; 4) здійснюється запуск.

У разі успішного підбору пароля зберігаються дані для входу та IP-адрес користувача. Ці дані в подальшому можуть бути використані

зловмисником в різних цілях. Одним з варіантів може бути отримання віддаленого доступу до ПК жертви та повного керування ним.

Тобто, брутфорс-атака – це атака спрямована на отримання доступу до облікового запису користувача через підбір пароля або ресурса.Щоб захиститися від даного методу доцільно використовувати наступні правила:

1. не створювати надто короткі паролі;
2. використовувати в паролі букви (різного регістру), цифри та спеціальні символи;
3. не створювати пароль на основі персональних даних (дати народження, імені, прізвища тощо);
4. для усіх облікових записів створювати різні паролі;
5. регулярно змінювати паролі;
6. Надати користувачеві можливість підключити MFA.

2.2. Аналіз атак за допомогою SQL-ін'єкції

SQL-ін'єкція – це метод отримання несанкціонованого доступу до даних або їх пошкодження, що здійснюється за допомогою вставки шкідливого коду просто в параметри запиту [10]. За допомогою цього методу можна як отримати дані з незахищеної бази даних так і видалити їх. Зловмисники можуть отримати доступ до персональних даних користувачів, їхніх логінів та паролів.

Щоб очистити ресурс від даного роду злому потрібно валідувати користувацькі дані або застосовувати до них екранування перед використанням їх в SQL-запитах. Це унеможливлює використання атаки методом SQL-ін'єкцій, що значно підвищує кібербезпеку ресурсу та безпеку його користувачів. Також потрібно завжди застосовувати хешування паролів, що збільшує складність злому для зловмисників навіть, якщо в них вийшло отримати доступ до даних бази, оскільки їх потрібно буде підбирати, наприклад, з використанням райдужних

таблиць.В свою чергу користувач, щоб запобігти несанкціонованому доступу до свого облікового запису може підключити MFA до свого акаунту, що значно знижує можливість злому облікового запису.

2.3. Аналіз кросс-сайт-скриптинг (XSS – Cross Site Scripting) атак

Кросс-сайт-скриптинг або XSS – це атака, яка здійснюється за допомогою впровадження JavaScript-коду на сторінку сайту для крадіжки та подальшого використання даних користувачів [12]. Це відбувається завдяки вразливості сайту, де користувач може будь-яким чином розмістити текст на сторінці сайту іншим користувачам, наприклад, написати коментар. Але замість звичайного тексту в поле вводу впроваджується спеціальний код на мові JavaScript, а браузер інтерпретує текст як код. Це дуже небезпечний тип атаки, так як без відома користувача та власника сайту, дані користувача можуть бути відправлені сторонній особі. Зазвичай таким чином зловмисник викрадає дані для автентифікації або перенаправляє користувача на сторінку клон (ту яку користувач очікує побачити) і там проводить маніпуляції для отримання корисних йому даних.

Запобігти даному типу атак можна такими способами:

1. валідувати дані від користувачів, які потенційно можуть бути розміщені на сторінці;
2. проводити екранування користувацьких даних перед передачею їх у браузер;
3. впровадити на ресурсі мультифакторну автентифікацію для зменшення ризиків викрадення даних користувачів.

2.4. Аналіз атак за допомогою кросс-сайт-запитів (CSRF – Cross-site request forgery)

Атака за допомогою кросс-сайт-запитів або CSRF – це різновид атак на веб-ресурси, які використовують довіру сайтів до авторизованих

користувачів, та використання цих користувачів для проведення певних дій на ресурсі від свого імені [12].

Алгоритм атаки наступний:

1. користувач авторизований на певному веб-сайті;
2. зловмисник якимось чином, наприклад, за допомогою фішингу, направляє користувача на потрібний йому сайт;
3. на сайті знаходиться прихована форма, яка в момент входу на сайт користувача відправляє запит до конкретного веб-ресурсу (де попередньо користувач авторизований) та виконує певні дії, які були визначені змістом форми.

Даний вид атак небезпечний для користувачів тим, що без його відома виконуються якісь дії на сайті, на якому вони зараз не знаходяться. Тому користувач про дану атаку може не знати тривалий час або і не дізнатися зовсім, якщо атака не змінила обліковий запис.

Дана атака можлива завдяки вразливості веб-ресурсу, який приймає запити. Вразливість полягає в тому, що веб-ресурс переглядає відправлені кукі (дані, які зберігаються на стороні користувача), в яких зберігаються дані автентифікації. Перевіривши, що користувач існує та авторизований, ресурс дозволяє запит, але не переглядає, що було надіслано в запиті.

Для збільшення безпеки веб-ресурсів, на яких присутня авторизація, рекомендовано використовувати токени доступу (access token), які будуть відправлятися при кожному запиті користувача, буде згенерованим на основі даних користувача на секретного ключа та буде періодично змінюватися. Тому під час атаки CSRF зловмисник не може заподіяти шкоди, оскільки веб-ресурсу для обробки запиту потрібно буде токен доступу, який зловмисник не буде знати, а отже не зможе і домогтися своєї мети.

2.5. Аналіз атаки на сесійні cookie-файли (крадіжка сесій)

Сесійні cookie-файли – дані, які зберігаються у браузері в поточному сеансі користувача (допоки користувач авторизований). Це дані автентифікації, які підтримують відкритоюі відслідковують активність сесії. Ці дані зберігаються в браузері поки користувач не вийде з системи веб-ресурсу власноруч або допоки не закінчиться час дії сесії [13].

Атака на сесійні cookie, або як це ще називають захват сеансу, здійснюється за допомогою багато способів, таких як XSS-атака, міжсайтовий скриптинг або використання шкідливого програмного забезпечення. Але популярним методом є метод “людина посередині” або “man in the middle” – це метод, отримання даних сесії шляхом надсилання користувачу фішингового посилання, яке переадресовує користувача на фішингову сторінку, копію ресурсу, який очікує побачити користувач. За допомогою цього посилання всі дані користувача будуть передаватися через спеціальний проксі, тобто всі запити, які користувач буде надсилати не будуть надходити до ресурсу напряму, а будуть проходити через зловмисника. Користувач нічого не підозрюючи авторизовується на фішинговому сайті, зловмисник отримує всі дані авторизації, що дає змогу авторизуватися від імені користувача і отримати повний доступ до даних та функціоналу облікового запису.

Така атака є цілеспрямованою, тобто зловмисник застосовує її проти конкретного користувача або у пошуку конкретної інформації, наприклад, даних банківських карт в публічній мережі wi-fi. Ця атака є доволі потужною, оскільки в деяких випадках дозволяє обходити наявні методи MFA (наприклад, OTP).

З такими атаками важко боротися, але легко попередити:

1. фішингові сайти часто мають дивний URL-адрес, наприклад, https://www.y0utube.com – заміна символу (в даному прикладі букву “o” на цифру “0”);

2. в публічній мережі часто спостерігається відключення від wi-fi. Зловмисник може відключати користувача, щоб при повторному підключенні перехопити дані автентифікації;

3. Використовувати мультифакторну автентифікацію, якщо це можливо.

Висновок до розділу 2

В цьому розділі ми розглянули популярні загрози кібербезпеці користувачів веб-ресурсів та самих ресурсів. Це допоможе нам глибше розуміти проблематику безпеки в Інтернеті та способи протидії їм, а також в огляді оптимального методу автентифікації користувача на веб-сайті.

Було наведено детальний огляд існуючих кіберзагроз. Дослідження та аналіз існуючих кіберзагроз дало загальне уявлення про загрози для користувачів та ресурсів в інтернеті, розуміння загроз та способи боротьби з ними, спрямоване на зменшення ризиків для користувачів та підвищення рівня кібербезпеки інтернет-ресурсів.

Подальший розгляд цих аспектів дозволить отримати глибше розуміння сучасної кібербезпеки та розробити ефективні стратегії захисту для забезпечення безпеки користувачів та інтернет-ресурсів у віртуальному просторі.

Було досліджено та проаналізовано наступні методи атак: брутфорс-атака, атака за допомогою SQL-ін’єкцій, XSS-атака, CSRF-атака, крадіжка сесій. Всі ці методи можуть бути використані злочинцями для заволодіння певними даними користувача або веб-ресурсу. Кожен метод має свої особливості та потребує певного підходу. Одні засновані на вразливості самого веб-ресурсу (XSS- та CSRF-атаки або метод SQL-ін’єкцій), інші на вразливості даних користувачів, а саме паролів, які можуть бути не надійними, легко підібраними тощо. Також популярний метод фішингу та соціальної інженерії, який базується на копіюванні інтерфейсу

оригінального веб-ресурсу, запевняє користувача перейти за посиланням зловмисника для заволодіння його даними автентифікації.

Всі ці методи є дієві та небезпечні як для користувача, так і для веб-ресурсу, оскільки можуть заподіяти шкоди обом сторонам, які несуть значні наслідки у вигляді інформаційних або матеріальних втрат, втрати персональних даних, облікового запису тощо.

Дані методи також можуть використовуватися спільно, тобто один метод може доповнювати інший, наприклад, XSS-атака та man-on-the-middle – перша використовує вразливість веб-ресурсу для виконання скрипта на сайті та переадресації користувача на фішинговий сайт, інша для отримання сесійних даних, наприклад, ідентифікатора сесії, та отримання доступу до облікового запису користувача.

Ці загрози є найбільш критичні для користувача, так як саме від його імені будуть проводитися маніпуляції з обліковим записом, а тому злочинець може вчиняти від його імені протиправні дії.

РОЗДІЛ 3. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ МУЛЬТИФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ВИМОГ ДО НИХ

3.1. Аналіз існуючих методів мультифакторної автентифікації

Аналіз існуючих методик багатофакторної автентифікації може сприяти кращому розумінню їх переваг, недоліків та потенційного застосування шляхом вивчення відомих протоколів та стандартів, таких як OpenID Connect, Мова ознак безпеки (SAML), Fast Identity Online (FIDO), Одноразовий пароль (OTP) та WebAuthn.

OpenID Connect є протоколом автентифікації, що ґрунтується на стандартах OAuth 2.0 та JWT. Вона надає можливість користувачам автентифікуватися за допомогою сторонніх служб автентифікації [14]. SAML є мовою для обміну ознаками безпеки між різними доменами довіри і допомагає користувачам отримувати доступ до веб-додатків однієї організації на основі автентифікації в іншій [11]. FIDO пропонує криптографічно підтверджену автентифікацію з використанням USB-токенів для забезпечення більш високого рівня безпеки [7]. OTP та WebAuthn також використовуються для багатофакторної автентифікації шляхом генерації одноразових паролів та підтвердження на пристроях користувача відповідно. Зв'язок між OpenID Connect та протоколом OAuth 2.0 має значення у забезпеченні безпеки та автентифікації в розподілених системах. OpenID Connect є розширенням протоколу OAuth 2.0, яке надає механізми для автентифікації користувачів, дозволяючи їм використовувати свої облікові записи з одного веб-сайту або додатку для входу на інші веб-сайти або додатки.

Протокол OAuth 2.0 використовується для авторизації, тобто надання доступу до ресурсів користувача третім сторонам, без необхідності передавати їм облікові дані. Він дозволяє користувачам надавати дозволи

на доступ до своїх ресурсів іншим додаткам або сервісам [15]. Однак, OAuth 2.0 не надає механізмів для самої автентифікації користувача.

OpenID Connect є додатком до OAuth 2.0 і надає механізми для автентифікації. Він використовує токени доступу, які отримуються під час автентифікації за допомогою OAuth 2.0, та додає ідентифікатори, які дозволяють перевірити та підтвердити особу користувача. Коли користувач намагається увійти на веб-сайт або додаток, який підтримує OpenID Connect, він перенаправляється на сервер автентифікації, який може бути ідентифікований за допомогою URL-адреси веб-сайту. Користувач автентифікується на сервері, зазвичай за допомогою свого логіну та пароля, або за допомогою інших механізмів, таких як соціальні мережі або біометричні дані. Після успішної автентифікації сервер генерує спеціальний токен, який називається ID-токеном. Цей токен зберігає інформацію про ідентифікатор користувача та інші додаткові дані, такі як імена, електронна пошта або ролі користувача. ID-токен підписується сервером автентифікації, щоб забезпечити його цілісність та захист від підробки. Після отримання ID-токена клієнтський додаток або веб-сайт може використовувати його для автентифікації користувача. Клієнтський додаток може перевірити підпис ID-токена, а також отримати додаткові відомості про користувача з нього.

OpenID Connect також надає механізми для обміну токенами доступу, які можуть бути використані для отримання доступу до ресурсів на сторонньому сервері. Це дозволяє користувачам використовувати свої облікові записи з одного веб-сайту або додатку для автоматичного входу на інші веб-сайти або додатки без необхідності повторно вводити свої дані автентифікації.

OpenID Connect є широко підтримуваним протоколом автентифікації, і його використовують у багатьох застосунках та месенджерах для забезпечення безпечної ідентифікації користувачів. Ось

кілька прикладів популярних застосунків, які підтримують OpenID Connect:

- Google імплементує OpenID Connect у своїх системах для автентифікації користувачів. Так, коли користувач вводить облікові дані Google, він може скористатися ними для автоматичного входу на інші веб-ресурси та додатки, які підтримують цей протокол.
- Facebook використовує OpenID Connect для ідентифікації користувачів. Користувачі мають змогу використати обліковий запис Facebook для входу на різні веб-сайти та онлайн-сервіси, сумісні з цим протоколом.
- Microsoft, включаючи сервіси такі як Microsoft Azure та Office 365, підтримує стандарт OpenID Connect для автентифікації користувачів. Користувачі можуть використовувати свій обліковий запис Microsoft для входу на різні платформи та сервіси, що сумісні з цим протоколом.
- Slack, популярний мессенджер для корпоративного спілкування, також підтримує OpenID Connect. Користувачі отримують змогу використовувати акаунт Slack для ідентифікації на інших платформах та додатках, які підтримують цей стандарт.
- GitHub, платформа для розробки ПЗ та спільної роботи над проектами, імплементує OpenID Connect. Це дає змогу користувачам автентифікуватися за допомогою облікового запису GitHub на інших веб-сайтах та додатках, які сумісні з цим протоколом.

Ці приклади демонструють широке застосування стандарту OpenID Connect провідними компаніями для забезпечення зручної системи ідентифікації користувачів. Це лише кілька прикладів популярних застосункі, що підтримують OpenID Connect. Багато інших платформ та сервісів також використовують цей протокол для забезпечення безпечної авторизації користувачів.

OpenID Connect часто обирають завдяки кільком ключовим перевагам. Насамперед, це стандарт з відкритим кодом, що має широку

підтримку у світі Інтернету. Багато популярних веб-сайтів, сервісів та мобільних додатків використовують OpenID Connect для автентифікації користувачів. Високий рівень безпеки є ще однією перевагою OpenID Connect. Він використовує протокол OAuth 2.0 та токени для передачі інформації про ідентичність користувача, що дозволяє забезпечити ефективний захист від витоку особистої інформації. OpenID Connect також вирізняється стандартизованим набором протоколів та токенів, що сприяє спільності в інтеграції та взаємодії різних систем. OpenID Connect підтримує різні потоки авторизації та може бути використаний для реалізації різних сценаріїв автентифікації, роблячи його масштабованим рішенням.

Загалом, OpenID Connect є потужним протоколом автентифікації, який побудований на основі протоколу OAuth 2.0. Він дозволяє розподіленим системам впроваджувати безпечну та надійну автентифікацію користувачів, спрощує вхід на різні веб-сайти та додатки і підвищує рівень безпеки в цих системах.

Security Assertion Markup Language (SAML) є стандартним протоколом обміну повідомленнями, який використовується для обміну інформацією про автентифікацію та авторизацію між ідентичністю постачальника (Identity Provider, IdP) та постачальником послуг (Service Provider, SP). SAML був розроблений для спрощення одноразової автентифікації та забезпечення безпеки у розподілених системах, таких як хмарні сервіси та федерація ідентичності.

Основна ідея SAML полягає в тому, що користувач автентифікується на IdP, який видає спеціальний об'єкт, який називається SAML-твердженням (SAML assertion). SAML-твердження містить інформацію про автентифікацію користувача, таку як ідентифікатор, ролі, атрибути тощо, а також цифровий підпис, щоб гарантувати цілісність та автентичність даних. Коли користувач намагається отримати доступ до ресурсу, який захищений за допомогою SAML, SP перенаправляє його на

IdP для автентифікації. IdP перевіряє облікові дані користувача та генерує SAML-твердження, яке надсилається назад до SP. SP перевіряє цифровий підпис SAML-твердження та користується інформацією, наданою в твердженні, для прийняття рішення щодо доступу користувача до ресурсу.

SAML дозволяє здійснювати федерацію ідентичності, що означає, що користувач може використовувати свій обліковий запис у одній системі для отримання доступу до ресурсів у різних системах. За допомогою SAML можна побудувати довірчі відносини між різними організаціями та дозволити користувачам безпечно увійти в системи партнерів без необхідності повторно вводити дані автентифікації.

Окрім одноразової автентифікації, SAML також підтримує одноразову авторизацію, що означає, що після успішної автентифікації користувач може отримувати доступ до різних ресурсів без потреби повторно вводити дані автентифікації. SAML є потужним протоколом, який дозволяє побудувати довірчі відносини між різними системами і забезпечити безпеку обміну інформацією про автентифікацію та авторизацію. Він широко використовується в різних галузях, включаючи хмарні сервіси, електронну комерцію, урядові системи та інші сфери, де необхідно забезпечити безпеку та довіру при обміні інформацією про ідентичність користувачів.

Варто відзначити, що SAML є одним з протоколів для роботи з федерацією ідентичності, але існують і інші протоколи, такі як OpenID Connect, OAuth і WS-Federation, які також використовуються для реалізації федерації ідентичності. Кожен з цих протоколів має свої особливості та використовується в різних сценаріях.

Мова ознак безпеки (Security Assertion Markup Language, SAML) широко впроваджується різноманітними застосунками та месенджерами для забезпечення інформаційної безпеки під час обміну даними про автентифікацію та авторизацію. Наведено приклади популярних сервісів, які імплементують SAML:

1. Microsoft Office 365 використовує SAML для федерації ідентичності та одноразової автентифікації, завдяки чому користувачі отримують можливість автоматично входити до сервісів Office 365 (Outlook, SharePoint, Teams та ін.) за допомогою облікових записів корпоративної мережі;

2. Salesforce, поширена CRM-система, також підтримує SAML, даючи змогу користувачам безпечно отримувати доступ до своїх облікових записів Salesforce з використанням ідентифікаторів ідентичності, сумісних із SAML;

3. G Suite від Google, що включає Gmail, Google Drive та інші онлайн-сервіси, імплементує SAML для федерації ідентичності, що дозволяє користувачам автоматично входити до G Suite за допомогою корпоративних облікових записів;

4. Slack, популярний месенджер для комунікацій та співпраці, також має підтримку SAML для налаштування федерації ідентичності та автентифікації користувачів у Slack за допомогою систем автентифікації на базі SAML;

5. Jira, система управління проєктами від Atlassian, підтримує SAML для автентифікації користувачів, забезпечуючи організаціям можливість безпечного доступу до Jira за допомогою наявних SAML-сумісних систем автентифікації.

Обирають Security Assertion Markup Language (SAML) зазвичай через кілька переваг. Він широко використовується в корпоративних середовищах для безпечного обміну заявками та повідомленнями про ідентичність між сторонами, роблячи його популярним для організацій, які шукають стандартизований та надійний засіб автентифікації [11]. Високий рівень безпеки є ще однією перевагою SAML. Використання сигнатур та шифрування для захисту інформації про ідентичність забезпечує ефективний захист конфіденційної інформації, що особливо важливо у корпоративних середовищах.

SAML також вирізняється тим, що він дозволяє створювати стандартизовані заявки та повідомлення про ідентичність, полегшуючи спільність та інтеграцію з різними системами та платформами. Можливість використовувати принцип один раз увійти (Single Sign-On - SSO) та підтримка для передачі різних атрибутів користувача додають гнучкість та функціональність до рішення. Таким чином, вибір SAML зазвичай пов'язаний із потребами організацій у високому рівні безпеки, стандартизованій інтеграції та спроможності впровадження ефективних механізмів автентифікації в корпоративному середовищі.

Імплементація SAML може варіюватися залежно від конкретного застосунку, але загальні принципи та механізми SAML залишаються однаковими. Узагалі, SAML є потужним і широко використовуваним протоколом для забезпечення безпеки та довіри при обміні інформацією про ідентичність між різними системами. Він дозволяє зручну та безпечну федерацію ідентичності, спрощує процес автентифікації та авторизації та допомагає забезпечити безпеку при обміні даними між системами, що співпрацюють.

Fast Identity Online (FIDO) є глобальним стандартом, розробленим альянсом FIDO, з метою покращення безпеки ідентифікації та автентифікації в онлайн-сервісах. Він ставить перед собою завдання замінити традиційні методи автентифікації, такі як використання паролів, на більш безпечні та зручні альтернативи. FIDO має кілька компонентів, які включають FIDO UAF (Universal Authentication Framework), FIDO2, FIDO U2F (Universal Second Factor) та процес сертифікації FIDO. FIDO UAF дозволяє користувачам автентифікуватися на основі різних методів, таких як біометричні дані або використання бездротових ключів [7].

FIDO2 є набором стандартів, що впроваджуються в сучасні браузери та платформи і включають WebAuthn і CTAP. WebAuthn дозволяє веб-додаткам взаємодіяти з автентифікаторами, тоді як CTAP забезпечує комунікацію між клієнтом і автентифікатором.

FIDO U2F використовується для використання фізичних пристроїв, таких як USB-ключі або NFC-модулі на смартфонах, як додатковий фактор автентифікації. Крім введення пароля, користувач повинен підтвердити свою особу за допомогою фізичного пристрою.

FIDO Alliance надає сертифікацію автентифікаторів та сервісів, що відповідають стандартам FIDO. Це дозволяє користувачам впевнитися у сумісності та безпеці використовуваних автентифікаторів.

Основні переваги використання FIDO включають високу безпеку, зручність для користувачів, універсальність та зменшення ризику атак на автентифікацію. FIDO стандартизований і широко використовується в різних сферах, включаючи фінансові послуги, хмарні сервіси, електронну комерцію та багато інших. Чим більше провайдерів послуг та виробників пристроїв підтримує FIDO, тим більше користувачів можуть скористатись безпечними та зручними методами автентифікації.

Кілька популярних компаній, які підтримують FIDO, включають Google, Microsoft, Meta, Dropbox, Twitter та Slack. Наприклад, Google дозволяє використовувати фізичні автентифікатори або біометричні дані для безпечного доступу до своїх сервісів, таких як Gmail, Google Drive та Google Аккаунт. Microsoft також інтегрує FIDO у свої сервіси, включаючи Microsoft Account та Azure Active Directory.

Ці застосунки надають можливість користувачам замінити традиційні методи автентифікації, такі як паролі, на більш безпечні та зручні альтернативи. Завдяки підтримці FIDO, користувачі можуть використовувати фізичні автентифікатори, такі як USB-ключі або NFC-модулі на смартфонах, або біометричні дані, наприклад, відбитки пальців або розпізнавання обличчя, для підтвердження своєї особи.

Fast Identity Online (FIDO) має декілька переваг. Він забезпечує високий рівень безпеки, використовуючи апаратні ключі та біометричні методи, ускладнюючи можливість несанкціонованого доступу. Друга перевага полягає в відсутності паролів, що зменшує ризик витоку чи

легкого вгадування. Це підвищує загальну безпеку та спрощує використання для користувачів.

Використання FIDO може бути дуже простим для кінцевого користувача, завдяки використанню біометричних даних чи фізичних ключів, забезпечуючи швидкий та зручний процес автентифікації. FIDO також масштабований та може застосовуватися для різних рівнів автентифікації, включаючи вхід на пристрої, фізичний доступ та віддалений доступ до різних служб. Стандартизований підхід, визначений FIDO Alliance, сприяє узгодженій та сумісній реалізації автентифікації для розробників та виробників пристроїв. FIDO може бути використаний на різних платформах та пристроях, що робить його універсальним рішенням для різних сценаріїв. З кожним днем все більше компаній приєднується до стандарту FIDO, що робить безпечні методи автентифікації доступними для більшої кількості користувачів. Це сприяє зростанню безпеки в онлайн-сервісах і полегшує процес автентифікації для користувачів, забезпечуючи високий рівень захисту від небажаних доступів та атак на облікові записи.

One-Time Password (OTP) – це одноразовий пароль, який використовується для автентифікації користувача в онлайн-сервісах. Він є тимчасовим і використовується лише один раз для конкретної транзакції або сеансу. OTP є ефективним засобом забезпечення безпеки, оскільки навіть якщо зловмисник отримує доступ до OTP, він не зможе їм скористатися в подальшому [16].

OTP може бути згенерований та надісланий користувачу різними способами. Один з поширених методів – це використання мобільних додатків або апаратних пристроїв для генерації OTP. Користувач отримує унікальний код, який зазвичай зберігається протягом короткого проміжку часу, наприклад, 30 секунд. Після цього код стає недійсним і генерується новий пароль.

Інший поширений спосіб використання OTP – це надсилання його через SMS або електронну пошту. Після введення OTP користувачем, він порівнюється зі значенням, збереженим на сервері. Якщо вони збігаються, користувач отримує доступ до системи або пов'язаної з ним послуги.

OTP широко використовується в онлайн-банкінгу, електронній комерції, соціальних мережах та інших сервісах, де забезпечення безпеки облікових записів є потрібною частиною. Він допомагає запобігти фішингу, атакам перехоплення паролів і злому паролів шляхом підвищення рівня автентифікації і зниження ризику несанкціонованого доступу.

Багато відомих компаній і сервісів використовують OTP для забезпечення безпеки облікових записів своїх користувачів. Розглянемо приклади:

1. Rozetka, лідер інтернет-торгівлі в Україні, надає можливість активувати OTP. Користувачі можуть вибрати отримання коду через мобільний додаток або SMS;
2. LinkedIn.UA, український аналог професійної соціальної мережі, підтримує налаштування OTP шляхом використання смартфон-додатку або SMS;
3. Allo.ua, онлайн-версія популярного українського торговельного центру, дає можливість скористатися OTP для посилення захисту облікового запису через мобільний додаток або текстові повідомлення;
4. Kuna.ua, сервіс обміну криптовалют, використовує OTP як складову додаткової автентифікації, забезпечуючи налаштування коду через мобільний додаток або SMS;
5. Instagram, соціальна мережа, надає можливість використовувати OTP для забезпечення безпеки облікових записів. Користувачі можуть вибрати між додатком автентифікації або отриманням OTP через SMS.

One-Time Password (OTP) обирають для систем автентифікації з кількох причин. Він надає додатковий шар безпеки, оскільки кожен пароль є одноразовим та використовується тільки один раз, що ускладнює задачу зловмисників. Також OTP забезпечує захист від перехоплення паролю, оскільки навіть якщо пароль буде перехоплений, його важко використати в майбутньому. Реалізація систем OTP може бути досить простою, що робить їх привабливими для впровадження. Це може бути апаратними токенами, програмними застосунками або відправленням кодів через SMS. З точки зору користувачів, використання OTP є зручним, оскільки вони отримують одноразові паролі на свої мобільні телефони чи інші пристрої, не пов'язані з основним паролем. Окрім того, OTP часто використовують як складову двофакторної автентифікації, підвищуючи рівень безпеки за рахунок двох різних форм ідентифікації. З усіма цими перевагами, OTP залишається популярним та ефективним методом автентифікації, особливо в областях, де важливі висока безпека та простота використання.

WebAuthn (Web Authentication) – це веб-стандарт, розроблений Консорціумом Всесвітньої павутини (W3C) та Альянсом FIDO (Fast Identity Online), який має на меті підвищити безпеку автентифікації в Інтернеті, усуваючи потребу в паролях та впроваджуючи надійні методи автентифікації на основі криптографії з відкритим ключем [17].

Основна мета WebAuthn – надати більш безпечну і зручну альтернативу традиційній парольній автентифікації. Вона дозволяє веб-сайтам і веб-додаткам використовувати різні фактори автентифікації, такі як біометричні дані (відбитки пальців, розпізнавання обличчя), апаратні токени (USB-ключі, NFC-пристрої) або інші автентифікатори, для підтвердження особи користувача. Це усуває ризик слабких паролів, повторного використання паролів та фішингових атак.

WebAuthn працює в контексті клієнт-серверної архітектури, де клієнтом зазвичай є веб-браузер або мобільний додаток, а сервером –

онлайн-сервіс або веб-сайт. Загальний алгоритм процесу автентифікації WebAuthn має наступну послідовність операцій:

- Реєстрація. Під час реєстрації користувач пов'язує свій пристрій або автентифікатор зі своїм обліковим записом на сервері. Автентифікатор генерує нову пару публічний-приватний ключ, де приватний ключ залишається надійно збереженим на пристрої, в той час як публічний ключ надсилається на сервер.
- Верифікація користувача. За бажанням, користувачеві може бути запропоновано надати зразок біометричних даних або PIN-код для підтвердження особи. Цей крок додає додатковий рівень безпеки до процесу автентифікації.
- Засвідчення. Автентифікатор надає серверу підписаний атестаційний звіт, який містить інформацію про сам автентифікатор. Ця заява допомагає серверу визначити автентичність і надійність автентифікатора.
- Аутентифікація. Коли користувач намагається увійти в систему, клієнт надсилає виклик автентифікатору. Автентифікатор використовує приватний ключ, що зберігається на пристрої, для підписання запиту і надсилає підписану відповідь назад клієнту.
- Затвердження. Клієнт надсилає підписану відповідь на сервер разом із запитом та іншою необхідною інформацією. Сервер перевіряє підпис за допомогою раніше зареєстрованого відкритого ключа і визначає, чи пройшла автентифікація успішно.

На ринку існують багато сервісів і платформ, які використовують або впроваджують підтримку WebAuthn для безпечної автентифікації, а саме:

1. Ощадбанк впровадив WebAuthn для другого фактора автентифікації при вході до Інтернет-банкінгу, даючи можливість користувачам реєструвати мобільні пристрої;

2. мережа обчислювальних центрів Ukrainian Centers використовує WebAuthn при адмініструванні хмарних облікових записів для підвищення їхньої безпеки;

3. сервіс електронної комерції Rozetka реалізував підтримку WebAuthn на етапі реєстрації для зміцнення захисту облікових записів покупців;

4. компанія з впровадження IT-рішень Evox впровадила WebAuthn у системах доступу працівників для підтвердження їхньої особи без використання паролів;

5. IT-школа Дніпро у своїй системі навчання та керування курсами запровадила WebAuthn для захисту облікових записів викладачів і студентів.

Вибір WebAuthn для систем автентифікації обумовлений кількома ключовими перевагами. WebAuthn підтримує різні методи автентифікації, такі як біометричні дані та фізичні USB-ключі, що забезпечує високий рівень безпеки. Зокрема, використання біометричних даних чи фізичних ключів робить процес автентифікації зручним для користувачів. Додатково, WebAuthn дозволяє відмовитися від паролів, що поліпшує безпеку та спрощує використання системи автентифікації. Цей стандарт є стандартом W3C, що робить його широко підтримуваним та інтегрованим. Це полегшує впровадження автентифікації на різних платформах. WebAuthn також може використовуватися як частина двофакторної автентифікації, де більшість основних методів (наприклад, пароль) поєднуються з біометричними даними чи фізичним ключем для додаткового підтвердження. Оскільки багато сучасних веб-браузерів вже підтримують WebAuthn без додаткових розширень чи плагінів, цей стандарт стає легко доступним для впровадження на різних веб-сервісах та онлайн-платформах.

Таблиця 3.1. Порівняльний аналіз існуючих методів MFA

Характеристика	**OpenID Connect**	**SAML**	**FIDO**	**OTP**	**WebAuthn**
Інтеграція	Відкритий стандарт, який може бути використаний для інтеграції в різні системи.	XML-оснований стандарт для обміну заявками та повідомленнями між користувачем та службою.	Серія відкритих стандартів для автентифікації, які можуть використовуватися для різних типів пристроїв.	Генерація одноразового пароля, часто через мобільний або апаратний токен.	WebAuthn використовує публічні і приватні ключі для автентифікації користувачів.
Стандарт	OAuth 2.0 та OpenID Connect	SAML	FIDO U2F, FIDO2	Різні протоколи (наприклад, TOTP, HOTP)	WebAuthn
Зручність використання	Забезпечує зручну автентифікацію за допомогою стороннього ідентифікатора та взаємодії із службами.	Зручний для корпоративного використання, але може бути складним для індивідуальних користувачів.	Використання апаратних ключів або біометричних методів для зручності та безпеки.	Зручний, але може вимагати фізичного доступу до генератора OTP або мобільного пристрою.	Використовує веб-стандарт для автентифікації, що може бути зручним для користувачів.
Переваги	Велика кількість підтримуючих служб, відкритий та широко використовуваний стандарт.	Висока рівень безпеки, особливо для корпоративних систем.	Висока безпека, можливість використання апаратних ключів.	Простота використання та можливість впровадження на різних платформах.	Сильна безпека, стандарт від W3C.

Характеристика	OpenID Connect	SAML	FIDO	OTP	WebAuthn
Недоліки	Складніша інтеграція для деяких систем, пов'язаних із безпекою.	Потребує налаштування та обслуговування, складніше для індивідуальних користувачів.	Вимагає підтримки апаратних ключів або біометричних пристроїв.	Залежить від мобільного пристрою або апаратного токена.	Потребує підтримки веб-браузерів та платформ.
Приклади	Google, Facebook, Microsoft	Salesforce, Okta	Yubico, Google Titan Security Key	Google Authenticator, Authy	Microsoft, Google, Dropbox
Популярність	Широко використовується у соціальних мережах та інших онлайн-службах.	Популярний у корпоративному середовищі та сервісах одного входу.	Зростає, особливо у сфері фізичного доступу.	Популярні для багатократних ситуацій автентифікації.	Зростає, особливо у веб-сервісах та онлайн-платформах.

В результаті порівняльного аналізу (Таблиця 3.1) існуючих систем мультифакторної автентифікації, таких як OpenID Connect, Security Assertion Markup Language (SAML), Fast Identity Online (FIDO), One-Time Password (OTP) та WebAuthn, можна визначити різні переваги та недоліки кожної системи (Рис. 3.1).

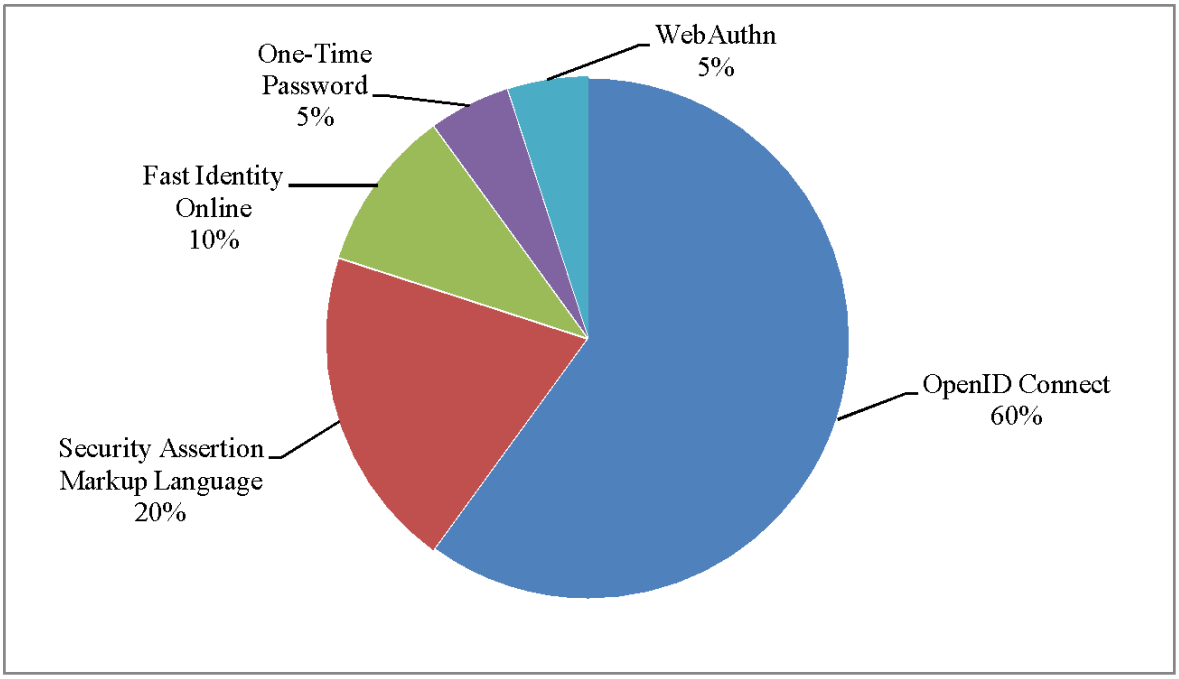

Рисунок 3.1 – Використання методів MFA в Інтернеті

Кожна система має свої властивості та застосування (Додаток Б**)**, і вибір між ними повинен враховувати конкретні потреби та умови використання. Обрана система MFA повинна бути сфокусована на забезпеченні найвищого рівня безпеки, враховуючи одночасно зручність використання для кінцевого користувача.

3.2. Вимоги до методів автентифікації та їх класифікація

Вимоги до автентифікації можуть варіюватися залежно від цінності інформації, яку потрібно надавати тільки авторизованим користувачам, та потенційній загрозі для неї, а отже для самого веб-ресурсу та його користувачів. Тобто, автентифікацію можна розділити на такі рівні за гарантією безпеки для веб-ресурсу та його користувачів:

1. Рівень перший.

Цей рівень автентифікації не містить вимог до підтвердження справжності ідентифікатора, але механізм автентифікації надає деяку впевненість в тому, що користувачем є той, за кого він себе видає. Автентифікація визнається успішною, якщо заявник (особа, яка звертається за транзакцією або даними) по протоколу безпечної автентифікації надає доказ володіння автентифікатором. Цей рівень не вимагає криптографічних методів шифрування, але дані не передаються у мережі у відкритому вигляді. У багатьох випадках зловмисник, що володіє доступом до каналу зв'язку, має можливість відновити пароль, використовуючи атаку зі словником [18].

2. Рівень другий.

Цей рівень передбачає використання однофакторної автентифікації на ресурсі, вводяться умови до підтвердження справжності ідентифікатора. Автентифікаційні дані тривалого зберігання не довіряються жодній зі сторін, за винятком заявника, а перевіряючий сторони підкоряються постачальнику служби електронних посвідчень (Credentials Service Provider, CSP). Обов'язкове застосування дозволених криптографічних методів [18].

3. Рівень третій.

Цей рівень передбачає використання мультифакторної автентифікації (не менше двох факторів) на ресурсі. Автентифікація на цьому рівні заснована на доказі володіння ключем або одноразовим паролем за криптографічним протоколом. Для цього потрібна наявність механізмів забезпечення строгості криптографії, що захищають первинний автентифікатор (секретний ключ, закритий ключ або одноразовий пароль) від компрометації методами прослуховування, відтворення, вгадування і атаки «man in the middle». Можуть використовуватися три види автентифікатора: «програмний» криптографічний автентифікатор, «апаратний» криптографічні автентифікатор і апаратні генератори

одноразових паролів. Автентифікаційні секрети тривалого зберігання не довіряються жодної зі сторін, за винятком заявника, а перевіряючи сторони підкоряються CSP. Для всіх операцій застосовуються легітимні криптографічні методи [18].

4. Рівень четвертий.

Призначений для забезпечення найсуворішої автентифікації на основі доказу володіння закритим ключем за криптографічним протоколом. Рівень 4 аналогічний рівню 3, за винятком того, що на ньому допускається використання тільки «апаратних» криптографічних автентифікаторів, посилені вимоги FIPS 140-2 до оцінки криптографічних модулів, і потрібно, щоб в подальшому справжність переданих конфіденційних даних підтверджувалася з використанням ключа, прив'язаного до процесу автентифікації [18].

Автентифікатор повинен бути апаратним криптографічним модулем, який має сертифікат відповідності FIPS 140-2 рівня 2 або вище із забезпеченням фізичної безпеки на рівні не нижче FIPS 140- 2 рівня 3. Потрібно сувора криптографічна автентифікація усіх боків і при всякій передачі конфіденційних даних між сторонами. Можуть використовуватися як симетричні, так і асиметричні криптографічні алгоритми. Автентифікація вимагає підтвердження заявником володіння автентифікатором з безпечного протоколу автентифікації.

Повинно запобігати атакам прослуховування, відтворення, вгадування і «man in the middle».

При використанні автентифікаційних секретів тривалого зберігання вони не довіряються жодної зі сторін, за винятком заявника, а перевіряючи сторони підкоряються CSP. Для всіх операцій використовуються стійкі, схвалені криптографічні методи. При будь-якій передачі конфіденційної інформації здійснюється криптографічна автентифікація з використанням ключів, прив'язаних до процесу автентифікації.

Висновок до розділу 3

Було визначено, що одним з найбільш поширених методів МФА є OpenID Connect. Це відкритий стандарт, що базується на протоколах OAuth 2.0 і дозволяє користувачам автентифікуватися за допомогою сторонніх сервісів-ідентифікаторів, наприклад Google чи Facebook. Перевагою є простота інтеграції та підтримка безліччю популярних онлайн-платформ. Проте існують ризики, пов'язані із довірою до третьої сторони.

Іншим поширеним стандартом є SAML, орієнтований на корпоративне середовище. Він передбачає обмін XML-даними для автентифікації між клієнтом та сервером і забезпечує високий рівень безпеки. Проте SAML є складнішим в інтеграції і менш зручним для кінцевих користувачів.

Серед фізичних методів МФА виділяються FIDO та OTP. FIDO передбачає використання стандартизованих апаратних ключів чи біометричних датчиків для ідентифікації, забезпечуючи високий ступінь захисту. OTP генерує одноразові коди, наприклад, за допомогою мобільних додатків, що є зручним, хоча і менш надійним.

Новим перспективним методом є WebAuthn, який застосовує криптографічні протоколи на основі відкритих та приватних ключів для ідентифікації в браузерах. Це дозволяє підвищити безпеку онлайн-облікових записів без додаткових паролів. Проте йому ще необхідно отримати більшу підтримку.

У даному розділі було описано вимоги до автентифікації. Було класифіковано автентифікацію за рівнями безпеки та ключові вимоги до її втілення. За наявними даними, автентифікація має чотири рівні безпеки, які відрізняються один від одного рівнем захищеності даних ресурсу та користувачів цього ресурсу. Ці рівні йдуть в порядку зростання від менш безпечного до більш безпечного, де перший рівень не вимагає від замовника підтвердження щодо справжності ідентифікатора, а четвертий –

вимагає найсуворішої мультифакторної автентифікації на рівні апаратних криптографічних автентифікаторів.

Розробляючи ПЗ, яке буде використовувати авторизацію користувачів в системі, автор повинен враховувати ці рівні безпеки. Вибір рівня може залежати від різних факторів, але ключовим фактором у виборі рівня захисту системи є цінність інформації, яку вона містить. Тому з ростом цінності інформації, враховуючи усі існуючі загрози, варто використовувати правила для реалізації вищого рівня безпеки системи.

РОЗДІЛ 4. РОЗРОБКА СИСТЕМИ РЕКОМЕНДАЦІЙ ЩОДО ВИБОРУ ОПТИМАЛЬНОГО МЕТОДУ МУЛЬТИФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

4.1. Визначення рекомендацій для вибору оптимального методу автентифікації

На основі аналізу існуючих поширених інтернет загроз та наявних методів мультифакторної автентифікації були розроблені рекомендації щодо вибору оптимального методу мультифакторної автентифікації для ресурсу користувача. Також були враховані такі фактори: зручність використання для користувачів, види взаємодії користувачів з ресурсом, використання сполучених додатків з основним. Далі наведено список методів автентифікації та критеріїв їх вибору:

- OpenID Connect: користувач має доступ до інтернету; має веб-інтерфейс; в сервісі можливо реалізувати вхід за допомогою облікових записів інших ресурсів (Google, GitHub тощо); обліковий запис користувача може бути пов’язаний з обліковим записом іншого сервісу; для користувача важлива швидкість авторизації; великий обсяг автентифікації; захист від атак (за допомогою шифрування даних) спрямованих на перехоплення даних; захист від брутфорс-атак; захист від CSRF-атак.
- SAML: користувач має доступ до інтернету; має веб-інтерфейс; користувач, який буде використовувати сервіс може потребувати інформації іншого сервісу; сервіс є або буде не єдиний і є корпоративним рішенням, користувачі якого потребують взаємодії між різними сервісами; невеликий обсяг автентифікації; захист від атак (за допомогою шифрування даних) спрямованих на перехоплення даних; захист від брутфорс-атак; захист від CSRF-атак.

- FIDO2: сервіс є корпоративним рішенням; користувачу потрібно забезпечити максимальний рівень безпеки; є можливість надати користувачам апаратні ідентифікатори або є можливість використання біометричних даних користувача; впевненість в підтримці технології з боку користувача (браузеру користувача); система користувача має можливість взаємодії з апаратними автентифікаторами; посилений захист від атак “man in the middle”; захист від брутфорс-атак; захист від CSRF-атак.
- OTP: користувач має доступ до інтернету, телефону та мобільного зв’язку; сервіс має можливість відправляти електронні листи на електронну скриньку користувача; сервіс має можливість відправляти SMS на номер користувача; користувачу потрібно час від часу підтверджувати свої дії в сервісі; є можливість прив’язки сервісу до мобільного додатку для генерації коду; у користувача буде достатньо часу пройти дану автентифікацію; можливість покриття затрат на розсилку повідомлень; захист від брутфорс-атак; захист від CSRF-атак.
- WebAuthn: користувач має доступ до інтернету; є можливість використання апаратних ідентифікаторів або біометричних даних користувача; сервіс не є корпоративним рішенням; впевненість в підтримці технології з боку користувача (браузеру користувача); значна кількість користувачів сервісу; інформація ресурсу є дуже цінна; захист від атак (за допомогою шифрування даних) спрямованих на перехоплення даних; захист від брутфорс-атак; захист від CSRF-атак.

5.2. Засоби розробки програмного рішення

Розроблений веб-сервіс складається виключно з клієнтської частини. Реалізація відбувалася за допомогою наступних технологій:

- HTML (Hyper Text Markup Language) – мова гіпертекстової розмітки, яка була використана для побудови каркасу, основних

компонентів та вузлів візуальної частини сервісу для можливості потенційному користувачу взаємодіяти з логікою застосунку;

- CSS (Cascading Style Sheets) – каскадні таблиці стилів, були використані для покращення візуальної частини інтерфейсу сервісу для зручної та інтуїтивно зрозумілої взаємодії користувача з веб-застосунком;
- JavaScript – мова програмування, яка дозволила побудувати логіку веб-сервісу відразу на клієнтській частині додатку без використання додаткового API (application programming interface).

Використання конкретних технологій у проєкті обґрунтоване їхньою ефективністю у створенні подібного роду сервісів.

HTML – дозволяє побудувати гнучкий каркас інтерфейсу користувача сервісу та надає можливість легкої взаємодії з його компонентами.

CSS – надає можливість створення зовнішнього вигляду інтерфейсу веб-сервісу за допомогою спеціальних правил, що дає можливість зручного використання сервісу користувачем та покращення загальної зрозумілості функціоналу додатку.

JavaScript – мова програмування, спеціально орієнтована на розробку веб-додатків, оскільки браузер по замовчуванню інтерпретує її код. Це дає можливість зручно взаємодіяти з об’єктом DOM (Document Object Model), тобто глобальним об’єктом, який формується браузером при парсінгу HTML-розмітки сторінки, та гнучко маніпулювати елементами DOM. Це дозволяє показувати та приховувати різні елементи сторінки для користувача, на основі отриманих даних. Також JavaScript дозволяє реалізувати складну логіку застосунку для обробки даних користувача та на основі проведених обчислень формувати кінцевий та потрібний для користувача сервісу результат.

Ці інструменти дають можливість максимально зручно, просто та зрозуміло написати потрібний веб-сервіс без використання сторонніх бібліотек та фреймворків.

5.3 Використання програмного рішення для розв’язку задачі дослідження

Після запуску файлу index.html з програмою за допомогою браузера відбувається формування DOM-об’єкта та CSSOM (CSS Object Model) на базі html-розмітки та CSS-стилів відповідно. Далі відбувається рендерінг сторінки на основі отриманих об’єктів, після чого інтерпретується код JavaScript.

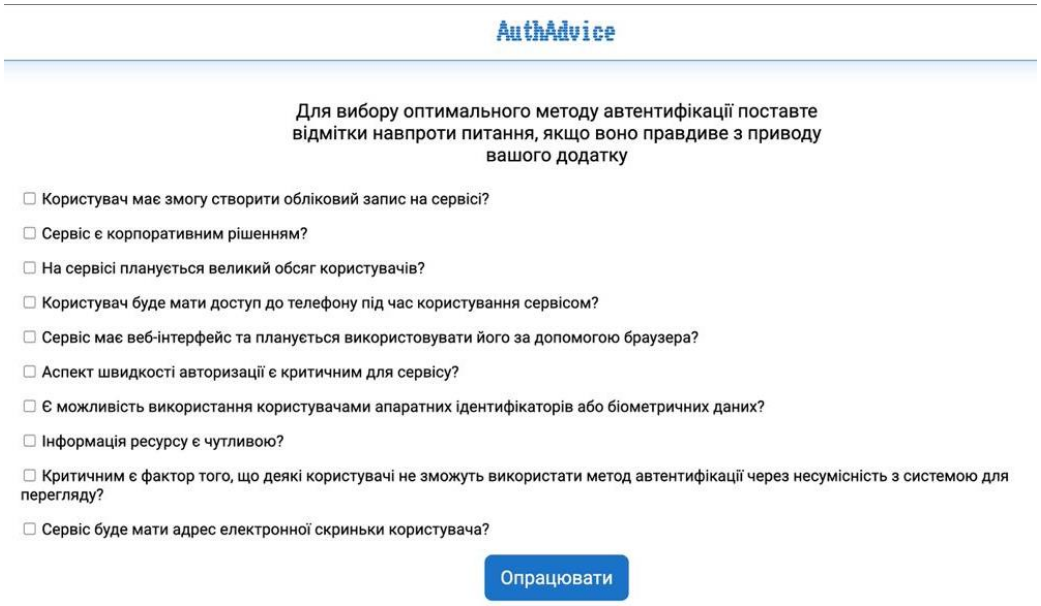

Рисунок 4.1 – інтерфейс сервісу.

Інтерфейс додатку (Рис. 4.1) орієнтований на максимальну швидкість використання та зручність для користувача, тому є односторінковим, де представлена назва сервісу, короткий опис його роботи та форма для заповнення користувачем. Форма представлена у вигляді питань та чекбоксу біля кожного з них для того, щоб користувач міг відмітити потрібну опцію. Після відмітки всіх необхідних питань, користувач повинен натиснути на кнопку “Опрацювати”, клік по якій викликає функцію обробки форми. На основі отриманих даних з форми формується відповідь для користувача. Відповідь представлена у вигляді тексту та показується знизу форми (Рис. 4.2).

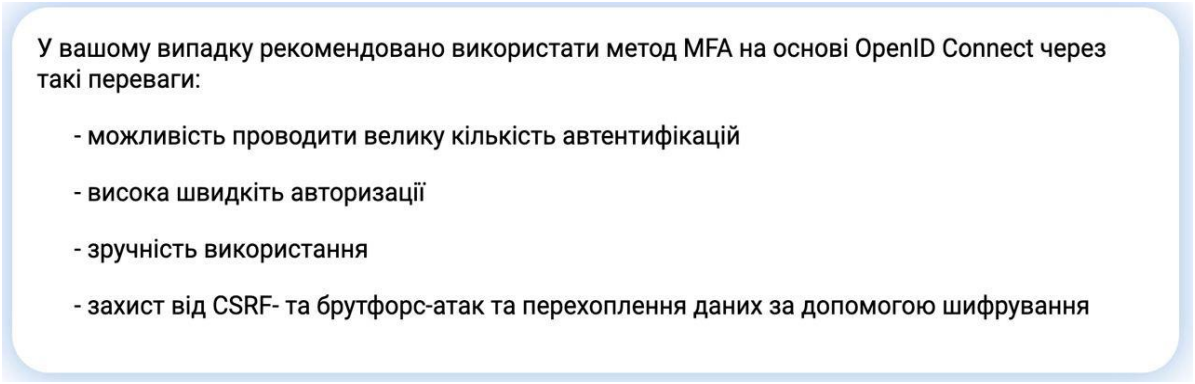

Рисунок 4.2 – Відповідь для користувача.

Представлений результат (Рис. 4.2) містить пораду щодо використання одного з методів автентифікації та обґрунтування, чому саме його потрібно використати для розробки додатку користувача, тобто зазначаються його переваги.

Висновок до розділу 4

У цьому розділі була розроблена система рекомендацій щодо вибору методу мультифакторної автентифікації на ресурсі користувача. Для цього було досліджено та проаналізовано поширені загрози для користувачів веб-сервісів та самих сервісів, а також наявні методи автентифікації для доцільного вибору методу MFA для системи користувача.

Сервіс є веб-додатком та слугує для надання порад потенційному користувачеві щодо вибору методу мультифакторної автентифікації, який в подальшому може бути використаний на ресурсі користувача, на основі відповідей користувача у формі даного веб-сервісу. Це надає користувачеві значну економію часу для пошуку та підбору правильного методу MFA, а також запобігає неправильному вибору його.

ВИСНОВКИ

Автентифікація та авторизація в Інтернеті є суттєвими факторами захисту ресурсів та персональних даних. В останні роки зростаюча загроза кібератак стимулює впровадження додаткових заходів безпеки, зокрема мультифакторної автентифікації (MFA).

У даній роботі було проаналізовано питання захисту персональних даних та онлайн-ресурсів користувачів шляхом застосування механізмів автентифікації та мультифакторної автентифікації.

У першому розділі розглядаються основні поняття автентифікації та авторизації в Інтернеті. Пояснюється, що автентифікація стосується ідентифікації користувача та перевірки його ідентичності, тоді як авторизація визначає, які ресурси та функціональні можливості доступні користувачеві. Також детально розглянулась концепція мультифакторної автентифікації, яка вимагає від користувачів надавати додаткові фактори ідентифікації для підтвердження своєї особи. Це може бути комбінація чогось, що користувач знає (наприклад, пароль), що він має (такий як фізичний ключ) та що він є (наприклад, біометричні дані).

У другому розділі вивчено поширені загрози для користувачів в інтернеті. Було розглянуто такі загрози як XSS, CSRF, брутфорс-атаки та атака “людини посередині”. Ці атаки є небезпечні як для самого користувача веб-ресурсу так і для самого веб-ресурсу. Більшість з них легко попередити та захиститись від них. Однак якщо зловмиснику все-таки вдалося провести атаку, наслідки можуть бути плачевними. Одним зі способів значно покращити безпеку використання ресурсу є впровадження мультифакторної автентифікації.

У третьому розділі було проаналізовано існуючі методи мультифакторної автентифікації, такі як OpenID Connect, SAML, FIDO, OTP, WebAuthn. Кожен метод має свої переваги та недоліки, а також підходящу сферу застосування. Ці параметри були враховані для розробки

веб-сервісу для вибору оптимальної системи автентифікації. У розділі було проаналізовано та класифіковано автентифікацію по рівню захищеності. Всього існує чотири рівні: перший рівень не вимагає підтвердження справжності ідентифікатора користувача; другий – вимагає проходження однофакторної автентифікації; третій рівень – вимагає проходження мультифакторної автентифікації (мінімум два фактори), автентифікація на цьому рівні заснована на доказі володіння ключем або одноразовим паролем за криптографічним протоколом; четвертий рівень – вимагає найсуворішої автентифікації на основі доказу володіння закритим ключем за криптографічним протоколом.

У четвертому розділі було застосовано результати дослідження та проаналізовані поширені загрози для користувачів веб-ресурс та наявні методи автентифікації для розробки системи рекомендацій щодо вибору мультифакторної автентифікації для ресурсу користувача.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Калинюк А. М., Kalyniuk A. Методи та засоби біометричної автентифікації користувачів web-сервісів : автореф. Thesis Abstract. 2018. URL: http://elartu.tntu.edu.ua/handle/lib/23719 (дата звернення: 24.12.2024).
2. Кавун С. В. Інформаційна безпека : підручник. Харків : ХНЕУ, 2009. 368 с.
3. Сабадаш В. П. Деякі аспекти проблеми розповсюдження шахрайства в Інтернеті. *Держава і право*. 2005. Вип. 30. С. 452–457.
4. Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ : Інформаційно-аналітичний дайджест. 2023. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf (дата звернення: 27.12.2024).
5. До питання безпечної багатофакторної аутентифікації у веб-застосунках / В. Дудикевич та ін. *Ukrainian Information Security Research Journal*. 2023. Т. 25, № 2. С. 76–82. URL: https://doi.org/10.18372/2410-7840.25.17675 (дата звернення: 28.12.2024).
6. Калініна І., Лісовиченко О. Системи авторизації з використанням різних методів аутентифікації. *Адаптивні системи автоматичного управління*. 2017. Т. 1, № 30. С. 78–85. URL: https://doi.org/10.20535/1560-8956.30.2017.117705 (дата звернення: 30.12.2024).
7. Мєшков О. Ю. Програмно-апаратний комплекс для задачі автентифікації особистості за голосовим сигналом. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2018. Вип. 6 (113). С. 15–20.

8. Заверцований Н. В., Zavertsovanyi N. Методи підвищення ефективності захисту комп'ютерних систем на основі біометричної автентифікації за параметрами ока : автореф. Thesis Abstract. 2018. URL: http://elartu.tntu.edu.ua/handle/lib/24081 (дата звернення: 02.01.2024).
9. Куриляк В. Платіжні системи в Інтернеті: порвняльний аналіз. *Банківська справа*. 2001. № 6. С. 29–33.
10. Мироненко Г. В. Особливості переживання кіберкористувачами суб'єктивної безпеки в інтернеті. *Наукові студії із соціальної та політичної психології*. 2010. Вип. 24 (27). С. 225–230.
11. Бойчук І. В. Специфіка моделей комунікації в Інтернеті : thesis. 2012. URL: http://essuir.sumdu.edu.ua/handle/123456789/28926 (дата звернення: 05.01.2024).
12. Муха А. В. Загрози використання персональних даних у мережі Інтернет. 2020. URL: https://bit.ly/3HLaazO (дата звернення: 08.01.2024).
13. Біленький В.С. Дослідження методів захисту Java додатків та їх програмна реалізація. 2021. URL: https://bit.ly/4bqp6Rq (дата звернення: 10.01.2024).
14. Кавин Б. Основні підходи до аутентифікації користувачів інформаційно-комунікаційних мереж. *Theoretical and practical aspects of modern scientific research* / chair: О. Кавин, С. Кавин, Я. Кавин. 2023. URL: https://doi.org/10.36074/logos-28.04.2023.43 (дата звернення: 13.01.2024).
15. Корнієнко Б. Я., Юдін О. К., Снігур О. С. Безпека аутентифікації у web-ресурсах. *Ukrainian Information Security Research Journal*. 2012. Т. 14, № 1 (54). URL: https://doi.org/10.18372/2410-7840.14.2056 (дата звернення: 14.01.2024).
16. Добровольська В. В. Оцінювання ефективності маркетингової стратегії компанії в Інтернеті : thesis. 2019. URL:

https://er.knutd.edu.ua/handle/123456789/12803 (дата звернення: 16.01.2024).

17. Метод блокування доступу до інформаційно-телекомунікаційних систем на основі біометричної ідентифікації/автентифікації користувачів / О. С. Бойченко та ін. *Технічна інженерія*. 2020. № 1(85). С. 171–176. URL: https://doi.org/10.26642/ten-2020-1(85)-171-176 (дата звернення: 13.01.2024).
18. Тупарєва В. А. Засоби аутентифікації об’єктів мережі на основі аналізу фізичних параметрів сигналів. *Комп‘ютерна інженерія. Системне програмування.* 2018. С. 41–43. URL: https://bit.ly/3HDApID (дата звернення: 31.01.2024).

ДОДАТКИ

Додаток А. Приклади використання фізичних ключів для MFA

Таблиця А.1. Приклади використання фізичних ключів для MFA

Застосування	**Yubico Security Key**	**Google Titan Security Key**	**Feitian FIDO U2F Key**	**SafeNet i.e. FIDO U2F Key**	**YubiKey 5C NFC**
Вхід до облікових записів	Підтримує більш ніж 500 веб-сайтів і додатків, включаючи Google, Microsoft, Dropbox, GitHub та інші.	Підтримує більш ніж 200 веб-сайтів і додатків, включаючи Google, Microsoft, Dropbox, GitHub та інші.	Підтримує більш ніж 1000 веб-сайтів і додатків, включаючи Google, Microsoft, Dropbox, GitHub та інші.	Підтримує більш ніж 500 веб-сайтів і додатків, включаючи Google, Microsoft, Dropbox, GitHub та інші.	Підтримує більш ніж 500 веб-сайтів і додатків, включаючи Google, Microsoft, Dropbox, GitHub та інші.
Захист від зловмисних програм	Фізичний ключ не може бути зламний зловмисною програмою.				
Безпека хмарних обчислень	Можна використовувати для безпечного доступу до хмарних служб, таких як Google Cloud Platform, Amazon Web Services та Microsoft Azure.				
Безпека VPN	Можна використовувати для безпечного підключення до VPN-мережі.				
Безпека Wi-Fi	Можна використовувати для безпечного підключення до Wi-Fi-мережі.				
Ціна	Від 50 доларів США.	Від 50 доларів США.	Від 50 доларів США.	Від 50 доларів США.	Від 50 доларів США.
Додаткові особливості	Вбудована індикація LED, яка повідомляє про стан операції.	Вбудована кнопка, яку потрібно натиснути, щоб підтвердити операцію.	Вбудований дисплей, який відображає коди доступу.	Вбудована кнопка, яку потрібно натиснути, щоб підтвердити операцію.	Вбудована NFC-антенна для бездротового підключення.

Додаток Б. Статистика поширеності різних методів MFA

Таблиця Б.1. Статистика поширеності різних методів MFA

Метод МФА	Доля користувачів	Примітки
SMS-підтвердження	60%	Найпоширеніший метод МФА. Простота використання і доступна ціна є його основними перевагами. Однак SMS-підтвердження може бути ненадійно, оскільки його можна перехопити зловмисниками.
Одноразові коди (OTP)	40%	Більш безпечний метод, ніж SMS-підтвердження, оскільки OTP генеруються на пристрої користувача і не можуть бути перехоплені зловмисниками. Однак OTP можуть бути незручно використовувати, оскільки користувачеві потрібно мати доступ до пристрою для їхнього введення.
Фізичні ключі	20%	Найбезпечніший метод MFA, оскільки фізичні ключі не можуть бути перехоплені зловмисниками. Однак фізичні ключі можуть бути загублені або пошкоджені.
Аутентифікація за геопозицією	10%	Цей метод MFA використовує геолокацію пристрою користувача для підтвердження його ідентичності. Це може бути зручним способом автентифікації, однак він може бути не надто надійним, оскільки геолокацію пристрою можна змінити.
Біометричне розпізнавання	5%	Цей метод MFA використовує біометричні дані користувача, такі як відбитки пальців або сканування обличчя, для підтвердження його ідентичності. Це може бути дуже надійним способом автентифікації, однак біометричні дані можуть бути скомпрометовані.